Microsoft

รายงานการป้องกันทางดิจิทัลของ Microsoft 2022

ชี้ให้เห็นถึงภัยคุกคาม และเพิ่มประสิทธิภาพการป้องกันทางดิจิทัล

สารบัญ

ข้อมูล ข้อมูลเชิงลึก และเหตุการณ์ในรายงานนี้มีตั้งแต่เดือนกรกฎาคม 2021 ถึงมิถุนายน 2022 (ปีงบประมาณของ Microsoft 2022) เว้นแต่จะระบุไว้เป็นอย่างอื่น

เพื่อประสบการณ์ที่ดีที่สุดในการดูและสำรวจรายงานนี้ เราขอแนะนำให้ใช้ Adobe Reader ซึ่งสามารถดาวน์โหลดได้ฟรีจากเว็บไซต์ Adobe

บทนำรายงาน 02

สถานการณ์ของอาชญากรรมไซเบอร์ 06

ภาพรวมของสถานะของอาชญากรรมทางไซเบอร์ 07
ข้อมูลเบื้องต้น 08
แรนซัมแวร์และการขู่กรรโชก: ภัยคุกคามระดับประเทศ 09
ข้อมูลเชิงลึกเกี่ยวกับแรนซัมแวร์จากเจ้าหน้าที่แนวหน้า 14
อาชญากรรมทางไซเบอร์ ในฐานะบริการ 18
วิวัฒนาการของภัยคุกคามฟิชชิ่ง 21
เส้นเวลาของการหยุดชะงักของบ็อตเน็ตจากวันแรกของการทำงานร่วมกันของ Microsoft 25
การใช้โครงสร้างพื้นฐานที่ถูกต้องในทางที่ผิด 26
การแฮ็กข้อมูลจะอยู่ที่นี่หรือไม่ 28

ภัยคุกคามระดับชาติ 30

ภาพรวมของภัยคุกคามระดับชาติ 31
ข้อมูลเบื้องต้น 32
ความเป็นมาเกี่ยวกับข้อมูลรัฐชาติ 33
ตัวอย่างนักแสดงรัฐชาติและกิจกรรมของพวกเขา 34
วิวัฒนาการของภัยคุกคาม 35
ห่วงโซ่อุปทานไอทีเป็นประตูสู่ระบบนิเวศดิจิทัล 37
การแสวงหาประโยชน์จากช่องโหว่อย่างรวดเร็ว 39
กลยุทธ์ทางไซเบอร์ในช่วงสงครามของผู้ดำเนินการของรัฐรัสเซียคุกคามยูเครนและที่อื่นๆ 41
จีนขยายการกำหนดเป้าหมายทั่วโลกเพื่อความได้เปรียบทางการแข่งขัน 44
อิหร่านก้าวร้าวมากขึ้นหลังจากการเปลี่ยนผ่านอำนาจ 46
ความสามารถทางไซเบอร์ของเกาหลีเหนือใช้เพื่อบรรลุเป้าหมายหลักสามประการของระบอบการปกครอง 49
ทหารรับจ้างไซเบอร์คุกคามความมั่นคงของไซเบอร์สเปซ 52
ดำเนินการตามบรรทัดฐานความปลอดภัยทางไซเบอร์เพื่อสันติภาพและความปลอดภัยในโลกไซเบอร์ 53

เครื่องมือและโครงสร้างพื้นฐาน 56

ภาพรวมของอุปกรณ์และโครงสร้างพื้นฐาน 57
ข้อมูลเบื้องต้น 58
รัฐบาลดำเนินการเพื่อปรับปรุงความปลอดภัยและความยืดหยุ่นของโครงสร้างพื้นฐานที่สำคัญ 59
IoT และ OT เปิดเผย: แนวโน้มและการโจมตี 62
ห่วงโซ่อุปทานและการแฮ็คเฟิร์มแวร์ 65
สปอตไลท์เกี่ยวกับช่องโหว่ของเฟิร์มแวร์ 66
การโจมตีเฟิร์มแวร์มีอยู่ทั่วไป 67
การโจมตี OT ตามการลาดตระเวน 68

ปฏิบัติการมีอิทธิพลทางไซเบอร์ 71

ภาพรวมของการปฏิบัติการอิทธิพลทางไซเบอร์ 72
ข้อมูลเบื้องต้น 73
แนวโน้มของการปฏิบัติการด้านอิทธิพลทางไซเบอร์ 74
จับตาการปฏิบัติการด้านอิทธิพลในช่วงโควิด-19 และการรุกรานยูเครนของรัสเซีย 76
การติดตามดัชนีโฆษณาชวนเชื่อของรัสเซีย 78
สื่อสังเคราะห์ 80
แนวทางแบบองค์รวมเพื่อป้องกันการปฏิบัติการด้านอิทธิพลทางไซเบอร์ 83

ความยืดหยุ่นทางไซเบอร์ 86

ภาพรวมของความยืดหยุ่นทางไซเบอร์ 87
ข้อมูลเบื้องต้น 88
ความยืดหยุ่นทางไซเบอร์: รากฐานที่สำคัญของสังคมที่มีการเชื่อมต่อ 89
ความสำคัญของการปรับปรุงระบบและสถาปัตยกรรมให้ทันสมัย 90
ท่าทางการรักษาความปลอดภัยขั้นพื้นฐานเป็นปัจจัยกำหนดประสิทธิภาพของโซลูชันขั้นสูง 92
การรักษาสุขภาพของเอกลักษณ์เป็นพื้นฐานของความเป็นอยู่ที่ดีขององค์กร 93
การตั้งค่าความปลอดภัยเริ่มต้นของระบบปฏิบัติการ 96
ศูนย์กลางห่วงโซ่อุปทานของซอฟต์แวร์ 97
การสร้างความยืดหยุ่นต่อการโจมตี DDoS, เว็บแอปพลิเคชัน และเครือข่ายที่เกิดขึ้นใหม่ 98
การพัฒนาแนวทางที่สมดุลในการรักษาความปลอดภัยข้อมูลและความยืดหยุ่นทางไซเบอร์ 101
ความยืดหยุ่นต่อปฏิบัติการมีอิทธิพลทางไซเบอร์: มิติของมนุษย์ 102
การเสริมสร้างปัจจัยมนุษย์ด้วยทักษะ 103
ข้อมูลเชิงลึกจากโปรแกรมกำจัดแรนซัมแวร์ของเรา 104
ดำเนินการในขณะนี้เกี่ยวกับผลกระทบด้านความปลอดภัย ควอนตัม 105
การผสานรวมธุรกิจ ความปลอดภัย และ IT เพื่อความยืดหยุ่นที่มากขึ้น 106
เส้นโค้งความยืดหยุ่นทางไซเบอร์ 108

ทีมงานที่มีส่วนร่วม 110

บทนำโดย Tom Burt

รองประธานบริษัท, การรักษาความปลอดภัยและความไว้วางใจของลูกค้า

“สัญญาณนับล้านล้านที่เราวิเคราะห์จากระบบนิเวศทั่วโลกของเราของผลิตภัณฑ์และบริการที่เปิดเผยความร้ายแรง ขอบเขต และขนาดของภัยคุกคามดิจิทัลทั่วโลก”

ภาพรวมของภูมิทัศน์ของเรา...

ขอบเขตและขนาดของภาพรวมภัยคุกคาม

ปริมาณการโจมตีด้วยรหัสผ่านเพิ่มขึ้นเป็นประมาณ 921 ครั้งต่อวินาที – เพิ่มขึ้น 74% ในเวลาเพียงหนึ่งปี

การทำลายล้างอาชญากรรมทางไซเบอร์

จนถึงปัจจุบัน Microsoft ได้ลบโดเมนมากกว่า 10,000 โดเมนที่อาชญากรไซเบอร์ใช้ และ 600 โดเมนที่ใช้โดยผู้ดำเนินการในระดับชาติ

ระบุช่องโหว่

93% ของการโต้ตอบเหตุการณ์แรนซัมแวร์ของเราเผยให้เห็นการควบคุมไม่เพียงพอในการเข้าถึงสิทธิ์และการเคลื่อนไหวด้านข้าง

ในวันที่ 23 กุมภาพันธ์ 2022 โลกของความปลอดภัยทางไซเบอร์ได้เข้าสู่ยุคใหม่ ยุคของสงครามลูกผสม ในวันนั้น ไม่กี่ชั่วโมงก่อนที่จะมีการยิงขีปนาวุธและรถถังเคลื่อนข้ามพรมแดน นักแสดงชาวรัสเซียได้เปิดการโจมตีทางไซเบอร์แบบทำลายล้างครั้งใหญ่ต่อเป้าหมายของรัฐบาล เทคโนโลยี และภาคการเงินของยูเครน คุณสามารถอ่านเพิ่มเติมเกี่ยวกับการโจมตีเหล่านี้และบทเรียนที่ต้องเรียนรู้จากการโจมตีเหล่านี้ได้ในบทภัยคุกคามจากรัฐของประเทศใน Microsoft Digital Defense Report (MDDR) ฉบับที่สามประจำปีนี้ สิ่งสำคัญในบทเรียนเหล่านี้คือระบบคลาวด์ให้การรักษาความปลอดภัยทางกายภาพและเชิงตรรกะที่ดีที่สุดต่อการโจมตีทางไซเบอร์ และช่วยให้เกิดความก้าวหน้าในด้านข่าวกรองภัยคุกคามและการป้องกันจุดสิ้นสุดที่พิสูจน์คุณค่าในยูเครน

แม้ว่าการสำรวจพัฒนาการด้านความปลอดภัยในโลกไซเบอร์ประจำปีจะต้องเริ่มต้นที่นั่น แต่รายงานปีนี้ให้ข้อมูลเชิงลึกมากขึ้น ในบทแรกของรายงาน เรามุ่งเน้นไปที่กิจกรรมของอาชญากรไซเบอร์ ตามด้วยภัยคุกคามของรัฐชาติในบทที่สอง ทั้งสองกลุ่มได้เพิ่มความซับซ้อนในการโจมตีอย่างมาก ซึ่งได้เพิ่มผลกระทบจากการกระทำของพวกเขาอย่างมาก ในขณะที่รัสเซียตกเป็นข่าวพาดหัวข่าว นักแสดงชาวอิหร่านก็เพิ่มการโจมตีของพวกเขาหลังจากการเปลี่ยนผ่านอำนาจของประธานาธิบดี เปิดการโจมตีแบบทำลายล้างโดยมุ่งเป้าไปที่อิสราเอลและแรนซัมแวร์และการปฏิบัติการแฮ็กและรั่วไหลโดยมุ่งเป้าไปที่โครงสร้างพื้นฐานที่สำคัญในสหรัฐอเมริกา จีนยังเพิ่มความพยายามในการจารกรรมในเอเชียตะวันออกเฉียงใต้และที่อื่นๆ ทางตอนใต้ของโลก โดยพยายามตอบโต้อิทธิพลของสหรัฐฯ และขโมยข้อมูลและสารสนเทศที่สำคัญ ผู้ดำเนินการต่างชาติยังใช้เทคนิคที่มีประสิทธิภาพสูงเพื่อให้การดำเนินการโฆษณาชวนเชื่อมีอิทธิพลในภูมิภาคต่างๆ ทั่วโลก ดังที่กล่าวถึงในบทที่สาม ตัวอย่างเช่น รัสเซียทำงานอย่างหนักเพื่อโน้มน้าวพลเมืองของตนและพลเมืองของประเทศอื่นๆ ว่าการรุกรานยูเครนนั้นเป็นสิ่งที่ชอบธรรม ในขณะเดียวกันก็หว่านโฆษณาชวนเชื่อที่ทำให้เสื่อมเสียชื่อเสียงของวัคซีนโควิดในตะวันตก และในขณะเดียวกันก็ส่งเสริมประสิทธิภาพของวัคซีนในประเทศ นอกจากนี้ ผู้ประกอบการกำลังกำหนดเป้าหมายอุปกรณ์ Internet of Things (IoT) หรืออุปกรณ์ควบคุมเทคโนโลยีการดำเนินงาน (OT) มากขึ้นเป็นจุดเริ่มต้นสู่เครือข่ายและโครงสร้างพื้นฐานที่สำคัญ ซึ่งจะกล่าวถึงในบทที่สี่ สุดท้ายนี้ ในบทสุดท้าย เราให้ข้อมูลเชิงลึกและบทเรียนที่เราได้เรียนรู้จากปีที่ผ่านมาเพื่อป้องกันการโจมตีที่มุ่งเป้าไปที่ Microsoft และลูกค้าของเรา ขณะที่เราตรวจสอบพัฒนาการของปีในด้านความยืดหยุ่นทางไซเบอร์

แต่ละบทให้บทเรียนสำคัญที่ได้เรียนรู้และข้อมูลเชิงลึกตามจุดได้เปรียบที่ไม่เหมือนใครของ Microsoft สัญญาณหลายล้านล้านรายการที่เราวิเคราะห์จากระบบนิเวศทั่วโลกของผลิตภัณฑ์และบริการเผยให้เห็นความดุร้าย ขอบเขต และขนาดของภัยคุกคามทางดิจิทัลทั่วโลก Microsoft กำลังดำเนินการเพื่อปกป้องลูกค้าของเราและระบบนิเวศดิจิทัลจากภัยคุกคามเหล่านี้ และคุณสามารถอ่านเกี่ยวกับเทคโนโลยีของเราที่ระบุและบล็อกความพยายามฟิชชิงนับพันล้านครั้ง การโจรกรรมข้อมูลประจำตัว และภัยคุกคามอื่นๆ ต่อลูกค้าของเรา

บทนำโดย Tom Burt

อย่างต่อเนื่อง

นอกจากนี้ เรายังใช้วิธีการทางกฎหมายและทางเทคนิคในการยึดและปิดโครงสร้างพื้นฐานที่ใช้โดยอาชญากรไซเบอร์และผู้มีบทบาทของรัฐ และแจ้งให้ลูกค้าทราบเมื่อพวกเขาถูกคุกคามหรือโจมตีโดยผู้มีบทบาทของรัฐ เราทำงานเพื่อพัฒนาฟีเจอร์และบริการที่มีประสิทธิภาพมากขึ้นซึ่งใช้เทคโนโลยี AI/ML เพื่อระบุและบล็อกภัยคุกคามทางไซเบอร์ และผู้เชี่ยวชาญด้านความปลอดภัยจะป้องกันและระบุการบุกรุกทางไซเบอร์ได้รวดเร็วและมีประสิทธิภาพมากขึ้น

บางทีสิ่งที่สำคัญที่สุดคือตลอด MDDR เราให้คำแนะนำที่ดีที่สุดเกี่ยวกับขั้นตอนที่บุคคล องค์กร และองค์กรสามารถดำเนินการเพื่อป้องกันภัยคุกคามดิจิทัลที่เพิ่มขึ้นเหล่านี้ การนำแนวทางปฏิบัติด้านสุขอนามัยในโลกไซเบอร์มาใช้เป็นการป้องกันที่ดีที่สุดและสามารถลดความเสี่ยงของการโจมตีทางไซเบอร์ได้อย่างมาก



สถานการณ์ของอาชญากรรมไซเบอร์

อาชญากรไซเบอร์ยังคงทำหน้าที่เป็นองค์กรที่แสวงหาผลกำไรที่ซับซ้อน ผู้โจมตีกำลังปรับตัวและค้นหาวิธีใหม่ๆ ในการใช้เทคนิคของตน เพิ่มความซับซ้อนของวิธีและตำแหน่งที่พวกเขาโฮสต์โครงสร้างพื้นฐานการดำเนินงานแคมเปญ ในขณะเดียวกัน อาชญากรไซเบอร์ก็ลดมากขึ้นเพื่อลดค่าใช้จ่ายและเพิ่มความถูกต้องตามกฎหมาย ผู้โจมตีกำลังประนีประนอมเครือข่ายธุรกิจและอุปกรณ์เพื่อโฮสต์แคมเปญฟิชชิ่ง มัลแวร์ หรือแม้กระทั่งใช้พลังการประมวลผลเพื่อขุดสกุลเงินดิจิทัล

ค้นหาข้อมูลเพิ่มเติมหน้า 6

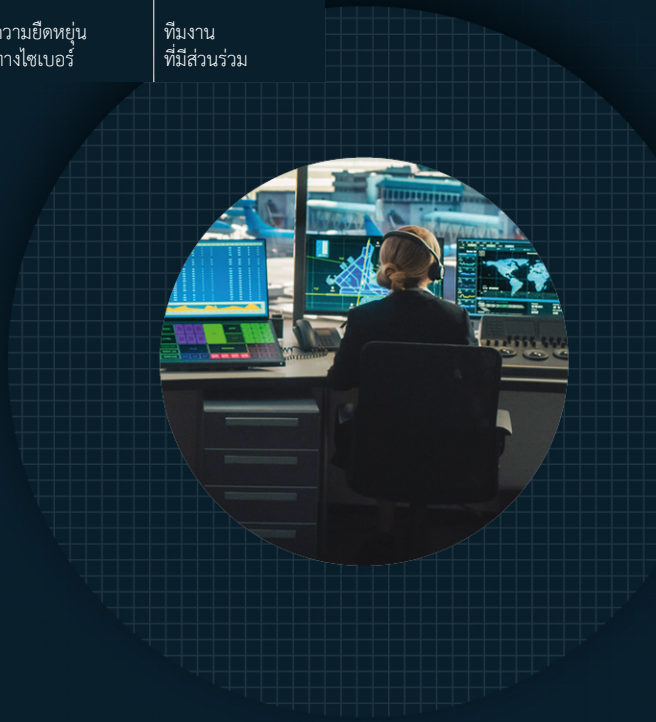
“การกำเนิดของการติดตั้งอาวุธไซเบอร์ในสงครามลูกผสมในยูเครนเป็นจุดเริ่มต้นของความขัดแย้งยุคใหม่”

ภัยคุกคามระดับชาติ

ผู้มีบทบาทในระดับชาติกำลังเปิดตัวการโจมตีทางไซเบอร์ที่ซับซ้อนมากขึ้น ซึ่งออกแบบมาเพื่อหลบเลี่ยงการตรวจจับและเสริมลำดับความสำคัญเชิงกลยุทธ์ของพวกเขา การกำเนิดของการติดตั้งอาวุธไซเบอร์ในสงครามลูกผสมในยูเครนเป็นจุดเริ่มต้นของความขัดแย้งยุคใหม่ รัสเซียยังสนับสนุนการทำสงครามกับการดำเนินการที่มีอิทธิพลต่อข้อมูล โดยใช้การโฆษณาชวนเชื่อเพื่อส่งผลกระทบต่อความคิดเห็นในรัสเซีย ยูเครน และทั่วโลก นอกประเทศยูเครน ผู้มีบทบาทของรัฐชาติได้เพิ่มกิจกรรมและเริ่มใช้ความก้าวหน้าในระบบอัตโนมัติ โครงสร้างพื้นฐานระบบคลาวด์ และเทคโนโลยีการเข้าถึงระยะไกลเพื่อโจมตีเป้าหมายที่กว้างขึ้น ห่วงโซ่อุปทานด้านไอทีขององค์กรที่เปิดใช้งานการเข้าถึงเป้าหมายสูงสุดมักถูกโจมตี สุขอนามัยของความปลอดภัยทางไซเบอร์กลายเป็นเรื่องที่สำคัญยิ่งขึ้นไปอีกเนื่องจากนักแสดงใช้ประโยชน์จากช่องโหว่ที่ยังไม่ได้แพตช์อย่างรวดเร็ว ใช้ทั้งเทคนิคที่ซับซ้อนและรุนแรงเพื่อขโมยข้อมูลประจำตัว และทำให้การทำงานของพวกเขายุ่งเหยิงโดยใช้โอเพ่นซอร์สหรือซอฟต์แวร์ที่ถูกกฎหมาย นอกจากนี้ อิหร่านยังเข้าร่วมกับรัสเซียในการใช้อาวุธทำลายล้างทางไซเบอร์ ซึ่งรวมถึงแรนซัมแวร์ เป็นหลักในการโจมตี

การพัฒนาเหล่านี้จำเป็นต้องอาศัยกรอบระดับโลกที่สอดคล้องกันอย่างเร่งด่วน ซึ่งให้ความสำคัญกับสิทธิมนุษยชนและปกป้องผู้คนจากพฤติกรรมของรัฐที่ประมาทในโลกออนไลน์ ทุกประเทศต้องทำงานร่วมกันเพื่อใช้บรรทัดฐานและกฎสำหรับการปฏิบัติที่รับผิดชอบของรัฐ

ค้นหาข้อมูลเพิ่มเติมหน้า 30



เครื่องมือและโครงสร้างพื้นฐาน

การระบาดใหญ่ควบคู่ไปกับการนำอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตทุกประเภทมาใช้อย่างรวดเร็วเป็นองค์ประกอบในการเร่งการเปลี่ยนแปลงทางดิจิทัลได้เพิ่มพื้นผิวการโจมตีของโลกดิจิทัลของเราอย่างมาก ด้วยเหตุนี้ อาชญากรไซเบอร์และประเทศกำลังฉวยโอกาสอย่างรวดเร็ว แม้ว่าความปลอดภัยของฮาร์ดแวร์และซอฟต์แวร์ด้านไอทีจะแข็งแกร่งขึ้นในช่วงไม่กี่ปีที่ผ่านมา แต่ความปลอดภัยของอุปกรณ์ IoT และการรักษาความปลอดภัยของอุปกรณ์ OT กลับไม่ก้าวทัน ผู้คุกคามกำลังใช้ประโยชน์จากอุปกรณ์เหล่านี้เพื่อสร้างการเข้าถึงบนเครือข่ายและเปิดใช้งานการเคลื่อนไหวด้านข้าง เพื่อสร้างหลักในห่วงโซ่อุปทานหรือขัดขวางการดำเนินงาน OT ขององค์กรเป้าหมาย

ค้นหาข้อมูลเพิ่มเติมหน้า 56

บทนำโดย Tom Burt

อย่างต่อเนื่อง

ปฏิบัติการมีอิทธิพลทางไซเบอร์

รัฐชาติกำลังใช้อิทธิพลที่ซับซ้อนมากขึ้นเพื่อเผยแพร่โฆษณาชวนเชื่อและส่งผลกระทบต่อความคิดเห็นของประชาชนทั้งในประเทศและต่างประเทศ แคมเปญเหล่านี้บั่นทอนความไว้วางใจ เพิ่มการแบ่งขั้ว และคุกคามกระบวนการประชาธิปไตย นักบงการขั้นสูงที่มีทักษะขั้นสูงกำลังใช้สื่อดั้งเดิมร่วมกับอินเทอร์เน็ตและโซเชียลมีเดียเพื่อเพิ่มขอบเขต ขนาด และประสิทธิภาพของแคมเปญของพวกเขาอย่างมหาศาล รวมถึงผลกระทบที่เกินขอบเขตที่พวกเขามีต่อระบบนิเวศข้อมูลทั่วโลก ในปีที่ผ่านมา เราได้เห็นปฏิบัติการเหล่านี้ใช้เป็นส่วนหนึ่งของสงครามลูกผสมของรัสเซียในยูเครน แต่ยังเห็นรัสเซียและประเทศอื่นๆ รวมถึงจีนและอิหร่าน ใช้ปฏิบัติการโฆษณาชวนเชื่อที่ขับเคลื่อนโดยสื่อสังคมออนไลน์มากขึ้นเพื่อขยายอิทธิพลไปทั่วโลกในด้านต่างๆ ของปัญหา

ค้นหาข้อมูลเพิ่มเติมหน้า 71





ความยืดหยุ่นทางไซเบอร์

การรักษาความปลอดภัยเป็นกุญแจสำคัญของความสำเร็จทางเทคโนโลยี นวัตกรรมและประสิทธิภาพที่เพิ่มขึ้นสามารถทำได้โดยการนำมาตรการรักษาความปลอดภัยที่ทำให้องค์กรมีความยืดหยุ่นมากที่สุดเท่าที่จะเป็นไปได้ จากการโจมตีสมัยใหม่ การแพร่ระบาดได้ท้าทายเราที่ Microsoft ในการปรับเปลี่ยนแนวปฏิบัติและเทคโนโลยีด้านความปลอดภัยของเราเพื่อปกป้องพนักงานของเรา ไม่ว่าจะทำงานที่ไหนก็ตาม ในปีที่ผ่านมา ผู้ก่อภัยคุกคามยังคงใช้ประโยชน์จากช่องโหว่ที่เปิดเผยระหว่างการแพร่ระบาดและการเปลี่ยนไปใช้สภาพแวดล้อมการทำงานแบบผสมผสาน ตั้งแต่นั้นมา ความท้าทายหลักของเราคือการจัดการความแพร่หลายและความซับซ้อนของวิธีการโจมตีต่างๆ และกิจกรรมของรัฐชาติที่เพิ่มขึ้น ในบทนี้ เราจะให้รายละเอียดเกี่ยวกับความท้าทายที่เราเผชิญ และแนวป้องกันที่เราระดมเพื่อตอบโต้กับพันธมิตรมากกว่า 15,000 รายของเรา

ค้นหาข้อมูลเพิ่มเติมหน้า 86

จุดได้เปรียบที่ไม่เหมือนใครของเรา

37 พันล้าน
ภัยคุกคามทางอีเมล
ที่ถูกบล็อก

34.7 พันล้าน
ภัยคุกคามข้อมูลประจำตัว
ที่ถูกบล็อก

43tn
สัญญาณสังเคราะห์ทุกวันโดยใช้การวิเคราะห์ข้อมูลที่ซับซ้อนและอัลกอริทึม AI เพื่อทำความเข้าใจและป้องกันภัยคุกคามดิจิทัลและกิจกรรมทางไซเบอร์ทางอาญา

2.5 พันล้าน
วิเคราะห์สัญญาณ
ปลายทางทุกวัน

8,500+
วิศวกร นักวิจัย นักวิทยาศาสตร์ข้อมูล ผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ นักล่าภัยคุกคาม นักวิเคราะห์ภูมิรัฐศาสตร์ ผู้สืบสวน และผู้เผชิญเหตุแนวหน้าใน 77 ประเทศ

15,000+
พันธมิตรในระบบนิเวศการรักษาความปลอดภัยของเรา
ที่เพิ่มความยืดหยุ่นทางไซเบอร์ให้กับลูกค้าของเรา

1 กรกฎาคม 2021 ถึง 30 มิถุนายน 2022

บทนำโดย Tom Burt
อย่างต่อเนื่อง

เราเชื่อว่า Microsoft—โดยอิสระและผ่านการเป็นหุ้นส่วนอย่างใกล้ชิดกับผู้อื่นในอุตสาหกรรมเอกชน ภาครัฐ และภาคประชาสังคม—มีหน้าที่รับผิดชอบในการปกป้องระบบดิจิทัลที่เป็นรากฐานโครงสร้างทางสังคมของสังคมของเราและส่งเสริมสภาพแวดล้อมคอมพิวเตอร์ที่ปลอดภัยสำหรับทุกคน ไม่ว่าพวกเขาจะตั้งอยู่ที่ใด ความรับผิดชอบนี้เป็นเหตุผลที่เราเผยแพร่ MDDR ทุกปีตั้งแต่ปี 2020 รายงานนี้เป็นผลสรุปของข้อมูลจำนวนมหาศาลและการวิจัยที่ครอบคลุมของ Microsoft ซึ่งแบ่งปันข้อมูลเชิงลึกที่ไม่เหมือนใครของเราเกี่ยวกับวิวัฒนาการของภัยคุกคามทางดิจิทัลและการดำเนินการที่สำคัญที่สามารถดำเนินการได้ในปัจจุบันเพื่อปรับปรุงความปลอดภัยของระบบนิเวศ

เราหวังว่าจะกระตุ้นความรู้สึกเร่งด่วน เพื่อให้ผู้อ่านดำเนินการทันทีตามข้อมูลและข้อมูลเชิงลึกที่เรานำเสนอทั้งที่นี่และในสิ่งพิมพ์ด้านความปลอดภัยทางไซเบอร์จำนวนมากของเราตลอดทั้งปี เมื่อเราพิจารณาถึงความรุนแรงของภัยคุกคามที่มีต่อภูมิทัศน์ดิจิทัล—และการเปลี่ยนแปลงสู่โลกความเป็นจริง—สิ่งสำคัญคือต้องจำไว้ว่าเราทุกคนมีอำนาจในการดำเนินการเพื่อปกป้องตนเอง องค์กรของเราและองค์กรต่างๆ จากภัยคุกคามทางดิจิทัล

ขอขอบคุณที่สละเวลาตรวจสอบรายงาน Microsoft Digital Defense ประจำปีนี้ เราหวังว่าคุณจะพบว่าข้อมูลนี้ให้ข้อมูลเชิงลึกและคำแนะนำที่เป็นประโยชน์เพื่อช่วยเราร่วมกันปกป้องระบบนิเวศดิจิทัล

Tom Burt
รองประธานบริษัท,
การรักษาความปลอดภัยและความไว้วางใจของลูกค้า

วัตถุประสงค์ของเราสำหรับรายงานนี้มีสองเท่า:

1. เพื่อให้แสงสว่างแก่ลูกค้า คู่ค้า และผู้มีส่วนได้ส่วนเสียในระบบนิเวศที่กว้างขึ้น ฉายแสงทั้งการโจมตีทางไซเบอร์ใหม่ๆ และแนวโน้มการพัฒนาของภัยคุกคามที่เกิดขึ้นอย่างต่อเนื่องในอดีต
2. เพื่อช่วยให้ลูกค้าและพันธมิตรของเราปรับปรุงความยืดหยุ่นทางไซเบอร์และตอบสนองต่อภัยคุกคามเหล่านี้



สถานการณ์ของอาชญากรรมไซเบอร์

ในขณะที่การป้องกันทางไซเบอร์ได้รับการปรับปรุงและองค์กรจำนวนมากกำลังใช้แนวทางเชิงรุกในการป้องกัน ผู้โจมตีก็กำลังปรับเปลี่ยนเทคนิคของตน

ภาพรวมของสถานะของอาชญากรรมทางไซเบอร์ 07
ข้อมูลเบื้องต้น 08
แรนซัมแวร์และการขู่กรรโชก: ภัยคุกคามระดับประเทศ 09
ข้อมูลเชิงลึกเกี่ยวกับแรนซัมแวร์จากเจ้าหน้าที่แนวหน้า 14
อาชญากรรมทางไซเบอร์ในฐานะบริการ 18
วิวัฒนาการของภัยคุกคามฟิชชิ่ง 21
เส้นเวลาของการหยุดชะงักของบ็อตเน็ตจากวันแรกของการทำงานร่วมกันของ Microsoft 25
การใช้โครงสร้างพื้นฐานที่ถูกต้องในทางที่ผิด 26
การแฮ็กข้อมูลจะอยู่ที่นี่หรือไม่ 28

ภาพรวมของ

สถานะของอาชญากรรมทางไซเบอร์

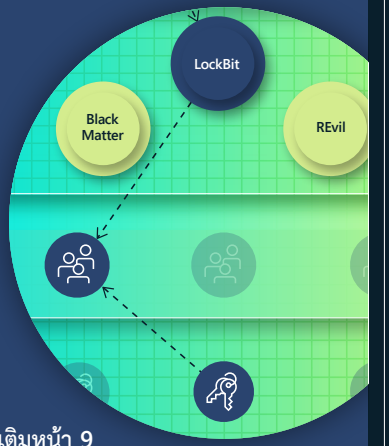
ในขณะที่การป้องกันทางไซเบอร์ได้รับการปรับปรุงและองค์กรจำนวนมากกำลังใช้แนวทางเชิงรุกในการป้องกัน ผู้โจมตีก็กำลังปรับเปลี่ยนเทคนิคของตน

อาชญากรไซเบอร์ยังคงทำหน้าที่เป็นองค์กรที่แสวงหาผลกำไรที่ซับซ้อน ผู้โจมตีกำลังปรับตัวและค้นหาวิธีใหม่ๆ ในการใช้เทคนิคของตน เพิ่มความซับซ้อนของวิธีและตำแหน่งที่พวกเขาโฮสต์โครงสร้างพื้นฐานการดำเนินงานแคมเปญ ในขณะเดียวกัน อาชญากรไซเบอร์ก็ลดมากขึ้นเพื่อลดค่าใช้จ่ายและเพิ่มความถูกต้องตามกฎหมาย ผู้โจมตีกำลังประนีประนอมเครือข่ายธุรกิจและอุปกรณ์เพื่อโฮสต์แคมเปญฟิชชิ่ง มัลแวร์ หรือแม้กระทั่งใช้พลังการประมวลผลเพื่อขุดสกุลเงินดิจิทัล

อาชญากรรมทางไซเบอร์ยังคงเพิ่มขึ้นอย่างต่อเนื่องเนื่องจากการพัฒนาอุตสาหกรรมของเศรษฐกิจอาชญากรรมทางไซเบอร์ได้ลดอุปสรรคด้านทักษะในการเข้าสู่ตลาดด้วยการให้การเข้าถึงเครื่องมือและโครงสร้างพื้นฐานที่มากขึ้น

ค้นหาข้อมูลเพิ่มเติมหน้า 18

ภัยคุกคามจากแรนซัมแวร์และการขู่กรรโชกรุนแรงขึ้นด้วยการโจมตีที่มีเป้าหมายเป็นรัฐบาล ธุรกิจ และโครงสร้างพื้นฐานที่สำคัญ

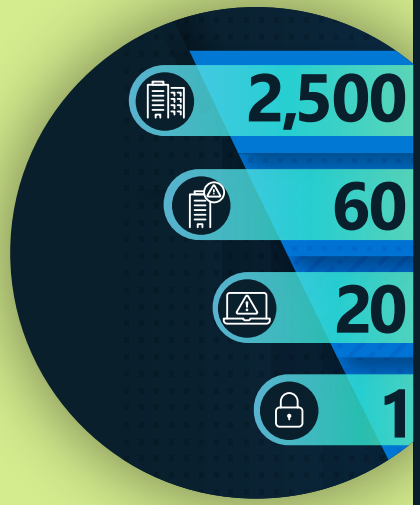


ค้นหาข้อมูลเพิ่มเติมหน้า 9

ผู้โจมตีขู่ว่าจะเปิดเผยข้อมูลที่ละเอียดอ่อนมากขึ้นเพื่อกระตุ้นให้มีการจ่ายเงินค่าไถ่

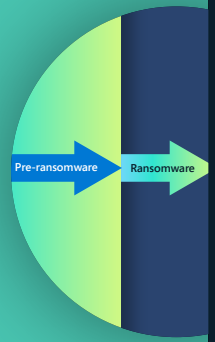
ค้นหาข้อมูลเพิ่มเติมหน้า 10

แรนซัมแวร์ที่ดำเนินการโดยมนุษย์นั้นแพร่หลายมากที่สุด เนื่องจากหนึ่งในสามของเป้าหมายถูกโจมตีสำเร็จโดยอาชญากรที่ใช้การโจมตีเหล่านี้และ 5% ของจำนวนดังกล่าวถูกเรียกค่าไถ่



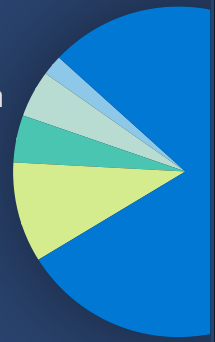
ค้นหาข้อมูลเพิ่มเติมหน้า 9

การป้องกันแรนซัมแวร์ที่มีประสิทธิภาพสูงสุด ได้แก่ การยืนยันตัวตนแบบหลายปัจจัย แพตช์ความปลอดภัยที่ใช้บ่อย และหลักการ Zero Trust ทั่วทั้งสถาปัตยกรรมเครือข่าย



ค้นหาข้อมูลเพิ่มเติมหน้า 13

แผนฟิชชิ่งข้อมูลรับรองซึ่งกำหนดเป้าหมายกล่องจดหมายทั้งหมดอย่างไม่เจาะจงกำลังเพิ่มขึ้น และการประนีประนอมทางอีเมลธุรกิจ รวมถึงการฉ้อโกงใบแจ้งหนี้ ก่อให้เกิดความเสี่ยงด้านอาชญากรรมทางไซเบอร์ที่สำคัญสำหรับองค์กรต่างๆ



ค้นหาข้อมูลเพิ่มเติมหน้า 21

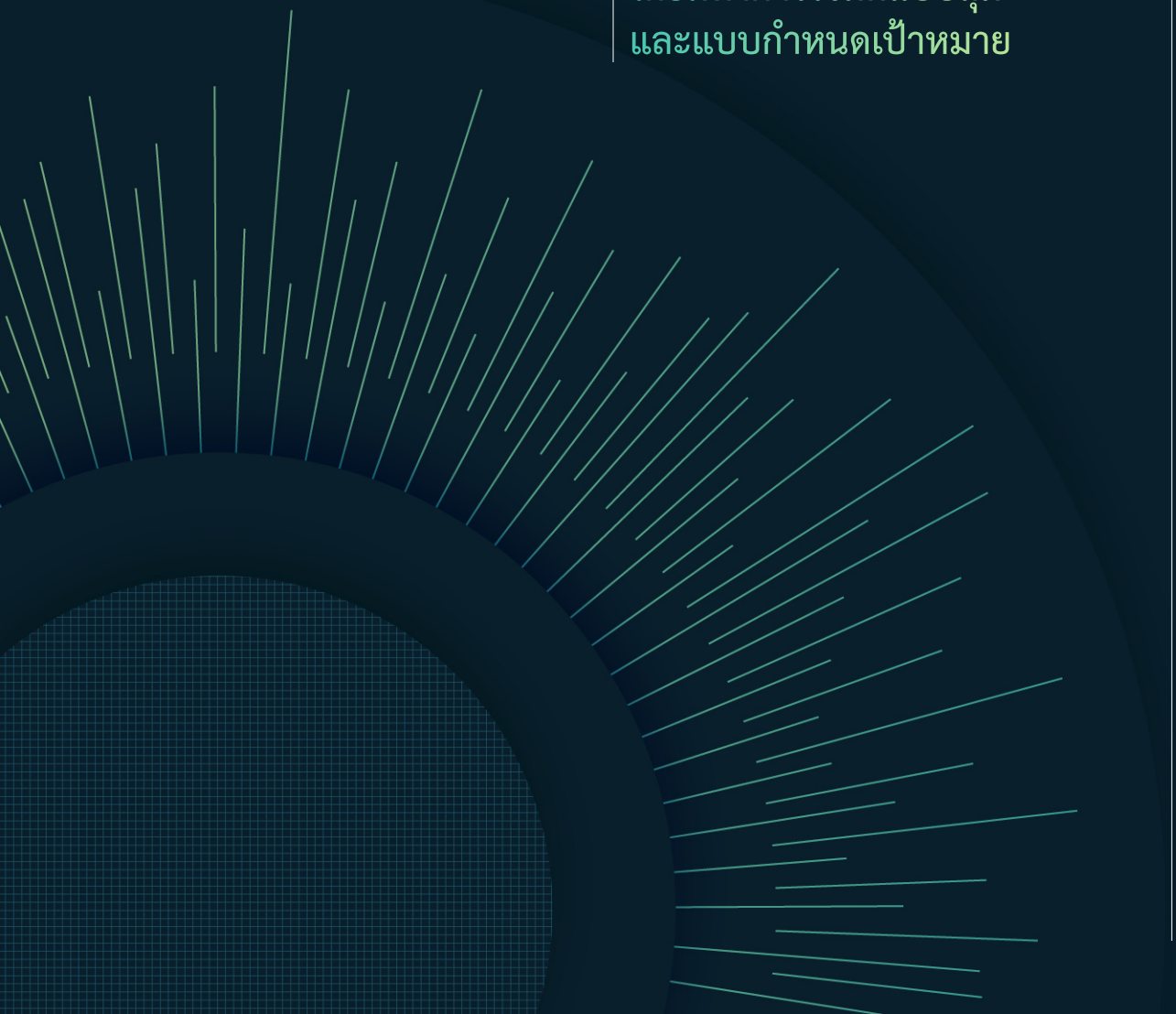
เพื่อขัดขวางโครงสร้างพื้นฐานที่เป็นอันตรายของอาชญากรไซเบอร์และผู้มีบทบาทในระดับชาติ Microsoft อาศัยแนวทางทางกฎหมายที่เป็นนวัตกรรมใหม่และความร่วมมือภาครัฐและเอกชนของเรา



ค้นหาข้อมูลเพิ่มเติมหน้า 25

ข้อมูลเบื้องต้น

อาชญากรรมทางไซเบอร์ยังคงเพิ่มสูงขึ้น โดยมีทั้งการโจมตีแบบสุ่มและแบบกำหนดเป้าหมาย



เมื่อการป้องกันทางไซเบอร์ดีขึ้น และรัฐบาลและภาคธุรกิจต่างๆ หันมาใช้แนวทางเชิงรุกในการป้องกันมากขึ้น เราจึงเห็นผู้โจมตีใช้กลยุทธ์สองประการเพื่อเข้าถึงที่จำเป็นเพื่ออำนวยความสะดวกในการก่ออาชญากรรมทางไซเบอร์ แนวทางหนึ่งคือแคมเปญที่มีเป้าหมายกว้างซึ่งขึ้นอยู่กับปริมาณ ส่วนอีกประเภทหนึ่งใช้การเฝ้าระวังและการกำหนดเป้าหมายแบบเลือกมากขึ้นเพื่อเพิ่มอัตราผลตอบแทน แม้ว่าการสร้างรายได้จะไม่ใช่วัตถุประสงค์ เช่น กิจกรรมของรัฐชาติเพื่อวัตถุประสงค์ทางภูมิรัฐศาสตร์ ก็ยังมีการใช้ทั้งการโจมตีแบบสุ่มและแบบกำหนดเป้าหมาย ในปีที่ผ่านมา อาชญากรไซเบอร์ยังคงอาศัยวิศวกรรมทางสังคมและการใช้ประโยชน์จากประเด็นเฉพาะเพื่อเพิ่มความสำเร็จของแคมเปญ ตัวอย่างเช่น แม้ว่าเหยื่อฟิชชิ่งธีม COVID จะถูกใช้น้อยลง แต่เราสังเกตว่าเหยื่อล่อนั้นเรี่ยไรเงินบริจาคเพื่อสนับสนุนพลเมืองของยูเครนเพิ่มมากขึ้น

ผู้โจมตีกำลังปรับตัวและค้นหาวิธีใหม่ๆ ในการใช้เทคนิคของตน เพิ่มความซับซ้อนของวิธีและตำแหน่งที่พวกเขาโฮสต์โครงสร้างพื้นฐานการดำเนินงานแคมเปญ เราสังเกตว่าอาชญากรไซเบอร์ประหยัดมากขึ้น และผู้โจมตีไม่จ่ายเงินซื้อเทคโนโลยีอีกต่อไป เพื่อลดค่าใช้จ่ายและเพิ่มความถูกต้องตามกฎหมาย ผู้โจมตีบางรายพยายามที่จะประนีประนอมธุรกิจมากขึ้นเพื่อโฮสต์แคมเปญฟิชชิ่ง มัลแวร์ หรือแม้กระทั่งใช้พลังการประมวลผลเพื่อขุดเหมืองสกุลเงินดิจิทัล

ในบทนี้ เรายังตรวจสอบการเพิ่มขึ้นของการแฮ็กข้อมูล ซึ่งเป็นการหยุดชะงักที่เกิดจากพลเมืองส่วนตัวทำการโจมตีทางไซเบอร์เพื่อเป้าหมายทางสังคมหรือการเมืองเพิ่มเติม บุคคลหลายพันคนทั่วโลก ทั้งผู้เชี่ยวชาญและผู้เริ่มต้นได้รวมตัวกันตั้งแต่เดือนกุมภาพันธ์ 2022 เพื่อเริ่มการโจมตี เช่น การปิดใช้งานเว็บไซต์ และการรั่วไหลของข้อมูลที่ถูกขโมย ซึ่งเป็นส่วนหนึ่งของสงครามรัสเซีย-ยูเครน ยังเร็วเกินไปที่จะคาดการณ์ว่าแนวโน้มนี้จะดำเนินต่อไปหรือไม่หลังการสู้รบที่ดำเนินอยู่สิ้นสุดลง

องค์กรต้องตรวจสอบอย่างสม่ำเสมอและเสริมสร้างการควบคุมการเข้าถึงและใช้กลยุทธ์ด้านความปลอดภัยเพื่อป้องกันการโจมตีทางไซเบอร์ อย่างไรก็ตาม นั่นไม่ใช่ทั้งหมดที่พวกเขาสามารถทำได้ เราอธิบายว่าหน่วยปราบปรามอาชญากรรมทางดิจิทัล (DCU) ของเราใช้คดีแพ่งเพื่อยึดโครงสร้างพื้นฐานที่เป็นอันตรายซึ่งอาชญากรไซเบอร์และหน่วยงานของรัฐใช้อย่างไร เราต้องต่อสู้กับภัยคุกคามนี้ร่วมกันผ่านความร่วมมือทั้งภาครัฐและเอกชน เราหวังว่าการแบ่งปันสิ่งที่เราได้เรียนรู้ในช่วง 10 ปีที่ผ่านมา เราจะช่วยให้ผู้อื่นเข้าใจและพิจารณามาตรการเชิงรุกที่พวกเขาสามารถทำได้เพื่อป้องกันตนเองและระบบนิเวศที่กว้างขึ้นจากภัยคุกคามที่เพิ่มขึ้นอย่างต่อเนื่องของอาชญากรรมทางไซเบอร์

Amy Hogan-Burney
ผู้จัดการทั่วไป หน่วยอาชญากรดิจิทัล

แรนซัมแวร์และการขู่กรรโชก: ภัยคุกคามระดับประเทศ

การโจมตีด้วยแรนซัมแวร์ก่อให้เกิดอันตรายเพิ่มขึ้นต่อทุกคน เนื่องจากโครงสร้างพื้นฐานที่สำคัญ ธุรกิจทุกขนาด และรัฐบาลของรัฐและท้องถิ่นตกเป็นเป้าหมายของอาชญากรที่ใช้ประโยชน์จากระบบนิเวศของอาชญากรไซเบอร์ที่กำลังเติบโต

ในช่วงสองปีที่ผ่านมา เหตุการณ์เกี่ยวกับแรนซัมแวร์ที่มีรายละเอียดสูง เช่น เหตุการณ์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานที่สำคัญ การดูแลสุขภาพ และผู้ให้บริการด้านไอทีได้ดึงดูดความสนใจของสาธารณชนเป็นอย่างมาก เนื่องจากการโจมตีของแรนซัมแวร์มีขอบเขตมากขึ้น ผลกระทบของแรนซัมแวร์จึงกลายเป็นวงกว้างมากขึ้น ต่อไปนี้คือตัวอย่างการโจมตีที่เราพบเห็นแล้วในปี 2022:

- ในเดือนกุมภาพันธ์ การโจมตีบริษัท 2 แห่งส่งผลกระทบต่อระบบการชำระเงินของปั๊มน้ำมันหลายร้อยแห่งทางตอนเหนือของเยอรมนี[1]
- ในเดือนมีนาคม การโจมตีบริการไปรษณีย์ของกรีซทำให้การส่งจดหมายหยุดชะงักชั่วคราวและส่งผลกระทบต่อการประมวลผลธุรกรรมทางการเงิน[2]
- ในช่วงปลายเดือนพฤษภาคม การโจมตีด้วยแรนซั่มแวร์ต่อหน่วยงานรัฐบาลของคอสตาริกาทำให้ต้องประกาศภาวะฉุกเฉินแห่งชาติหลังจากโรงพยาบาลปิดตัวลง ศุลกากรและการจัดเก็บภาษีหยุดชะงัก[3]
- นอกจากนี้ ในเดือนพฤษภาคม การโจมตียังทำให้เกิดความล่าช้าและการยกเลิกเที่ยวบินของหนึ่งในสายการบินที่ใหญ่ที่สุดของอินเดีย ทำให้ผู้โดยสารหลายร้อยคนติดอยู่[4]

ความสำเร็จของการโจมตีเหล่านี้และขอบเขตของผลกระทบในโลกแห่งความเป็นจริงเป็นผลมาจากการพัฒนาอุตสาหกรรมของเศรษฐกิจอาชญากรรมไซเบอร์ ทำให้สามารถเข้าถึงเครื่องมือและโครงสร้างพื้นฐาน และขยายขีดความสามารถของอาชญากรไซเบอร์โดยลดอุปสรรคด้านทักษะลง

ในช่วงไม่กี่ปีที่ผ่านมา แรนซัมแวร์ได้เปลี่ยนจากรูปแบบที่ “กลุ่ม” เดียวจะทั้งพัฒนาและแจกจ่ายเพย์โหลดแรนซัมแวร์ไปยังแรนซัมแวร์ในรูปแบบบริการ (RaaS) RaaS ช่วยให้กลุ่มหนึ่งสามารถจัดการการพัฒนาเพย์โหลดของแรนซัมแวร์และให้บริการสำหรับการชำระเงินและการขู่กรรโชกผ่านการรั่วไหลของข้อมูลไปยังอาชญากรไซเบอร์รายอื่นๆ ซึ่งเป็นผู้เปิดการโจมตีแรนซัมแวร์จริงๆ ซึ่งเรียกว่า “พันธมิตร” เพื่อตัดผลกำไร แฟรนไชส์ของเศรษฐกิจอาชญากรรมไซเบอร์ได้ขยายกลุ่มผู้โจมตี การพัฒนาอุตสาหกรรมของเครื่องมืออาชญากรไซเบอร์ทำให้ผู้โจมตีทำการบุกรุก กรองข้อมูล และปรับใช้แรนซัมแวร์ได้ง่ายขึ้น

แรนซัมแวร์ที่ดำเนินการโดยมนุษย์[5]—คำที่นักวิจัยของ Microsoft บัญญัติขึ้นเพื่ออธิบายถึงภัยคุกคามที่ขับเคลื่อนโดยมนุษย์ซึ่งทำการตัดสินใจในทุกขั้นตอนของการโจมตีตามสิ่งที่พวกเขาค้นพบในเครือข่ายของเป้าหมายและวิเคราะห์ ภัยคุกคามจากการโจมตีแรนซัมแวร์สินค้ายังคงเป็นภัยคุกคามที่สำคัญต่อองค์กร



โมเดลอิงจากข้อมูล Microsoft Defender for Endpoint (EDR) (มกราคม–มิถุนายน 2022)

แรนซัมแวร์และการขู่กรรโชก: ภัยคุกคามระดับประเทศ

ต่อไป

การโจมตีด้วยแรนซัมแวร์มีผลกระทบมากยิ่งขึ้นเนื่องจากการปรับใช้กลยุทธ์การสร้างรายได้แบบทวีคูณกลายเป็นแนวทางปฏิบัติมาตรฐาน สิ่งนี้เกี่ยวข้องกับการกรองข้อมูลจากอุปกรณ์ที่ถูกบุกรุก การเข้ารหัสข้อมูลบนอุปกรณ์ จากนั้นโพสต์หรือขู่ว่าจะโพสต์ข้อมูลที่ถูกขโมยสู่สาธารณะเพื่อกดดันเหยื่อให้จ่ายค่าไถ่

แม้ว่าผู้โจมตีแรนซัมแวร์ส่วนใหญ่จะใช้แรนซัมแวร์ฉวยโอกาสกับเครือข่ายใดก็ตามที่พวกเขาเข้าถึงได้ แต่บางคนก็ซื้อการเข้าถึงจากอาชญากรไซเบอร์รายอื่น โดยใช้ประโยชน์จากการเชื่อมต่อระหว่างนายหน้าการเข้าถึงและผู้ให้บริการแรนซัมแวร์

ความครอบคลุมของสัญญาณอัจฉริยะที่ไม่เหมือนใครของเรานั้นรวบรวมมาจากหลายแหล่ง เช่น ข้อมูลประจำตัว อีเมล จุดสิ้นสุด และระบบคลาวด์ และให้ข้อมูลเชิงลึกเกี่ยวกับเศรษฐกิจของแรนซัมแวร์ที่กำลังเติบโต พร้อมด้วยระบบพันธมิตรซึ่งมีเครื่องมือที่ออกแบบมาสำหรับผู้โจมตีที่มีความสามารถทางเทคนิคน้อย

การขยายความสัมพันธ์ระหว่างอาชญากรไซเบอร์ที่เชี่ยวชาญได้เพิ่มความเร็ว ความซับซ้อน และความสำเร็จของการโจมตีแรนซัมแวร์ สิ่งนี้ได้ขับเคลื่อนวิวัฒนาการของระบบนิเวศของอาชญากรไซเบอร์ให้กลายเป็นผู้เล่นที่เชื่อมต่อกันด้วยเทคนิค เป้าหมาย และชุดทักษะที่แตกต่างกัน ซึ่งสนับสนุนซึ่งกันและกันในการเข้าถึงเป้าหมายเบื้องต้น บริการชำระเงิน และเครื่องมือหรือไซต์ถอดรหัสหรือเผยแพร่

ขณะนี้ผู้ให้บริการแรนซัมแวร์สามารถซื้อการเข้าถึงองค์กรหรือเครือข่ายของรัฐบาลทางออนไลน์ หรือรับข้อมูลประจำตัวและการเข้าถึงผ่านความสัมพันธ์ระหว่างบุคคลกับนายหน้าที่มีวัตถุประสงค์หลักเพื่อสร้างรายได้จากการเข้าถึงที่ได้รับเท่านั้น

จากนั้นผู้ให้บริการจะใช้การเข้าถึงที่ซื้อเพื่อปรับใช้เพย์โหลดแรนซัมแวร์ที่ซื้อผ่านตลาดหรือฟอรัมเว็บมืด ในหลายกรณี การเจรจากับเหยื่อดำเนินการโดยทีม RaaS ไม่ใช่ผู้ดำเนินการเอง ธุรกรรมทางอาญาเหล่านี้ดำเนินไปอย่างราบรื่น และผู้เข้าร่วมมีความเสี่ยงน้อยที่จะถูกจับกุมและถูกตั้งข้อหาเนื่องจากการไม่เปิดเผยตัวตนของเว็บมืดและความยากลำบากในการบังคับใช้กฎหมายข้ามชาติ

ความพยายามที่ยั่งยืนและประสบความสำเร็จในการต่อต้านภัยคุกคามนี้จะต้องดำเนินการตามยุทธศาสตร์ทั้งหมดของรัฐบาลโดยร่วมมือกับภาคเอกชนอย่างใกล้ชิด





ตรงกันข้ามกับการแสดงแรนซัมแวร์ในสื่อในบางครั้ง เป็นเรื่องยากที่แรนซัมแวร์รูปแบบเดียวจะได้รับการจัดการโดย “แก๊งแรนซัมแวร์” แบบ end-to-end แต่มีหน่วยงานแยกต่างหากที่สร้างมัลแวร์ เข้าถึงผู้ที่ตกเป็นเหยื่อ ติดตั้งแรนซัมแวร์ และจัดการการเจรจากรรโชก อุตสาหกรรมของระบบนิเวศอาชญากรรมได้นำไปสู่:

- นายหน้าเข้าถึงที่เจาะและส่งต่อการเข้าถึง (การเข้าถึงเป็นบริการ)
- นักพัฒนามัลแวร์ที่ขายเครื่องมือ
- ผู้ดำเนินการทางอาญาและบริษัทในเครือที่ดำเนินการบุกรุก
- ผู้ให้บริการการเข้ารหัสและการกรรโชกที่รับช่วงการสร้างรายได้จากบริษัทในเครือ (RaaS)

แคมเปญแรนซัมแวร์ที่ดำเนินการโดยมนุษย์ทั้งหมดใช้การพึ่งพาร่วมกันในจุดอ่อนด้านความปลอดภัย โดยเฉพาะอย่างยิ่ง ผู้โจมตีมักจะใช้ประโยชน์จากสุขอนามัยทางไซเบอร์ที่ไม่ดีขององค์กร ซึ่งมักจะรวมถึงการแพตช์ไม่บ่อยนักและความล้มเหลวในการใช้การรับรองความถูกต้องแบบหลายปัจจัย (MFA)

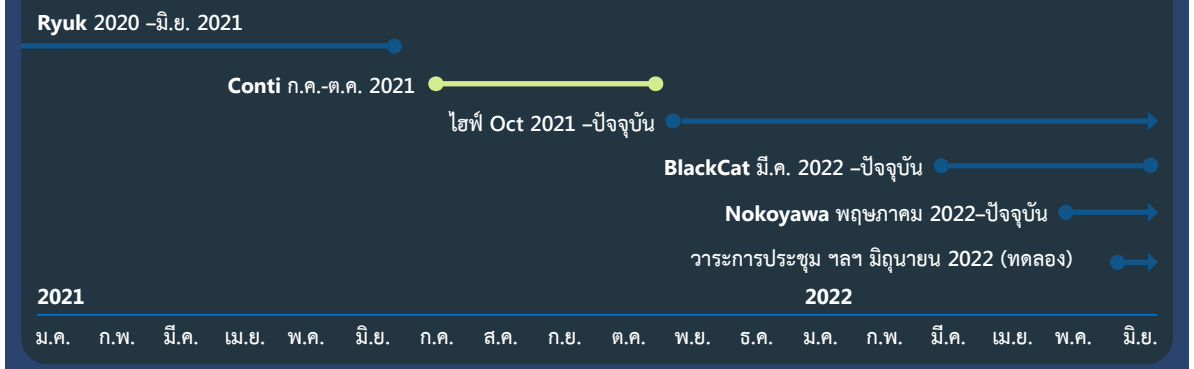
กรณีศึกษา: การสลายตัวของ Conti

Conti ซึ่งเป็นหนึ่งในแรนซัมแวร์สายพันธุ์ยอดนิยมในช่วงสองปีที่ผ่านมา เริ่มปิดการดำเนินงานในช่วงกลางปี 2022 โดยศูนย์ข่าวกรองภัยคุกคามของ Microsoft (MSTIC) สังเกตว่ากิจกรรมลดลงอย่างมากในช่วงปลายเดือนมีนาคมและต้นเดือนเมษายน เราสังเกตการใช้งานแรนซัมแวร์ Conti ครั้งล่าสุดในช่วงกลางเดือนเมษายน อย่างไรก็ตาม เช่นเดียวกับการปิดการดำเนินการของแรนซัมแวร์อื่นๆ การเลิกกิจการของ Conti ไม่ได้ส่งผลกระทบอย่างมีนัยสำคัญต่อการปรับใช้แรนซัมแวร์ เนื่องจาก MSTIC สังเกตว่าบริษัทในเครือของ Conti กำลังหันไปใช้เพย์โหลดแรนซัมแวร์อื่นๆ รวมถึง BlackBasta, Lockbit 2.0, LockbitBlack และ HIVE สิ่งนี้สอดคล้องกับข้อมูลจากปีก่อนหน้า และชี้ให้เห็นว่าเมื่อแก๊งแรนซัมแวร์ออฟไลน์ พวกเขาจะกลับมาอีกหลายเดือนต่อมาหรือกระจายความสามารถทางเทคนิคและทรัพยากรของตนไปยังกลุ่มใหม่

ทีมข่าวกรองภัยคุกคามของ Microsoft ของเราติดตามผู้คุกคามแรนซัมแวร์เป็นกลุ่มบุคคล (ระบุว่าเป็น DEV) ตามเครื่องมือเฉพาะของพวกเขา แทนที่จะติดตามพวกเขาโดยมัลแวร์ที่พวกเขาใช้ ซึ่งหมายความว่าเมื่อบริษัทในเครือของ Conti แยกย้ายกันไป เราสามารถติดตาม DEV เหล่านี้ต่อไปได้ผ่านการใช้เครื่องมืออื่นๆ หรือชุด RaaS ตัวอย่างเช่น:

- DEV-0230 ซึ่งเป็นบริษัทในเครือของ Trickbot เป็นผู้ใช้ Conti อย่างเต็มรูปแบบ ในช่วงปลายเดือนเมษายน MSTIC สังเกตเห็นโดยใช้ QuantumLocker
- DEV-0237 เปลี่ยนจากชุดแรนซัมแวร์ของ Conti เป็น HIVE และ Nokoyawa รวมถึงการใช้ HIVE ในการโจมตีหน่วยงานรัฐบาลคอสตาริกาเมื่อวันที่ 31 พฤษภาคม
- DEV-0506 ซึ่งเป็นผู้ใช้ที่แพร่หลายอีกรายของชุดแรนซัมแวร์ Conti ถูกสังเกตเห็นโดยใช้ BlackBasta

ตัวอย่างของ Affiliate (DEV-0237) เปลี่ยนไปมาระหว่างโปรแกรม RaaS อย่างรวดเร็ว



หลังจากที่โปรแกรม RaaS เช่น Conti ปิดตัวลง พันธมิตรของแรนซัมแวร์จะเปลี่ยนไปใช้โปรแกรมอื่น (Hive) เกือบจะในทันที

RaaS พัฒนาระบบนิเวศของแรนซัมแวร์และขัดขวางการระบุแหล่งที่มา

เนื่องจากแรนซั่มแวร์ที่ดำเนินการโดยมนุษย์นั้นขับเคลื่อนโดยผู้ให้บริการแต่ละราย รูปแบบการโจมตีจึงแตกต่างกันไปตามเป้าหมายและสลับกันไปตลอดระยะเวลาของการโจมตี ในอดีต เราสังเกตเห็นความสัมพันธ์ที่ใกล้ชิดระหว่างเวกเตอร์รายการเริ่มต้น เครื่องมือ และตัวเลือกเพย์โหลดแรนซัมแวร์ในแต่ละแคมเปญของแรนซัมแวร์สายพันธุ์เดียว สิ่งนี้ทำให้การระบุแหล่งที่มาง่ายขึ้น อย่างไรก็ตามรูปแบบพันธมิตรของ RaaS แยกความสัมพันธ์นี้ออกด้วยเหตุนี้ Microsoft จึงติดตามบริษัทในเครือแรนซัมแวร์ที่ใช้เพย์โหลดในการโจมตีเฉพาะเจาะจง แทนที่จะติดตามผู้พัฒนาเพย์โหลดแรนซัมแวร์ในฐานะผู้ดำเนินการ

กล่าวอีกนัยหนึ่ง เราไม่ถือว่าผู้พัฒนา HIVE เป็นผู้ดำเนินการที่อยู่เบื้องหลังการโจมตีแรนซัมแวร์ของ HIVE อีกต่อไป มีแนวโน้มที่จะเป็นพันธมิตร

อุตสาหกรรมการรักษาความปลอดภัยทางไซเบอร์ได้พยายามที่จะจับภาพรายละเอียดนี้อย่างเพียงพอระหว่างนักพัฒนาและผู้ดำเนินการ อุตสาหกรรมยังคงรายงานเหตุการณ์แรนซัมแวร์บ่อยครั้งโดยใช้ชื่อเพย์โหลด ทำให้เกิดความรู้สึกผิดๆ ว่าเอนทิตีเดียวหรือกลุ่มแรนซัมแวร์อยู่เบื้องหลังการโจมตีทั้งหมดโดยใช้เพย์โหลดแรนซัมแวร์นั้น และเหตุการณ์ทั้งหมดที่เกี่ยวข้องจะใช้เทคนิคและโครงสร้างพื้นฐานร่วมกัน เพื่อสนับสนุนผู้ปกป้องเครือข่าย สิ่งสำคัญคือต้องเรียนรู้เพิ่มเติมเกี่ยวกับขั้นตอนก่อนการโจมตีของบริษัทในเครือต่างๆ เช่น การกรองข้อมูลและกลไกการคงอยู่เพิ่มเติม ตลอดจนโอกาสในการตรวจหาและการป้องกันที่อาจมี

มากกว่ามัลแวร์ ผู้โจมตีต้องการข้อมูลประจำตัวเพื่อให้ดำเนินการได้สำเร็จ การติดแรนซัมแวร์ที่ดำเนินการโดยมนุษย์ที่ประสบความสำเร็จของทั้งองค์กรต้องอาศัยการเข้าถึงบัญชีที่มีสิทธิพิเศษสูง

จับตาการโจมตีแรนซัมแวร์ที่ดำเนินการโดยมนุษย์

ในปีที่ผ่านมา ผู้เชี่ยวชาญด้านแรนซัมแวร์ของ Microsoft ได้ทำการตรวจสอบเชิงลึกในเหตุการณ์แรนซัมแวร์ที่ดำเนินการโดยมนุษย์มากกว่า 100 ครั้ง เพื่อติดตามเทคนิคของผู้โจมตีและทำความเข้าใจวิธีการปกป้องลูกค้าของเราให้ดียิ่งขึ้น

สิ่งสำคัญคือต้องทราบว่าการวิเคราะห์ที่เราแบ่งปันที่นี่เป็นไปได้เฉพาะกับอุปกรณ์ที่ออนบอร์ด มีการจัดการเท่านั้น อุปกรณ์ที่ไม่ได้ออนบอร์ดและไม่มีการจัดการแสดงถึงส่วนที่ปลอดภัยน้อยที่สุดของสินทรัพย์ฮาร์ดแวร์ขององค์กร

เทคนิคขั้นตอนแรนซัมแวร์ที่แพร่หลายมากที่สุด:

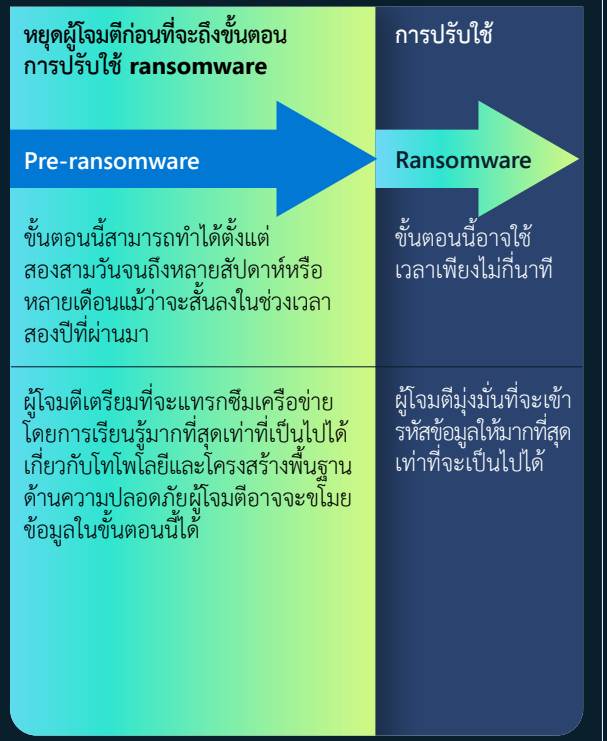
75%
ใช้เครื่องมือผู้ดูแลระบบ

75%
ใช้บัญชีผู้ใช้ที่ถูกบุกรุกที่ยกระดับที่ได้มาเพื่อกระจายเพย์โหลดที่เป็นอันตรายผ่านโปรโตคอล SMB

99%
พยายามยุ่งเกี่ยวกับความปลอดภัยและผลิตภัณฑ์สำรองที่ค้นพบโดยใช้เครื่องมือที่สร้างขึ้นโดย OS

การโจมตีโดยมนุษย์โดยทั่วไป

การโจมตีแรนซัมแวร์ที่ดำเนินการโดยมนุษย์สามารถแบ่งออกได้เป็นระยะก่อนแรนซัมแวร์และระยะการติดตั้งแรนซัมแวร์ ในช่วงก่อนแรนซัมแวร์ ผู้โจมตีเตรียมที่จะแทรกซึมเครือข่ายโดยการเรียนรู้เกี่ยวกับรูปแบบขององค์กรและโครงสร้างพื้นฐานด้านความปลอดภัย



การตรวจสอบของเราพบว่าผู้ที่อยู่เบื้องหลังการโจมตีแรนซัมแวร์ที่ดำเนินการโดยมนุษย์ส่วนใหญ่ใช้ประโยชน์จากจุดอ่อนด้านความปลอดภัยที่คล้ายคลึงกัน และแบ่งปันรูปแบบและเทคนิคการโจมตีทั่วไป

กลยุทธ์การรักษาความปลอดภัยที่ทนทาน

การต่อสู้และป้องกันการโจมตีในลักษณะนี้จำเป็นต้องเปลี่ยนกรอบความคิดขององค์กรเพื่อมุ่งเน้นไปที่การป้องกันที่ครอบคลุมซึ่งจำเป็นในการชะลอและหยุดผู้โจมตีก่อนที่จะสามารถย้ายจากระยะก่อนแรนซัมแวร์ไปสู่ระยะการปรับใช้แรนซัมแวร์

องค์กรต่างๆ ต้องใช้แนวทางปฏิบัติด้านความปลอดภัยที่ดีที่สุดอย่างสม่ำเสมอและจริงจังกับเครือข่ายของตน โดยมีเป้าหมายเพื่อลดการโจมตีประเภทต่างๆ เนื่องจากการตัดสินใจโดยมนุษย์ การโจมตีแรนซัมแวร์เหล่านี้สามารถสร้างการแจ้งเตือนผลิตภัณฑ์รักษาความปลอดภัยหลายรายการที่ดูเหมือนแตกต่างกัน ซึ่งอาจสูญหายหรือไม่ได้รับการตอบสนองได้ทันท่วงที ความเหนื่อยล้าจากการแจ้งเตือนเป็นเรื่องจริง และศูนย์ปฏิบัติการด้านความปลอดภัย (SOC) สามารถทำให้ชีวิตของพวกเขาง่ายขึ้นได้ด้วยการดูแนวโน้มในการแจ้งเตือนหรือจัดกลุ่มการแจ้งเตือนเป็นเหตุการณ์ เพื่อให้พวกเขามองเห็นภาพใหญ่ขึ้น จากนั้น SOC สามารถลดการแจ้งเตือนโดยใช้ความสามารถในการเสริมประสิทธิภาพ เช่น กฎการลดพื้นผิวการโจมตี การป้องกันภัยคุกคามทั่วไปไม่เพียงลดปริมาณการแจ้งเตือน แต่ยังหยุดผู้โจมตีจำนวนมากก่อนที่พวกเขาจะเข้าถึงเครือข่าย

องค์กรต้องรักษามาตรฐานการรักษาความปลอดภัยและสุขอนามัยของเครือข่ายในระดับสูงอย่างต่อเนื่องเพื่อป้องกันตนเองจากการโจมตีของแรนซัมแวร์ที่ดำเนินการโดยมนุษย์

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

ผู้โจมตีด้วยแรนซัมแวร์มีแรงจูงใจจากกำไรที่ได้มาง่าย ดังนั้น การเพิ่มต้นทุนผ่านการรักษาความปลอดภัยที่แข็งแกร่งจึงเป็นกุญแจสำคัญในการทำลายเศรษฐกิจของอาชญากรไซเบอร์

1. สร้างสุขอนามัยข้อมูลประจำตัว มากกว่ามัลแวร์ ผู้โจมตีต้องการข้อมูลประจำตัวเพื่อให้ดำเนินการได้สำเร็จ การติดแรนซัมแวร์ที่ดำเนินการโดยมนุษย์ที่ประสบความสำเร็จของทั้งองค์กรต้องอาศัยการเข้าถึงบัญชีที่มีสิทธิพิเศษสูง เช่น ผู้ดูแลระบบโดเมน หรือความสามารถในการแก้ไขนโยบายกลุ่ม
2. ตรวจสอบการเปิดเผยข้อมูลประจำตัว
3. จัดลำดับความสำคัญของการปรับใช้การอัปเดต Active Directory
4. จัดลำดับความสำคัญของการดำเนินงานที่ไม่ซับซ้อนของระบบคลาวด์
5. ลดพื้นที่ในการถูกโจมตี
6. ทำให้ทรัพย์สินที่เชื่อมต่อกับอินเทอร์เน็ตแข็งแกร่งขึ้นและเข้าใจขอบเขตของคุณ
7. ลดความล้าของการแจ้งเตือน SOC โดยทำให้เครือข่ายของคุณแข็งแกร่งขึ้นเพื่อลดปริมาณและรักษาแบนด์วิธไว้สำหรับเหตุการณ์ที่มีลำดับความสำคัญสูง

ลิงค์ไปยังข้อมูลเพิ่มเติม

- RaaS: ทำความเข้าใจเศรษฐกิจอาชญากรรมไซเบอร์และวิธีป้องกันตัวเอง | บล็อกความปลอดภัยของ Microsoft
- การโจมตีด้วยแรนซัมแวร์ที่ดำเนินการโดยมนุษย์: ภัยพิบัติที่ป้องกันได้ | บล็อกความปลอดภัยของ Microsoft

ข้อมูลเชิงลึกเกี่ยวกับแรนซัมแวร์จากเจ้าหน้าที่แนวหน้า

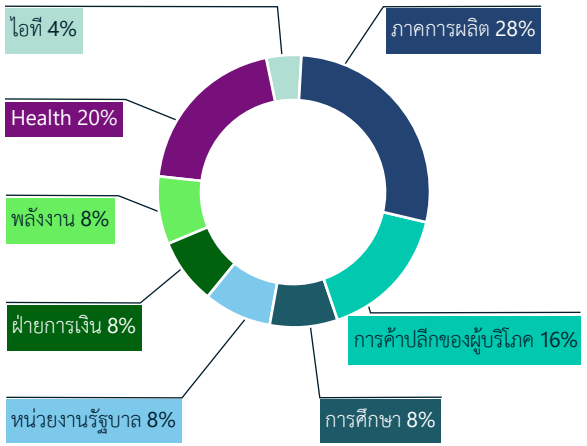
องค์กรต่างๆ ทั่วโลกประสบกับการเติบโตอย่างต่อเนื่องในการโจมตีแรนซัมแวร์ที่ดำเนินการโดยมนุษย์ โดยเริ่มต้นในปี 2019 อย่างไรก็ตาม การบังคับใช้กฎหมายและเหตุการณ์ทางการเมืองในปีที่แล้วมีผลกระทบอย่างมีนัยสำคัญต่อองค์กรอาชญากรไซเบอร์

Security Service Line ของ Microsoft สนับสนุนลูกค้าผ่านการโจมตีทางไซเบอร์ทั้งหมด ตั้งแต่การสืบสวนไปจนถึงกิจกรรมการกักกันและการกู้คืนที่ประสบความสำเร็จ บริการตอบสนองและการกู้คืนนำเสนอผ่านสองทีมที่มีการบูรณาการสูง โดยทีมหนึ่งมุ่งเน้นไปที่การสืบสวนและการวางรากฐานสำหรับการกู้คืน และอีกทีมหนึ่งเกี่ยวกับการกักกันและการกู้คืน ส่วนนี้นำเสนอบทสรุปของการค้นพบโดยพิจารณาจากการมีส่วนร่วมของแรนซัมแวร์ในปีที่ผ่านมา

93%

จากการสืบสวนของ Microsoft ระหว่างภารกิจกู้คืนแรนซัมแวร์ เผยให้เห็นสิทธิ์การเข้าถึงไม่เพียงพอและการควบคุมการเคลื่อนไหวด้านข้าง

เหตุการณ์แรนซัมแวร์และการกู้คืนตามอุตสาหกรรม

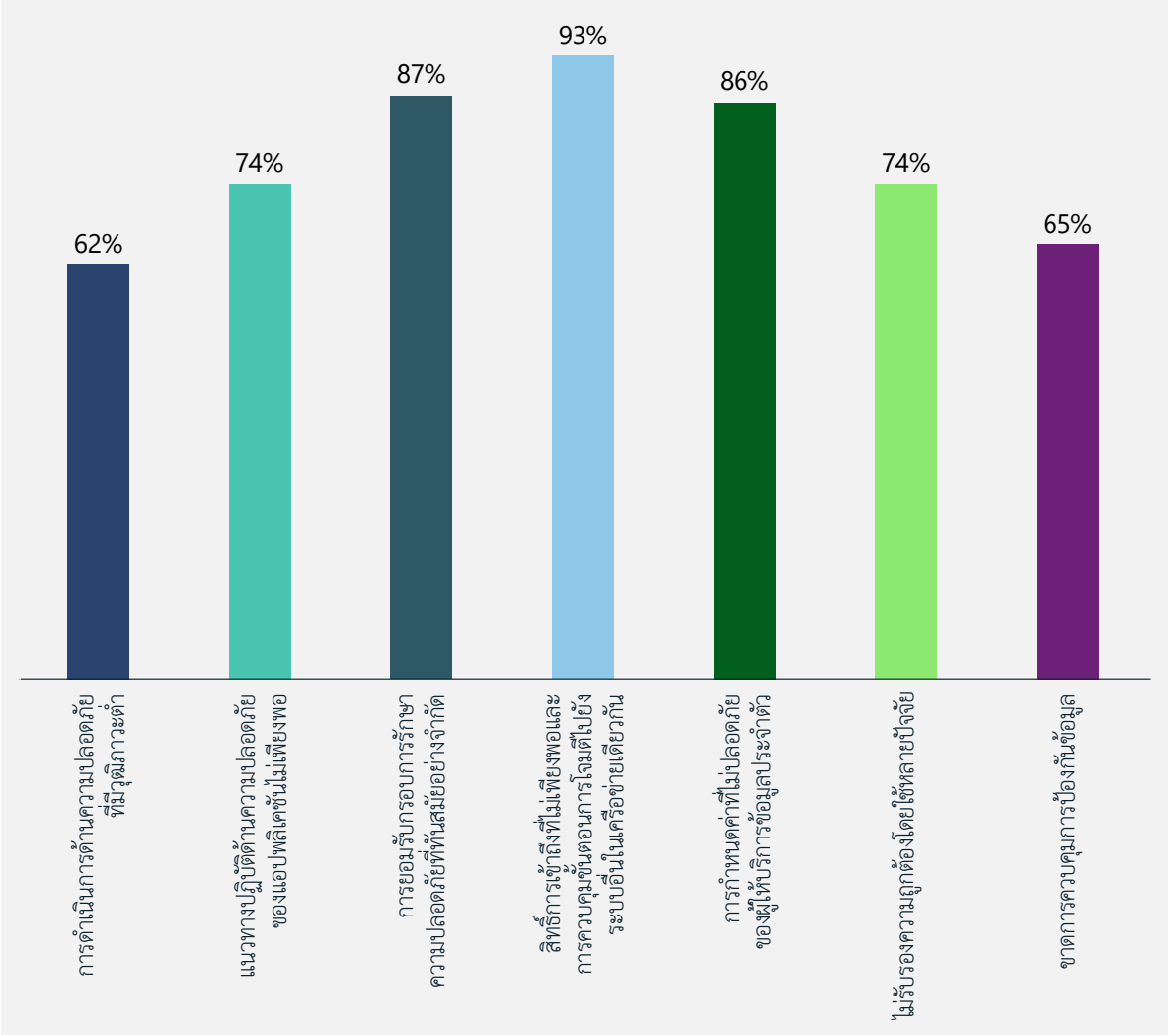


เมื่อกลุ่มเล็กๆ และภัยคุกคามใหม่ๆ ปรากฏขึ้น ทีมป้องกันจะต้องตระหนักถึงภัยคุกคามแรนซัมแวร์ที่พัฒนาไปเรื่อยๆ ในขณะเดียวกันก็ป้องกันตระกูลมัลแวร์แรนซัมแวร์ที่ไม่รู้จักก่อนหน้านี้ แนวทางการพัฒนาอย่างรวดเร็วที่กลุ่มอาชญากรใช้นำไปสู่การสร้างแรนซัมแวร์อัจฉริยะที่บรรจุอยู่ในชุดอุปกรณ์ที่ใช้งานง่าย สิ่งนี้ทำให้มีความยืดหยุ่นมากขึ้นในการโจมตีเป้าหมายจำนวนมากขึ้นอย่างกว้างขวาง

หน้าต่อไปนี้ให้ข้อมูลเชิงลึกเกี่ยวกับปัจจัยที่มักพบได้บ่อยที่สุดในการป้องกันแรนซัมแวร์ที่อ่อนแอ โดยแบ่งกลุ่มผลลัพธ์ออกเป็นสามประเภท:

1. การควบคุมตัวตนที่อ่อนแอ
2. การดำเนินการรักษาความปลอดภัยที่ไม่มีประสิทธิภาพ
3. การปกป้องข้อมูลที่จำกัด

สรุปการค้นพบที่พบบ่อยที่สุดในการโต้ตอบกับแรนซัมแวร์



สิ่งที่พบได้บ่อยที่สุดในการโต้ตอบกับเหตุการณ์แรนซัมแวร์คือการเข้าถึงสิทธิ์ไม่เพียงพอและการควบคุมการเคลื่อนไหวด้านข้าง

ข้อมูลเชิงลึกเกี่ยวกับแรนซัมแวร์จากเจ้าหน้าที่แนวหน้า

ต่อไป

ปัจจัยหลักสามประการที่เห็นได้จากการมีส่วนร่วมตอบสนองในสถานที่ของเรา:

① **การควบคุมตัวตนที่อ่อนแอ:** การโจมตีการโจรกรรมข้อมูลประจำตัวยังคงเป็นหนึ่งในปัจจัยที่มีส่วนสนับสนุนสูงสุด

② **กระบวนการดำเนินการด้านความปลอดภัยที่ไม่มีประสิทธิภาพ** ไม่เพียงแค่นำเสนอหน้าต่างแห่งโอกาสสำหรับผู้โจมตีเท่านั้น แต่ยังส่งผลกระทบอย่างมากต่อเวลาในการกู้คืน

③ ในที่สุดก็จบลงที่ข้อมูล องค์กรต่างๆ พยายามที่จะใช้ **กลยุทธ์การปกป้องข้อมูลที่มีประสิทธิภาพ** ที่สอดคล้องกับความต้องการทางธุรกิจของพวกเขา

① การควบคุมตัวตนที่อ่อนแอ

แรนซั่มแวร์ที่ดำเนินการโดยมนุษย์ยังคงพัฒนาอย่างต่อเนื่องและใช้วิธีขโมยข้อมูลประจำตัวและวิธีการเคลื่อนไหวด้านข้างแบบดั้งเดิมที่เกี่ยวข้องกับการโจมตีแบบกำหนดเป้าหมาย การโจมตีที่ประสบความสำเร็จมักเป็นผลมาจากการรณรงค์ที่ดำเนินมายาวนานซึ่งเกี่ยวข้องกับการบุกรุกระบบข้อมูลประจำตัว เช่น Active Directory (AD) ซึ่งช่วยให้ผู้ปฏิบัติงานที่เป็นมนุษย์สามารถขโมยข้อมูลประจำตัว เข้าถึงระบบ และยังคงอยู่ในเครือข่ายได้

Active Directory (AD) and Azure AD security

88%

ของลูกค้าที่ได้รับผลกระทบไม่ได้ใช้แนวทางปฏิบัติที่ดีที่สุดด้านความปลอดภัยของ AD และ Azure AD สิ่งนี้ได้กลายเป็นเวกเตอร์โจมตีทั่วไป เนื่องจากผู้โจมตีใช้ประโยชน์จากการกำหนดค่าที่ไม่ถูกต้องและมาตรการรักษาความปลอดภัยที่อ่อนแอกว่าในระบบข้อมูลประจำตัวที่สำคัญ เพื่อให้เข้าถึงได้กว้างขึ้นและส่งผลกระทบต่อธุรกิจ

สิทธิ์เข้าถึงน้อยที่สุดและการใช้ Privileged Access Workstations (PAW)

ไม่มีองค์กรใดที่ได้รับผลกระทบใช้การแยกข้อมูลประจำตัวของผู้ดูแลระบบที่เหมาะสมและหลักการการเข้าถึงที่มีสิทธิพิเศษน้อยที่สุดผ่านเวิร์กสเตชันเฉพาะในระหว่างการจัดการข้อมูลประจำตัวที่สำคัญและทรัพย์สินที่มีมูลค่าสูง เช่น ระบบที่เป็นกรรมสิทธิ์และแอปพลิเคชันที่สำคัญต่อธุรกิจ

ความปลอดภัยของบัญชีสิทธิพิเศษ

88%

ในการนัดหมายนั้น MFA ไม่ได้ถูกนำมาใช้กับบัญชีที่ละเอียดอ่อนและมีสิทธิ์สูง ทิ้งช่องว่างด้านความปลอดภัยสำหรับผู้โจมตีที่จะประนีประนอมข้อมูลรับรองและเปลี่ยนการโจมตีเพิ่มเติมโดยใช้ข้อมูลประจำตัวที่ถูกต้องตามกฎหมาย

84%

ผู้ดูแลระบบใน 84 เปอร์เซ็นต์ขององค์กรไม่ได้ใช้การควบคุมข้อมูลประจำตัวของสิทธิพิเศษ เช่น การเข้าถึงแบบทันท่วงที เพื่อป้องกันการใช้ข้อมูลประจำตัวที่มีสิทธิพิเศษที่ถูกบุกรุกในทางที่ผิด

ข้อมูลเชิงลึกเกี่ยวกับแรนซัมแวร์จากเจ้าหน้าที่แนวหน้า

ต่อไป

② การดำเนินการรักษาความปลอดภัยที่ไม่มีประสิทธิภาพ

ข้อมูลของเราแสดงให้เห็นว่าองค์กรที่ได้รับการโจมตีจากแรนซัมแวร์มีช่องว่างที่สำคัญในการดำเนินงานด้านความปลอดภัย เครื่องมือ และการจัดการวงจรชีวิตของสินทรัพย์เทคโนโลยีสารสนเทศ จากข้อมูลที่มีอยู่ ช่องว่างต่อไปนี้ถูกสังเกตมากที่สุด:

การแก้ไขจุดบกพร่อง:

68%

ขององค์กรที่ได้รับผลกระทบไม่มีช่องโหว่และกระบวนการจัดการแพตช์ที่มีประสิทธิภาพ และการพึ่งพากระบวนการด้วยตนเองสูงเมื่อเทียบกับการแพตช์อัตโนมัตินำไปสู่การเปิดที่สำคัญ การผลิตและโครงสร้างพื้นฐานที่สำคัญยังคงต่อสู้กับการบำรุงรักษาและการแพตช์ระบบเทคโนโลยีการดำเนินงาน (OT) รุ่นเก่า

การขาดเครื่องมือปฏิบัติการด้านความปลอดภัย:

องค์กรส่วนใหญ่รายงานว่าขาดการมองเห็นการรักษาความปลอดภัยแบบครอบคลุม เนื่องจากขาดหรือการกำหนดค่าเครื่องมือการรักษาความปลอดภัยที่ไม่ถูกต้อง ทำให้ประสิทธิภาพการตรวจจับและการตอบสนองลดลง

60%

ขององค์กรรายงานว่าไม่มีการใช้เครื่องมือ EDR[6] ซึ่งเป็นเทคโนโลยีพื้นฐานสำหรับการตรวจหาและการตอบสนอง

60%

ไม่ได้ลงทุนในเทคโนโลยีการจัดการข้อมูลและเหตุการณ์ด้านความปลอดภัย (SIEM) ซึ่งนำไปสู่การตรวจสอบไซโล ความสามารถที่จำกัดในการตรวจจับภัยคุกคามแบบ end-to-end และการดำเนินการด้านความปลอดภัยที่ไม่มีประสิทธิภาพ ระบบอัตโนมัติยังคงเป็นช่องว่างที่สำคัญในเครื่องมือและกระบวนการ SOC ทำให้เจ้าหน้าที่ SOC ต้องใช้เวลานับไม่ถ้วนในการทำความเข้าใจเกี่ยวกับการวัดและส่งข้อมูลทางไกลเพื่อความปลอดภัย

84%

ขององค์กรที่ได้รับผลกระทบไม่ได้เปิดใช้งานการรวมสภาพแวดล้อมแบบมัลติคลาวด์เข้ากับเครื่องมือปฏิบัติการด้านความปลอดภัย

กระบวนการตอบสนองและการกู้คืน:

76%

การขาดแผนรับมือที่มีประสิทธิภาพเป็นพื้นที่สำคัญที่สังเกตพบใน 76 เปอร์เซ็นต์ขององค์กรที่ได้รับผลกระทบ ทำให้องค์กรไม่สามารถเตรียมพร้อมรับมือกับวิกฤตได้อย่างเหมาะสม และส่งผลเสียต่อเวลาในการตอบสนองและฟื้นตัว

③ การปกป้องข้อมูลที่จำกัด

องค์กรที่ถูกบุกรุกจำนวนมากขาดกระบวนการปกป้องข้อมูลที่เหมาะสม ซึ่งนำไปสู่ผลกระทบที่รุนแรงต่อเวลาในการกู้คืนข้อมูลและความสามารถในการกลับไปดำเนินธุรกิจ ช่องว่างที่พบบ่อยที่สุด ได้แก่ :

การสำรองข้อมูลที่ไม่เปลี่ยนรูป:

44%

ขององค์กรไม่มีการสำรองข้อมูลที่ไม่เปลี่ยนรูปแบบสำหรับระบบที่ได้รับผลกระทบ ข้อมูลยังแสดงให้เห็นว่าผู้ดูแลระบบไม่มีแผนสำรองและกู้คืนสำหรับสินทรัพย์ที่สำคัญ เช่น AD

การป้องกันข้อมูลสูญหาย:

ผู้โจมตีมักจะหาทางประนีประนอมระบบโดยใช้ประโยชน์จากช่องโหว่ในองค์กร กรองข้อมูลสำคัญเพื่อขู่กรรโชกขโมยทรัพย์สินทางปัญญา หรือการสร้างรายได้

92%

ขององค์กรที่ได้รับผลกระทบไม่ได้ใช้การควบคุมการป้องกันการสูญหายของข้อมูลที่มีประสิทธิภาพเพื่อลดความเสี่ยงเหล่านี้ ซึ่งนำไปสู่การสูญเสียข้อมูลที่สำคัญ

แรนซัมแวร์ลดลงในบางภูมิภาคและเพิ่มขึ้นในบางภูมิภาค

ในปีนี้เราสังเกตว่าจำนวนรวมของกรณีแรนซัมแวร์ที่รายงานไปยังทีมตอบสนองของเราในอเมริกาเหนือและยุโรปลดลงเมื่อเทียบกับปีที่แล้ว ในขณะเดียวกัน รายงานผู้ป่วยในลาตินอเมริกาก็เพิ่มขึ้น

การตีความอย่างหนึ่งของข้อสังเกตนี้คืออาชญากรไซเบอร์หันเหออกจากพื้นที่ที่รับรู้ว่ามีความเสี่ยงสูงที่จะกระตุ้นการตรวจสอบของหน่วยงานบังคับใช้กฎหมายเพื่อสนับสนุนเป้าหมายที่อ่อนแอกว่า เนื่องจาก Microsoft ไม่ได้สังเกตเห็นการปรับปรุงที่สำคัญในการรักษาความปลอดภัยเครือข่ายองค์กรทั่วโลกเพื่ออธิบายการลดลงของการโทรสนับสนุนที่เกี่ยวข้องกับแรนซัมแวร์ เราเชื่อว่าสาเหตุที่เป็นไปได้มากที่สุดคือการรวมกันของกิจกรรมการบังคับใช้กฎหมายในปี 2021 และ 2022 ซึ่งเพิ่มต้นทุนของกิจกรรมทางอาญากับเหตุการณ์ทางภูมิรัฐศาสตร์ในปี 2022

หนึ่งในปฏิบัติการ RaaS ที่แพร่หลายมากที่สุดเป็นของกลุ่มอาชญากรที่พูดภาษารัสเซียที่รู้จักกันในชื่อ REvil (หรือที่เรียกว่า Sodinokibi) ซึ่งเปิดใช้งานมาตั้งแต่ปี 2019 ในเดือนตุลาคม 2021 เซิร์ฟเวอร์ของ REvil ถูกออฟไลน์โดยเป็นส่วนหนึ่งของปฏิบัติการบังคับใช้กฎหมายระหว่างประเทศ GoldDust[7] ในเดือนมกราคม 2022 รัสเซียจับกุมสมาชิก REvil ที่ถูกกล่าวหา 14 คน และบุกค้นสถานที่ที่เกี่ยวข้องกับพวกเขา 25 แห่ง[8] นี่เป็นครั้งแรกที่รัสเซียดำเนินการต่อต้านผู้ให้บริการแรนซัมแวร์บนพื้นฐานของตน

แม้ว่ากิจกรรมการบังคับใช้กฎหมายจะทำให้ความถี่ของการโจมตีช้าลงในปี 2022 แต่ผู้คุกคามอาจพัฒนากลยุทธ์ใหม่เพื่อหลีกเลี่ยงการถูกจับได้ในอนาคต

2X

การโจมตีด้วยแรนซัมแวร์ลดลงในบางภูมิภาค แต่ความต้องการค่าไถ่เพิ่มขึ้นกว่าสองเท่า

แม้ว่ากิจกรรมการบังคับใช้กฎหมายจะทำให้ความถี่ของการโจมตีช้าลงในปี 2022 แต่ผู้คุกคามอาจพัฒนากลยุทธ์ใหม่เพื่อหลีกเลี่ยงการถูกจับได้ในอนาคต ยิ่งไปกว่านั้น ความตึงเครียดระหว่างรัสเซียและสหรัฐอเมริกาเกี่ยวกับการรุกรานยูเครนของรัสเซียดูเหมือนจะยุติความร่วมมือที่เพิ่งเกิดขึ้นของรัสเซียในการต่อสู้กับแรนซัมแวร์ทั่วโลกหลังจากช่วงเวลาสั้นๆ ของความไม่แน่นอนหลังจากการจับกุม REvil สหรัฐอเมริกาและรัสเซียยุติความร่วมมือในการติดตามผู้ดำเนินการแรนซัมแวร์ ซึ่งหมายความว่าอาชญากรไซเบอร์อาจมองว่ารัสเซียเป็นที่หลบภัยอีกครั้ง

เมื่อมองไปข้างหน้า เราคาดการณ์ว่าความเร็วของกิจกรรมแรนซัมแวร์จะขึ้นอยู่กับผลลัพธ์ของคำถามสำคัญบางข้อ:

1. รัฐบาลจะดำเนินการเพื่อป้องกันมิให้อาชญากรแรนซัมแวร์ดำเนินการภายในเขตแดนของตน หรือพยายามขัดขวางผู้กระทำการจากต่างแดนหรือไม่
2. กลุ่มแรนซัมแวร์จะเปลี่ยนกลยุทธ์เพื่อขจัดความจำเป็นในการใช้แรนซัมแวร์และใช้การโจมตีในรูปแบบการขู่กรรโชกหรือไม่
3. องค์กรต่างๆ จะสามารถปรับปรุงและเปลี่ยนแปลงการดำเนินงานด้านไอทีให้ทันสมัยได้เร็วกว่าที่อาชญากรสามารถใช้ประโยชน์จากช่องโหว่ได้หรือไม่
4. ความก้าวหน้าในการติดตามและติดตามการจ่ายค่าไถ่จะบังคับให้ผู้รับค่าไถ่เปลี่ยนกลยุทธ์และการเจรจาหรือไม่

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. มุ่งเน้นไปที่กลยุทธ์การรักษาความปลอดภัยแบบองค์รวม เนื่องจากตระกูลแรนซัมแวร์ทั้งหมดใช้ประโยชน์จากจุดอ่อนด้านความปลอดภัยเดียวกันเพื่อส่งผลกระทบต่อเครือข่าย
2. อัปเดตและบำรุงรักษาพื้นฐานการรักษาความปลอดภัยเพื่อเพิ่มระดับการป้องกันเชิงลึกของการป้องกันและปรับปรุงการดำเนินการรักษาความปลอดภัยให้ทันสมัย การย้ายไปยังระบบคลาวด์ช่วยให้คุณตรวจจับภัยคุกคามได้รวดเร็วขึ้นและตอบสนองได้เร็วขึ้น

ลิงค์ไปยังข้อมูลเพิ่มเติม

- ปกป้ององค์กรของคุณจากแรนซัมแวร์ | ความมั่นคงปลอดภัยของ Microsoft
- 7 วิธีในการทำให้สภาพแวดล้อมของคุณแข็งแกร่งขึ้นจากการประนีประนอม | บล็อกความปลอดภัยของ Microsoft
- การปรับปรุงการป้องกันโดยใช้ AI เพื่อขัดขวางแรนซัมแวร์ที่ดำเนินการโดยมนุษย์ | ทีมวิจัย Microsoft 365 Defender
- Security Insider: สำรวจข้อมูลเชิงลึกและการอัปเดตด้านความปลอดภัยในโลกไซเบอร์ล่าสุด | ความปลอดภัยของไมโครซอฟต์

อาชญากรรมทางไซเบอร์ในฐานะบริการ

อาชญากรรมทางไซเบอร์ในรูปแบบบริการ (CaaS) เป็นภัยคุกคามที่เพิ่มขึ้นและพัฒนาต่อลูกค้าทั่วโลก หน่วยอาชญากรรมดิจิทัลของ Microsoft (DCU) สังเกตเห็นการเติบโตอย่างต่อเนื่องของระบบนิเวศ CaaS ด้วยจำนวนบริการออนไลน์ที่เพิ่มขึ้นซึ่งอำนวยความสะดวกแก่อาชญากรรมทางไซเบอร์ต่างๆ รวมถึง BEC และแรนซัมแวร์ที่ดำเนินการโดยมนุษย์ ฟิชชิงยังคงเป็นวิธีโจมตียอดนิยม เนื่องจากอาชญากรไซเบอร์สามารถได้รับมูลค่ามหาศาลจากการขโมยและขายการเข้าถึงบัญชีที่ถูกขโมยได้สำเร็จ

เพื่อตอบสนองต่อตลาด CaaS ที่ขยายตัว DCU ได้ปรับปรุงระบบการฟังเพื่อตรวจจับและระบุข้อเสนอ CaaS ทั่วทั้งระบบนิเวศของอินเทอร์เน็ต เว็บลึก ฟอรัมที่ได้รับการตรวจสอบ[9] เว็บไซต์เฉพาะทางออนไลน์ กระดานสนทนาและแพลตฟอร์มการส่งข้อความ อาชญากรไซเบอร์กำลังทำงานร่วมกันข้ามโซนเวลาและภาษาเพื่อส่งผลลัพธ์ที่เฉพาะเจาะจง ตัวอย่างเช่น เว็บไซต์ CaaS แห่งหนึ่งที่ดูแลโดยบุคคลในเอเชียมีการดำเนินการในยุโรป และสร้างบัญชีที่เป็นอันตรายในแอฟริกา ลักษณะที่มีหลายเขตอำนาจศาลของการดำเนินการเหล่านี้ทำให้เกิดความท้าทายด้านกฎหมายและการบังคับใช้ที่ซับซ้อน ในการตอบสนอง DCU มุ่งเน้นไปที่ความพยายามในการปิดใช้งานโครงสร้างพื้นฐานอาชญากรที่เป็นอันตรายซึ่งใช้เพื่ออำนวยความสะดวกในการโจมตี CaaS และร่วมมือกับหน่วยงานบังคับใช้กฎหมายทั่วโลกเพื่อรับผิดชอบต่ออาชญากร

อาชญากรไซเบอร์ใช้การวิเคราะห์มากขึ้นเรื่อยๆ เพื่อเพิ่มการเข้าถึง ขอบเขต และผลประโยชน์สูงสุด เช่นเดียวกับธุรกิจที่ถูกกฎหมาย เว็บไซต์ CaaS จะต้องตรวจสอบความถูกต้องของผลิตภัณฑ์และบริการเพื่อรักษาชื่อเสียงที่มั่นคง ตัวอย่างเช่น เว็บไซต์ CaaS ทำการเข้าถึงบัญชีที่ถูกบุกรุกโดยอัตโนมัติเป็นประจำเพื่อให้แน่ใจว่าข้อมูลประจำตัวที่ถูกบุกรุกนั้นถูกต้อง อาชญากรไซเบอร์จะยุติการขายบัญชีเฉพาะเมื่อมีการรีเซ็ตรหัสผ่านหรือแก้ไขช่องโหว่ ยิ่งกว่านั้น เราพบว่าเว็บไซต์ CaaS ให้บริการการตรวจสอบตามความต้องการแก่ผู้ซื้อเป็นกระบวนการควบคุมคุณภาพ ด้วยเหตุนี้ ผู้ซื้อจึงรู้สึกมั่นใจว่าเว็บไซต์ CaaS ขายบัญชีและรหัสผ่านที่ใช้งานอยู่ ขณะเดียวกันก็ลดค่าใช้จ่ายที่อาจเกิดขึ้นให้กับผู้ค้า CaaS หากข้อมูลประจำตัวที่ถูกขโมยได้รับการแก้ไขก่อนการขาย

นอกจากนี้ DCU ยังสังเกตเว็บไซต์ CaaS ที่เสนอตัวเลือกให้ผู้ซื้อในการซื้อบัญชีที่ถูกบุกรุกจากที่ตั้งทางภูมิศาสตร์ที่เฉพาะเจาะจง ผู้ให้บริการออนไลน์ที่กำหนด และบุคคลอาชีพ และอุตสาหกรรมที่เป็นเป้าหมายโดยเฉพาะ บัญชีที่สั่งซื้อบ่อยเน้นที่ผู้เชี่ยวชาญหรือแผนกที่ดำเนินการออกใบแจ้งหนี้ เช่น CFO หรือ "บัญชีลูกหนี้" ในทำนองเดียวกัน อุตสาหกรรมที่เข้าร่วมในการทำสัญญาสาธารณะมักจะถูกกำหนดเป้าหมายเนื่องจากปริมาณของข้อมูลที่มีให้ผ่านกระบวนการประมูลสาธารณะ

การตรวจสอบของ DCU เกี่ยวกับ CaaS แสดงให้เห็นแนวโน้มสำคัญหลายประการ:

จำนวนและความซับซ้อนในการให้บริการเพิ่มมากขึ้น

ตัวอย่างหนึ่งคือวิวัฒนาการของเว็บเชลล์ซึ่งโดยทั่วไปประกอบด้วยเว็บเชิร์ฟเวอร์ที่ถูกบุกรุกซึ่งใช้ในการโจมตีแบบฟิชชิงโดยอัตโนมัติ DCU สังเกตว่าผู้ค้าปลีก CaaS ทำให้การอัปโหลดชุดฟิชชิ่งหรือมัลแวร์ง่ายขึ้นผ่านแดชบอร์ดบนเว็บเฉพาะ ผู้ขาย CaaS มักจะพยายามขายบริการเพิ่มเติมให้กับผู้คุกคามผ่านแดชบอร์ด เช่น บริการข้อความสแปมและรายชื่อผู้รับสแปมเฉพาะตามคุณลักษณะที่กำหนด รวมถึงที่ตั้งทางภูมิศาสตร์หรืออาชีพ ในบางกรณี เราสังเกตว่าเว็บเชลล์เดียวถูกใช้ในแคมเปญโจมตีหลายรายการ ซึ่งบ่งชี้ว่าผู้คุกคามอาจรักษาการเข้าถึงอย่างต่อเนื่องไปยังเซิร์ฟเวอร์ที่ถูกบุกรุก นอกจากนี้ เรายังสังเกตเห็นการเพิ่มขึ้นของบริการลบข้อมูลระบุตัวตนซึ่งเป็นส่วนหนึ่งของระบบนิเวศ CaaS เช่นเดียวกับข้อเสนอสำหรับเครือข่ายส่วนตัวเสมือน (VPN) และบัญชีเซิร์ฟเวอร์ส่วนตัวเสมือน (VPS) ในกรณีส่วนใหญ่ ในตอนแรก VPN/VPS นั้นจัดหามาจากบัตรเครดิตที่ถูกขโมยมา เว็บไซต์ CaaS ยังเสนอโปรโตคอลเดสก์ท็อประยะไกล (RDP) เชลล์ที่ปลอดภัย (SSH) และ cPanels จำนวนมากเพื่อใช้เป็นแพลตฟอร์มในการควบคุมการโจมตีอาชญากรรมทางไซเบอร์ ผู้ค้า CaaS กำหนดค่า RDP, SSH และ cPanels ด้วยเครื่องมือและสคริปต์ที่เหมาะสมเพื่ออำนวยความสะดวกในการโจมตีทางไซเบอร์ประเภทต่างๆ

บริการสร้างโดเมน Homoglyph ต้องการการชำระเงินเป็นสกุลเงินดิจิทัลมากขึ้นเรื่อยๆ

โดเมน Homoglyph เลียนแบบชื่อโดเมนที่ถูกต้องตามกฎหมายโดยใช้อักขระที่มีลักษณะเหมือนกันหรือเกือบเหมือนกันกับอักขระอื่น เป้าหมายคือการหลอกลวงผู้ชมให้คิดว่าโดเมน Homoglyph เป็นโดเมนของแท้ โดเมนเหล่านี้เป็นภัยคุกคามที่แพร่หลายและเป็นประตูสู่อาชญากรรมทางไซเบอร์จำนวนมาก ขณะนี้ไซต์ CaaS ขายชื่อโดเมน Homoglyph แบบกำหนดเอง ซึ่งช่วยให้ผู้ซื้อสามารถขอชื่อบริษัทและชื่อโดเมนที่ต้องการเพื่อเลียนแบบได้ หลังจากได้รับการชำระเงินแล้ว ผู้ค้า CaaS จะใช้เครื่องมือกำเนิด Homoglyph เพื่อเลือกชื่อโดเมนจากนั้นลงทะเบียน Homoglyph ที่เป็นอันตราย การชำระเงินสำหรับบริการนี้เกือบจะเป็นสกุลเงินดิจิทัลเท่านั้น

2,750,000

การลงทะเบียนไซต์ประสบความสำเร็จในการบล็อกโดย DCU ในปีนี้ เพื่อนำหน้าอาชญากรที่วางแผนจะใช้พวกเขาเพื่อมีส่วนร่วมในอาชญากรรมทางไซเบอร์ทั่วโลก

อาชญากรรมทางไซเบอร์ในฐานะบริการ

ต่อไป

ผู้ขาย CaaS เสนอข้อมูลประจำตัวที่ถูกบุกรุกเพื่อซื้อมากขึ้นเรื่อยๆ

ข้อมูลประจำตัวที่ถูกบุกรุกทำให้สามารถเข้าถึงบัญชีผู้ใช้โดยไม่ได้รับอนุญาต รวมถึงบริการส่งข้อความอีเมล ทรัพยากรการแชร์ไฟล์ขององค์กร และ OneDrive for Business หากข้อมูลประจำตัวของผู้ดูแลระบบถูกบุกรุก ผู้ใช้ที่ไม่ได้รับอนุญาตอาจเข้าถึงไฟล์ที่เป็นความลับ ทรัพยากร Azure และบัญชีผู้ใช้ของบริษัทได้ ในหลายกรณี การตรวจสอบของ DCU ระบุการใช้ข้อมูลรับรองเดียวกันโดยไม่ได้รับอนุญาตในเซิร์ฟเวอร์หลายเครื่อง เป็นวิธีการตรวจสอบข้อมูลประจำตัวโดยอัตโนมัติ รูปแบบนี้บ่งชี้ว่าผู้ใช้ที่ถูกบุกรุกอาจตกเป็นเหยื่อของการโจมตีแบบฟิชชิ่งหลายครั้ง หรือมีมัลแวร์ในอุปกรณ์ที่อนุญาตให้บอทเน็ตคีย์ล็อกเกอร์รวบรวมข้อมูลประจำตัว

บริการและผลิตภัณฑ์ CaaS ที่มีคุณสมบัติขั้นสูงกำลังเกิดขึ้นเพื่อหลีกเลี่ยงการตรวจจับ

ผู้ขาย CaaS รายหนึ่งเสนอชุดฟิชชิ่งที่มีความซับซ้อนเพิ่มขึ้นและคุณลักษณะการลบข้อมูลระบุตัวตน ซึ่งออกแบบมาเพื่อหลบเลี่ยงระบบตรวจจับและป้องกันในราคาเพียง $6 USD ต่อวัน บริการนี้เสนอชุดการเปลี่ยนเส้นทางที่ดำเนินการตรวจสอบก่อนที่จะอนุญาตให้รับส่งข้อมูลไปยังเลเยอร์หรือไซต์ถัดไป หนึ่งในนั้นดำเนินการตรวจสอบลายนิ้วมือของอุปกรณ์มากกว่า 90 รายการ รวมถึงตรวจสอบว่าเป็นเครื่องเสมือนหรือไม่ การรวบรวมรายละเอียดเกี่ยวกับเบราว์เซอร์และฮาร์ดแวร์ที่ใช้ และอื่นๆ หากการตรวจสอบทั้งหมดผ่าน การเข้าชมจะถูกส่งไปยังหน้าเริ่มต้นที่ใช้สำหรับฟิชชิง

บริการอาชญากรรมไซเบอร์แบบครบวงจรกำลังขายการสมัครสมาชิกบริการที่มีการจัดการ

โดยปกติแล้ว แต่ละขั้นตอนในการก่ออาชญากรรมออนไลน์สามารถเปิดโปงผู้ที่เป็นภัยคุกคามได้ หากการรักษาความปลอดภัยในการปฏิบัติงานไม่ดีพอ ความเสี่ยงของการเปิดเผยและการระบุตัวตนจะเพิ่มขึ้นหากมีการซื้อบริการจากไซต์ CaaS หลายแห่ง DCU สังเกตเห็นแนวโน้มที่เกี่ยวข้องในเว็บมืดซึ่งมีบริการเพิ่มขึ้นในการเสนอรหัสซอฟต์แวร์ที่ไม่ระบุตัวตนและสร้างข้อความเว็บไซต์ทั่วไปเพื่อลดการเปิดเผย ผู้ให้บริการสมัครสมาชิกอาชญากรรมไซเบอร์แบบครบวงจรจะจัดการบริการทั้งหมดและรับประกันผลลัพธ์ซึ่งช่วยลดความเสี่ยงในการเปิดเผยต่อ OCN ที่สมัครรับข้อมูล ความเสี่ยงที่ลดลงได้เพิ่มความนิยมของบริการแบบครบวงจรเหล่านี้

ฟิชชิ่งในฐานะบริการ (PhaaS) เป็นตัวอย่างหนึ่งของบริการอาชญากรรมไซเบอร์แบบครบวงจร PhaaS เป็นวิวัฒนาการของบริการก่อนหน้าที่เรียกว่าบริการตรวจหาไม่ได้ทั้งหมด (FUD) และให้บริการแบบสมัครสมาชิก ข้อกำหนดทั่วไปของ PhaaS รวมถึงการทำให้เว็บไซต์ฟิชชิ่งใช้งานได้เป็นเวลาหนึ่งเดือน

DCU ยังระบุผู้ค้า CaaS ที่เสนอการปฏิเสธการให้บริการแบบกระจาย (DDoS) ในรูปแบบการสมัครรับข้อมูล โมเดลนี้เป็นการจัดหาจากภายนอกในการสร้างและบำรุงรักษาบ็อตเน็ตที่จำเป็นต่อการโจมตีผู้ค้า CaaS ลูกค้าที่สมัครสมาชิก DDoS แต่ละรายจะได้รับบริการเข้ารหัส

PhaaS อาชญากรไซเบอร์เสนอบริการหลายอย่างภายในการสมัครสมาชิกครั้งเดียว โดยทั่วไปแล้ว ผู้ซื้อต้องดำเนินการเพียงสามประการเท่านั้น:

1. เลือกเทมเพลต/การออกแบบไซต์ฟิชชิงจากในหลายร้อยรายการที่มีให้
2. ระบุที่อยู่อีเมลเพื่อรับข้อมูลประจำตัวจากผู้ตกเป็นเหยื่อฟิชชิ่ง
3. ชำระเงินให้ผู้ค้า PhaaS เป็นสกุลเงินดิจิทัล

เมื่อขั้นตอนเหล่านี้เสร็จสมบูรณ์แล้ว ผู้ค้า PhaaS จะสร้างบริการที่มีการเปลี่ยนเส้นทางและการโฮสต์ของทรัพยากรสามหรือสี่ชั้นเพื่อกำหนดเป้าหมายให้กับผู้ใช้ที่เฉพาะเจาะจง หลังจากนั้นแคมเปญจะเปิดตัว และข้อมูลประจำตัวของเหยื่อจะถูกเก็บไว้ตรวจสอบและส่งไปยังที่อยู่อีเมลที่ผู้ซื้อจัดหาให้ เพื่อความพิเศษ ร้านค้า PhaaS หลายรายเสนอให้โฮสต์ไซต์ฟิชชิ่งบนบล็อกเชนสาธารณะเพื่อให้สามารถเข้าถึงได้โดยเบราว์เซอร์ใด ๆ และการเปลี่ยนเส้นทางสามารถชี้ผู้ใช้ไปยังแหล่งข้อมูลในบัญชีแยกประเภทที่แจกจ่าย

เพื่อเพิ่มความปลอดภัยในการปฏิบัติงานและการสนับสนุนตลอด 24 ชั่วโมงทุกวันตลอด 1 ปี บริการสมัครสมาชิก DDoS นำเสนอสถาปัตยกรรมและวิธีการโจมตีที่แตกต่างกัน ดังนั้นผู้ซื้อเพียงแค่เลือกทรัพยากรที่จะโจมตี และผู้ขายให้สิทธิ์เข้าถึงชุดอุปกรณ์ที่ถูกบุกรุกบนบอตเน็ตเพื่อทำการโจมตี ค่าสมัครสมาชิก DDoS อยู่ที่ $500 USD เท่านั้น

งานของ DCU ในการพัฒนาเครื่องมือและเทคนิคที่ระบุและขัดขวางอาชญากรไซเบอร์ CaaS กำลังดำเนินอยู่ วิวัฒนาการของบริการ CaaS นำเสนอความท้าทายที่สำคัญ โดยเฉพาะอย่างยิ่งในการขัดขวางการชำระเงินด้วยสกุลเงินดิจิทัล

การใช้สกุลเงินดิจิทัลในทางอาญา

เนื่องจากการยอมรับของสกุลเงินดิจิทัลกลายเป็นกระแสหลัก อาชญากรจึงใช้มากขึ้นเพื่อหลบเลี่ยงการบังคับใช้กฎหมายและมาตรการต่อต้านการฟอกเงิน (AML) สิ่งนี้เพิ่มความท้าทายในการบังคับใช้กฎหมายในการติดตามและติดตามการชำระเงินสกุลเงินดิจิทัลให้กับอาชญากรไซเบอร์

การใช้จ่ายทั่วโลกในโซลูชั่นบล็อกเชนเพิ่มขึ้นประมาณ 340 เปอร์เซ็นต์ในช่วงสี่ปีที่ผ่านมา ในขณะที่กระเป๋าเงินดิจิทัลใหม่เพิ่มขึ้นประมาณ 270 เปอร์เซ็นต์ มีกระเป๋าเงินที่ไม่ซ้ำกันมากกว่า 83 ล้านใบทั่วโลก และมูลค่าตลาดรวมของสกุลเงินดิจิตอลทั้งหมดอยู่ที่ประมาณ 1.1 ล้านล้านเหรียญสหรัฐ ณ วันที่ 28 กรกฎาคม 2022[10]



ที่มา: Twitter.com—@PeckShieldAlert (PeckShield เป็นบริษัทรักษาความปลอดภัยบล็อกเชนในจีน)

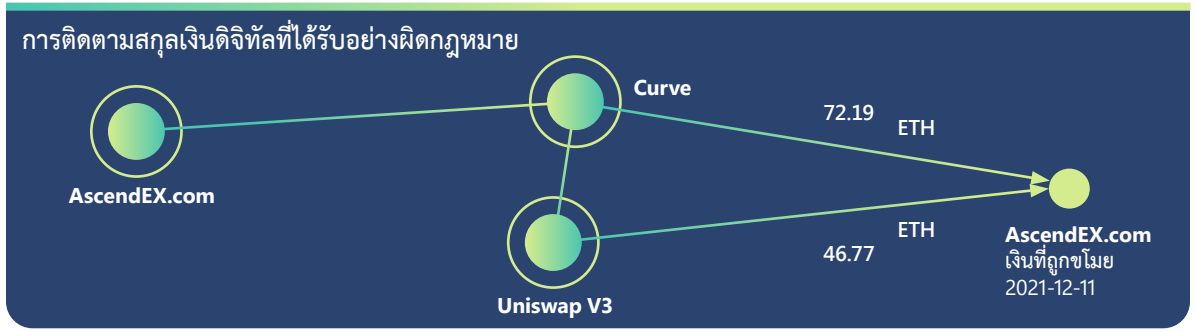
การติดตามการชำระแรนซัมแวร์

แรนซัมแวร์เป็นหนึ่งในแหล่งที่ใหญ่ที่สุดของสกุลเงินดิจิทัลที่รับโดยผิดกฎหมาย ในความพยายามที่จะขัดขวางโครงสร้างพื้นฐานทางเทคนิคที่เป็นอันตรายซึ่งใช้ในการโจมตีแรนซัมแวร์ ตัวอย่างเช่น การหยุดชะงักของ Zloader ในเดือนเมษายน 2022[11]—DCU ของ Microsoft ติดตามกระเป๋าอาชญากรเพื่อเปิดใช้งานความสามารถในการติดตามและกู้คืนสกุลเงินดิจิทัล

เจ้าหน้าที่สืบสวนของ DCU สังเกตเห็นว่าแรนซัมแวร์กำลังพัฒนากลยุทธ์การสื่อสารของตนกับเหยื่อเพื่อปกปิดเส้นทางเงิน เดิมทีอาชญากรไซเบอร์รวมที่อยู่ Bitcoin ไว้ในบันทึกเรียกค่าไถ่ อย่างไรก็ตาม สิ่งนี้ทำให้การติดตามธุรกรรมการชำระเงินบนบล็อกเชนทำได้ง่าย ดังนั้นผู้ให้บริการแรนซัมแวร์จึงหยุดรวมที่อยู่กระเป๋าเงินและใส่ที่อยู่อีเมลหรือลิงก์ไปยังเว็บไซต์แชทแทนเพื่อสื่อสารที่อยู่การชำระค่าไถ่ให้กับผู้ที่ตกเป็นเหยื่อ ผู้ดำเนินการบางคนถึงกับสร้างหน้าเว็บและการเข้าสู่ระบบที่ไม่ซ้ำกันสำหรับเหยื่อแต่ละรายเพื่อป้องกันไม่ให้นักวิจัยด้านความปลอดภัยและหน่วยงานบังคับใช้กฎหมายได้รับที่อยู่กระเป๋าเงินของอาชญากรโดยการแสร้งทำเป็นเหยื่อ แม้จะมีความพยายามของอาชญากรในการซ่อนร่องรอยของพวกเขา แต่การจ่ายเงินค่าไถ่บางส่วนยังคงสามารถกู้คืนได้ด้วยการทำงานร่วมกับหน่วยงานบังคับใช้กฎหมายและบริษัทวิเคราะห์คริปโตที่สามารถติดตามความเคลื่อนไหวบนบล็อกเชนได้

แนวโน้ม: DEX การฟอกเงินที่ผิดกฎหมาย

ปัญหาสำคัญสำหรับอาชญากรไซเบอร์คือการแปลงสกุลเงินดิจิทัลเป็นสกุลเงินคงที่ อาชญากรไซเบอร์มีช่องทางที่เป็นไปได้มากมายสำหรับการแปลง ซึ่งแต่ละช่องทางมีความเสี่ยงที่แตกต่างกัน วิธีหนึ่งที่ใช้ในการลดความเสี่ยงคือการฟอกเงินผ่านการแลกเปลี่ยนแบบกระจายศูนย์ (DEX) ก่อนที่จะถอนเงินออกผ่านตัวเลือกการถอนเงินที่มีอยู่ เช่น การแลกเปลี่ยนแบบรวมศูนย์ (CEX), เพียร์ทูเพียร์ (P2P) และผ่านเคาน์เตอร์ (OTC) การแลกเปลี่ยน DEXes เป็นสถานที่ฟอกเงินที่น่าสนใจเนื่องจากมักไม่ปฏิบัติตามมาตรการ AML



เมื่อใช้ Chainalysis เครื่องมือตรวจสอบสกุลเงินดิจิทัล หน่วยอาชญากรรมดิจิทัลของ Microsoft ค้นพบว่าแฮ็กเกอร์ AcendEX แลกเปลี่ยนเงินที่ถูกขโมยไปที่ DEX ที่เล็กกว่าที่เรียกว่า Curve นอกเหนือจาก Uniswap แผนผังนี้แสดงเส้นทางการฟอกที่ทีมค้นพบ วงกลมแต่ละวงแสดงถึงกลุ่มกระเป๋าเงินและตัวเลขในแต่ละบรรทัดแสดงถึงจำนวนรวมของ Ethereum ที่ส่งไปเพื่อการฟอก

ในเดือนธันวาคม 2021 แฮ็กเกอร์โจมตีแพลตฟอร์มซื้อขายสกุลเงินดิจิทัลระดับโลก AscendEx และขโมยเงินดิจิทัลของลูกค้าไปประมาณ 77.7 ล้านเหรียญสหรัฐ[12] AscendEx ได้จ้างบริษัทวิเคราะห์บล็อกเชนและติดต่อ CEX อื่นๆ ดังนั้นกระเป๋าเงินที่รับเงินที่ถูกขโมยอาจถูกขึ้นบัญชีดำ นอกจากนี้ที่อยู่ที่ส่งเหรียญถูกระบุว่าเป็น Ethereum blockchain explorer Etherscan[13] เพื่อหลีกเลี่ยงการแจ้งเตือนและการขึ้นบัญชีดำ แฮ็กเกอร์ได้ส่งเงิน 1.5 ล้านเหรียญสหรัฐใน Ethereum ไปยัง Uniswap ซึ่งเป็นหนึ่งใน DEX ที่ใหญ่ที่สุดในโลก ในวันที่ 18 กุมภาพันธ์ 2022[14]

การนำมาตรการ AML ที่เข้มงวดขึ้นมาใช้โดย DEX อาจทำให้กิจกรรมการฟอกบนแพลตฟอร์มไม่ชัดเจนและบังคับให้อาชญากรไซเบอร์ใช้วิธีการที่คลุมเครืออื่นๆ เช่น การโยนเหรียญหรือการแลกเปลี่ยนที่ไม่มีใบอนุญาต ตัวอย่างเช่น Uniswap ประกาศเมื่อเร็วๆ นี้ว่าจะเริ่มใช้บัญชีดำเพื่อบล็อกกระเป๋าเงินที่ทราบว่ามีส่วนร่วมในกิจกรรมที่ผิดกฎหมายจากการทำธุรกรรมในการแลกเปลี่ยน[15]

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. หากคุณตกเป็นเหยื่อของอาชญากรไซเบอร์ที่จ่ายเงินให้อาชญากรโดยใช้สกุลเงินดิจิทัล ให้ติดต่อหน่วยงานบังคับใช้กฎหมายในท้องถิ่นซึ่งอาจสามารถช่วยติดตามและกู้คืนเงินที่หายไปได้
2. ทำความคุ้นเคยกับมาตรการ ALM ที่ใช้เมื่อเลือก DEX

ลิงค์ไปยังข้อมูลเพิ่มเติม

- การป้องกันภัยคุกคามด้วยฮาร์ดแวร์ต่อผู้โจมตีสกุลเงินดิจิทัลที่ซับซ้อนมากขึ้น | ทีมวิจัย Microsoft 365 Defender

วิวัฒนาการของภัยคุกคามฟิชชิ่ง

แผนการฟิชชิ่งข้อมูลประจำตัวกำลังเพิ่มขึ้นและยังคงเป็นภัยคุกคามต่อผู้ใช้ทุกที่ เนื่องจากพวกเขากำหนดเป้าหมายกล่องจดหมายทั้งหมดอย่างไม่เลือกหน้า ในบรรดาภัยคุกคามต่างๆ ที่นักวิจัยของเราติดตามและป้องกันนั้น ปริมาณของการโจมตีแบบฟิชชิ่งนั้นมีลำดับความสำคัญมากกว่าภัยคุกคามอื่นๆ ทั้งหมด

เมื่อใช้ข้อมูลจาก Defender for Office เราเห็นอีเมลที่เป็นอันตรายและกิจกรรมระบุตัวตนที่ถูกบุกรุก การปกป้องข้อมูลประจำตัว Azure Active Directory ให้ข้อมูลเพิ่มเติมผ่านการแจ้งเตือนเหตุการณ์ข้อมูลประจำตัวที่ถูกบุกรุก การใช้ Defender สำหรับแอประบบคลาวด์ เราเห็นเหตุการณ์การเข้าถึงข้อมูลประจำตัวที่ถูกบุกรุก และ Microsoft 365 Defender (M365D) ให้ความสัมพันธ์ทั่วทั้งผลิตภัณฑ์ เมตริกการเคลื่อนไหวด้านข้างมาจาก Defender for Endpoint (การแจ้งเตือนและเหตุการณ์พฤติกรรมการโจมตี), Defender for Office (อีเมลที่เป็นอันตราย) และอีกครั้ง M365D สำหรับความสัมพันธ์ทั่วทั้งผลิตภัณฑ์)

710 ล้าน
อีเมลฟิชชิ่งที่ถูกบล็อกต่อสัปดาห์

1 ชั่วโมง 12 นาที
เวลาเฉลี่ยที่ผู้โจมตีใช้ในการเข้าถึงข้อมูลส่วนตัวของคุณ หากคุณตกเป็นเหยื่อของอีเมลฟิชชิ่ง[16]

1 ชั่วโมง 42 นาที
เวลาเฉลี่ยที่ผู้โจมตีจะเริ่มเคลื่อนไหวด้านข้างภายในเครือข่ายองค์กรของคุณเมื่ออุปกรณ์ถูกบุกรุก[17]

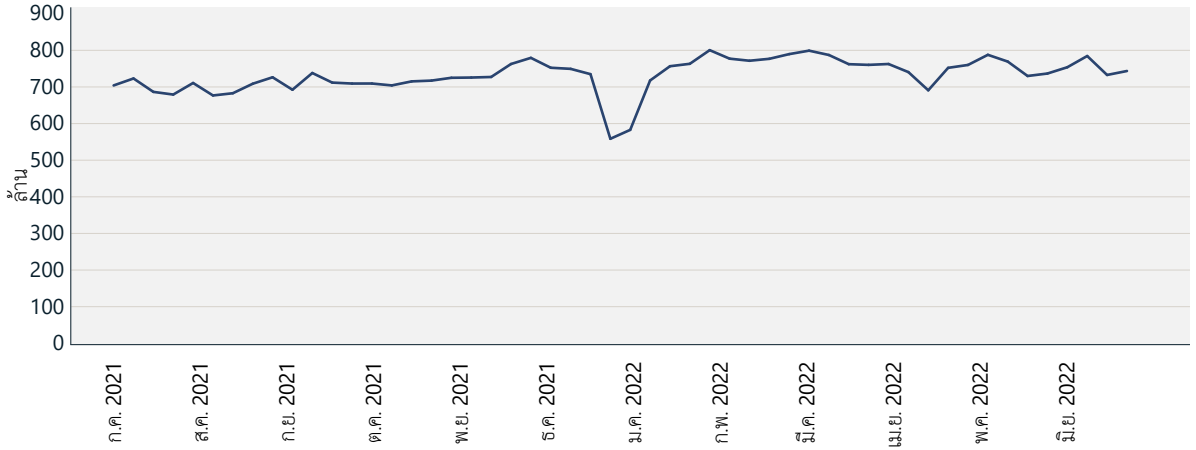
ข้อมูลรับรอง Microsoft 365 ยังคงเป็นหนึ่งในประเภทบัญชีที่เป็นที่ต้องการมากที่สุดสำหรับผู้โจมตี เมื่อข้อมูลรับรองการเข้าสู่ระบบถูกบุกรุก ผู้โจมตีสามารถเข้าสู่ระบบคอมพิวเตอร์ที่เชื่อมโยงกับองค์กรเพื่ออำนวยความสะดวกในการติดมัลแวร์และแรนซัมแวร์ ขโมยข้อมูลและสารสนเทศของบริษัทที่เป็นความลับโดยการเข้าถึงไฟล์ SharePoint และดำเนินการแพร่กระจายของฟิชโดยการส่งอีเมลที่เป็นอันตรายเพิ่มเติมโดยใช้ Outlook รวมถึงการดำเนินการอื่นๆ

นอกเหนือจากแคมเปญที่มีเป้าหมายที่กว้างขึ้น การหลอกลวงขอข้อมูลรับรอง การบริจาค และข้อมูลส่วนบุคคลแล้ว ผู้โจมตียังกำหนดเป้าหมายไปยังธุรกิจที่เลือกเพื่อรับเงินที่มากขึ้น การโจมตีด้วยฟิชชิงทางอีเมลต่อธุรกิจเพื่อผลประโยชน์ทางการเงินเรียกรวมกันว่าการโจมตี BEC Microsoft ตรวจพบอีเมล BEC หลายล้านฉบับทุกเดือน คิดเป็น 0.6 เปอร์เซ็นต์ของอีเมลฟิชชิ่งทั้งหมดที่ตรวจพบ รายงานจาก IC3[18] ที่เผยแพร่ในเดือนพฤษภาคม 2022 บ่งชี้ถึงแนวโน้มที่สูงขึ้นของการขาดทุนเนื่องจากการโจมตี BEC

เทคนิคที่ใช้ในการโจมตีแบบฟิชชิ่งมีความซับซ้อนเพิ่มขึ้นอย่างต่อเนื่อง ในการตอบสนองต่อมาตรการตอบโต้ ผู้โจมตีกำลังปรับใช้วิธีใหม่ๆ ในการใช้เทคนิคของตนและเพิ่มความซับซ้อนของวิธีและตำแหน่งที่พวกเขาโฮสต์โครงสร้างพื้นฐานการดำเนินงานแคมเปญ ซึ่งหมายความว่าองค์กรต่างๆ จะต้องประเมินกลยุทธ์ของตนใหม่อย่างสม่ำเสมอสำหรับการนำโซลูชันด้านความปลอดภัยมาใช้เพื่อบล็อกอีเมลที่เป็นอันตรายและเสริมความแข็งแกร่งในการควบคุมการเข้าถึงสำหรับบัญชีผู้ใช้แต่ละบัญชี

531,000
นอกจาก URL ที่ถูกบล็อกโดย Defender for Office แล้ว หน่วยอาชญากรรมดิจิทัลของเรายังสั่งการให้ลบ URL ฟิชชิ่งที่ไม่ซ้ำกัน 531,000 รายการที่โฮสต์ภายนอก Microsoft

ตรวจพบอีเมลฟิช



จำนวนการตรวจจับฟิชต่อสัปดาห์ยังคงเพิ่มขึ้น การลดลงในเดือนธันวาคม–มกราคมเป็นการลดลงตามฤดูกาลที่คาดไว้ ซึ่งรายงานในรายงานของปีที่แล้วเช่นกัน แหล่งที่มา: สัญญาณการป้องกัน Exchange Online

วิวัฒนาการของภัยคุกคามฟิชชิ่ง

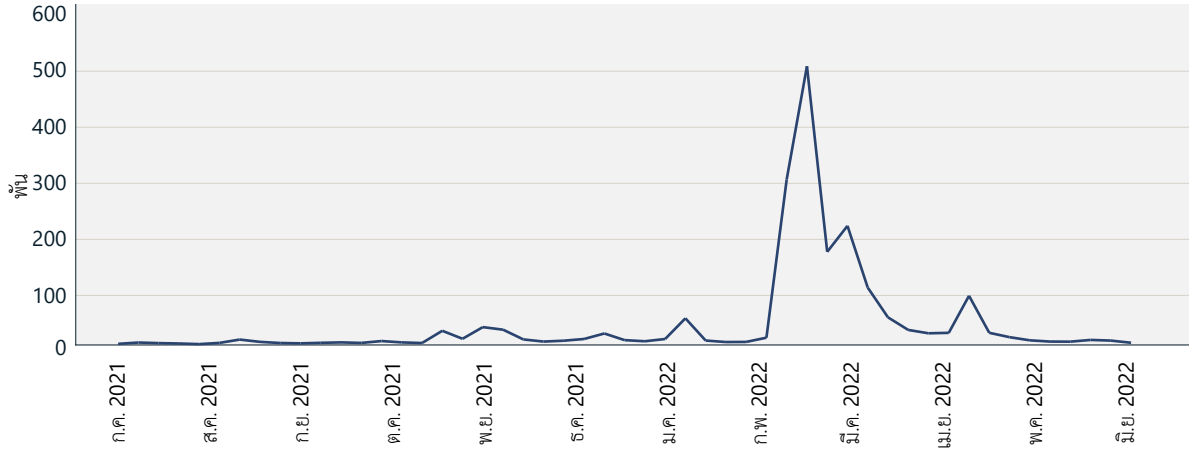
ต่อไป

เรายังคงสังเกตเห็นการเพิ่มขึ้นของอีเมลฟิชชิ่งอย่างต่อเนื่องทุกปี การเปลี่ยนไปทำงานทางไกลในปี 2020 และ 2021 มีการโจมตีแบบฟิชชิ่งเพิ่มขึ้นอย่างมาก โดยมีเป้าหมายเพื่อใช้ประโยชน์จากสภาพแวดล้อมการทำงานที่เปลี่ยนแปลง ผู้ดำเนินการฟิชสามารถนำแม่แบบอีเมลใหม่มาใช้ได้อย่างรวดเร็วโดยใช้เหยื่อล่อที่สอดคล้องกับเหตุการณ์สำคัญของโลก เช่น การแพร่ระบาดของ COVID-19 และธีมที่เชื่อมโยงกับเครื่องมือทำงานร่วมกันและเพิ่มประสิทธิภาพ เช่น Google Drive หรือการแชร์ไฟล์ OneDrive แม้ว่าประเด็นเรื่อง COVID-19 จะลดน้อยลง แต่สงครามในยูเครนก็กลายเป็นสิ่งล่อใจใหม่ที่เริ่มตั้งแต่ต้นเดือนมีนาคม 2022 นักวิจัยของเราสังเกตเห็นการเพิ่มขึ้นของอีเมลที่แอบอ้างเป็นองค์กรที่ถูกต้องตามกฎหมายซึ่งเรียกร้องการบริจาคสกุลเงินดิจิทัลใน Bitcoin และ Ethereum ซึ่งถูกกล่าวหาว่าสนับสนุนพลเมืองยูเครน

เพียงไม่กี่วันหลังจากการเริ่มต้นของสงครามในยูเครนในปลายเดือนกุมภาพันธ์ 2022 จำนวนอีเมลฟิชชิ่งที่ตรวจพบซึ่งมีที่อยู่ Ethereum ที่พบในลูกค้าองค์กรเพิ่มขึ้นอย่างมาก การพบทั้งหมดพุ่งสูงสุดในสัปดาห์แรกของเดือนมีนาคม เมื่ออีเมลฟิชชิ่งกว่าครึ่งล้านรายการมีที่อยู่กระเป๋าเงิน Ethereum ก่อนเริ่มสงคราม จำนวนที่อยู่กระเป๋าเงิน Ethereum ในอีเมลอื่นๆ ที่ตรวจพบว่าเป็นฟิชนั้นน้อยลงอย่างมาก โดยเฉลี่ยแล้วอยู่ที่สองสามพันอีเมลต่อวัน

ยิ่งกว่าที่เคย นักฟิชชิ่งอาศัยโครงสร้างพื้นฐานที่ถูกต้องตามกฎหมายในการดำเนินการ ผลักดันให้มีแคมเปญฟิชชิ่งเพิ่มขึ้นโดยมุ่งเป้าไปที่การประนีประนอมในแง่มุมต่างๆ ของ

อีเมลฟิชชิ่งที่มีที่อยู่กระเป๋าเงิน Ethereum



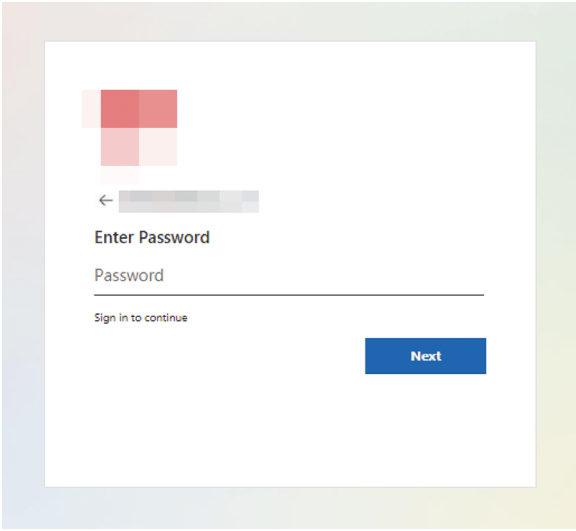
อีเมลทั้งหมดที่ตรวจพบว่าเป็นฟิชชิ่งที่มีที่อยู่กระเป๋าเงิน Ethereum เพิ่มขึ้นในช่วงเริ่มต้นของความขัดแย้งระหว่างยูเครนและรัสเซีย และลดลงหลังจากการพุชครั้งแรก

การดำเนินการ ดังนั้นพวกเขาจึงไม่จำเป็นต้องซื้อ โฮสต์ หรือดำเนินการด้วยตนเอง ตัวอย่างเช่น อีเมลที่เป็นอันตรายอาจมาจากบัญชีผู้ส่งที่ถูกบุกรุก ผู้โจมตีได้ประโยชน์จากการใช้ที่อยู่อีเมลเหล่านี้ซึ่งมีคะแนนชื่อเสียงสูงกว่าและเชื่อถือได้มากกว่าบัญชีและโดเมนที่สร้างขึ้นใหม่ ในแคมเปญฟิชชิ่งขั้นสูงบางแคมเปญ เราสังเกตว่าผู้โจมตีเลือกที่จะส่งและปลอมแปลงจากโดเมนที่มี DMARC[19] ตั้งค่าอย่างไม่ถูกต้องด้วยนโยบาย "ไม่ดำเนินการ" ซึ่งเป็นการเปิดประตูสู่อีเมล การปลอมแปลง

การดำเนินการฟิชชิ่งขนาดใหญ่มักจะใช้บริการคลาวด์และเครื่องเสมือนบนคลาวด์ (VM) เพื่อดำเนินการโจมตีขนาดใหญ่ ผู้โจมตีสามารถทำให้กระบวนการปรับใช้และส่งอีเมลจาก VM เป็นไปโดยอัตโนมัติโดยใช้การส่งต่ออีเมล SMTP หรือโครงสร้างพื้นฐานอีเมลบนคลาวด์ เพื่อรับประโยชน์จากอัตราการส่งที่สูงและชื่อเสียงที่ดีของบริการที่ถูกต้องเหล่านี้ หากอนุญาตให้ส่งอีเมลที่เป็นอันตรายผ่านบริการคลาวด์เหล่านี้ ผู้ปกป้องจะต้องพึ่งพาความสามารถในการกรองอีเมลที่แข็งแกร่งเพื่อบล็อกอีเมลไม่ให้เข้าสู่สภาพแวดล้อม

บัญชี Microsoft ยังคงเป็นเป้าหมายสูงสุดสำหรับนักฟิชชิ่ง โดยเห็นได้จากหน้าเริ่มต้นการฟิชชิ่งจำนวนมากที่แอบอ้างเป็นหน้าเข้าสู่ระบบ Microsoft 365 ตัวอย่างเช่น นักฟิชชิ่งพยายามจับคู่ประสบการณ์การเข้าสู่ระบบของ Microsoft ในชุดฟิชของตนโดยสร้าง URL เฉพาะที่ปรับแต่งให้เหมาะกับผู้รับ URL นี้ชี้ไปยังหน้าเว็บที่เป็นอันตรายซึ่งพัฒนาขึ้นเพื่อรวบรวมข้อมูลประจำตัว แต่พารามิเตอร์ใน URL จะมีที่อยู่อีเมลของผู้รับที่ระบุ เมื่อเป้าหมายนำทางไปยังหน้านั้น ชุดฟิชชิ่งจะเติมข้อมูลการเข้าสู่ระบบของผู้ใช้ไว้ล่วงหน้าและโลโก้ของบริษัทที่ปรับแต่งให้เหมาะกับผู้รับอีเมล โดยจำลองลักษณะที่ปรากฏของหน้าการเข้าสู่ระบบ Microsoft 365 แบบกำหนดเองของบริษัทเป้าหมาย

หน้าฟิชชิ่งที่แอบอ้างการเข้าสู่ระบบ Microsoft ด้วยเนื้อหาแบบไดนามิก

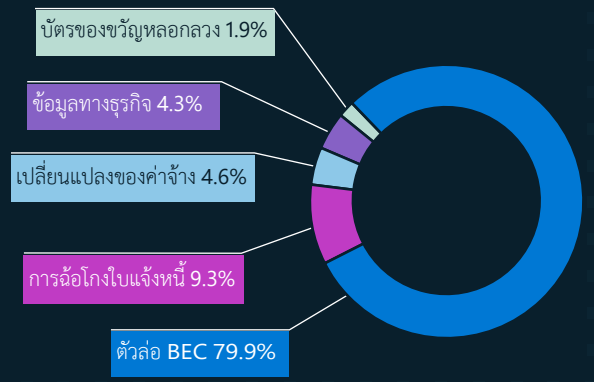


สปอตไลต์เกี่ยวกับการประนีประนอมอีเมลธุรกิจ

อาชญากรไซเบอร์กำลังพัฒนารูปแบบและเทคนิคที่ซับซ้อนมากขึ้นเพื่อเอาชนะการตั้งค่าความปลอดภัยและกำหนดเป้าหมายเป็นบุคคล ธุรกิจ และองค์กร เรากำลังลงทุนทรัพยากรจำนวนมากเพื่อปรับปรุงโปรแกรมการบังคับใช้ BEC เพื่อตอบสนอง

BEC เป็นอาชญากรรมทางไซเบอร์ทางการเงินที่ก่อให้เกิดความเสียหายมากที่สุด โดยมีมูลค่าความเสียหายที่ปรับปรุงแล้วประมาณ 2.4 พันล้านดอลลาร์สหรัฐในปี 2021 ซึ่งคิดเป็นมากกว่าร้อยละ 59 ของการสูญเสียจากอาชญากรรมทางอินเทอร์เน็ตห้าอันดับแรกทั่วโลก[20] เพื่อทำความเข้าใจเกี่ยวกับ ขอบเขตของปัญหาและวิธีที่ดีที่สุดในการปกป้องผู้ใช้จาก BEC นักวิจัยด้านความปลอดภัยของ Microsoft ได้ติดตามรูปแบบที่พบบ่อยที่สุดที่ใช้ในการโจมตี

ธีม BEC (มกราคม–มิถุนายน 2022)



ธีม BEC ตามเปอร์เซ็นต์ของเหตุการณ์

แนวโน้ม BEC

ในฐานะที่เป็นจุดเริ่มต้น ผู้โจมตี BEC มักจะพยายามเริ่มการสนทนากับผู้ที่อาจเป็นเหยื่อเพื่อสร้างสายสัมพันธ์ โดยสวมรอยเป็นเพื่อนร่วมงานหรือคนรู้จักทางธุรกิจ ผู้โจมตีจะค่อยๆ นำการสนทนาไปในทิศทางของการโอนเงิน อีเมลแนะนำตัวที่เราติดตามว่าเป็นอีเมลล่อของ BEC คิดเป็นเกือบ 80 เปอร์เซ็นต์ของอีเมล BEC ที่ตรวจพบ แนวโน้มอื่นๆ ที่ระบุโดยนักวิจัยด้านความปลอดภัยของ Microsoft ในปีที่ผ่านมา ได้แก่:

- เทคนิคที่ใช้บ่อยที่สุดในการโจมตี BEC ที่สังเกตได้ในปี 2022 คือการปลอมแปลง[21] และการแอบอ้างบุคคลอื่น[22]
- ประเภทย่อยของ BEC ที่สร้างความเสียหายทางการเงินให้กับผู้ที่ตกเป็นเหยื่อมากที่สุดคือการฉ้อโกงใบแจ้งหนี้ (ขึ้นอยู่กับปริมาณและจำนวนเงินที่ขอเป็นดอลลาร์ที่เห็นในการตรวจสอบแคมเปญ BEC ของเรา)
- การโจรกรรมข้อมูลทางธุรกิจ เช่น รายงานบัญชีเจ้าหนี้และการติดต่อลูกค้า ทำให้ผู้โจมตีสามารถสร้างการฉ้อโกงใบแจ้งหนี้ที่น่าเชื่อถือได้
- คำขอเปลี่ยนเส้นทางบัญชีเงินเดือนส่วนใหญ่ถูกส่งมาจากบริการอีเมลฟรี และแทบจะไม่ส่งมาจากบัญชีที่ถูกบุกรุก ปริมาณอีเมลจากแหล่งที่มาเหล่านี้พุ่งสูงขึ้นประมาณวันที่ 1 และ 15 ของแต่ละเดือน ซึ่งเป็นวันที่จ่ายบ่อยที่สุด
- แม้จะเป็นช่องทางที่รู้จักกันดีในการฉ้อโกง แต่การหลอกลวงบัตรของขวัญมีเพียง 1.9 เปอร์เซ็นต์ของการโจมตี BEC ที่ตรวจพบ

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

การป้องกันฟิชชิ่ง

เพื่อลดความเสี่ยงต่อฟิชชิ่งขององค์กรของคุณ ผู้ดูแลระบบ IT ควรปฏิบัติตามนโยบายและคุณลักษณะต่อไปนี้:

1. กำหนดให้ใช้ MFA ในทุกบัญชีเพื่อจำกัดการเข้าถึงโดยไม่ได้รับอนุญาต
2. เปิดใช้คุณลักษณะการเข้าถึงแบบมีเงื่อนไขสำหรับบัญชีที่มีสิทธิพิเศษสูงเพื่อบล็อกการเข้าถึงจากประเทศ ภูมิภาค และ IP ที่โดยปกติแล้วจะไม่สร้างการรับส่งข้อมูลในองค์กรของคุณ
3. พิจารณาใช้คีย์ความปลอดภัยทางกายภาพสำหรับผู้บริหาร พนักงานที่เกี่ยวข้องกับกิจกรรมการชำระเงินหรือการซื้อ และบัญชีสิทธิพิเศษอื่นๆ
4. บังคับใช้เบราว์เซอร์ที่สนับสนุนบริการต่างๆ เช่น Microsoft SmartScreen เพื่อวิเคราะห์ URL เพื่อหาพฤติกรรมที่น่าสงสัยและบล็อกการเข้าถึงเว็บไซต์ที่เป็นอันตรายที่รู้จัก[23]
5. ใช้โซลูชันรักษาความปลอดภัยที่ใช้การเรียนรู้ของเครื่องซึ่งจะกักกันฟิชชิที่มีความเป็นไปได้สูง และทำลาย URL และไฟล์แนบใน Sandbox ก่อนที่อีเมลจะไปถึงกล่องจดหมาย เช่น Microsoft Defender สำหรับ Office 365[24]
6. เปิดใช้งานคุณลักษณะการป้องกันการแอบอ้างบุคคลอื่นและการปลอมแปลงทั่วทั้งองค์กรของคุณ
7. กำหนดค่านโยบายการดำเนินการ DomainKeys Identified Mail (DKIM) และ Domain-based Message Authentication Reporting & Conformance (DMARC) เพื่อป้องกันการส่งอีเมลที่ไม่ผ่านการตรวจสอบสิทธิ์ซึ่งอาจปลอมแปลงผู้ส่งที่มีชื่อเสียง
8. ตรวจสอบผู้เช่าและผู้ใช้ที่สร้างกฎอนุญาตและลบโดเมนแบบกว้างและข้อยกเว้นตาม IP กฎเหล่านี้มักจะมีความสำคัญกว่าและสามารถอนุญาตให้อีเมลที่เป็นอันตรายที่รู้จักผ่านการกรองอีเมล
9. เรียกใช้โปรแกรมจำลองฟิชชิ่งเป็นประจำเพื่อวัดความเสี่ยงที่อาจเกิดขึ้นทั่วทั้งองค์กรของคุณ และเพื่อระบุและให้ความรู้แก่ผู้ใช้ที่มีช่องโหว่

ลิงค์ไปยังข้อมูลเพิ่มเติม

- จากการขโมยคุกกี้ไปจนถึง BEC: ผู้โจมตีใช้ไซต์ฟิชชิ่ง AiTM เป็นจุดเริ่มต้นในการฉ้อโกงทางการเงินเพิ่มเติม | ทีมวิจัย Microsoft 365 Defender, Microsoft Threat Intelligence Center (MSTIC)

การหลอกลวงแบบ Homoglyph

BEC และฟิชชิ่งเป็นกลยุทธ์ทางวิศวกรรมสังคมทั่วไป วิศวกรรมสังคมมีบทบาทสำคัญในการก่ออาชญากรรม โน้มน้าวให้เป้าหมายโต้ตอบกับอาชญากรโดยได้รับความไว้วางใจ

ในการค้าทางกายภาพ เครื่องหมายการค้าถูกใช้เพื่อรับประกันความเชื่อถือในที่มาของผลิตภัณฑ์หรือบริการ และผลิตภัณฑ์ลอกเลียนแบบถือเป็นการใช้เครื่องหมายการค้าในทางที่ผิด ในทำนองเดียวกัน อาชญากรไซเบอร์วางตัวเป็นผู้ติดต่อที่คุ้นเคยกับเป้าหมายในระหว่างการโจมตีแบบฟิชชิง โดยใช้ Homoglyph เพื่อหลอกลวงผู้ที่อาจเป็นเหยื่อ

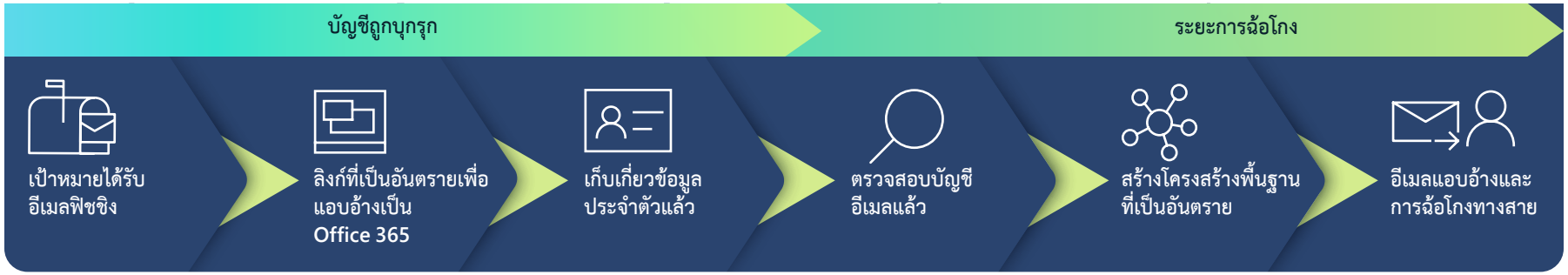
Homoglyph เป็นชื่อโดเมนที่ใช้สำหรับการสื่อสารทางอีเมลใน BEC ซึ่งอักขระจะถูกแทนที่ด้วยอักขระที่มีลักษณะเหมือนกันหรือเกือบเหมือนกันเพื่อหลอกลวงเป้าหมาย

เทคนิค Homoglyph ที่ใช้ในการทดลอง BEC

โดยทั่วไป BEC มีสองขั้นตอน ระยะแรกเกี่ยวข้องกับการประนีประนอมข้อมูลประจำตัว การรั่วไหลของข้อมูลประจำตัวประเภทนี้อาจเป็นผลมาจากการโจมตีแบบฟิชชิ่งหรือการละเมิดข้อมูลขนาดใหญ่ จากนั้นข้อมูลประจำตัวจะถูกขายหรือซื้อขายบนเว็บมืด

ขั้นตอนที่สองคือขั้นตอนการฉ้อโกง ซึ่งผู้โจมตีใช้ข้อมูลประจำตัวที่ถูกบุกรุกเพื่อมีส่วนร่วมในวิศวกรรมสังคมที่ซับซ้อนโดยใช้โดเมนอีเมลแบบ Homoglyph

ความคืบหน้าการโจมตี BEC



เทคนิค	% ของโดเมนแสดงเทคนิค homoglyph
sub l สำหรับ I	25%
sub i สำหรับ l	12%
sub q สำหรับ g	7%
sub rn สำหรับ m	6%
sub .cam สำหรับ .com	6%
sub 0 สำหรับ o	5%
sub ll สำหรับ l	3%
sub ii สำหรับ i	2%
sub vv สำหรับ w	2%
sub l สำหรับ ll	2%
sub e สำหรับ a	2%
sub nn สำหรับ m	1%
sub ll สำหรับ I, sub l สำหรับ i	1%
sub o สำหรับ u	1%

การวิเคราะห์โดเมน Homoglyph มากกว่า 1,700 โดเมนระหว่างเดือนมกราคมถึงกรกฎาคม 2022 แม้ว่าจะใช้เทคนิค Homoglyph 170 เทคนิค แต่ 75% ของโดเมนใช้เพียง 14 เทคนิค

การทำงานแบบ Homoglyph

โดเมน Homoglyph ที่มีลักษณะเหมือนกับโดเมนเมลที่เหยื่อรู้จักนั้นลงทะเบียนกับผู้ให้บริการเมลด้วยชื่อผู้ใช้ที่เหมือนกัน จากนั้นอีเมลที่ถูกไฮแจ็กจะถูกส่งจากโดเมนที่ถูกไฮแจ็กพร้อมคำแนะนำในการชำระเงินใหม่

อาชญากรใช้ประโยชน์จากข้อมูลโอเพ่นซอร์สและการเข้าถึงเธรดอีเมล เพื่อระบุตัวบุคคลที่มีหน้าที่รับผิดชอบในการออกใบแจ้งหนี้และการชำระเงิน จากนั้นจึงสร้างการเลียนแบบที่อยู่อีเมลของผู้ส่งใบแจ้งหนี้แต่ละราย การเลียนแบบนี้ประกอบด้วยชื่อผู้ใช้และโดเมนเมลที่เหมือนกันซึ่งเป็น homoglyph ของผู้ส่งที่แท้จริง

ผู้โจมตีคัดลอกการส่งอีเมลที่มีใบแจ้งหนี้ที่ถูกต้อง จากนั้นเปลี่ยนใบแจ้งหนี้ให้มีรายละเอียดธนาคารของตนเอง จากนั้นใบแจ้งหนี้ที่แก้ไขใหม่นี้จะถูกส่งอีกครั้งจากอีเมลการแอบอ้าง homoglyph ไปยังเป้าหมาย เนื่องจากบริบทเหมาะสมและอีเมลดูเป็นของแท้ เป้าหมายมักทำตามคำแนะนำที่ฉ้อฉล

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. บังคับใช้เบราว์เซอร์ที่สนับสนุนบริการต่างๆ เพื่อวิเคราะห์ URL เพื่อหาพฤติกรรมที่น่าสงสัย และบล็อกการเข้าถึงเว็บไซต์ที่เป็นอันตรายที่รู้จัก เช่น Safe Links และ SmartScreen[25]
2. ใช้โซลูชันรักษาความปลอดภัยที่ใช้การเรียนรู้ของเครื่องซึ่งจะกักกันฟิชที่มีความเป็นไปได้สูง และทำลาย URL และไฟล์แนบใน Sandbox ก่อนที่อีเมลจะไปถึงกล่องจดหมาย

ลิงค์ไปยังข้อมูลเพิ่มเติม

- ศูนย์รับเรื่องร้องเรียนอาชญากรรมทางอินเทอร์เน็ต (IC3) | การประนีประนอมทางอีเมลธุรกิจ: การหลอกลวงมูลค่า 43 พันล้านดอลลาร์
- ข้อมูลเชิงลึกด้านข่าวกรองปลอม — Office 365 | Microsoft Docs
- ข้อมูลเชิงลึกเกี่ยวกับการเลียนแบบ — Office 365 | Microsoft Docs

เส้นเวลาของการหยุดชะงักของบ็อตเน็ตจากวันแรกของการทำงานร่วมกันของ Microsoft

เป็นเวลากว่าทศวรรษที่ DCU ได้ทำงานเชิงรุกเพื่อหยุดยั้งอาชญากรรมทางไซเบอร์ ซึ่งส่งผลให้เกิดมัลแวร์ 26 รายการและการหยุดชะงักของประเทศ ในขณะที่ทีม DCU ใช้กลวิธีและเครื่องมือขั้นสูงในการปิดปฏิบัติการที่ผิดกฎหมายเหล่านี้ เราเห็นว่าอาชญากรไซเบอร์ก็พัฒนาวิธีการของพวกเขาเพื่อพยายามเป็นผู้นำ นี่คือไทม์ไลน์ที่แสดงตัวอย่างบอตเน็ตที่ถูกรบกวนโดย DCU และกลยุทธ์ที่ Microsoft นำมาใช้เพื่อปิดระบบ

2008

บอทเน็ต Conficker

คำอธิบาย: เวิร์มที่แพร่กระจายอย่างรวดเร็วโดยมีเป้าหมายที่ระบบปฏิบัติการ Windows แพร่ระบาดในคอมพิวเตอร์และอุปกรณ์หลายล้านเครื่องในเครือข่ายทั่วไป สร้างเครือข่ายขัดข้องทั่วโลก

การทำงานร่วมกัน: การก่อตัวของ Conficker Working Group ซึ่งเป็นกลุ่มแรกในประเภทเดียวกัน Microsoft ร่วมมือกับ 16 องค์กรทั่วโลกเพื่อกำจัดบอท

การตอบสนอง Microsoft: กลุ่มนี้ทำงานร่วมกันในเขตอำนาจศาลระหว่างประเทศหลายแห่งและประสบความสำเร็จในการกำจัด Conficker

2009

บอทเน็ต Waledac

คำอธิบาย: บอทเน็ตสแปมที่ซับซ้อนซึ่งมีโดเมนของสหรัฐอเมริกาที่รวบรวมที่อยู่อีเมลและกระจายสแปมที่ติดไวรัสในคอมพิวเตอร์มากถึง 90,000 เครื่องทั่วโลก[26]

การทำงานร่วมกัน: การสร้างกลุ่มความร่วมมืออื่น Microsoft Malware Protection Center (MMPC) โดยมุ่งเน้นการทำงานร่วมกันอย่างใกล้ชิดกับนักวิชาการ[27]

การตอบสนอง Microsoft: Microsoft ใช้วิธีการขัดขวางแบบแบ่งชั้นของ C2 และทำให้ผู้ไม่หวังดีประหลาดใจด้วยการยึดโดเมนในสหรัฐอเมริกาโดยไม่แจ้งให้ทราบล่วงหน้า[28] Microsoft ให้สิทธิ์ความเป็นเจ้าของชั่วคราวแก่โดเมนเกือบ 280 โดเมนที่ใช้โดยเซิร์ฟเวอร์ของ Waledac

2011

หน่วยอาชญากรรมดิจิทัลของ Microsoft ถูกสร้างขึ้น

การทำงานร่วมกัน: ออกแบบมาเพื่อขัดขวางอาชญากรรมทางไซเบอร์ที่ส่งผลกระทบต่อระบบนิเวศของ Microsoft ผ่านการผสานรวมอย่างใกล้ชิดระหว่างทีมสืบสวน ทนายความ และวิศวกร

วิธีการ Microsoft: เป้าหมายคือเพื่อทำความเข้าใจด้านเทคนิคของมัลแวร์ต่างๆ ให้ดียิ่งขึ้น และให้ข้อมูลเชิงลึกเหล่านี้แก่ทีมกฎหมายของ Microsoft เพื่อพัฒนากลยุทธ์การหยุดชะงักที่มีประสิทธิภาพ

2013

บอทเน็ต Rustock

คำอธิบาย: บอทอีเมลสแปมโทรจันลับๆ โดยใช้ผู้ให้บริการอินเทอร์เน็ตเป็น C2 หลักที่ออกแบบมาเพื่อขายยา

การทำงานร่วมกัน: Microsoft ปลอมแปลงความร่วมมือกับ Pfizer Pharmaceuticals เพื่อทำความเข้าใจเกี่ยวกับยาที่ขายโดย Rustock และทำงานอย่างใกล้ชิดกับเจ้าหน้าที่บังคับใช้กฎหมายของเนเธอร์แลนด์[29]

การตอบสนอง Microsoft: Microsoft ทำงานร่วมกับ Marshalls ของสหรัฐฯ และหน่วยงานบังคับใช้กฎหมายในเนเธอร์แลนด์เพื่อปิดเซิร์ฟเวอร์ C2 ในประเทศนั้น ลงทะเบียนและบล็อกอัลกอริทึมตัวสร้างโดเมนในอนาคตทั้งหมด (DGA)

บอทเน็ต Sirefef/Zero Access

คำอธิบาย: บ็อตเน็ตโฆษณาที่ออกแบบมาเพื่อนำผู้คนไปยังเว็บไซต์อันตรายที่จะติดตั้งมัลแวร์หรือขโมยข้อมูลส่วนบุคคล ติดไวรัสมากกว่าสองล้านเครื่องและทำให้ผู้ลงโฆษณาเสียเงินมากกว่า 2.7 ล้านเหรียญสหรัฐต่อเดือน ส่วนใหญ่ในสหรัฐอเมริกาและยุโรปตะวันตก

การทำงานร่วมกัน: ทำงานอย่างใกล้ชิดกับ FBI และศูนย์อาชญากรรมไซเบอร์ของ Europol เพื่อลดโครงสร้างพื้นฐานแบบเพียร์ทูเพียร์

การตอบสนอง Microsoft: เข้าร่วมเครือข่าย Zero Access แทนที่เซิร์ฟเวอร์ C2 ของอาชญากรและยึดโดเมนเซิร์ฟเวอร์ดาวน์โหลดได้สำเร็จ

2019

บอทเน็ต Trickbot

คำอธิบาย: บอทเน็ตที่ซับซ้อนพร้อมโครงสร้างพื้นฐานที่กระจัดกระจายทั่วโลก ซึ่งกำหนดเป้าหมายไปที่อุตสาหกรรมบริการทางการเงิน อุปกรณ์ IoT ที่ถูกบุกรุก

การทำงานร่วมกัน: Microsoft ร่วมมือกับ Financial Services Information Sharing and Analysis Center (FS-ISAC) เพื่อกำจัด Trickbot[30]

การตอบสนอง Microsoft: DCU สร้างระบบเพื่อระบุและติดตามโครงสร้างพื้นฐานของบอท และสร้างการแจ้งเตือนสำหรับผู้ให้บริการอินเทอร์เน็ตที่ใช้งานอยู่ โดยคำนึงถึงกฎหมายเฉพาะในประเทศต่างๆ

ยังคงมุ่งเน้นไปที่การหยุดชะงัก

คำอธิบาย: Microsoft ขัดขวางโครงสร้างพื้นฐานของผู้คุกคามเจ็ดรายในปีที่ผ่านมา ป้องกันไม่ให้พวกเขากระจายมัลแวร์เพิ่มเติม ควบคุมคอมพิวเตอร์ของเหยื่อ และกำหนดเป้าหมายเหยื่อเพิ่มเติม

การทำงานร่วมกัน: ด้วยความร่วมมือกับผู้ให้บริการอินเทอร์เน็ต รัฐบาล การบังคับใช้กฎหมาย และอุตสาหกรรมเอกชน Microsoft ได้แบ่งปันข้อมูลเพื่อแก้ไขผู้ที่ตกเป็นเหยื่อของมัลแวร์กว่า 17 ล้านรายทั่วโลก

2022

มองไปข้างหน้า

DCU ยังคงสร้างสรรค์สิ่งใหม่ๆ และกำลังมองหาที่จะใช้ประสบการณ์ในการหยุดชะงักของบ็อตเน็ตเพื่อดำเนินการประสานงานที่นอกเหนือไปจากมัลแวร์ ความสำเร็จอย่างต่อเนื่องของเราต้องใช้วิศวกรรมที่สร้างสรรค์ การแบ่งปันข้อมูล ทฤษฎีทางกฎหมายที่เป็นนวัตกรรมใหม่ และความร่วมมือระหว่างภาครัฐและเอกชน

การใช้โครงสร้างพื้นฐานที่ถูกต้องในทางที่ผิด

อินเทอร์เน็ตเกตเวย์เป็นคำสั่งทางอาญาและโครงสร้างพื้นฐานในการควบคุม

อุปกรณ์ IoT กำลังกลายเป็นเป้าหมายที่ได้รับความนิยมมากขึ้นสำหรับอาชญากรไซเบอร์ที่ใช้บอทเน็ตที่แพร่หลาย เมื่อเราเตอร์ไม่ได้แพตช์และปล่อยให้แสดงต่ออินเทอร์เน็ตโดยตรง ผู้คุกคามสามารถใช้ในทางที่ผิดเพื่อเข้าถึงเครือข่าย ดำเนินการโจมตีที่เป็นอันตราย และแม้แต่สนับสนุนการดำเนินงานของพวกเขา

ทีม Microsoft Defender สำหรับ IoT ดำเนินการวิจัยเกี่ยวกับอุปกรณ์ ตั้งแต่ตัวควบคุมระบบควบคุมอุตสาหกรรมแบบดั้งเดิม ไปจนถึงเซ็นเซอร์ IoT ที่ล้ำสมัย ทีมตรวจสอบมัลแวร์เฉพาะ IoT และ OT เพื่อนำไปสู่รายการตัวบ่งชี้การประนีประนอมที่ใช้ร่วมกัน

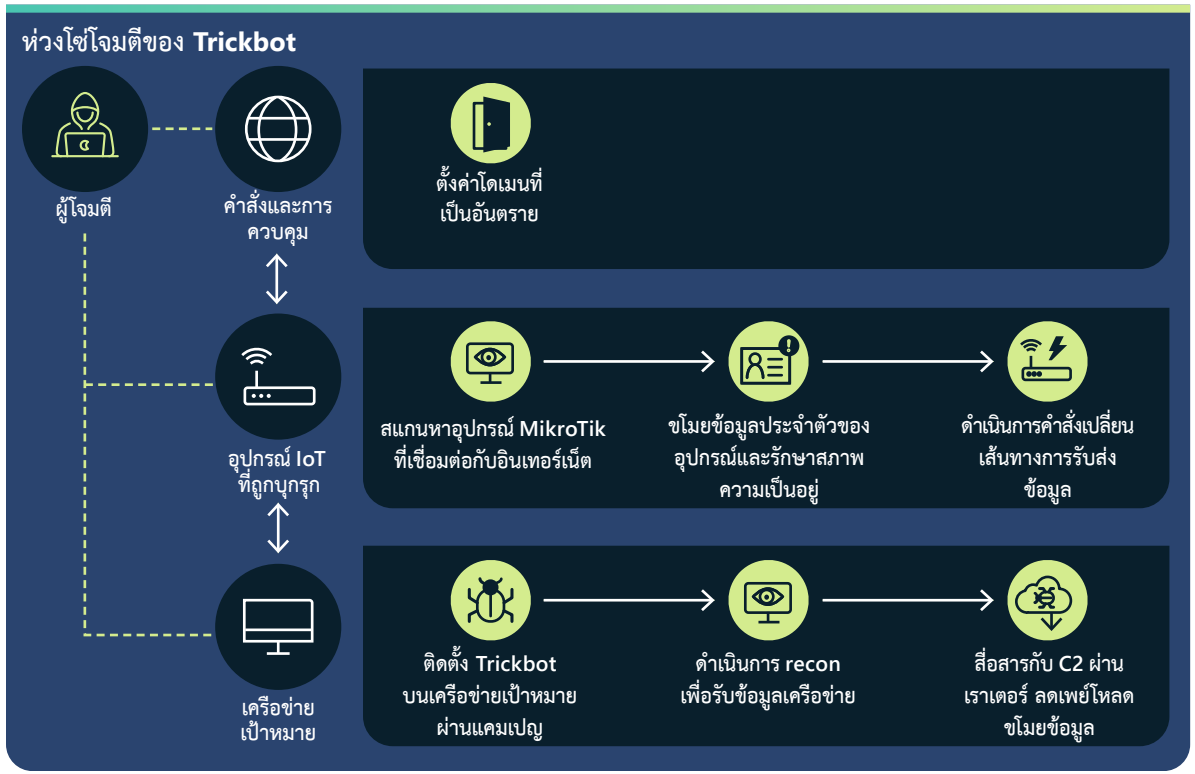
เราเตอร์เป็นพาหะของการโจมตีที่เปราะบางเป็นพิเศษ เนื่องจากมีอยู่ทุกหนทุกแห่งในบ้านและองค์กรที่เชื่อมต่ออินเทอร์เน็ต เราได้ติดตามกิจกรรมของเราเตอร์ MikroTik ซึ่งเป็นเราเตอร์ที่ได้รับความนิยมทั่วโลกทั้งในที่พักอาศัยและในเชิงพาณิชย์ โดยระบุวิธีที่พวกมันถูกใช้สำหรับคำสั่งและการควบคุม (C2) การโจมตีระบบชื่อโดเมน (DNS) และการจี้การขุดคริปโต

โดยเฉพาะอย่างยิ่ง เราได้ระบุวิธีที่ผู้ให้บริการ Trickbot ใช้เราเตอร์ MikroTik ที่ถูกบุกรุกและกำหนดค่าใหม่เพื่อให้ทำงานเป็นส่วนหนึ่งของโครงสร้างพื้นฐาน C2 ของพวกเขา ความนิยมของอุปกรณ์เหล่านี้เพิ่มความรุนแรงของการละเมิดโดย Trickbot และฮาร์ดแวร์และซอฟต์แวร์ที่เป็นเอกลักษณ์ช่วยให้ผู้คุกคามสามารถหลบเลี่ยงมาตรการรักษาความปลอดภัยแบบดั้งเดิม ขยายโครงสร้างพื้นฐาน และบุกรุกอุปกรณ์และเครือข่ายได้มากขึ้น



เราเตอร์ที่เปิดเผยมีความเสี่ยงที่จะถูกโจมตีจากช่องโหว่ที่อาจเกิดขึ้น

ด้วยการติดตามและวิเคราะห์ทราฟฟิกที่มีคำสั่ง Secure Shell (SSH) เราสังเกตเห็นผู้โจมตีที่ใช้เราเตอร์ MikroTik เพื่อสื่อสารกับโครงสร้างพื้นฐานของ Trickbot หลังจากได้รับข้อมูลประจำตัวที่ถูกต้องไปยังอุปกรณ์ ข้อมูลประจำตัวเหล่านี้สามารถได้รับจากการโจมตีแบบเดรัจฉาน การใช้ประโยชน์จากช่องโหว่ที่ทราบด้วยแพตช์ที่พร้อมใช้งาน และใช้รหัสผ่านเริ่มต้น เมื่อเข้าถึงอุปกรณ์แล้ว ผู้โจมตีจะออกคำสั่งเฉพาะที่เปลี่ยนเส้นทางการรับส่งข้อมูลระหว่างสองพอร์ตในเราเตอร์ สร้างสายการสื่อสารระหว่างอุปกรณ์ที่ได้รับผลกระทบจาก Trickbot และ C2



ห่วงโซ่การโจมตี Trickbot แสดงการใช้อุปกรณ์ MikroTik IoT เป็นพร็อกซีเซิร์ฟเวอร์สำหรับ C2

เราได้รวบรวมความรู้ของเราเกี่ยวกับวิธีต่างๆ ในการโจมตีอุปกรณ์ MikroTik นอกเหนือจาก Trickbot เท่านั้น ตลอดจนช่องโหว่และความเสี่ยงทั่วไป (CVEs) ที่รู้จัก เป็นเครื่องมือโอเพ่นซอร์สสำหรับอุปกรณ์ MikroTik ซึ่งสามารถแยกสิ่งประดิษฐ์ทางนิติวิทยาศาสตร์ที่เกี่ยวข้องกับการโจมตีอุปกรณ์ MikroTik เหล่านี้ อุปกรณ์[31]

อุปกรณ์ที่ทำหน้าที่เป็นพร็อกซีย้อนกลับสำหรับมัลแวร์ C2 ไม่ได้มีเฉพาะในเราเตอร์ Trickbot และ MikroTik เท่านั้น ด้วยความร่วมมือกับทีม Microsoft RiskIQ เราได้ตรวจสอบย้อนกลับไปยัง C2 ที่เกี่ยวข้อง และผ่านการสังเกตใบรับรอง SSL เพื่อระบุอุปกรณ์ Ubiquiti และ LigoWave ที่ได้รับผลกระทบเช่นกัน[32] นี่คือ บ่งชี้อย่างชัดเจนว่าอุปกรณ์ IoT กำลังกลายเป็นส่วนประกอบสำคัญของการโจมตีที่ประสานกันโดยรัฐชาติ และเป็นเป้าหมายยอดนิยมสำหรับอาชญากรไซเบอร์ที่ใช้บอทเน็ตอย่างแพร่หลาย

อาชญากรคริปโต ใช้อุปกรณ์ IoT ในทางที่ผิด

อุปกรณ์เกตเวย์เป็นเป้าหมายที่มีค่ามากขึ้นสำหรับผู้คุกคามเนื่องจากจำนวนช่องโหว่ที่รู้จักเพิ่มขึ้นอย่างต่อเนื่องทุกปี พวกเขากำลังถูกใช้สำหรับการขุดคริปโตและกิจกรรมที่เป็นอันตรายประเภทอื่นๆ

เนื่องจากสกุลเงินดิจิทัลได้รับความนิยมมากขึ้น บุคคลและองค์กรจำนวนมากได้ลงทุนพลังการคำนวณและทรัพยากรเครือข่ายจากอุปกรณ์ต่างๆ เช่น เราเตอร์ เพื่อขุดเหรียญบนบล็อกเชน อย่างไรก็ตาม การทำเหมืองสกุลเงินดิจิทัลเป็นกระบวนการที่ใช้ทรัพยากรและเวลาสูงและมีความเป็นไปได้น้อยที่จะประสบความสำเร็จ เพื่อเพิ่มโอกาสในการขุดเหรียญ นักขุดจะรวมตัวกันในเครือข่ายความร่วมมือแบบกระจาย รับแฮชเทียบกับเปอร์เซ็นต์ของเหรียญที่พวกเขาประสบความสำเร็จในการขุดด้วยทรัพยากรที่เชื่อมต่อกัน

ในปีที่ผ่านมา Microsoft สังเกตเห็นการโจมตีจำนวนมากขึ้นเรื่อยๆ ที่ใช้เราเตอร์ในทางที่ผิดเพื่อเปลี่ยนเส้นทางการทำเหมืองสกุลเงินดิจิทัล อาชญากรไซเบอร์บุกรุกเราเตอร์ที่เชื่อมต่อกับแหล่งขุดและเปลี่ยนเส้นทางการรับส่งข้อมูลการขุดไปยังที่อยู่ IP ที่เกี่ยวข้องด้วยการโจมตี DNS พิษ ซึ่งจะเปลี่ยนแปลงการตั้งค่า DNS ของอุปกรณ์เป้าหมาย เราเตอร์ที่ได้รับผลกระทบจะลงทะเบียนที่อยู่ IP ที่ไม่ถูกต้องกับชื่อโดเมนที่กำหนด ส่งทรัพยากรการขุดหรือแฮชไปยังกลุ่มที่ใช้โดยผู้คุกคาม แหล่งรวมเหล่านี้อาจขุดเหรียญที่ไม่ระบุตัวตนที่เกี่ยวข้องกับกิจกรรมทางอาญาหรือใช้แฮชที่ถูกกฎหมายซึ่งสร้างขึ้นโดยนักขุดเพื่อรับเปอร์เซ็นต์ของเหรียญที่พวกเขาขุด จึงจะได้รับรางวัล

> มากกว่าครึ่งหนึ่งของช่องโหว่ที่พบในปี 2021 ขาดแพตช์ การอัปเดตและการรักษาความปลอดภัยเราเตอร์บนเครือข่ายองค์กรและเครือข่ายส่วนตัวยังคงเป็นความท้าทายที่สำคัญสำหรับเจ้าของอุปกรณ์และผู้ดูแลระบบ



พิษ DNS ของอุปกรณ์เกตเวย์ทำให้กิจกรรมการขุดที่ถูกกฎหมายลดลงและเปลี่ยนเส้นทางทรัพยากรไปยังกิจกรรมการขุดทางอาญา

เครื่องเสมือนเป็นโครงสร้างพื้นฐานทางอาญา

การย้ายไปยังระบบคลาวด์อย่างแพร่หลายนั้นรวมถึงอาชญากรไซเบอร์ที่ใช้ประโยชน์จากทรัพย์สินส่วนตัวของเหยื่อโดยไม่รู้ตัวที่ได้รับจากการฟิชชิ่งหรือแจกจ่ายมัลแวร์ขโมยข้อมูลประจำตัว อาชญากรไซเบอร์จำนวนมากเลือกที่จะตั้งค่าโครงสร้างพื้นฐานที่เป็นอันตรายบนเครื่องเสมือนบนระบบคลาวด์ (VM) คอนเทนเนอร์ และบริการไมโคร

เมื่ออาชญากรไซเบอร์เข้าถึงได้ เหตุการณ์ต่อเนื่องอาจเกิดขึ้นเพื่อตั้งค่าโครงสร้างพื้นฐาน เช่น ชุดเครื่องเสมือนผ่านสคริปต์และกระบวนการอัตโนมัติ กระบวนการอัตโนมัติที่เป็นสคริปต์เหล่านี้ใช้เพื่อเริ่มกิจกรรมที่เป็นอันตราย รวมถึงการโจมตีด้วยอีเมลสแปมขนาดใหญ่ การโจมตีแบบฟิชชิงและเว็บเพจที่โฮสต์เนื้อหาที่เป็นอันตราย อาจรวมถึงการตั้งค่าสภาพแวดล้อมเสมือนจริงที่ปรับขนาดซึ่งดำเนินการขุด cryptocurrency ทำให้เหยื่อปลายทางต้องเรียกเก็บเงินหลายแสนดอลลาร์เมื่อสิ้นเดือน

อาชญากรไซเบอร์เข้าใจว่ากิจกรรมที่เป็นอันตรายของพวกเขามีช่วงชีวิตที่จำกัดก่อนที่จะถูกตรวจพบและปิดตัวลง เป็นผลให้พวกเขาขยายขนาดและตอนนี้ทำงานเชิงรุกโดยคำนึงถึงสิ่งที่อาจเกิดขึ้นเป็นอันดับแรก มีการสังเกตว่าพวกเขาเตรียมบัญชีที่ถูกบุกรุกล่วงหน้าและตรวจสอบสภาพแวดล้อมของพวกเขา ทันทีที่ตรวจพบบัญชี (ตั้งค่าโดยใช้เครื่องเสมือนหลายแสนเครื่อง) พวกเขาข้ามไปยังบัญชีถัดไป—ซึ่งเตรียมสคริปต์ไว้แล้วเพื่อเปิดใช้งานทันที—และกิจกรรมที่เป็นอันตรายของพวกเขาจะดำเนินต่อไปโดยไม่มีการหยุดชะงักเพียงเล็กน้อยหรือไม่มีเลย

เช่นเดียวกับโครงสร้างพื้นฐานระบบคลาวด์ โครงสร้างพื้นฐานในสถานที่สามารถใช้ในการโจมตีด้วยสภาพแวดล้อมภายในเสมือนที่ผู้ใช้ในองค์กรไม่รู้จัก สิ่งนี้ต้องการให้จุดเชื่อมต่อเริ่มต้นยังคงเปิดอยู่และเข้าถึงได้ ทรัพย์สินส่วนตัวในสถานที่ยังถูกอาชญากรไซเบอร์ใช้ในทางที่ผิดเพื่อเริ่มห่วงโซ่ต่อไปของโครงสร้างพื้นฐานระบบคลาวด์ ตั้งค่าให้สับสนที่มาเพื่อหลีกเลี่ยงการตรวจจับการสร้างโครงสร้างพื้นฐานที่น่าสงสัย

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ใช้สุขอนามัยทางไซเบอร์ที่ดีและจัดการฝึกอบรมด้านความปลอดภัยทางไซเบอร์สำหรับพนักงาน พร้อมคำแนะนำเพื่อหลีกเลี่ยงการถูกออกแบบโดยสังคม
2. ดำเนินการตรวจสอบความผิดปกติของกิจกรรมของผู้ใช้โดยอัตโนมัติเป็นประจำผ่านการตรวจจับตามขนาดเพื่อช่วยลดการโจมตีประเภทเหล่านี้
3. อัปเดตและรักษาความปลอดภัยเราเตอร์บนเครือข่ายองค์กรและเครือข่ายส่วนตัว

การแฮ็กข้อมูล จะอยู่ที่นี่หรือไม่

แม้ว่าการแฮ็กข้อมูลจะไม่ใช่ปรากฏการณ์ใหม่ แต่สงครามในยูเครนก็มีกลุ่มแฮ็กเกอร์อาสาสมัครจำนวนมาก รวมถึงบางส่วนที่ได้รับคำสั่งจากรัฐบาลให้ใช้เครื่องมือทางไซเบอร์เพื่อทำลายชื่อเสียงหรือทรัพย์สินของฝ่ายตรงข้ามทางการเมือง องค์กรต่างๆ และแม้แต่รัฐชาติ

ในเดือนกุมภาพันธ์ 2022 รัฐบาลยูเครนเรียกร้องให้พลเรือนเอกชนทั่วโลกทำการโจมตีทางไซเบอร์ในรัสเซีย ซึ่งเป็นส่วนหนึ่งของ “กองทัพไอที” ที่แข็งแกร่งกว่า 300,000 นาย[33] พร้อมกันนี้ ได้จัดตั้ง กลุ่มแฮกเกอร์ เช่น Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans และ RaidForum2 เริ่มทำการโจมตีเพื่อสนับสนุนยูเครน กลุ่มอื่นๆ รวมถึง แก๊งแรนซัมแวร์ Conti เข้าข้างรัสเซีย [34]

หลายเดือนต่อมา กิจกรรมของผู้ไม่ระบุชื่อก็ปรากฏให้เห็นอย่างชัดเจน แฮ็กเกอร์ที่ดำเนินการในนามของกลุ่ม หรือในนามของหนึ่งในบริษัทในเครือ ปิดใช้งานเว็บไซต์รัสเซียและเบลารุสหลายพันแห่งเป็นการชั่วคราว รั่วไหลของข้อมูลที่ขโมยไปหลายร้อยกิกะไบต์ แฮ็กช่องทีวีของรัสเซียเพื่อเล่นเนื้อหาที่สนับสนุนยูเครน และเสนอที่จะจ่าย Bitcoin สำหรับรถถังรัสเซียที่ยอมจำนน

การเพิ่มขึ้นของแฮ็กเกอร์สมัครเล่น

แพลตฟอร์มโซเชียลมีเดียช่วยให้สามารถจัดระเบียบและระดมพลแฮ็กเกอร์มือสมัครเล่นหลายพันคนได้อย่างรวดเร็ว ซึ่งได้รับคำแนะนำในการดำเนินการโจมตีที่สั่งการได้ง่าย เช่น การโจมตี DDoS ผู้จัดงานใช้ประโยชน์จาก Twitter, Telegram และฟอรัมส่วนตัวเพื่อระดมแฮ็กเกอร์ จัดระเบียบการดำเนินงาน และเผยแพร่คู่มือแนะนำการแฮ็ก

อย่างไรก็ตาม แฮ็กเกอร์เหล่านี้ส่วนใหญ่มักมีทักษะจำกัด แม้จะได้รับคำแนะนำก็ตาม สิ่งนี้ชี้ให้เห็นถึงอนาคตที่เป็นไปได้สองประการ: หนึ่งซึ่งบุคคลหลายร้อยหรือหลายพันคนที่มีความสามารถทางเทคนิคขั้นพื้นฐานใช้เทมเพลตการโจมตีเพื่อดำเนินการในอนาคตที่ประสานกันหรือนักแฮ็กรายบุคคลโจมตีเป้าหมาย หรือสอง อนาคตที่การสิ้นสุดของสงครามในยูเครนในที่สุดเห็นว่าพวกเขาทิ้งการแฮ็กข้อมูลไว้เบื้องหลัง อย่างน้อยก็จนกว่าประเด็นทางการเมืองหรือสังคมครั้งต่อไปจะเป็นแรงบันดาลใจให้พวกเขาดำเนินการ

การเมืองของแฮกเกอร์

ความเสี่ยงที่มากขึ้นจากการเคลื่อนไหวทางการเมืองนี้คือการใช้แฮ็กเกอร์ที่เชี่ยวชาญด้านเทคโนโลยีซึ่งอาจดำเนินการโจมตีทางไซเบอร์ต่อเป้าหมายของรัฐบาลต่างประเทศเพื่อสนับสนุนลำดับความสำคัญของประเทศของตนเอง ไม่ว่าจะดำเนินการโดยตนเองหรือตามคำสั่งของรัฐบาล

อิหร่าน จีน และรัสเซียใช้การแฮ็กข้อมูลเป็นตัวป้อนสำหรับการรับสมัครเข้ากลุ่มแฮ็กข้อมูลของรัฐ ตัวอย่างเช่น ในเดือนเมษายน พ.ศ. 2022 กลุ่มแฮ็กเกอร์ชาวรัสเซียที่สนับสนุน Killnet ได้ทำการโจมตี DDoS กับทางรถไฟ สนามบิน ภูมิภาค และเซิร์ฟเวอร์ราชการของเช็ก แม้ว่าเช็กเกียจะไม่ได้เกี่ยวข้องโดยตรงกับสงครามก็ตาม[35] ในเวลาเดียวกัน รัฐบาลบางแห่งอาจใช้การแฮ็กข้อมูลเพื่อปกปิดปฏิบัติการจารกรรมทางไซเบอร์หรือการก่อวินาศกรรมแบบดั้งเดิม ตัวอย่างเช่น กิจกรรมของอิหร่านต่ออิสราเอล

ในสภาพแวดล้อมที่มีการโจมตี DDoS เพิ่มขึ้นซึ่งเชื่อมโยงกับการแฮ็กข้อมูล อุตสาหกรรมเทคโนโลยีถูกท้าทายให้ถอดรหัสความแตกต่างอย่างรวดเร็วระหว่างปริมาณการรับส่งข้อมูลปกติและผิดปกติไปยังเว็บไซต์ Microsoft และคู่ค้าได้พัฒนาชุดเครื่องมือที่แยกทราฟฟิก DDoS ที่เป็นอันตรายและติดตามกลับไปยังต้นทาง นอกจากนี้ แพลตฟอร์ม Azure ของ Microsoft สามารถระบุเครื่องบนแพลตฟอร์มที่สร้างการรับส่งข้อมูลขาออกในระดับสูงเป็นพิเศษและปิดเครื่องได้

การเกิดขึ้นของ Protestware

Protestware กลายเป็นผลโดยตรงจากปฏิกิริยาทางอารมณ์ต่อสงครามระหว่างรัสเซียและยูเครน นักพัฒนาซอฟต์แวร์โอเพ่นซอร์สบางรายใช้ความนิยมของซอฟต์แวร์ของตนเป็นช่องทางในการพูดหรือดำเนินการกับสถานการณ์ทางภูมิรัฐศาสตร์ที่กำลังเกิดขึ้น ซึ่งรวมถึงไฟล์ข้อความที่ไม่เป็นอันตรายที่เปิดบนเดสก์ท็อปหรือเบราว์เซอร์เพื่อเผยแพร่ข้อความแห่งสันติภาพ แต่ยังรวมถึงการโจมตีแบบกำหนดเป้าหมายตามตำแหน่งทางภูมิศาสตร์ของที่อยู่ IP และการกระทำที่ทำลายล้าง เช่น การล้างข้อมูลในฮาร์ดไดรฟ์ เมื่อเหตุการณ์ระดับโลกอื่นๆ คลี่คลาย เราคาดหวังได้ว่าจะได้เห็น Protoware ปรากฏขึ้นอีกในอนาคต เนื่องจากสิ่งเหล่านี้มักเป็นกรณีที่ผู้ดูแลโอเพ่นซอร์สที่ได้รับการยอมรับอย่างดีกำลังตัดสินใจสร้างข้อความส่วนตัวโดยใช้ส่วนประกอบโอเพ่นซอร์สของตนเอง ในปัจจุบันจึงไม่มีการป้องกันเพื่อหยุดการเปลี่ยนแปลงประเภทนี้ไม่ให้เกิดขึ้นในแพ็กเกจไฟล์ซอร์ส และผู้ใช้ควรดูแลรักษา ตระหนักถึงผลกระทบที่อาจเกิดขึ้น

แพลตฟอร์มโซเชียลมีเดียช่วยให้สามารถจัดระเบียบและระดมพลแฮ็กเกอร์มือสมัครเล่นหลายพันคนได้ ซึ่งได้รับคำแนะนำในการดำเนินการโจมตีที่สั่งการได้ง่าย เช่น การโจมตี DDoS

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. อุตสาหกรรมเทคโนโลยีต้องร่วมกันออกแบบการตอบสนองต่อภัยคุกคามใหม่นี้อย่างครอบคลุม
2. บริษัทเทคโนโลยีชั้นนำ รวมถึง Microsoft มีเครื่องมือในการระบุการรับส่งข้อมูลที่เป็นอันตรายที่เกี่ยวข้องกับการโจมตี DDoS และปิดใช้งานเครื่องที่รับผิดชอบ
3. ผู้ใช้โอเพ่นซอร์สควรจับตามองในช่วงเวลาที่เกิดความขัดแย้งทางภูมิรัฐศาสตร์

อ้างอิงท้ายเอกสาร

1. https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
2. https://www.bleepingcomputer.com/news/security/greeces-public-postal-service-offline-due-to-ransomware-attack/
3. https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive- ransomware/; https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/
4. https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/
5. https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
6. การตรวจจับและการตอบสนองอุปกรณ์ปลายทาง https://www.microsoft.com/en-us/security/business/threat-protection/
7. https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html
8. https://www.bbc.com/news/technology-59998925
9. ฟอรัม Vetted เป็นฟอรัมสนทนาออนไลน์ที่กำหนดให้สมาชิกปัจจุบันต้องรับรองการเพิ่มสมาชิกใหม่
10. https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/; https://www.blockchain.com/charts/my-wallet-n-users; https://coinmarketcap.com
11. https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/
12. https://www.coindesk.com/business/2021/12/13/crypto-exchange-ascendex-hacked-losses-estimated-at-77m/ ; https://www.zdnet.com/article/after-77-million-hack-crypto-platform-ascendex-to-reimburse-customers/
13. https://etherscan.io/address/0x73326b6764187b7176ed3c00109ddc1e6264eb8b
14. https://finance.yahoo.com/news/ethereum-worth-over-1-5m-160249300.html
15. https://news.bitcoin.com/decentralized-finance-crypto-exchange-uniswap-starts-blocking-addresses-linked-to-blocked-activities/
16. แหล่งข้อมูล: Defender for Office (อีเมลที่เป็นอันตราย/กิจกรรมข้อมูลประจำตัวที่ถูกบุกรุก), Azure Active Directory Identity Protection (เหตุการณ์/การแจ้งเตือนข้อมูลประจำตัวที่ถูกบุกรุก), Defender for Cloud Apps (เหตุการณ์การเข้าถึงข้อมูลข้อมูลประจำตัวที่ถูกบุกรุก) และ M365D (ความสัมพันธ์ระหว่างผลิตภัณฑ์)
17. แหล่งข้อมูล: Defender for Endpoint (การแจ้งเตือนพฤติกรรมการโจมตี/เหตุการณ์), Defender for Office (อีเมลอันตราย) และ M365D (ความสัมพันธ์ระหว่างผลิตภัณฑ์)
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. การตรวจสอบข้อความตามโดเมน การรายงาน และการปฏิบัติตามข้อกำหนด: การตรวจสอบสิทธิ์อีเมล นโยบาย และโปรโตคอลการรายงานที่ออกแบบมาเพื่อให้เจ้าของโดเมนอีเมลสามารถปกป้องโดเมนของตนจากการใช้งานโดยไม่ได้รับอนุญาต
20. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
21. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/learn-about-spoof-intelligence?view=o365-worldwide
22. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/impersonation-insight?view=o365-worldwide
23. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
24. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365
25. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
26. Microsoft Corporation v. John Does 1-27, et. al., No. 1:10CV156, (E.D.Va. 22 ก.พ. 2010)
27. ดูที่ Bowden, Mark. Worm: สงครามโลกดิจิทัลครั้งที่หนึ่ง Grove/Atlantic, Inc., 27 กันยายน 2011
28. โดยเฉพาะอย่างยิ่ง กฎข้อ 65 ของกฎกลางของกระบวนการทางแพ่งอนุญาตให้ฝ่ายหนึ่งฝ่ายใดร้องขอการเยียวยาดังกล่าวหาก: 1) ฝ่ายนั้นจะได้รับอันตรายในทันทีและไม่สามารถแก้ไขได้หากไม่ได้รับการบรรเทาทุกข์ และ 2) ฝ่ายพยายามที่จะแจ้งอีกฝ่ายหนึ่งให้ทราบอย่างทันท่วงที ยิ่งกว่านั้น กฎหมายกำหนดให้ใช้การทดสอบการทรงตัว ซึ่งเป็นการทดสอบที่สมดุลระหว่างสิทธิของจำเลยในการแจ้งให้ทราบกับความตื่นตัวของอันตรายต่อสาธารณะ
29. Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D. Wa. 9 ก.พ. 2011)
30. Microsoft Corp. v. Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. 12 ส.ค. 2021)
31. https://github.com/microsoft/routeros-scanner
32. RiskIQ: อุปกรณ์ Ubiquiti ถูกบุกรุกและใช้เป็นมัลแวร์ C2 Reverse Proxies | ฉบับชุมชน RiskIQ
33. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
34. https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/
35. https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks

ภัยคุกคามระดับชาติ

ผู้มีบทบาทในระดับชาติกำลังเปิดตัวการโจมตีทางไซเบอร์ที่ซับซ้อนมากขึ้นเพื่อหลบเลี่ยงการตรวจจับและเสริมลำดับความสำคัญเชิงกลยุทธ์ของพวกเขา

ภาพรวมของภัยคุกคามระดับชาติ 31
ข้อมูลเบื้องต้น 32
ความเป็นมาเกี่ยวกับข้อมูลรัฐชาติ 33
ตัวอย่างนักแสดงรัฐชาติและกิจกรรมของพวกเขา 34
วิวัฒนาการของภัยคุกคาม 35
ห่วงโซ่อุปทานไอทีเป็นประตูสู่ระบบนิเวศดิจิทัล 37
การแสวงหาประโยชน์จากช่องโหว่อย่างรวดเร็ว 39
กลยุทธ์ทางไซเบอร์ ในช่วงสงครามของผู้ดำเนินการของรัฐรัสเซียคุกคามยูเครนและที่อื่นๆ 41
จีนขยายการกำหนดเป้าหมายทั่วโลกเพื่อความได้เปรียบทางการแข่งขัน 44
อิหร่านก้าวร้าวมากขึ้นหลังจากการเปลี่ยนผ่านอำนาจ 46
ความสามารถทางไซเบอร์ของเกาหลีเหนือใช้เพื่อบรรลุเป้าหมายหลักสามประการของระบอบการปกครอง 49
ทหารรับจ้างไซเบอร์คุกคามความมั่นคงของไซเบอร์สเปซ 52
ดำเนินการตามบรรทัดฐานความปลอดภัยทางไซเบอร์เพื่อสันติภาพและความปลอดภัยในโลกไซเบอร์ 53

ภาพรวมของ

ภัยคุกคามระดับชาติ

ผู้มีบทบาทในระดับชาติกำลังเปิดตัวการโจมตีทางไซเบอร์ที่ซับซ้อนมากขึ้นเพื่อหลบเลี่ยงการตรวจจับและเสริมลำดับความสำคัญเชิงกลยุทธ์ของพวกเขา การกำเนิดของการติดตั้งอาวุธไซเบอร์ในสงครามลูกผสมในยูเครนเป็นจุดเริ่มต้นของความขัดแย้งยุคใหม่

รัสเซียยังสนับสนุนการทำสงครามกับการดำเนินการที่มีอิทธิพลต่อข้อมูล โดยใช้การโฆษณาชวนเชื่อเพื่อส่งผลกระทบต่อความคิดเห็นในรัสเซีย ในยูเครน และทั่วโลก ความขัดแย้งแบบผสมผสานอย่างเต็มรูปแบบครั้งแรกนี้ได้สอนบทเรียนสำคัญอื่นๆ ประการแรก ความปลอดภัยของการดำเนินการทางดิจิทัลและข้อมูลสามารถได้รับการปกป้องอย่างดีที่สุด ทั้งในโลกไซเบอร์และในพื้นที่ทางกายภาพ โดยการย้ายไปยังระบบคลาวด์ การโจมตีครั้งแรกของรัสเซียมุ่งเป้าบริการในสถานที่ด้วยมัลแวร์ไวเปอร์ และกำหนดเป้าหมายศูนย์ข้อมูลทางกายภาพด้วยหนึ่งในขีปนาวุธตัวแรกที่เปิดตัว ยูเครนตอบสนองด้วยการย้ายปริมาณงานและข้อมูลอย่างรวดเร็วไปยังคลาวด์แบบไฮเปอร์สเกลที่โฮสต์ในศูนย์ข้อมูลนอกยูเครน ประการที่สอง ความก้าวหน้าในด้านข่าวกรองภัยคุกคามทางไซเบอร์และการป้องกันปลายทางที่ขับเคลื่อนโดยข้อมูลและบริการ AI และ ML ขั้นสูงในระบบคลาวด์ได้ช่วยยูเครนป้องกันการโจมตีทางไซเบอร์ของรัสเซีย

นอกประเทศยูเครน ผู้มีบทบาทของรัฐชาติได้เพิ่มกิจกรรมและเริ่มใช้ความก้าวหน้าในระบบอัตโนมัติ โครงสร้างพื้นฐานระบบคลาวด์ และเทคโนโลยีการเข้าถึงระยะไกลเพื่อโจมตีเป้าหมายที่กว้างขึ้น ห่วงโซ่อุปทานด้านไอทีขององค์กรที่เปิดใช้งานการเข้าถึงเป้าหมายสูงสุดมักถูกโจมตี สุดอนามัยของความปลอดภัยทางไซเบอร์กลายเป็นเรื่องที่สำคัญยิ่งขึ้นไปอีกเนื่องจากนักแสดงใช้ประโยชน์จากช่องโหว่ที่ยังไม่ได้แพตช์อย่างรวดเร็ว ใช้ทั้งเทคนิคที่ซับซ้อนและรุนแรงเพื่อขโมยข้อมูลประจำตัว และทำให้การทำงานของพวกเขายุ่งเหยิงโดยใช้โอเพ่นซอร์สหรือซอฟต์แวร์ที่ถูกกฎหมาย และอิหร่านยังเข้าร่วมกับรัสเซียในการใช้อาวุธทำลายล้างทางไซเบอร์ ซึ่งรวมถึงแรนซัมแวร์ เป็นหลักในการโจมตี

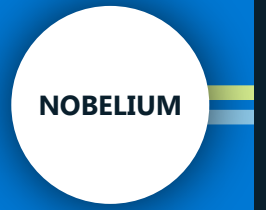
การพัฒนาเหล่านี้จำเป็นต้องอาศัยกรอบระดับโลกที่สอดคล้องกันอย่างเร่งด่วน ซึ่งให้ความสำคัญกับสิทธิมนุษยชนและปกป้องผู้คนจากพฤติกรรมของรัฐที่ประมาทในโลกออนไลน์ ทุกประเทศต้องทำงานร่วมกันเพื่อใช้บรรทัดฐานและกฎที่ตกลงกันไว้สำหรับการปฏิบัติที่รับผิดชอบของรัฐ

› การปกป้องยูเครน: บทเรียนแรกจากสงครามไซเบอร์ — Microsoft On the Issues

เพิ่มการกำหนดเป้าหมายของโครงสร้างพื้นฐานที่สำคัญ โดยเฉพาะภาคไอที บริการทางการเงิน ระบบขนส่ง และโครงสร้างพื้นฐานด้านการสื่อสาร

› ค้นหาข้อมูลเพิ่มเติมหน้า 35

ห่วงโซ่อุปทานไอทีถูกใช้เป็นเกตเวย์ในการเข้าถึงเป้าหมาย



› ค้นหาข้อมูลเพิ่มเติมหน้า 36

ประเทศจีนขยายการกำหนดเป้าหมายทั่วโลกโดยเฉพาะประเทศเล็กๆ ในเอเชียตะวันออกเฉียงใต้ เพื่อรับข่าวกรองและความได้เปรียบในการแข่งขัน



› ค้นหาข้อมูลเพิ่มเติมหน้า 44

อิหร่านเริ่มก้าวร้าวมากขึ้นหลังจากการเปลี่ยนผ่านอำนาจ การโจมตีด้วยแรนซัมแวร์ที่ขยายวงกว้างออกไปนอกเหนือศัตรูระดับภูมิภาคไปจนถึงเหยื่อของสหรัฐฯ และสหภาพยุโรป และพุ่งเป้าไปที่โครงสร้างพื้นฐานที่สำคัญที่สำคัญของสหรัฐฯ

› ค้นหาข้อมูลเพิ่มเติมหน้า 46

การระบุและการใช้ประโยชน์จากช่องโหว่ที่ไม่ได้แพตช์อย่างรวดเร็วกลายเป็นกลยุทธ์หลัก การปรับใช้การอัปเดตความปลอดภัยอย่างรวดเร็วเป็นกุญแจสำคัญในการป้องกัน



› ค้นหาข้อมูลเพิ่มเติมหน้า 39

เกาหลีเหนือกำหนดเป้าหมายบริษัทด้านการป้องกันและการบินและอวกาศ สกุลเงินดิจิทัล สำนักข่าว ผู้แปรพักตร์ และองค์กรช่วยเหลือ เพื่อให้บรรลุเป้าหมายของรัฐบาล: เพื่อสร้างการป้องกัน หนุนเศรษฐกิจ และประกันเสถียรภาพภายในประเทศ

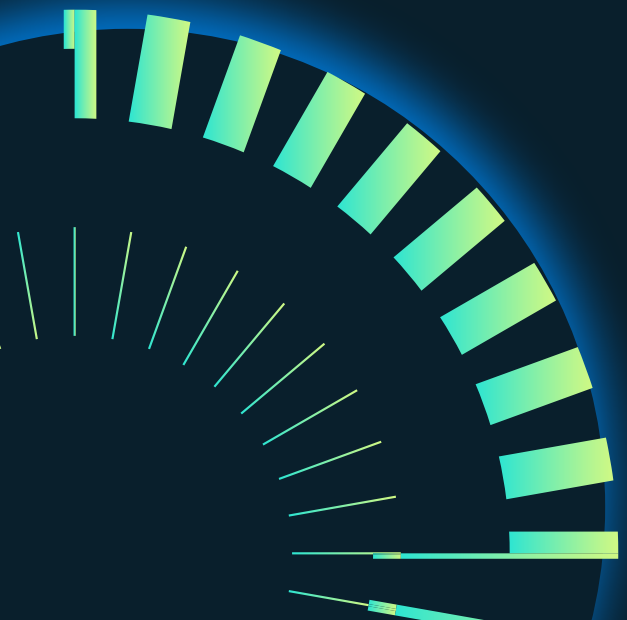
› ค้นหาข้อมูลเพิ่มเติมหน้า 49

ทหารรับจ้างไซเบอร์คุกคามความเสถียรของโลกไซเบอร์เนื่องจากอุตสาหกรรมที่กำลังเติบโตของบริษัทเอกชนกำลังพัฒนาและขายเครื่องมือ เทคนิค และบริการขั้นสูงเพื่อให้ลูกค้าของพวกเขา (มักเป็นรัฐบาล) สามารถเจาะเข้าไปในเครือข่ายและอุปกรณ์ได้

› ค้นหาข้อมูลเพิ่มเติมหน้า 52

ข้อมูลเบื้องต้น

หลังจากการโจมตีที่มีรายละเอียดสูงในปี 2020 และ 2021 ผู้คุกคามระดับประเทศได้ใช้ทรัพยากรจำนวนมากในการปรับให้เข้ากับการป้องกันความปลอดภัยแบบใหม่ที่นำมาใช้โดยองค์กรต่างๆ เพื่อป้องกันภัยคุกคามที่ซับซ้อน



เช่นเดียวกับองค์กรระดับองค์กร ฝ่ายตรงข้ามเริ่มใช้ความก้าวหน้าในระบบอัตโนมัติ โครงสร้างพื้นฐานระบบคลาวด์ และเทคโนโลยีการเข้าถึงระยะไกลเพื่อขยายการโจมตีไปยังเป้าหมายที่กว้างขึ้น การปรับยุทธวิธีเหล่านี้ส่งผลให้เกิดแนวทางใหม่และการโจมตีขนาดใหญ่ต่อห่วงโซ่อุปทานขององค์กร สุขอนามัยด้านความปลอดภัยด้านไอทีมีความสำคัญในระดับที่สูงขึ้น เนื่องจากผู้ดำเนินการได้พัฒนาวิธีการใหม่ๆ เพื่อใช้ประโยชน์จากช่องโหว่ที่ไม่ได้รับการแพตช์อย่างรวดเร็ว ขยายเทคนิคสำหรับการประนีประนอมกับเครือข่ายขององค์กร และทำให้การดำเนินงานของพวกเขายุ่งเหยิงโดยใช้โอเพ่นซอร์สหรือซอฟต์แวร์ที่ถูกกฎหมาย เทคนิคการโจมตีใหม่ให้เวกเตอร์ใหม่และยากต่อการตรวจจับเพื่อเข้าถึงเครือข่ายของเป้าหมาย ในที่สุด เมื่อการโจมตีทางกายภาพในช่วงสงครามทวีความรุนแรงขึ้น เราเห็นว่าการโจมตีทางไซเบอร์มีบทบาทสำคัญในกิจกรรมทางทหาร

ความขัดแย้งในยูเครนได้ให้ตัวอย่างที่รุนแรงเกินไปของการโจมตีทางไซเบอร์ที่มีวิวัฒนาการจนส่งผลกระทบต่อโลกควบคู่ไปกับความขัดแย้งทางทหารบนพื้นดิน ระบบไฟฟ้า ระบบโทรคมนาคม สื่อ และโครงสร้างพื้นฐานที่สำคัญอื่นๆ ล้วนตกเป็นเป้าหมายของการโจมตีทางกายภาพและการโจมตีทางไซเบอร์ ความพยายามในการประนีประนอมเครือข่ายที่สังเกตได้ทั่วไปว่าเป็นส่วนหนึ่งของแคมเปญการจารกรรมและการกรองข้อมูลกลายเป็นจุดสนใจในสงครามแบบผสมผสานกับการโจมตีมัลแวร์ไวเปอร์แบบทำลายล้างต่อระบบโครงสร้างพื้นฐานที่สำคัญ การเชื่อมต่อความปลอดภัยของระบบเหล่านี้กับคลาวด์ส่งผลให้ตรวจพบได้ตั้งแต่เนิ่นๆ และขัดขวางการโจมตีที่อาจทำลายล้างได้[1]

นับเป็นครั้งแรกในเหตุการณ์ทางไซเบอร์ที่สำคัญ การตรวจจับพฤติกรรมโดยใช้การเรียนรู้ของเครื่องใช้รูปแบบการโจมตีที่รู้จักเพื่อระบุและหยุดการโจมตีเพิ่มเติมได้สำเร็จโดยไม่ต้องมีความรู้ล่วงหน้าเกี่ยวกับมัลแวร์ที่ซ่อนอยู่ แม้กระทั่งก่อนที่มนุษย์จะรู้ตัวถึงภัยคุกคามดังกล่าว นอกจากนี้ เรายังยืนยันถึงคุณค่าของการแบ่งปันข่าวกรองภัยคุกคามแบบเรียลไทม์กับผู้ปกป้องที่ปกป้องระบบเหล่านี้ โดยให้ข้อมูลที่สำคัญแก่พวกเขาเพื่อคาดการณ์และป้องกันการโจมตีที่ดำเนินอยู่

ผู้คุกคามรัฐชาติทั่วโลกยังคงขยายการดำเนินงานในรูปแบบใหม่และเก่า จีน เกาหลีเหนือ อิหร่าน และรัสเซียล้วนทำการโจมตีลูกค้าของ Microsoft ห่วงโซ่อุปทานบริการด้านไอทีกลายเป็นเป้าหมายร่วมกันเนื่องจากนักแสดงเปลี่ยนโฟกัสไปที่บริการอัปสตรีมที่สามารถเป็นจุดเชื่อมต่อไปยังหลายองค์กร เราคาดหวังให้ผู้ให้บริการยังคงใช้ประโยชน์จากความสัมพันธ์ที่เชื่อถือได้ในห่วงโซ่อุปทานขององค์กร โดยเน้นย้ำถึงความสำคัญของการบังคับใช้กฎการตรวจสอบสิทธิ์อย่างครอบคลุม การแพตช์อย่างขยันขันแข็ง และการกำหนดค่าบัญชีสำหรับโครงสร้างพื้นฐานการเข้าถึงระยะไกล และการตรวจสอบความสัมพันธ์ของคู่ค้าบ่อยครั้งเพื่อยืนยันความถูกต้อง

ผู้มีบทบาทระดับประเทศ เช่น แรนซัมแวร์และอาชญากรได้ตอบสนองต่อการเปิดเผยที่เพิ่มขึ้นโดยมุ่งไปที่การกำหนดเป้าหมายระบบองค์กรที่มีการกำหนดค่าไม่ดีหรือไม่ได้แพตช์ (โครงสร้างพื้นฐาน VPN/VPS เซิร์ฟเวอร์ในสถานที่ ซอฟต์แวร์ของบุคคลที่สาม) เพื่อใช้ชีวิตนอกสถานที่ การโจมตีทางบก หลายคนใช้มัลแวร์สินค้าโภคภัณฑ์และเครื่องมือ Red Team แบบโอเพ่นซอร์สเพิ่มขึ้นเพื่อทำให้กิจกรรมที่เป็นอันตรายของพวกเขายุ่งเหยิง

ผลที่ตามมาคือ การรักษามาตรฐานความปลอดภัยด้านไอทีที่แข็งแกร่งผ่านการแพตช์ที่จัดลำดับความสำคัญ การเปิดใช้งานคุณสมบัติต่อต้านการงัดแงะ การใช้เครื่องมือการจัดการพื้นผิวการโจมตี เช่น RiskIQ เพื่อรับมุมมองภายนอกของพื้นผิวการโจมตี และการเปิดใช้งานการพิสูจน์ตัวตนแบบหลายปัจจัยทั่วทั้งองค์กรเต็มรูปแบบได้ กลายเป็นพื้นฐานพื้นฐานเพื่อป้องกันในเชิงรุกจากนักแสดงที่มีความซับซ้อนมากมาย

ผู้มีบทบาทในระดับประเทศยังได้เพิ่มการใช้แรนซัมแวร์เป็นกลวิธีในการโจมตี โดยมักจะใช้มัลแวร์เรียกค่าไถ่ที่สร้างโดยระบบนิเวศของอาชญากรนั้นซ้ำในการโจมตี เราได้เห็นทั้งนักแสดงที่มีฐานอยู่ในอิหร่านและเกาหลีเหนือใช้เครื่องมือแรนซัมแวร์สินค้าโภคภัณฑ์เพื่อสร้างความเสียหายให้กับระบบเป้าหมาย ซึ่งมักจะรวมถึงโครงสร้างพื้นฐานที่สำคัญภายในคู่แข่งระดับภูมิภาค ในที่สุด เราได้เห็นภัยคุกคามที่เพิ่มขึ้นของทหารรับจ้างในโลกไซเบอร์ที่พัฒนาและขายเครื่องมือ เทคนิค และบริการต่างๆ เพื่อขยายขอบเขตการหาประโยชน์จากโซลูชันของบุคคลที่สามที่มีช่องโหว่ ความซับซ้อนและความว่องไวของการโจมตีโดยผู้มีบทบาทในระดับประเทศจะยังคงพัฒนาต่อไปในแต่ละปี องค์กรต้องตอบสนองด้วยการได้รับแจ้งถึงการเปลี่ยนแปลงตัวแสดงเหล่านี้ และพัฒนาการป้องกันควบคู่กันไป

John Lambert
รองประธานองค์กรและวิศวกรทรงคุณวุฒิ ศูนย์ข่าวกรองภัยคุกคามของ Microsoft

ความเป็นมาเกี่ยวกับข้อมูลรัฐชาติ

ภัยคุกคามของรัฐชาติคือกิจกรรมภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในประเทศใดประเทศหนึ่ง โดยมีเจตนาที่ชัดเจนในการส่งเสริมผลประโยชน์ของชาติ ผู้มีส่วนได้ส่วนเสียของรัฐชาตินำเสนอภัยคุกคามขั้นสูงและถาวรที่ลูกค้าของเราเผชิญ รวมถึงการโจรกรรมทรัพย์สินทางปัญญา การจารกรรม การสอดแนม การโจรกรรมข้อมูลประจำตัว การโจมตีแบบทำลายล้าง และอื่นๆ

เราลงทุนทรัพยากรจำนวนมากในการค้นหา ทำความเข้าใจ และต่อต้านภัยคุกคามเหล่านี้ เมื่อองค์กรหรือเจ้าของบัญชีรายบุคคลตกเป็นเป้าหมายหรือถูกโจมตีโดยกิจกรรมของรัฐชาติที่สังเกตการณ์ Microsoft จะส่งการแจ้งเตือนในรูปแบบของการแจ้งเตือนสถานะประเทศ (NSN) โดยตรงไปยังลูกค้า รวมถึงข้อมูลที่จำเป็นในการตรวจสอบกิจกรรม ในเดือนมิถุนายน 2022 เราได้ส่งมอบ NSN ไปแล้วกว่า 67,000 รายการนับตั้งแต่เริ่มดำเนินการในปี 2018

ข้อมูลการแจ้งเตือน Microsoft NSN แสดงในบทนี้ เพื่อให้มุมมองของกิจกรรมที่วัดได้ ระดับของกิจกรรมของรัฐชาติที่แสดงในแผนภูมิจะขึ้นอยู่กับจำนวนของ NSN ที่ Microsoft ออกให้แก่ลูกค้าเพื่อตอบสนองต่อการตรวจจับผู้กระทำของรัฐชาติที่กำหนดเป้าหมายหรือประนีประนอมกับบัญชีอย่างน้อยหนึ่งบัญชีในองค์กรของลูกค้า

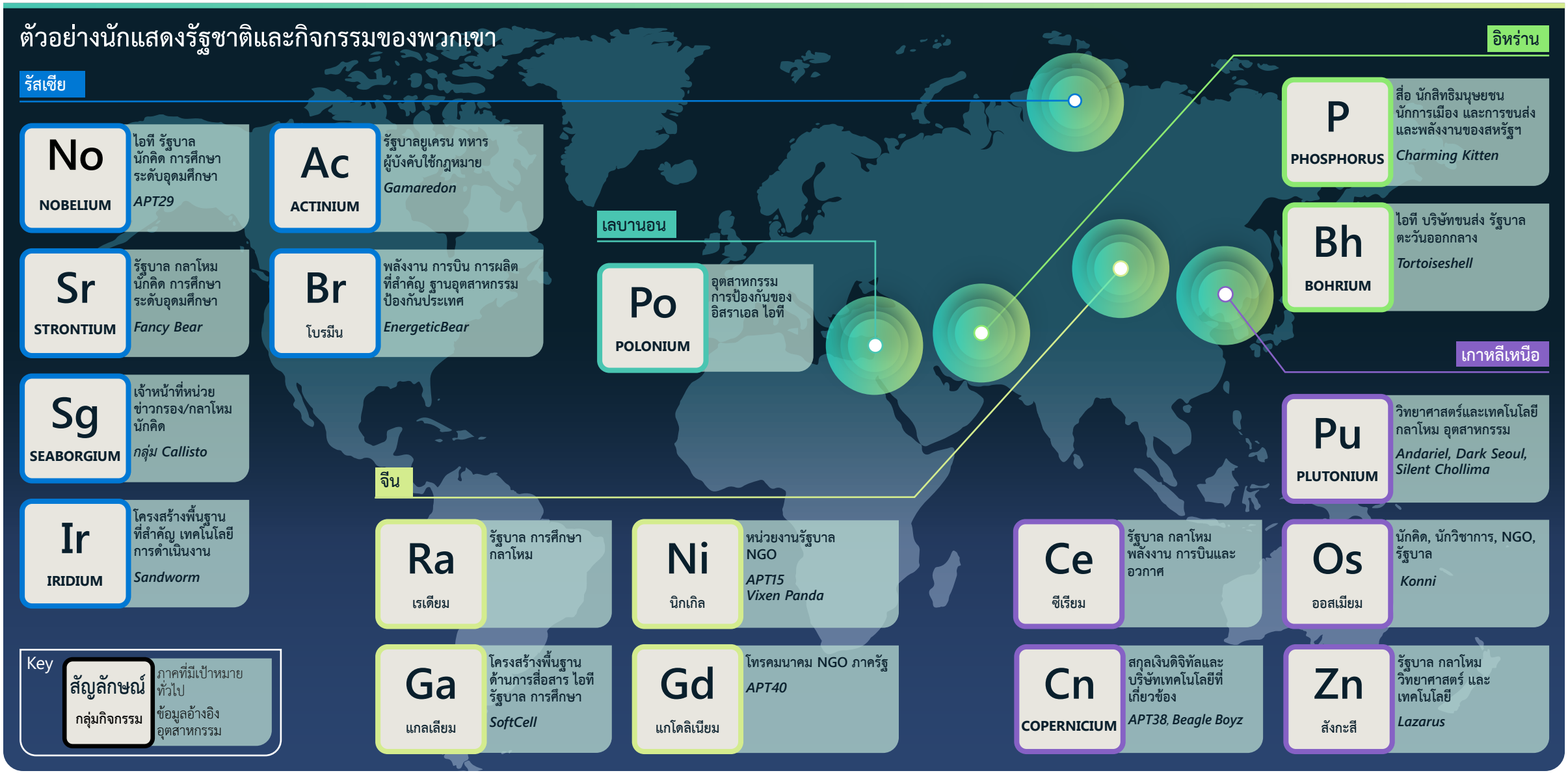


สี่ประเทศหลักที่เรารวมกลุ่มภัยคุกคามไว้ในรายงานฉบับนี้ ได้แก่ รัสเซีย จีน อิหร่าน และเกาหลีเหนือ สิ่งเหล่านี้แสดงถึงประเทศต้นทางสำหรับนักแสดงที่สังเกตได้บ่อยที่สุดที่กำหนดเป้าหมายเป็นลูกค้าของ Microsoft ในช่วงปีที่ผ่านมา รายงานยังรวมข้อสังเกตของเราเกี่ยวกับกลุ่มภัยคุกคามจากเลบานอนและจากทหารรับจ้างทางไซเบอร์ หรือจ้างผู้โจมตีภาคเอกชน

Microsoft ระบุกลุ่มรัฐชาติตามชื่อองค์ประกอบทางเคมี (เช่น NOBELIUM) ซึ่งจะแสดงเพียงบางส่วนในหน้าต่อไปนี้ เราใช้ชื่อ DEV-#### เป็นชื่อชั่วคราวที่กำหนดให้กับกลุ่มกิจกรรมการคุกคามที่ไม่รู้จัก เกิดขึ้นใหม่ หรือกำลังพัฒนา ทำให้เราสามารถติดตามมันเป็นชุดข้อมูลเฉพาะจนกว่าเราจะมั่นใจระดับสูงเกี่ยวกับที่มาหรือ ตัวตนของผู้มีบทบาทที่อยู่เบื้องหลังกิจกรรม

เมื่อเป็นไปตามเกณฑ์แล้ว DEV จะถูกแปลงเป็นนักแสดงที่มีชื่อหรือรวมเข้ากับนักแสดงที่มีอยู่ ตลอดบทนี้ เรายกตัวอย่างของรัฐชาติและกลุ่ม DEV เพื่อให้มุมมองเชิงลึกเกี่ยวกับเป้าหมายการโจมตี เทคนิค และการวิเคราะห์แรงจูงใจ แม้ว่ากลุ่มเหล่านี้หลายกลุ่มจะใช้เครื่องมือเดียวกันกับอาชญากรไซเบอร์ แต่พวกเขาก็นำเสนอภัยคุกคามเฉพาะในรูปแบบของมัลแวร์ ความสามารถในการค้นพบและใช้ประโยชน์จากช่องโหว่ซีโร่เดย์ และการไม่ต้องรับโทษทางกฎหมาย

ตัวอย่างนักแสดงรัฐชาติและกิจกรรมของพวกเขา



วิวัฒนาการของภัยคุกคาม

ภารกิจของ Microsoft ในการติดตามกิจกรรมของผู้มีบทบาทในระดับชาติและแจ้งให้ลูกค้าทราบเมื่อเราเห็นว่าพวกเขาตกเป็นเป้าหมายหรือถูกบุกรุกนั้นมีรากฐานมาจากภารกิจของเราในการปกป้องลูกค้าจากการถูกโจมตี

การแจ้งเตือนนี้เป็นส่วนสำคัญของความมุ่งมั่นของเราในการแจ้งให้ลูกค้าทราบว่าการโจมตีที่สังเกตพบนั้นป้องกันได้สำเร็จด้วยการป้องกันผลิตภัณฑ์รักษาความปลอดภัยของเรา หรือหากการโจมตีนั้นได้ผลเนื่องจากจุดอ่อนด้านความปลอดภัยที่ไม่รู้จัก การติดตามการแจ้งเตือนในช่วงเวลาหนึ่งช่วยให้ Microsoft ระบุแนวโน้มภัยคุกคามที่เปลี่ยนแปลงโดยผู้ดำเนินการ และมุ่งเน้นที่การป้องกันผลิตภัณฑ์ในการบรรเทาภัยคุกคามเชิงรุกต่อลูกค้าทั่วทั้งบริการคลาวด์ของเรา

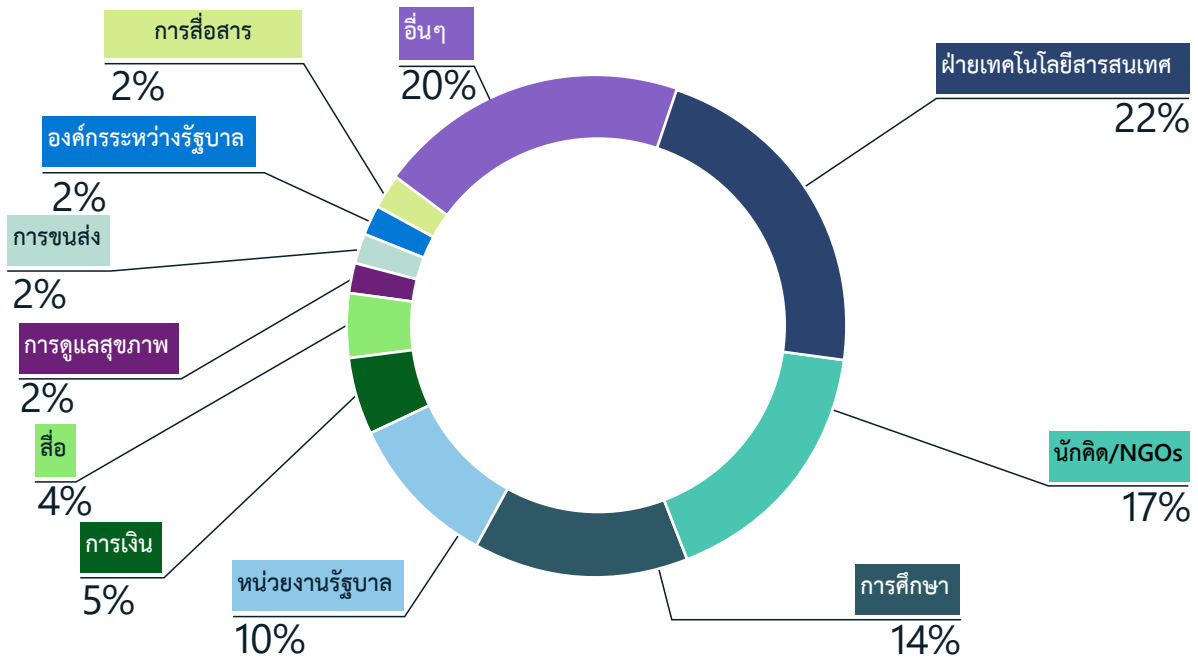
การติดตามนี้ยังช่วยให้เราแบ่งปันข้อมูลและข้อมูลเชิงลึกเกี่ยวกับสิ่งที่เราเห็น นักวิเคราะห์ที่ติดตามตัวแสดงเหล่านี้และติดตามการโจมตีของพวกเขาอาศัยการผสมผสานระหว่างตัวบ่งชี้ทางเทคนิคและความเชี่ยวชาญด้านภูมิรัฐศาสตร์เพื่อทำความเข้าใจแรงจูงใจของตัวแสดง โดยผสมผสานบริบททางเทคนิคและระดับโลกเข้ากับข้อมูลเชิงลึกใหม่ การดูแลจัดการนี้ให้มุมมองที่ไม่เหมือนใครเกี่ยวกับลำดับความสำคัญของผู้มีบทบาททางไซเบอร์ของรัฐชาติ และดูว่าแรงจูงใจของพวกเขาอาจสะท้อนถึงลำดับความสำคัญทางการเมือง การทหาร และเศรษฐกิจของรัฐชาติที่จ้างพวกเขาได้อย่างไร

การพัฒนาการทางการเมืองในปีที่ผ่านมาได้กำหนดลำดับความสำคัญและการยอมรับความเสี่ยงของกลุ่มภัยคุกคามที่ได้รับการสนับสนุนจากรัฐทั่วโลก เนื่องจากความสัมพันธ์ทางภูมิรัฐศาสตร์ได้พังทลายลงและองค์ประกอบที่สายเหยี่ยวได้รับการควบคุมมากขึ้นในบางประเทศ ผู้ดำเนินการทางไซเบอร์จึงกลายเป็นคนหน้าด้านและก้าวร้าวมากขึ้น ตัวอย่างเช่น:

- รัสเซียกำหนดเป้าหมายรัฐบาลยูเครนและโครงสร้างพื้นฐานที่สำคัญของประเทศอย่างไม่ลดละเพื่อเสริมปฏิบัติการทางทหารภาคพื้นดิน[2]
- อิหร่านพยายามรุกล้ำเข้าไปในโครงสร้างพื้นฐานที่สำคัญของสหรัฐฯ เช่น เจ้าหน้าที่ท่าเรือ
- เกาหลีเหนือยังคงรณรงค์ขโมยสกุลเงินดิจิทัลจากบริษัทการเงินและเทคโนโลยี
- จีนขยายปฏิบัติการจารกรรมทางไซเบอร์ทั่วโลก

แม้ว่าผู้ดำเนินการในระดับชาติจะมีความซับซ้อนทางเทคนิคและใช้กลวิธีที่หลากหลาย แต่การโจมตีของพวกเขามักสามารถบรรเทาได้ด้วยการรักษาสุขอนามัยทางไซเบอร์ที่ดี ผู้มีบทบาทเหล่านี้จำนวนมากอาศัยวิธีการที่ค่อนข้างใช้เทคโนโลยีต่ำ เช่น อีเมลสเปียร์ฟิชชิ่ง เพื่อส่งมัลแวร์ที่ซับซ้อน แทนที่จะลงทุนในการพัฒนาการหาประโยชน์ที่ปรับแต่งเองหรือใช้วิศวกรรมสังคมที่กำหนดเป้าหมายเพื่อให้บรรลุวัตถุประสงค์

ภาคอุตสาหกรรมที่ตกเป็นเป้าหมายของผู้มีบทบาทในระดับชาติ



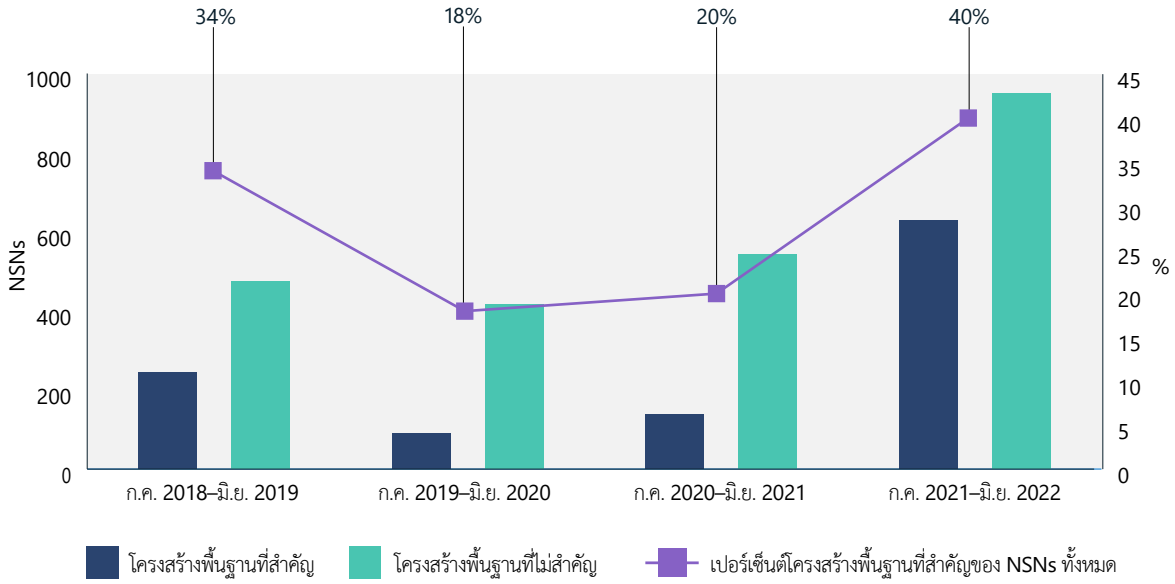
กลุ่มรัฐชาติมุ่งเป้าไปที่ภาคส่วนต่างๆ ผู้มีบทบาทของรัฐรัสเซียและอิหร่านกำหนดเป้าหมายอุตสาหกรรมไอทีเพื่อเข้าถึงลูกค้าของบริษัทไอที นักคิด องค์กรพัฒนาเอกชน (NGOs) มหาวิทยาลัย และหน่วยงานของรัฐยังคงเป็นเป้าหมายร่วมกันอื่นๆ ของผู้มีบทบาทในระดับชาติ

ผู้ดำเนินการในระดับชาติมีวัตถุประสงค์ที่หลากหลาย ซึ่งอาจส่งผลให้มีการกำหนดเป้าหมายเฉพาะกลุ่มขององค์กรหรือบุคคล ในปีที่ผ่านมา การโจมตีในห่วงโซ่อุปทานได้เพิ่มขึ้น โดยเน้นไปที่บริษัทไอทีโดยเฉพาะโดยการประนีประนอมกับผู้ให้บริการด้านไอที ผู้ก่อภัยคุกคามมักจะสามารถเข้าถึงเป้าหมายดั้งเดิมของพวกเขาได้ผ่านความสัมพันธ์ที่เชื่อถือได้กับบริษัทที่จัดการระบบที่เชื่อมต่อ หรืออาจดำเนินการโจมตีในระดับที่ใหญ่กว่ามากโดยประนีประนอมลูกค้าปลายน้ำหลายร้อยรายในการโจมตีครั้งเดียว รองจากภาคไอที หน่วยงานที่ตกเป็นเป้าหมายบ่อยที่สุดคือคลังความคิด นักวิชาการที่สังกัดมหาวิทยาลัย และเจ้าหน้าที่รัฐ สิ่งเหล่านี้เป็น “เป้าหมายที่อ่อนแอ” ที่น่าพึงประสงค์สำหรับการจารกรรมเพื่อรวบรวมข้อมูลข่าวกรองเกี่ยวกับประเด็นทางภูมิรัฐศาสตร์

วิวัฒนาการของภัยคุกคาม

ต่อไป

แนวโน้มโครงสร้างพื้นฐานที่สำคัญ

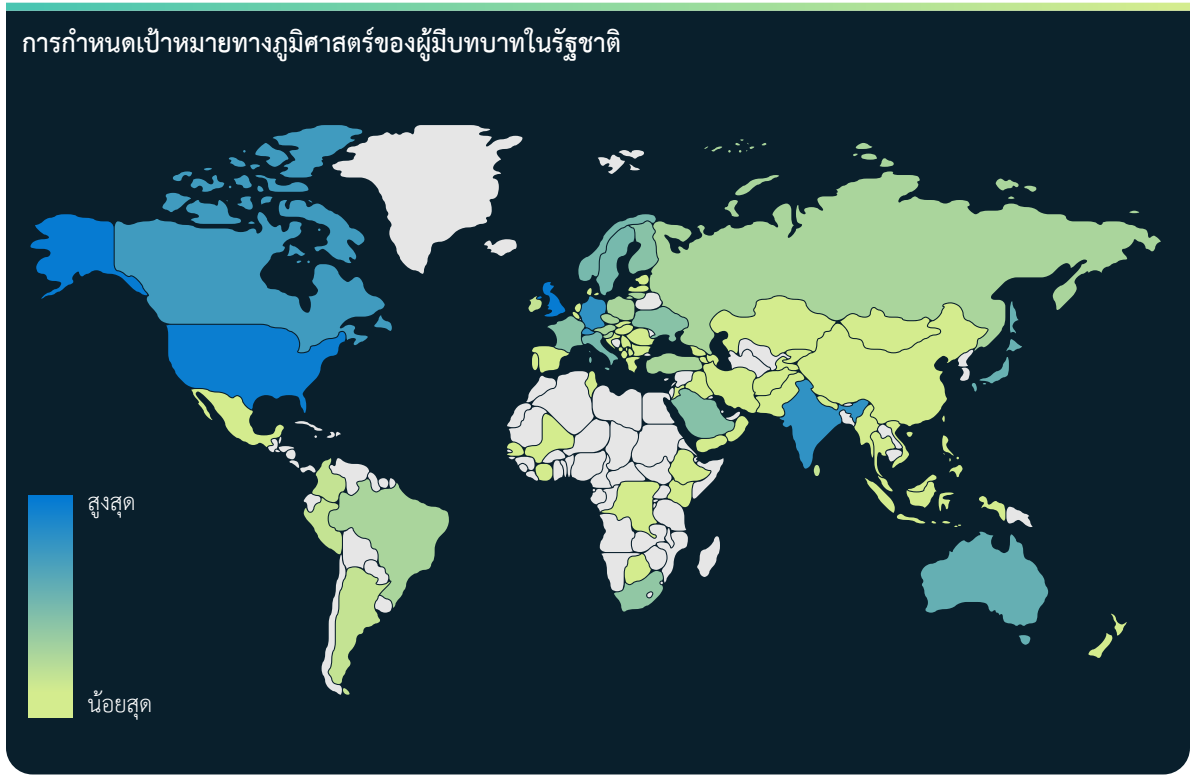


การกำหนดเป้าหมายโครงสร้างพื้นฐานที่สำคัญของกลุ่มประเทศของรัฐ[3] เพิ่มขึ้นในปีที่ผ่านมา โดยผู้มีบทบาทมุ่งเน้นไปที่บริษัทในภาคไอที บริการทางการเงิน ระบบขนส่ง และโครงสร้างพื้นฐานด้านการสื่อสาร

“ก่อนการรุกรานของยูเครน รัฐบาลต่างๆ คิดว่าข้อมูลจำเป็นต้องอยู่ภายในประเทศเพื่อความปลอดภัย หลังจากการบุกรุก การย้ายข้อมูลไปยังระบบคลาวด์และการย้ายออกนอกพรมแดนเป็นส่วนหนึ่งของการวางแผนความยืดหยุ่นและการกำกับดูแลที่ดี”

Cristin Flynn Goodwin,
รองที่ปรึกษาทั่วไป ความปลอดภัยและความน่าเชื่อถือของลูกค้า

การกำหนดเป้าหมายทางภูมิศาสตร์ของผู้มีบทบาทในรัฐชาติ



การกำหนดเป้าหมายทางไซเบอร์ของกลุ่มรัฐชาติแผ่ขยายไปทั่วโลก ในปีที่ผ่านมา โดยเน้นหนักไปที่องค์กรของสหรัฐฯ และอังกฤษ องค์กรในอิสราเอล, สหรัฐอาหรับเอมิเรตส์, แคนาดา, เยอรมนี, อินเดีย, สวิตเซอร์แลนด์ และญี่ปุ่น ก็เป็นหนึ่งในองค์กรที่ตกเป็นเป้าหมายบ่อยที่สุดเช่นกัน ตามข้อมูล NSN ของเรา

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ระบุและปกป้องเป้าหมายข้อมูลที่มีมูลค่าสูง เทคโนโลยีที่มีความเสี่ยง ข้อมูล และการดำเนินธุรกิจซึ่งอาจสอดคล้องกับลำดับความสำคัญเชิงกลยุทธ์ของกลุ่มรัฐชาติ
2. เปิดใช้งานการป้องกันบนระบบคลาวด์เพื่อระบุและบรรเทาภัยคุกคามที่รู้จักและแปลกใหม่ต่อเครือข่ายของคุณตามขนาด

ห่วงโซ่อุปทานไอทีเป็นประตูสู่ระบบนิเวศดิจิทัล

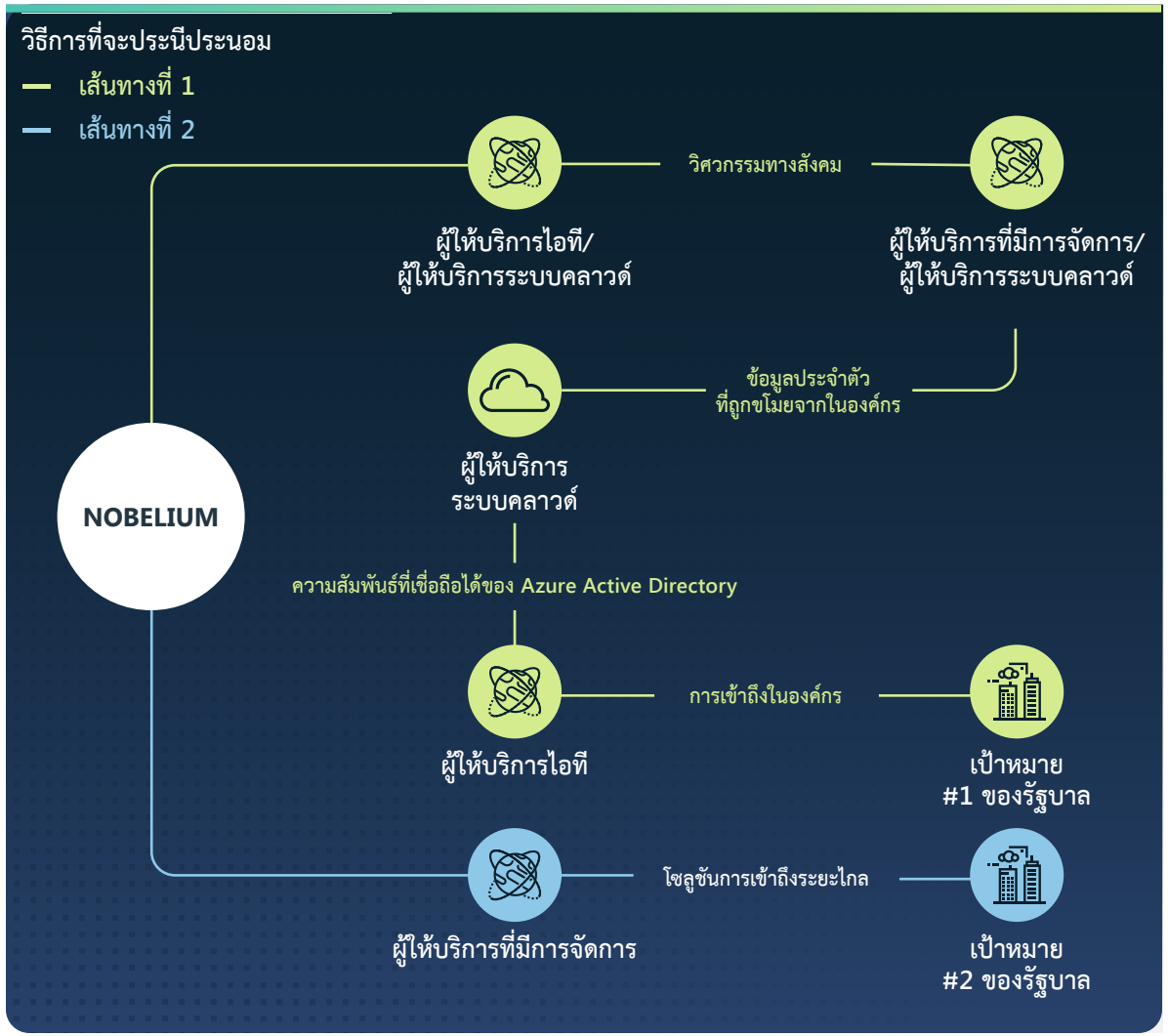
การกำหนดเป้าหมายผู้ให้บริการด้านไอทีในระดับประเทศอาจทำให้ผู้คุกคามสามารถใช้ประโยชน์จากองค์กรอื่นๆ ที่น่าสนใจได้โดยการใช้ประโยชน์จากความไว้วางใจและการเข้าถึงที่มอบให้กับผู้ให้บริการซัพพลายเชนเหล่านี้ ในปีที่ผ่านมา กลุ่มภัยคุกคามทางไซเบอร์ในระดับประเทศกำหนดเป้าหมายผู้ให้บริการด้านไอทีเพื่อโจมตีเป้าหมายบุคคลที่สามและเข้าถึงลูกค้าปลายน้ำในภาครัฐบาล นโยบาย และโครงสร้างพื้นฐานที่สำคัญ

ผู้ให้บริการด้านไอทีเป็นเป้าหมายตัวกลางที่น่าสนใจ เนื่องจากพวกเขาให้บริการลูกค้าทางตรงและทางอ้อมหลายร้อยรายที่สนใจบริการข่าวกรองต่างประเทศ หากมีการใช้ประโยชน์ การดำเนินธุรกิจตามปกติและสิทธิ์ในการดูแลระบบที่ได้รับมอบอำนาจจากบริษัทเหล่านี้อาจเปิดโอกาสให้ผู้ไม่ประสงค์ดีเข้าถึงและควบคุมเครือข่ายไคลเอ็นต์ของผู้ให้บริการไอทีโดยไม่ส่งการแจ้งเตือนทันที

ในปีที่ผ่านมา NOBELIUM พยายามที่จะประนีประนอมและใช้ประโยชน์จากบัญชีที่มีสิทธิพิเศษในโซลูชันระบบคลาวด์และผู้ให้บริการที่มีการจัดการอื่นๆ เพื่อพยายามเข้าถึงดาวน์สตรีมแบบกำหนดเป้าหมายไปยังรัฐบาลและลูกค้าตามนโยบายของสหรัฐฯ และยุโรปเป็นหลัก

NOBELIUM แสดงให้เห็นว่าวิธีการ “ประนีประนอมหนึ่งเพื่อประนีประนอมหลายคน” สามารถชี้นำต่อศัตรูทางภูมิรัฐศาสตร์ที่รับรู้ได้ ในปีที่ผ่านมา ผู้ก่อภัยคุกคามได้ติดตามทั้งบุคคลที่สามและการบุกรุกโดยตรงไปยังองค์กรที่ละเอียดอ่อนซึ่งมีฐานอยู่ในรัฐสมาชิกขององค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (NATO) ซึ่งรัฐบาลรัสเซียมองว่าเป็นภัยคุกคามที่มีอยู่จริง ระหว่างเดือนกรกฎาคม 2021 ถึงต้นเดือนมิถุนายน 2022 การแจ้งเตือนลูกค้าของ Microsoft ถึง 48 เปอร์เซ็นต์เกี่ยวกับกิจกรรมการคุกคามของรัสเซียต่อลูกค้าบริการออนไลน์ส่งไปยังบริษัทภาคส่วนไอทีที่ตั้งอยู่ในประเทศสมาชิก NATO ซึ่งน่าจะเป็นจุดเชื่อมต่อสื่อกลาง โดยรวมแล้ว 90 เปอร์เซ็นต์ของการแจ้งเตือนเกี่ยวกับกิจกรรมการคุกคามของรัสเซียในช่วงเวลาเดียวกันนั้นส่งไปยังลูกค้าที่อยู่ในประเทศสมาชิกของ NATO โดยหลักแล้วอยู่ในกลุ่มไอที คลังความคิดและองค์กรพัฒนาเอกชน (NGOs) และภาครัฐ โดยเสนอแนะกลยุทธ์ในการดำเนินการหลายวิธีในการเริ่มต้น เข้าถึงเป้าหมายเหล่านี้

มีการเปลี่ยนแปลงจากการใช้ประโยชน์จากห่วงโซ่อุปทานของซอฟต์แวร์เป็นการใช้ประโยชน์จากห่วงโซ่อุปทานบริการด้านไอที โดยกำหนดเป้าหมายโซลูชันคลาวด์และผู้ให้บริการที่มีการจัดการเพื่อเข้าถึงลูกค้าปลายทาง



แผนผังนี้แสดงวิธีการหลายขั้นตอนของ NOBELIUM ในการประนีประนอมเป้าหมายสูงสุดและความเสียหายต่อเหยื่อรายอื่นไปพร้อมกัน นอกเหนือจากการกระทำที่แสดงไว้ข้างต้นแล้ว NOBELIUM ยังเปิดตัวสเปรย์รหัสผ่านและการโจมตีแบบฟิชชิ่งกับหน่วยงานที่เกี่ยวข้อง แม้กระทั่งการกำหนดเป้าหมายบัญชีส่วนบุคคลของพนักงานของรัฐอย่างน้อยหนึ่งคนเพื่อเป็นอีกช่องทางหนึ่งในการประนีประนอม

ห่วงโซ่อุปทานไอทีเป็นประตูสู่ระบบนิเวศดิจิทัล

ต่อไป

ตลอดทั้งปี Microsoft Threat Intelligence Center (MSTIC) ตรวจพบจำนวนที่เพิ่มขึ้นของรัฐอิหร่านและผู้เกี่ยวข้องในอิหร่านที่ประนีประนอมกับบริษัทไอทีในหลายกรณี ผู้กระทำถูกตรวจพบว่าขโมยข้อมูลรับรองการลงชื่อเข้าใช้เพื่อเข้าถึงไคลเอ็นต์ดาวน์สตรีมสำหรับวัตถุประสงค์ต่างๆ ตั้งแต่การรวบรวมข่าวกรองไปจนถึงการโจมตีแบบทำลายล้างเพื่อตอบโต้

- ในเดือนกรกฎาคมและสิงหาคม 2021 DEV-0228 โจมตีผู้ให้บริการซอฟต์แวร์ธุรกิจของอิสราเอลเพื่อประนีประนอมลูกค้าปลายน้ำในภาคการป้องกันประเทศ พลังงาน และกฎหมายของอิสราเอลในภายหลัง[4]
- ตั้งแต่เดือนสิงหาคมถึงกันยายน 2021 Microsoft ตรวจพบการเพิ่มขึ้นอย่างรวดเร็วในหน่วยงานของรัฐของอิหร่านที่กำหนดเป้าหมายบริษัทไอทีที่อยู่ในอินเดีย การไม่มีปัญหาภูมิรัฐศาสตร์เร่งด่วนที่จะกระตุ้นให้เกิดการเปลี่ยนแปลงดังกล่าว ชี้ให้เห็นว่าการกำหนดเป้าหมายนี้มีไว้สำหรับการเข้าถึงทางอ้อมไปยังบริษัทสาขาและลูกค้านอกประเทศอินเดีย
- ในเดือนมกราคม 2022 DEV-0198 ซึ่งเป็นกลุ่มที่เราประเมินว่ามีความเกี่ยวข้องกับรัฐบาลอิหร่าน ได้บุกรุกผู้ให้บริการโซลูชันระบบคลาวด์ของอิสราเอล Microsoft ประเมินว่าผู้กระทำน่าจะใช้ข้อมูลรับรองที่ถูกบุกรุกจากผู้ให้บริการเพื่อยืนยันตัวตนกับบริษัทโลจิสติกส์ของอิสราเอล MSTIC สังเกตเห็นผู้กระทำการรายเดียวกันที่พยายามทำการโจมตีทางไซเบอร์แบบทำลายล้างต่อบริษัทโลจิสติกส์ในเดือนนั้น
- ในเดือนเมษายน 2022 POLONIUM ซึ่งเป็นกลุ่มในเลบานอนที่เราประเมินว่าได้ร่วมมือกับกลุ่มรัฐของอิหร่านเกี่ยวกับเทคนิคด้านซัพพลายเชนไอที ได้บุกรุกบริษัทไอทีของอิสราเอลอีกแห่งเพื่อเข้าถึงองค์กรด้านการป้องกันและกฎหมายของอิสราเอล[5]

กิจกรรมในปีที่ผ่านมานี้แสดงให้เห็นว่าผู้ก่อภัยคุกคามอย่าง NOBELIUM และ DEV-0228 กำลังทำความรู้จักกับภูมิทัศน์ของความสัมพันธ์ที่เชื่อถือได้ขององค์กรดีกว่าตัวองค์กรเอง ภัยคุกคามที่เพิ่มขึ้นนี้เน้นย้ำถึงความจำเป็นที่องค์กรต่างๆ จะต้องเข้าใจและเสริมความแข็งแกร่งให้กับพรมแดนและจุดเข้าสู่ฐานดิจิทัลของตน นอกจากนี้ยังเน้นย้ำถึงความสำคัญของผู้ให้บริการด้านไอทีในการตรวจสอบสถานะความปลอดภัยทางไซเบอร์ของตนเองอย่างเข้มงวด ตัวอย่างเช่น องค์กรควรใช้นโยบายการยืนยันตัวตนแบบหลายปัจจัยและการเข้าถึงแบบมีเงื่อนไข ซึ่งทำให้ผู้ไม่ประสงค์ดีสามารถดักจับบัญชีที่มีสิทธิพิเศษหรือแพร่กระจายไปทั่วเครือข่ายได้ยากขึ้น

การดำเนินการตรวจสอบและตรวจสอบความสัมพันธ์ของคู่ค้าอย่างละเอียดถี่ถ้วนช่วยลดการอนุญาตที่ไม่จำเป็นระหว่างองค์กรของคุณกับผู้ให้บริการอัปสตรีม และลบการเข้าถึงทันทีสำหรับความสัมพันธ์ที่ดูไม่คุ้นเคย การเพิ่มความคุ้นเคยกับบันทึกกิจกรรมและการตรวจสอบกิจกรรมที่มีอยู่ทำให้ง่ายต่อการตรวจพบความผิดปกติที่อาจจุดประกายการตรวจสอบเพิ่มเติม

> การกำหนดเป้าหมายของรัฐชาติจากบุคคลที่สามช่วยให้พวกเขาสามารถใช้ประโยชน์จากองค์กรที่ละเอียดอ่อนได้โดยการใช้ประโยชน์จากความไว้วางใจและการเข้าถึงในห่วงโซ่อุปทาน

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ตรวจสอบและตรวจสอบความสัมพันธ์ของผู้ให้บริการต้นทางและปลายทางและสิทธิ์การเข้าถึงที่ได้รับมอบอำนาจเพื่อลดสิทธิ์ที่ไม่จำเป็น ลบสิทธิ์การเข้าถึงสำหรับความสัมพันธ์ของคู่ค้าที่ดูไม่คุ้นเคยหรือยังไม่ได้ตรวจสอบโดยทันที[6]
2. เปิดใช้งานการบันทึกและตรวจสอบกิจกรรมการตรวจสอบสิทธิ์ทั้งหมดสำหรับโครงสร้างพื้นฐานการเข้าถึงระยะไกลและเครือข่ายส่วนตัวเสมือน (VPN) โดยเน้นที่บัญชีที่กำหนดค่าด้วยการตรวจสอบสิทธิ์แบบปัจจัยเดียว เพื่อยืนยันความถูกต้องและตรวจสอบกิจกรรมที่ผิดปกติ
3. เปิดใช้งาน MFA สำหรับบัญชีทั้งหมด (รวมถึงบัญชีบริการ) และตรวจสอบให้แน่ใจว่ามีการบังคับใช้ MFA สำหรับการเชื่อมต่อระยะไกลทั้งหมด
4. ใช้โซลูชันที่ไม่ต้องใช้รหัสผ่านเพื่อรักษาความปลอดภัยบัญชี[7]

ลิงค์ไปยังข้อมูลเพิ่มเติม

- NOBELIUM กำหนดเป้าหมายสิทธิ์ผู้ดูแลระบบที่ได้รับมอบอำนาจเพื่ออำนวยความสะดวกในการโจมตีในวงกว้าง | ศูนย์ข่าวกรองภัยคุกคามของ Microsoft (MSTIC)
- การกำหนดเป้าหมายของอิหร่านในภาคไอทีที่เพิ่มขึ้น | ศูนย์ข่าวกรองภัยคุกคามของ Microsoft (MSTIC), หน่วยรักษาความปลอดภัยแบบดิจิทัล Microsoft
- เปิดเผยกิจกรรมและโครงสร้างพื้นฐานของ POLONIUM ที่กำหนดเป้าหมายองค์กรของอิสราเอล | ศูนย์ข่าวกรองภัยคุกคามของ Microsoft (MSTIC)

การแสวงหาประโยชน์จากช่องโหว่อย่างรวดเร็ว

ในขณะที่องค์กรต่างๆ เสริมความแข็งแกร่งให้กับท่าทางการรักษาความปลอดภัยทางไซเบอร์ ผู้มีบทบาทของรัฐชาติก็ตอบโต้ด้วยการไล่ตามกลยุทธ์ใหม่ๆ ที่ไม่เหมือนใครเพื่อส่งการโจมตีและหลบเลี่ยงการตรวจจับ การระบุและการใช้ประโยชน์จากช่องโหว่ที่ไม่รู้จักก่อนหน้านี้ ซึ่งเรียกว่าช่องโหว่แบบ Zero-day เป็นกลยุทธ์หลักในความพยายามนี้

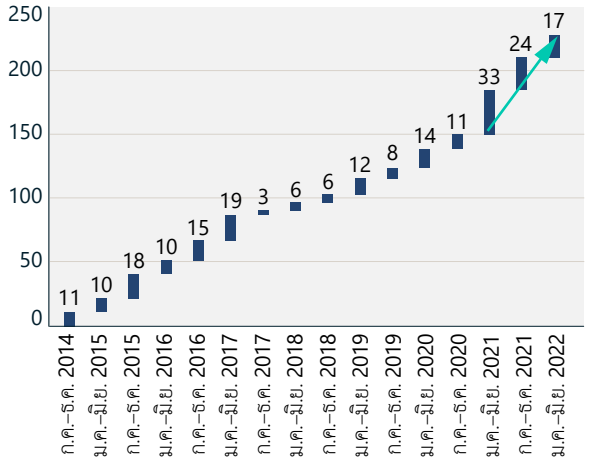
ช่องโหว่ Zero-day เป็นวิธีที่มีประสิทธิภาพเป็นพิเศษสำหรับการแสวงหาผลประโยชน์เบื้องต้น และเมื่อเปิดเผยต่อสาธารณะแล้ว ช่องโหว่จะถูกนำมาใช้ซ้ำอย่างรวดเร็วโดยรัฐชาติอื่นๆ และผู้กระทำความผิดทางอาญา จำนวนของช่องโหว่ Zero-day ที่เปิดเผยต่อสาธารณะในปีที่ผ่านมานั้นเทียบเท่ากับปีที่แล้ว ซึ่งสูงที่สุดเป็นประวัติการณ์

เนื่องจากผู้ก่อภัยคุกคามทางไซเบอร์ ทั้งในระดับรัฐและอาชญากร มีความเชี่ยวชาญมากขึ้นในการใช้ประโยชน์จากช่องโหว่เหล่านี้ เราได้สังเกตเห็นการลดเวลาระหว่างการประกาศช่องโหว่และการทำให้เป็นสินค้าของช่องโหว่นั้น สิ่งนี้ทำให้องค์กรจำเป็นต้องหาช่องโหว่ในทันที ในทำนองเดียวกัน จำเป็นอย่างยิ่งที่องค์กรหรือบุคคลที่เปิดเผยช่องโหว่ใหม่ๆ จะต้องเปิดเผยหรือรายงานอย่างมีความรับผิดชอบต่อผู้ให้บริการที่ได้รับผลกระทบโดยเร็วที่สุดเท่าที่จะเป็นไปได้ โดยสอดคล้องกับขั้นตอนการเปิดเผยช่องโหว่ที่ประสานงานกัน

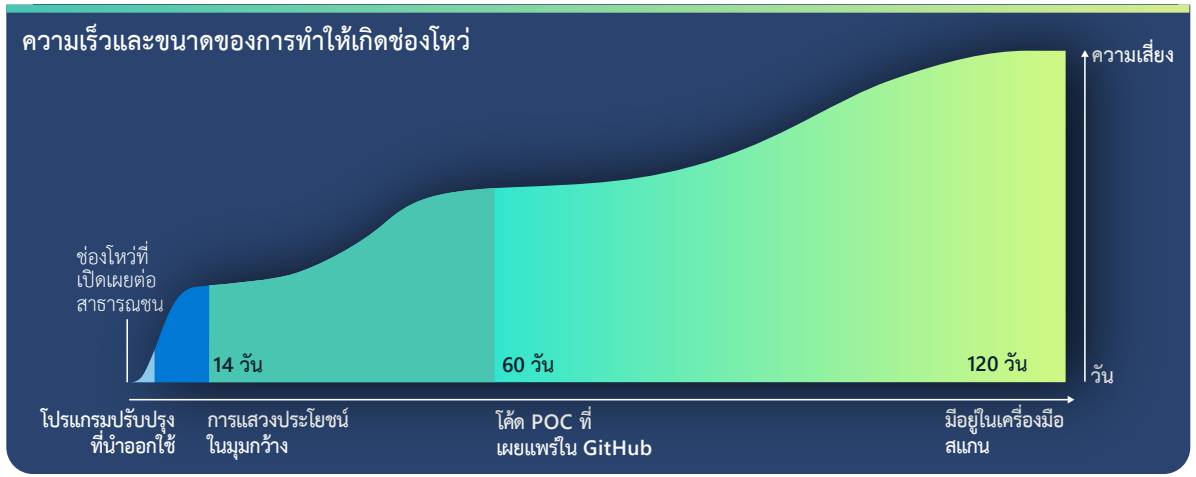
สิ่งนี้ทำให้มั่นใจได้ว่ามีการระบุช่องโหว่และพัฒนาแพตช์ในเวลาที่เหมาะสมเพื่อปกป้องลูกค้าจากภัยคุกคามที่ไม่รู้จักก่อนหน้านี้

องค์กรหลายแห่งถือว่าพวกเขามีโอกาสน้อยที่จะตกเป็นเหยื่อของการโจมตีแบบเจาะช่องโหว่แบบ Zero-day หากการจัดการช่องโหว่เป็นส่วนสำคัญในการรักษาความปลอดภัยเครือข่าย อย่างไรก็ตาม การทำให้เป็นสินค้าของการแสวงประโยชน์ทำให้พวกเขามีอัตราที่เร็วกว่ามาก การโจมตีแบบ Zero-day มักจะถูกค้นพบโดยผู้กระทำการคนอื่นๆ และนำกลับมาใช้ในวงกว้างในช่วงเวลาสั้นๆ ทำให้ระบบที่ไม่ได้แพตช์ตกอยู่ในความเสี่ยง แม้ว่าการแสวงหาผลประโยชน์แบบ Zero-day จะตรวจจับได้ยาก แต่การกระทำหลังการแสวงหาผลประโยชน์ของผู้กระทำมักจะตรวจจับได้ง่ายกว่า และหากมาจากซอฟต์แวร์ที่ได้รับการแพตช์อย่างสมบูรณ์ อาจเป็นสัญญาณเตือนถึงการประนีประนอม

แพตช์ที่ปล่อยออกมาสำหรับช่องโหว่ Zero-day



จำนวนของการโจมตีแบบ Zero-day ที่เปิดเผยต่อสาธารณะจากรายการช่องโหว่และการเปิดเผยข้อมูลทั่วไป (CVEs)



โดยเฉลี่ยแล้วจะใช้เวลาเพียง 14 วันในการหาช่องโหว่เพื่อใช้งานจริงหลังจากที่มีการเปิดเผยช่องโหว่ต่อสาธารณะ มุมมองนี้แสดงการวิเคราะห์ไทม์ไลน์ของการใช้ประโยชน์จากช่องโหว่ซีโร่เดย์ พร้อมด้วยจำนวนของระบบที่เสี่ยงต่อการโจมตีดังกล่าวและใช้งานอยู่บนอินเทอร์เน็ตนับจากเวลาที่มีการเปิดเผยต่อสาธารณะเป็นครั้งแรก

> แม้ว่าการโจมตีด้วยช่องโหว่แบบ Zero-day มักจะมุ่งเป้าหมายไปที่กลุ่มองค์กรที่จำกัดในตอนแรก การโจมตีเหล่านั้นจะถูกนำไปใช้อย่างรวดเร็วในระบบนิเวศของผู้คุกคามที่ใหญ่กว่า นี่เป็นการเริ่มต้นการแข่งขันสำหรับนักคุกคามเพื่อใช้ประโยชน์จากช่องโหว่ให้กว้างขวางที่สุดเท่าที่จะเป็นไปได้ก่อนที่เป้าหมายที่มีศักยภาพจะติดตั้งแพตช์

ในขณะที่เราสังเกตเห็นผู้มีบทบาทจากรัฐชาติจำนวนมากพัฒนาช่องโหว่จากช่องโหว่ที่ไม่รู้จัก ผู้คุกคามจากรัฐชาติที่มีฐานในจีนมีความเชี่ยวชาญเป็นพิเศษในการค้นพบและพัฒนาช่องโหว่แบบ Zero-day กฎระเบียบการรายงานช่องโหว่ของจีนมีผลบังคับใช้ในเดือนกันยายน 2021 ถือเป็นครั้งแรกในโลกที่รัฐบาลกำหนดให้การรายงานช่องโหว่ไปยังหน่วยงานของรัฐเพื่อตรวจสอบก่อนที่จะแบ่งปันช่องโหว่กับเจ้าของผลิตภัณฑ์หรือบริการ กฎระเบียบใหม่นี้อาจช่วยให้หน่วยงานต่างๆ ในรัฐบาลจีนสามารถสะสมช่องโหว่ที่รายงานไว้เพื่อใช้เป็นอาวุธได้ การใช้ Zero-day ที่เพิ่มขึ้นจากปีที่แล้วจากผู้ดำเนินการในจีนน่าจะสะท้อนถึงปีแรกของข้อกำหนดการเปิดเผยช่องโหว่ของจีนสำหรับชุมชนความปลอดภัยของจีน และเป็นขั้นตอนสำคัญในการใช้ช่องโหว่ zero-day เป็นลำดับความสำคัญของรัฐ ช่องโหว่ที่อธิบายไว้ด้านล่างนี้ได้รับการพัฒนาและปรับใช้โดยผู้มีบทบาทของรัฐชาติที่มีฐานอยู่ในจีนในการโจมตีก่อนที่จะถูกค้นพบและแพร่กระจายไปยังผู้มีบทบาทอื่นๆ ในระบบนิเวศภัยคุกคามที่ใหญ่กว่า

การแสวงหาประโยชน์จากช่องโหว่อย่างรวดเร็ว

ต่อไป

แม้แต่องค์กรที่ไม่ได้ตกเป็นเป้าหมายของผู้คุกคามจากรัฐชาติก็ยังมีระยะเวลาที่จำกัดในการแก้ไขช่องโหว่แบบ Zero-day ในระบบที่ได้รับผลกระทบก่อนที่ช่องโหว่นั้นจะถูกนำไปใช้โดยระบบนิเวศของผู้ประสงค์ร้ายในวงกว้าง

ตัวอย่างของช่องโหว่ที่พบใหม่เหล่านี้แสดงให้เห็นว่าองค์กรมีเวลาโดยเฉลี่ย 60 วันนับจากเวลาที่มีการแก้ไขช่องโหว่และรหัสพิสูจน์แนวคิด (POC) พร้อมใช้งานทางออนไลน์ และมักถูกนำไปใช้โดยบุคคลอื่นเพื่อนำมาใช้ซ้ำ ในทำนองเดียวกันองค์กรมีเวลาเฉลี่ย 120 วันก่อนที่ช่องโหว่จะพร้อมใช้งานในเครื่องมือสแกนช่องโหว่อัตโนมัติและเครื่องมือหาช่องโหว่ เช่น Metasploit ซึ่งมักจะส่งผลให้ช่องโหว่ถูกใช้ในวงกว้าง สิ่งนี้ชี้ให้เห็นว่าแม้แต่องค์กรที่ไม่ได้ตกเป็นเป้าหมายของผู้คุกคามจากรัฐชาติก็ยังมีระยะเวลาที่จำกัดในการแก้ไขช่องโหว่แบบ Zero-day ในระบบที่ได้รับผลกระทบก่อนที่ช่องโหว่นั้นจะถูกนำไปใช้โดยระบบนิเวศของนักแสดงในวงกว้าง

CVE-2021-35211 SolarWinds Serv-U

ในเดือนกรกฎาคม 2021 SolarWinds ออกคำแนะนำด้านความปลอดภัยสำหรับ CVE-2021-35211 โดยให้เครดิต Microsoft ในการแจ้งเตือน[8] ในขณะนั้น เราค้นพบตัวแสดงภัยคุกคาม DEV-0322 ที่สอดคล้องกับรัฐชาติใช้ประโยชน์จากช่องโหว่ของ SolarWinds Serv-U อย่างแข็งขัน ทีม RiskIQ ของเราสังเกตที่อยู่ IP 12,646 รายการที่โฮสต์อุปกรณ์ที่ได้รับผลกระทบในเวอร์ชันที่เชื่อมต่ออินเทอร์เน็ตระหว่างวันที่ 15 มิถุนายนถึง 9 กรกฎาคม

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

ในเดือนกันยายน 2021 นักวิจัยของเราสังเกตเห็นนักแสดงที่เกี่ยวข้องกับจีนใช้ประโยชน์จาก Zoho ManageEngine ในหน่วยงานหลายแห่งในสหรัฐอเมริกา ช่องโหว่ดังกล่าวได้รับการรายงานต่อสาธารณะในวันที่ 6 กันยายน ในชื่อ CVE-2021-40539 Zoho ManageEngine ADSelfService Plus ซึ่งองค์กรต่างๆ มักจะใช้เพื่อจัดการกับการรีเซ็ตรหัสผ่าน[9] DEV-0322 ใช้ประโยชน์จากช่องโหว่ดังกล่าวในภายหลัง กันยายน โดยใช้เป็นเวกเตอร์เริ่มต้นเพื่อตั้งหลักในเครือข่ายและดำเนินการเพิ่มเติม รวมถึงการทิ้งข้อมูลประจำตัว การติดตั้งไบนารีที่กำหนดเองและการปล่อยมัลแวร์เพื่อรักษาความคงอยู่ ในช่วงเวลาของการเปิดเผยข้อมูล RiskIQ สังเกต 4,011 อินสแตนซ์ของระบบเหล่านี้ที่ใช้งานอยู่และบนอินเทอร์เน็ต

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

ปลายเดือนตุลาคม 2021 เราสังเกตเห็นว่า DEV-0322 ใช้ประโยชน์จากช่องโหว่ (CVE-2021-44077) ในผลิตภัณฑ์ Zoho ManageEngine ตัวที่สอง นั่นคือ ServiceDesk Plus ซึ่งเป็นซอฟต์แวร์แผนกช่วยเหลือด้านไอทีที่มีการจัดการสินทรัพย์ DEV-0322 ใช้ช่องโหว่นี้เพื่อกำหนดเป้าหมายและประนีประนอมหน่วยงานด้านการดูแลสุขภาพ เทคโนโลยีสารสนเทศ การศึกษาระดับสูง และภาคการผลิตที่สำคัญ เมื่อวันที่ 2 ธันวาคม สำนักงานสืบสวนกลางแห่งสหรัฐอเมริกา (FBI) และหน่วยงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐาน (CISA) ได้ออกคำแนะนำร่วมกันเพื่อเตือนประชาชนเกี่ยวกับผู้คุกคามรัฐชาติที่ใช้ประโยชน์จากช่องโหว่นี้ ในช่วงเวลาของการเปิดเผยข้อมูล RiskIQ สังเกต 7,956 อินสแตนซ์ของระบบเหล่านี้ที่ใช้งานอยู่และบนอินเทอร์เน็ต

CVE-2021-42321 Microsoft Exchange

การใช้ประโยชน์จากช่องโหว่แบบ Zero-day สำหรับช่องโหว่ Exchange CVE-2021-42321 ถูกเปิดเผยในระหว่างงาน Tianfu Cup ซึ่งเป็นการประชุมสุดยอดด้านความปลอดภัยทางไซเบอร์ระหว่างประเทศและการแข่งขันการแฮ็กที่จัดขึ้นในวันที่ 16 และ 17 ตุลาคม 2021 ที่เมืองเฉิงตู ประเทศจีน นักวิจัยด้านความปลอดภัยของ Microsoft สังเกตเห็นการใช้ประโยชน์จากช่องโหว่ของ Exchange ที่ใช้ทั่วไปเมื่อวันที่ 21 ตุลาคม เพียงสามวันหลังจากช่องโหว่ดังกล่าวถูกเปิดเผย ในช่วงเวลาของการเปิดเผยข้อมูล RiskIQ สังเกต 61,559 อินสแตนซ์ของระบบเหล่านี้ที่ใช้งานอยู่และบนอินเทอร์เน็ต ในเวลาที่เปิดเผย เรายังคงติดตามกิจกรรมการแสวงประโยชน์จนถึงเดือนพฤศจิกายน 2021

CVE-2022-26134 การบรรจบกัน

ผู้ดำเนินการในจีนน่าจะมีรหัสการโจมตีช่องโหว่แบบ Zero-day สำหรับช่องโหว่ Confluence (CVE-2022-26134) สี่วันก่อนที่ช่องโหว่จะถูกเปิดเผยต่อสาธารณะในวันที่ 2 มิถุนายน และน่าจะใช้ประโยชน์จากช่องโหว่ดังกล่าวกับบริษัทในสหรัฐฯ ในช่วงเวลาของการเปิดเผยข้อมูล RiskIQ สังเกต 53,621 อินสแตนซ์ของระบบการบรรจบกันที่มีช่องโหว่บนอินเทอร์เน็ต

ช่องโหว่ถูกหยิบขึ้นมาและใช้ประโยชน์ในวงกว้างและในกรอบเวลาที่สั้นลงมากขึ้นเรื่อยๆ

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. จัดลำดับความสำคัญของการแพตช์ช่องโหว่แบบ Zero-day ทันทีที่มีการเผยแพร่ อย่ารอให้วงจรการจัดการแพทช์ปรับใช้
2. จัดทำเอกสารและจัดทำรายการสินทรัพย์ฮาร์ดแวร์และซอฟต์แวร์ขององค์กรทั้งหมด เพื่อกำหนดความเสี่ยงและกำหนดได้อย่างรวดเร็วว่าเมื่อใดควรดำเนินการกับแพตช์

กลยุทธ์ทางไซเบอร์ในช่วงสงครามของผู้ดำเนินการของรัฐรัสเซียคุกคามยูเครนและที่อื่นๆ

ในปีนี้ ผู้มีบทบาทของรัฐรัสเซียเริ่มปฏิบัติการทางไซเบอร์เพื่อเสริมปฏิบัติการทางทหารระหว่างการรุกรานยูเครนของรัสเซีย โดยมักใช้กลยุทธ์และเทคนิคเดียวกันกับที่ใช้กับเป้าหมายนอกยูเครน จำเป็นอย่างยิ่งที่องค์กรต่างๆ ทั่วโลกจะต้องดำเนินมาตรการเพื่อเสริมความปลอดภัยทางไซเบอร์จากภัยคุกคามทางดิจิทัลที่เกิดจากผู้คุกคามที่มีแนวร่วมในรัสเซีย

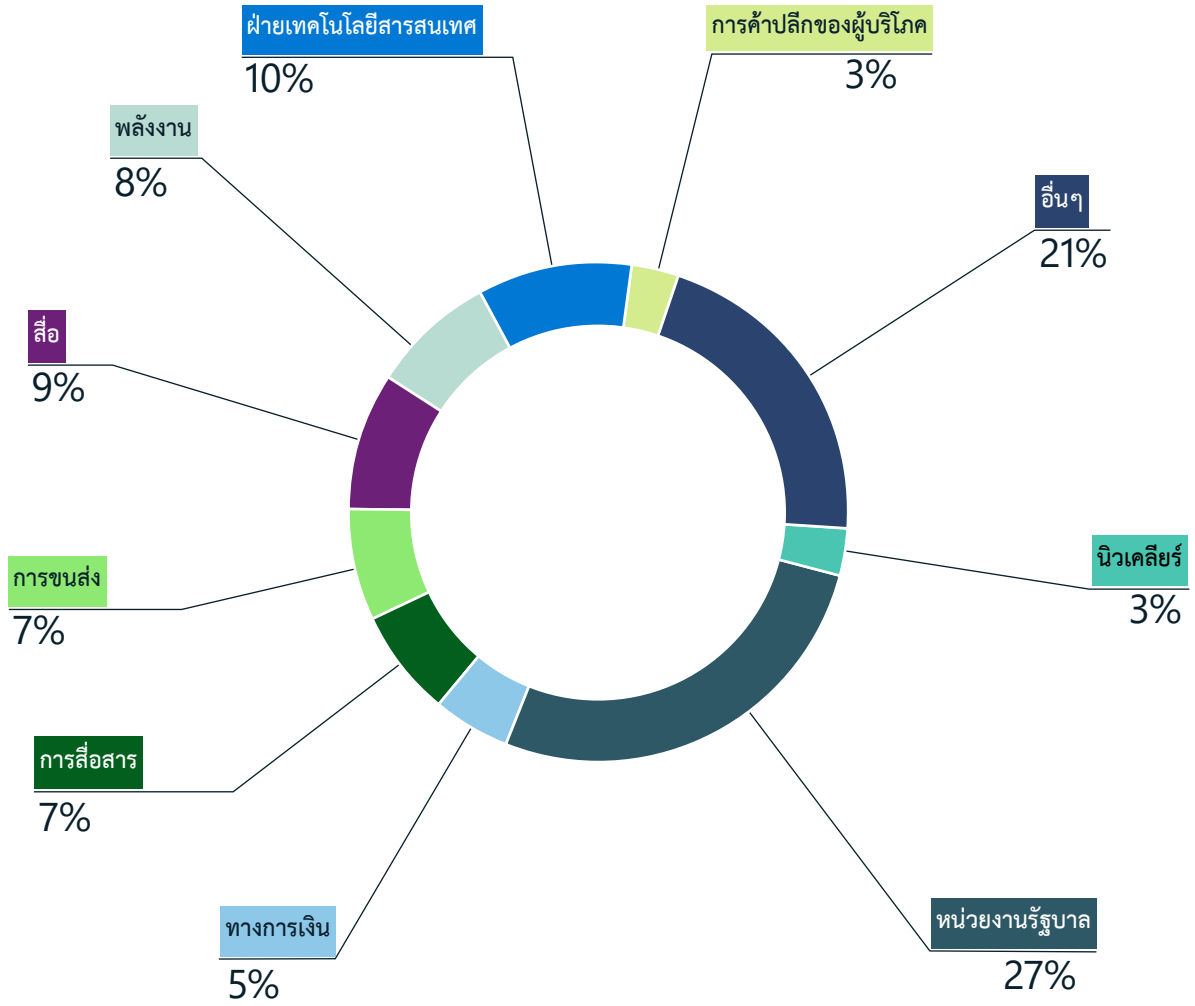
สถานการณ์ในพื้นที่ยังคงผันผวนเนื่องจากความขัดแย้งทางทหารยังคงมีอยู่ และยูเครนและพันธมิตรควรเตรียมพร้อมที่จะป้องกันตนเองหากผู้ให้บริการไซเบอร์ของรัฐรัสเซียเพิ่มความถี่หรือความรุนแรงของการบุกรุกตามวัตถุประสงค์ทางทหาร ในช่วงสี่เดือนแรกของสงคราม ไมโครซอฟท์สังเกตเห็นผู้คุกคามที่เกี่ยวข้องกับกองทัพรัสเซียเปิดการโจมตีทางไซเบอร์แบบทำลายล้างหลายระลอกต่อหน่วยงานและองค์กรต่างๆ ของยูเครนเกือบ 50 แห่ง และการบุกรุกที่เน้นการจารกรรมต่อหน่วยงานอื่นๆ จำนวนมาก หากไม่รวมการดำเนินการกับลูกค้าบริการออนไลน์ 64 เปอร์เซ็นต์ของกิจกรรมการคุกคามของรัสเซียต่อเป้าหมายที่ทราบนั้นมุ่งเป้าไปที่องค์กรในยูเครนระหว่างปลายเดือนกุมภาพันธ์ถึงมิถุนายน

ในการปฏิบัติการแต่ละครั้ง ผู้ก่อภัยคุกคามชาวรัสเซียใช้กลยุทธ์ เทคนิค และขั้นตอน (TTP) หลายอย่างที่เราสังเกตเห็นว่าถูกใช้ก่อนที่จะบุกโจมตีเป้าหมายทั้งภายในและภายนอกยูเครน ผู้กระทำการเหล่านี้ตั้งใจที่จะทำลายข้อมูลและทำให้หน่วยงานรัฐบาลยูเครนเสียสมดุลในช่วงแรกของความขัดแย้ง ตั้งแต่นั้นเป็นต้นมาพวกเขาพยายามขัดขวางการขนส่งความช่วยเหลือทางทหารและมนุษยธรรมไปยังยูเครน ขัดขวางการเข้าถึงบริการและสื่อสาธารณะ และขโมยข้อมูลข่าวกรองระยะยาวหรือมูลค่าทางเศรษฐกิจของรัสเซีย

การกำหนดเป้าหมายการขนส่งคุกคามพื้นที่ที่มีความสำคัญอย่างยิ่งยวดต่อพลเมืองยูเครนที่พยายามเอาชีวิตรอดจากความขัดแย้ง จากการสำรวจที่สนับสนุนโดย UNICEF ในเดือนพฤษภาคม ผู้ตอบแบบสำรวจในเขตเมืองที่ได้รับผลกระทบจากความขัดแย้งกังวลมากที่สุดเกี่ยวกับการขนส่งและเชื้อเพลิง การหยุดชะงักของอุปทาน ความปลอดภัย และการเข้าถึงอาหาร บริการทางการแพทย์ และบริการทางการเงินที่จำกัด[10] ในเดือนมิถุนายน ผู้ประสานงานวิกฤตการณ์ของสหประชาชาติประจำยูเครนกล่าวว่า ผู้คน 15.7 ล้านคนในยูเครนต้องการความช่วยเหลือด้านมนุษยธรรมอย่างเร่งด่วน และจำนวนจะเพิ่มขึ้นเมื่อสงครามดำเนินต่อไป[11]

นอกยูเครน Microsoft ตรวจพบความพยายามในการบุกรุกเครือข่ายของรัสเซียต่อ 128 องค์กรใน 42 ประเทศระหว่างปลายเดือนกุมภาพันธ์ถึงมิถุนายน สหรัฐอเมริกาเป็นเป้าหมายอันดับหนึ่งของรัสเซีย โปแลนด์ซึ่งความช่วยเหลือทางทหารและมนุษยธรรมระหว่างประเทศจำนวนมากผ่านการขนส่งทางบกของยูเครนก็เป็นเป้าหมายสำคัญในช่วงเวลานี้เช่นกัน ผู้คุกคามที่เชื่อมโยงกับรัฐรัสเซียไล่ตามองค์กรต่างๆ ในประเทศแถบบอลติกและเครือข่ายคอมพิวเตอร์ในเดนมาร์ก นอร์เวย์ ฟินแลนด์ และสวีเดนในเดือนเมษายนและพฤษภาคมเช่นกัน

ภาคอุตสาหกรรมที่เป็นเป้าหมายมากที่สุดในยูเครนตั้งแต่การรุกราน



องค์กรรัฐบาลกลาง มลรัฐ และท้องถิ่นในยูเครนยังคงเป็นเป้าหมายสำคัญสำหรับกลุ่มภัยคุกคามของรัฐและรัฐในเครือของรัสเซียตลอดความขัดแย้ง การมุ่งเน้นที่องค์กรภาคการขนส่ง พลังงาน การเงิน และสื่อเน้นย้ำถึงความเสี่ยงที่การดำเนินการทางไซเบอร์เหล่านี้ก่อให้เกิดบริการที่พลเมืองยูเครนไว้วางใจ

กลยุทธ์ทางไซเบอร์ในช่วงสงครามของผู้ดำเนินการของรัฐรัสเซียคุกคามยูเครนและที่อื่นๆ

ต่อไป

เราได้เห็นการเพิ่มขึ้นของกิจกรรมที่คล้ายกันที่กำหนดเป้าหมายกระทรวงต่างประเทศของประเทศในกลุ่ม NATO

กลุ่มภัยคุกคามของรัฐรัสเซียยังคงสนใจที่จะประนีประนอมโครงสร้างพื้นฐานที่สำคัญทั้งในและนอกยูเครนในปีที่ผ่านมา IRIDIUM ติดตั้งมัลแวร์ Industroyer2 ในความพยายามที่ล้มเหลวในการปล่อยให้ผู้คนหลายล้านคนในยูเครนไม่มีไฟฟ้าใช้ นอกยูเครน BROMINE ดำเนินการบุกรุกกับองค์กรที่เกี่ยวข้องกับการผลิตและระบบควบคุมอุตสาหกรรมในต้นปี 2022

ผู้มีบทบาทของรัฐและรัฐในสังกัดของรัสเซียได้กำกับปฏิบัติการทางไซเบอร์ต่อยูเครน พันธมิตร และเป้าหมายอื่นๆ ที่มีค่าข่าวกรองในปีนี้โดยใช้ TTP จำนวนมากดังต่อไปนี้:

ทำการฟิชชิ่งด้วยไฟล์แนบหรือลิงก์ที่เป็นอันตราย

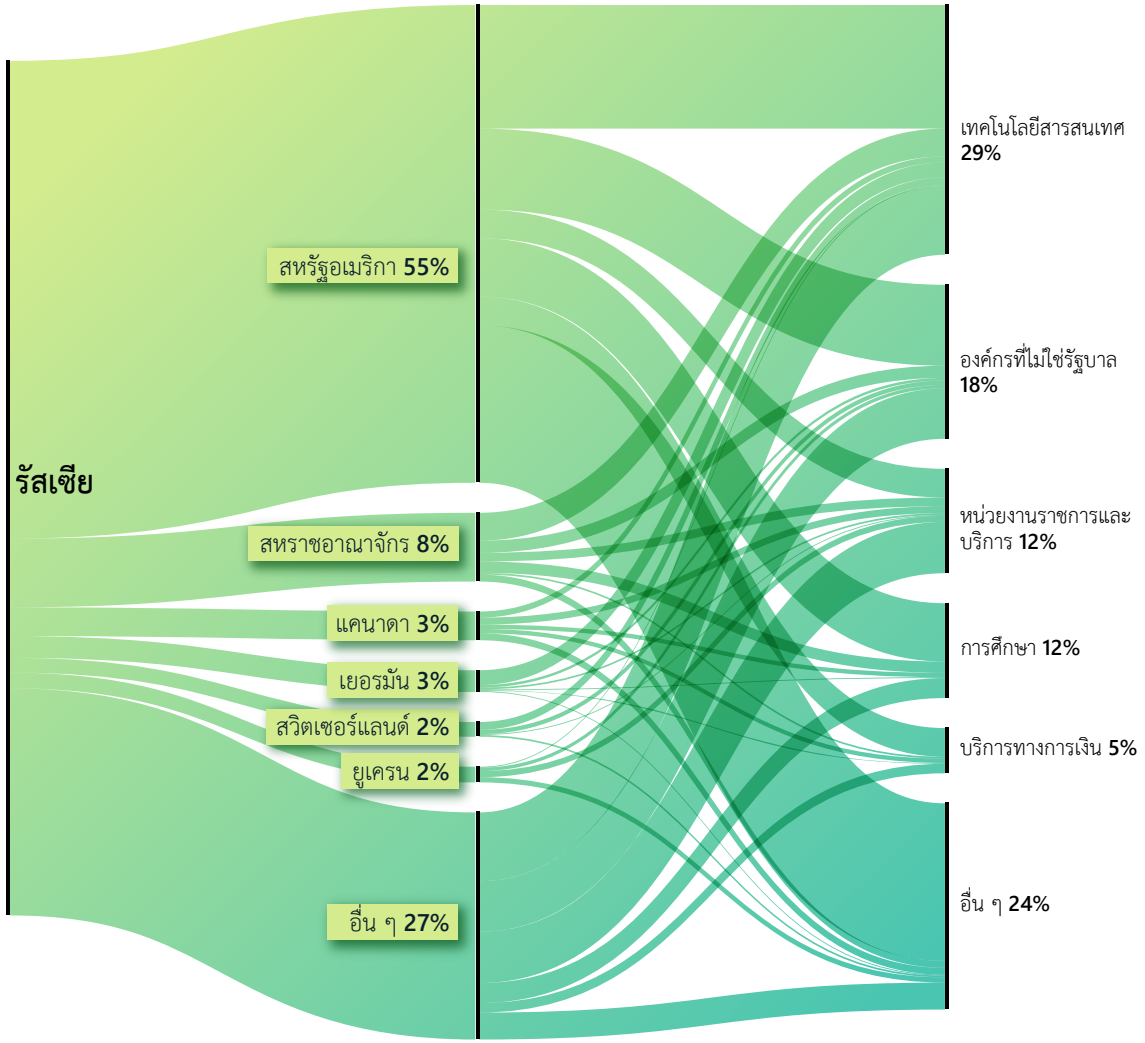
รัฐของรัสเซียและกลุ่มที่เกี่ยวข้องกับรัสเซีย เช่น ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM และ IRIDIUM ล้วนใช้แคมเปญฟิชชิ่งเพื่อเข้าถึงบัญชีและเครือข่ายที่ต้องการในเบื้องต้นในองค์กรภายในและภายนอกยูเครน แคมเปญจำนวนมากใช้บัญชีที่ถูกบุกรุกหรือปลอมแปลงที่องค์กรเป้าหมายหรือในอุตสาหกรรมเดียวกัน และใช้ธีมที่น่าสนใจเพื่อหลอกล่อเหยื่อ NOBELIUM ใช้บัญชีทางการทูตที่ถูกบุกรุกเพื่อส่งฟิชชิ่งเมลที่ปลอมเป็นการสื่อสารทางการทูตไปยังพนักงานกระทรวงต่างประเทศทั่วโลก STRONTIUM สร้างบัญชีปลอมตามชื่อเจ้าของบัญชีที่เปิดเผยต่อสาธารณะที่คลังสมองในสหรัฐอเมริกา และส่งข้อความฟิชชิ่งเพื่อเข้าถึงบัญชีที่นักคิดเหล่านั้น SEABORGIUM ทำการฟิชชิ่งโดยใช้เหยื่อล่อที่เกี่ยวข้องกับการรายงานความขัดแย้งในยูเครนเพื่อให้สามารถเข้าถึงบัญชีเบื้องต้นที่หน่วยงานวิเทศสัมพันธ์ในกลุ่มประเทศนอร์ดิก

การใช้ประโยชน์จากห่วงโซ่อุปทานบริการด้านไอทีเพื่อส่งผลกระทบต่อลูกค้าปลายทาง

ในช่วงปลายปี 2021 เจ้าหน้าที่รัฐของรัสเซียบุกรุกผู้ให้บริการด้านไอทีและใช้การเข้าถึงเพื่ออำนวยความสะดวกในการทำให้เสียโฉมเว็บไซต์และการติดตั้งมัลแวร์ทำลายล้าง Whispergate โดย DEV-0586 ในเดือนมกราคม[12] DEV-0586 ยังทำลายเครือข่ายของบริษัทไอทีที่สร้างระบบการจัดการทรัพยากรสำหรับกระทรวงกลาโหมของยูเครนและองค์กรอื่นๆ ในภาคการสื่อสารและการขนส่ง ซึ่งบ่งชี้ว่ากลุ่มนี้กำลังสำรวจตัวเลือกการโจมตีของบุคคลที่สามในภาคส่วนเหล่านั้นเช่นกัน

ทั่วโลก แต่โดยเฉพาะอย่างยิ่งในสหรัฐอเมริกาและยุโรปตะวันตก NOBELIUM กำหนดเป้าหมายผู้ให้บริการด้านไอทีเพื่อเข้าถึงรัฐบาลและเครือข่ายที่ละเอียดอ่อนอื่นๆ ตลอดปี 2021-2022(ดูการอภิปรายเกี่ยวกับช่องโหว่ของห่วงโซ่อุปทานก่อนหน้าในบทนี้)

รัสเซีย: ประเทศเป้าหมายสูงสุดและภาคอุตสาหกรรม



แม้จะมุ่งเน้นที่องค์กรในยูเครนอย่างเข้มข้นตั้งแต่ต้นปี 2022 แต่องค์กรในอเมริกาเหนือและยุโรปตะวันตกยังคงเป็นบริการออนไลน์ที่ลูกค้าชาวรัสเซียกำหนดเป้าหมายมากที่สุด การรณรงค์ต่อต้านภาคไอทีของ NOBELIUM ทำให้ภาคส่วนนี้เป็นเป้าหมายมากที่สุดในปีที่ผ่านมา

กลยุทธ์ทางไซเบอร์ในช่วงสงครามของผู้ดำเนินการของรัฐรัสเซียคุกคามยูเครนและที่อื่นๆ

ต่อไป

การใช้ประโยชน์จากแอปพลิเคชันสาธารณะเพื่อเข้าถึงเครือข่ายเบื้องต้น

ตั้งแต่ปลายปี 2021 เป็นต้นมา STRONTIUM ได้ทำงานเพื่อพัฒนาและปรับปรุงความสามารถในการใช้ประโยชน์จากบริการสาธารณะ เช่น เซิร์ฟเวอร์ Microsoft Exchange เพื่อขโมยข้อมูล STRONTIUM ใช้ประโยชน์จากเซิร์ฟเวอร์ Exchange ที่ไม่ได้แพตช์เพื่อเข้าถึงบัญชีของรัฐบาลยูเครน ตลอดจนองค์กรที่เกี่ยวข้องกับการทหารและการป้องกันประเทศในสหรัฐอเมริกา เลบานอน เปรู และโรมาเนีย และหน่วยงานรัฐบาลอื่นๆ ที่อยู่ในอาร์เมเนีย บอสเนีย โคโซโว และมาเลเซีย DEV-0586 ซึ่งเป็นหน่วยงานในสังกัดของกองทัพรัสเซีย ใช้ประโยชน์จากช่องโหว่ของเซิร์ฟเวอร์ Confluence เพื่อเข้าถึงรัฐบาลและองค์กรภาคไอทีในยูเครนและประเทศอื่นๆ ในยุโรปตะวันออก

ผู้คุกคามของรัฐรัสเซียและในเครือใช้ TTP เดียวกันจำนวนมากเพื่อประนีประนอมองค์กรที่น่าสนใจในช่วงเวลาที่เกิดสงครามและสันติภาพ

การใช้บัญชีการดูแลระบบและโปรโตคอล และยูทิลิตี้ดั้งเดิมสำหรับการค้นหาเครือข่ายและการเคลื่อนไหวด้านข้าง

หลังจากได้รับสิทธิ์เข้าถึงเครือข่ายในเบื้องต้นแล้ว Microsoft สังเกตเห็นเจ้าหน้าที่รัฐของรัสเซียใช้ประโยชน์จากบัญชีที่ถูกต้องตามกฎหมายและโปรแกรมอรรถประโยชน์ซอฟต์แวร์ที่ใช้ในการดำเนินการบำรุงรักษาขั้นพื้นฐานเพื่อหลบเลี่ยงการตรวจจับให้นานที่สุด พวกเขาอาศัยข้อมูลประจำตัวที่ถูกบุกรุกซึ่งมีความสามารถในการดูแลระบบและโปรโตคอลการดูแลระบบ เครื่องมือและวิธีการที่ถูกต้องในการย้ายด้านข้างภายในเครือข่ายโดยไม่ดึงดูดความสนใจจากจอภาพอัตโนมัติและผู้ปกป้องเครือข่ายในทันที

สุขอนามัยไซเบอร์ขั้นพื้นฐานและการใช้เครื่องมือตรวจจับปลายทางและเครื่องมือตอบสนองสามารถช่วยลดผลกระทบด้านลบของปฏิบัติการประเภทนี้ทั้งในยามสงบและในช่วงสงคราม

ความไม่แน่นอนของความขัดแย้งที่กำลังดำเนินอยู่ทำให้องค์กรต่างๆ ทั่วโลกต้องใช้มาตรการในการรักษาความปลอดภัยทางไซเบอร์เพื่อป้องกันภัยคุกคามทางดิจิทัลที่มาจากรัฐรัสเซียและผู้คุกคามที่เกี่ยวข้องกับรัสเซีย

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ลดการขโมยข้อมูลประจำตัวและการใช้บัญชีในทางที่ผิดโดยการปกป้องข้อมูลประจำตัวของผู้ใช้ของคุณโดยการใช้เครื่องมือป้องกันข้อมูลประจำตัวของ MFA และบังคับใช้การเข้าถึงสิทธิ์ขั้นต่ำเพื่อรักษาความปลอดภัยบัญชีและระบบที่ละเอียดอ่อนและมีสิทธิ์มากที่สุด
2. ใช้การอัปเดตเพื่อให้แน่ใจว่าระบบทั้งหมดของคุณได้รับการป้องกันในระดับสูงสุดโดยเร็วที่สุดเท่าที่จะเป็นไปได้และได้รับการอัปเดตอยู่เสมอ
3. ปรับใช้โซลูชันป้องกันมัลแวร์ การตรวจจับปลายทาง และการป้องกันข้อมูลประจำตัวทั่วทั้งองค์กรของคุณ การผสมผสานของโซลูชันการรักษาความปลอดภัยในเชิงลึกในเชิงป้องกัน เมื่อจับคู่กับบุคลากรที่ผ่านการฝึกอบรมและมีความสามารถจะช่วยให้องค์กรของคุณสามารถระบุ ตรวจจับ และป้องกันการบุกรุกที่ส่งผลกระทบต่อธุรกิจของคุณได้
4. เปิดใช้งานการตรวจสอบและการกู้คืนในกรณีที่คุณตรวจพบหรือได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามต่อสภาพแวดล้อมของคุณโดยสำรองระบบที่สำคัญและเปิดใช้งานการบันทึก การสร้างแผนการตอบสนองต่อเหตุการณ์ได้รับการสนับสนุนอย่างยิ่ง

ลิงค์ไปยังข้อมูลเพิ่มเติม

- การปกป้องยูเครน: บทเรียนแรกจากสงครามไซเบอร์ | Microsoft On the Issues
- สงครามไฮบริดในยูเครน | Microsoft On the Issues
- กิจกรรมภัยคุกคามทางไซเบอร์ในยูเครน: การวิเคราะห์และทรัพยากร | ศูนย์ตอบสนองด้านความปลอดภัยของ Microsoft (MSRC)
- การรบกวนการโจมตีทางไซเบอร์ที่กำหนดเป้าหมายไปที่ยูเครน | Microsoft On the Issues
- มัลแวร์โจมตีเป้าหมายรัฐบาลยูเครน | Microsoft On the Issues
- MagicWeb: เคล็ดลับหลังการประนีประนอมของ NOBELIUM เพื่อรับรองว่าเป็นใครก็ได้ | Microsoft Threat Intelligence Center (MSTIC), Detection and Response Team (DART), Microsoft 365 Defender Research Team

จีนขยายการกำหนดเป้าหมายทั่วโลกเพื่อความได้เปรียบทางการแข่งขัน

ในสภาพภูมิอากาศทางการเมืองที่ซับซ้อนในปัจจุบัน ผู้คุกคามของรัฐและหน่วยงานของรัฐของจีนที่ดำเนินการทางไซเบอร์มักมีเป้าหมายเพื่อส่งเสริมเป้าหมายทางยุทธศาสตร์ทางทหาร เศรษฐกิจ และความสัมพันธ์ระหว่างประเทศของประเทศ ซึ่งเป็นส่วนหนึ่งของวัตถุประสงค์ของจีนในการบรรลุความได้เปรียบในการแข่งขัน ในปีที่ผ่านมา Microsoft ได้สังเกตเห็นกิจกรรมการคุกคามของจีนที่แพร่หลายซึ่งมีเป้าหมายไปยังประเทศต่างๆ ทั่วโลก

ตั้งแต่กลางปี 2021 เป็นต้นมา จีนได้ดำเนินกลยุทธ์เพื่อรักษาเสถียรภาพทางเศรษฐกิจและการเงินท่ามกลางการแพร่ระบาดของโควิด-19 ที่เลวร้ายที่สุดในรอบสองปี[13] จีนยังคงแสดงจุดยืนของตนต่อเหตุการณ์ทางภูมิรัฐศาสตร์ เช่น การต่อสู้เพื่อสร้างสมดุลความเป็นหุ้นส่วนที่ “ไร้ขีดจำกัด” กับรัสเซีย[14] และรักษาตำแหน่งของตนในเวทีโลก[15] นอกจากนี้ ท่าทีของจีนต่อสหรัฐอเมริกาและพันธมิตรที่มีต่อไต้หวัน[16] และทะเลจีนใต้ยังคงตึงเครียดต่อความสัมพันธ์ระหว่างประเทศกับนานาประเทศ[17]

กลุ่มภัยคุกคามระดับรัฐและรัฐในเครือของจีนเพิ่มการกำหนดเป้าหมายไปยังประเทศขนาดเล็กทั่วโลกโดยเน้นที่เอเชียตะวันออกเฉียงใต้เพื่อให้ได้เปรียบในการแข่งขันในทุกด้าน

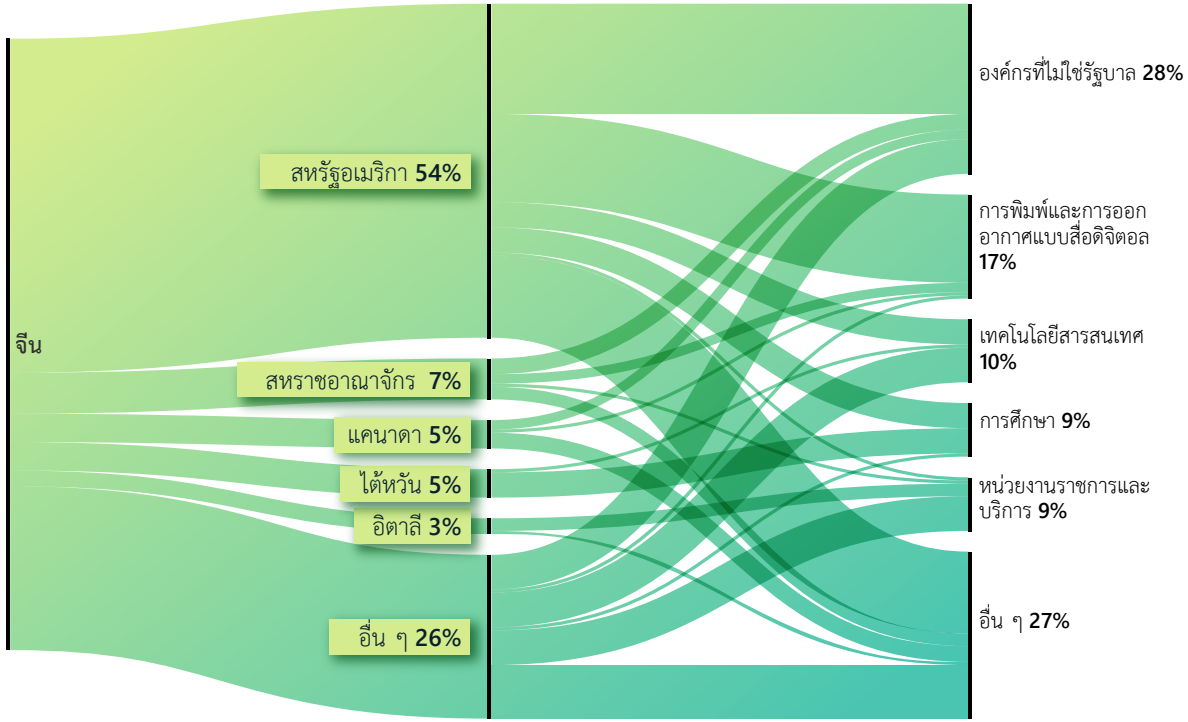


จีนยังคงขยายอิทธิพลทางเศรษฐกิจไปทั่วโลกผ่านโครงการ Belt and Road Initiatives (BRI) ที่จัดตั้งขึ้นก่อนหน้านี้ โดยพยายามรื้อฟื้นกรอบการลงทุนที่ครอบคลุมกับสหภาพยุโรป[18] และเจรจาการค้าระดับภูมิภาคใหม่ข้อตกลงกับ 15 ประเทศในเอเชียแปซิฟิกที่เรียกว่าหุ้นส่วนทางเศรษฐกิจระดับภูมิภาค[19] Microsoft ประเมินว่าจีนจะยังคงใช้การรวบรวมทางไซเบอร์เป็นเครื่องมือในการช่วยพัฒนากลยุทธ์ทางการเมือง การทหาร และเป้าหมายทางเศรษฐกิจเนื่องจากการปฏิบัติการทางไซเบอร์ที่สังเกตได้และความกว้างของหน่วยงานที่เป็นเป้าหมาย

การกำหนดเป้าหมายทางไซเบอร์มีแนวโน้มที่จะสร้างผลประโยชน์ทางเศรษฐกิจและการทหาร

Microsoft สังเกตเห็นการกำหนดเป้าหมายอย่างกว้างขวางในประเทศเล็กๆ ทั่วโลกโดยกลุ่มภัยคุกคามของรัฐและรัฐในเครือของจีน โดยบ่งชี้ว่าจีนมีแนวโน้มว่าจะใช้หน่วยสืบราชการลับทางไซเบอร์เป็นส่วนประกอบของอิทธิพลทางเศรษฐกิจและการทหารทั่วโลก

จีน: ประเทศเป้าหมายสูงสุดและภาคอุตสาหกรรม



นักคิด/NGO สื่อ ไอที รัฐบาล และภาคการศึกษาเป็นกลุ่มที่ตกเป็นเป้าหมายมากที่สุดสำหรับกลุ่มภัยคุกคามในจีน ซึ่งน่าจะเป็นการรวบรวมข่าวกรองและการลาดตระเวนอย่างต่อเนื่อง

ขอบเขตของเป้าหมายรวมถึงแต่ไม่จำกัดเฉพาะประเทศในแอฟริกา แคริบเบียน ตะวันออกกลาง โอเชียเนีย และเอเชียใต้ โดยเน้นเฉพาะที่ประเทศเหล่านั้นในเอเชียตะวันออกเฉียงใต้และหมู่เกาะแปซิฟิก

สอดคล้องกับกลยุทธ์ BRI ของจีน กลุ่มภัยคุกคามที่มีฐานอยู่ในจีนกำหนดเป้าหมายหน่วยงานในอัฟกานิสถาน คาซัคสถาน มอริเชียส นามิเบีย และตรินิแดดและโตเบโก[20]

ตัวอย่างเช่น ตรินิแดดและโตเบโกเป็น ประเทศแรกในแคริบเบียนที่รับรองยุทธศาสตร์ BRI ของจีนในปี 2018 และจีนถือว่าจีนเป็นหุ้นส่วนที่สำคัญในภูมิภาคนี้ NICKEL มีการดำเนินงานเครือข่ายอย่างต่อเนื่องโดยมีเป้าหมายที่ตรินิแดดและโตเบโกตั้งแต่ปี 2021 ตัวอย่างเช่น ในเดือนมีนาคม 2022 NICKEL ได้ดำเนินกิจกรรมลาดตระเวนโดยมีเป้าหมายที่หน่วยงานรัฐบาล ซึ่งน่าจะมีวัตถุประสงค์ในการรวบรวมข้อมูลข่าวกรอง

จีนขยายการกำหนดเป้าหมายทั่วโลกเพื่อความได้เปรียบทางการแข่งขัน

ต่อไป

ในขณะเดียวกัน Microsoft สังเกตเห็นกลุ่มภัยคุกคามของรัฐและรัฐในเครือของจีนที่มุ่งเน้นการดำเนินงานเครือข่ายกับหน่วยงานในเอเชียตะวันออกเฉียงใต้และขยายไปยังประเทศในหมู่เกาะแปซิฟิก ขณะที่จีนเปลี่ยนลำดับความสำคัญทางทหารและเศรษฐกิจเพื่อรับมือกับความท้าทายของความสนใจใหม่ในภูมิภาคของสหรัฐฯ . ในเดือนมกราคม 2022 Microsoft สังเกตว่า RADIUM กำหนดเป้าหมายบริษัทพลังงานและหน่วยงานรัฐบาลที่เกี่ยวข้องกับพลังงานในเวียดนาม และหน่วยงานรัฐบาลชาวอินโดนีเซีย กิจกรรมของ RADIUM มีแนวโน้มที่จะสอดคล้องกับเป้าหมายเชิงกลยุทธ์ของจีนในทะเลจีนใต้[21] ในช่วงปลายเดือนกุมภาพันธ์และต้นเดือนมีนาคม GALLIUM ได้บุกรุกบัญชีมากกว่า 100 บัญชีที่เชื่อมโยงกับองค์กรระหว่างรัฐบาล (IGO) ที่มีชื่อเสียง ในภูมิภาคเอเชียตะวันออกเฉียงใต้ ช่วงเวลาของการกำหนดเป้าหมาย IGO ในภูมิภาคของ GALLIUM นั้นใกล้เคียงกับการประกาศกำหนดการประชุมระหว่างสหรัฐอเมริกาและผู้นำระดับภูมิภาค ผู้ดำเนินการ GALLIUM มักจะได้รับมอบหมายให้ตรวจสอบการสื่อสารและรวบรวมข่าวกรองก่อนงาน

เมื่อจีนขยายอิทธิพลในประเทศหมู่เกาะแปซิฟิก กิจกรรมของกลุ่มภัยคุกคามจีนก็ตามมา ในเดือนเมษายน จีนและหมู่เกาะโซโลมอนได้ลงนามในข้อตกลงด้านความปลอดภัยที่มีจุดประสงค์เพื่อ “ส่งเสริมสันติภาพและความมั่นคง” ข้อตกลงดังกล่าวอาจเปิดโอกาสให้จีนส่งกำลังตำรวจและทหารติดอาวุธไปยังหมู่เกาะโซโลมอน[22] ในเดือนพฤษภาคม จีนเป็นเจ้าภาพจัดการประชุมรัฐมนตรีต่างประเทศจีน-แปซิฟิก (PICs) ครั้งที่สองใน ฟิจิและเสนอที่จะพัฒนา “หุ้นส่วนทางยุทธศาสตร์ที่ครอบคลุม" เพื่อส่งเสริมผลประโยชน์ทางการเมือง วัฒนธรรม สังคม ความมั่นคง และการเปลี่ยนแปลงสภาพภูมิอากาศ และต่อสู้กับโรคระบาด[23] ในเวลาเดียวกัน ในเดือนพฤษภาคม Microsoft ตรวจพบมัลแวร์ของ GADOLINIUM ในระบบของรัฐบาลหมู่เกาะโซโลมอน RADIUM ยังรันโค้ดอันตรายบนระบบของบริษัทโทรคมนาคมในปาปัวนิวกินีอีกด้วย เราประเมินว่ากิจกรรมเหล่านี้น่าจะมีวัตถุประสงค์ในการรวบรวมข่าวกรองเพื่อสนับสนุนยุทธศาสตร์ระดับภูมิภาคโดยรวมของจีน

Microsoft หยุดชะงักการทำงาน NICKEL แต่กลุ่มภัยคุกคามแสดงให้เห็นถึงความเป็นไปได้

ในเดือนธันวาคม 2021 หน่วยอาชญากรรมดิจิทัลของ Microsoft (DCU) ที่ยื่นคำวิงวอนกับศาลเขตสหรัฐอเมริกาสำหรับภาคตะวันออกของเวอร์จิเนียกำลังมองหาผู้มีอำนาจที่จะยึดตามโดเมน 42 คำสั่งและการควบคุม (C2) ที่ควบคุมโดย NICKEL โดเมน C2 เหล่านี้ถูกนำมาใช้ในการดำเนินงานกับรัฐบาลหน่วยงานทางการทูตและองค์กรเอกชนทั่วทั้งอเมริกากลางและอเมริกาใต้, แคริบเบียน, ยุโรป และอเมริกาเหนือตั้งแต่เดือนกันยายน 2019[24] ผ่านการดำเนินการเหล่านี้ NICKEL ประสบความสำเร็จในการเข้าถึงระยะยาวไปยังหลายเอนทิตีและถอนข้อมูลอย่างต่อเนื่องจากผู้ตกเป็นเหยื่อบางอย่างตั้งแต่ปลาย 2019

ในฐานะที่ประเทศจีนยังคงสร้างความสัมพันธ์ทางเศรษฐกิจระดับทวิภาคีกับประเทศอื่นๆ ซึ่งมักจะอยู่ในข้อตกลงที่เกี่ยวข้องกับ BRI อิทธิพลทั่วโลกของจีนจะเติบโตต่อไป เราประเมินสถานะของจีนและผู้ให้บริการด้านการคุกคามในภาครัฐจะติดตามเป้าหมายในภาครัฐบาลองค์กรทางการทูตและ NGO เพื่อรับข้อมูลเชิงลึกใหม่ๆ มีแนวโน้มที่จะแสวงหาหน่วยสืบราชการทางเศรษฐกิจหรือวัตถุประสงค์ในการเก็บข้อมูลอัจฉริยะแบบดั้งเดิม ตั้งแต่การหยุดชะงักของ Microsoft NICKEL ได้กำหนดเป้าหมายหน่วยงานรัฐบาลหลายหน่วย ซึ่งมีแนวโน้มที่จะพยายามที่จะเข้าถึงสิทธิการเข้าถึงที่หายไปอีกครั้ง ระหว่างช่วงปลายเดือนมีนาคมและพฤษภาคม 2022 NICKEL ถูกบุกรุกอย่างน้อยห้าหน่วยงานรัฐบาลทั่วโลก ซึ่งจะแสดงให้เห็นว่ากลุ่มมีจุดเข้าใช้งานเพิ่มเติมสำหรับเอนทิตีเหล่านั้นหรือได้การเข้าถึงผ่านโดเมน C2 ใหม่อีกครั้ง การคงอยู่ของ NICKEL ในการประนีประนอมกับหน่วยงานรัฐบาลเดียวกันซ้ำแล้วซ้ำเล่าทั่วโลก บ่งชี้ถึงความสำคัญของงานในระดับสูง

> จีนมีจุดยืนที่ชัดเจนมากขึ้นเกี่ยวกับนโยบายต่างประเทศ เราประเมินว่าการจารกรรมทางเศรษฐกิจโดยใช้ไซเบอร์และการรวบรวมข่าวกรองมีแนวโน้มที่จะดำเนินต่อไป

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. เพิ่มการป้องกันทางไซเบอร์เพื่อบรรเทาภัยคุกคามทางไซเบอร์เชิงรุก การคงอยู่ของผู้คุกคามในจีนทำให้องค์กรต่างๆ ต้องระบุ ป้องกัน ตรวจจับ และตอบโต้การบุกรุกที่อาจเกิดขึ้นได้ทันท่วงที
2. ผู้คุกคามใช้งานตามกำหนดเวลา[25] เป็นวิธีการทั่วไปในการคงอยู่และการหลีกเลี่ยงการป้องกัน ตรวจสอบให้แน่ใจว่าสภาพแวดล้อมของคุณใช้หลักเกณฑ์ด้านความปลอดภัยเพิ่มเติมเพื่อป้องกันเทคนิคที่ใช้กันทั่วไปนี้[26]
3. เรายังคงสังเกตการใช้ web shell เป็นเวคเตอร์เริ่มต้นในเครือข่ายเป้าหมาย[27] องค์กรควรเสริมความแข็งแกร่งให้กับระบบของตนจากการโจมตีของเว็บเชลล์ที่สามารถให้ผู้โจมตีเข้าถึงเพื่อเรียกใช้คำสั่งระยะไกล[28]

ลิงค์ไปยังข้อมูลเพิ่มเติม

- NICKEL กำหนดเป้าหมายองค์กรรัฐบาลทั่วละตินอเมริกาและยุโรป | Microsoft Threat Intelligence Center (MSTIC), หน่วยรักษาความปลอดภัยแบบดิจิทัล Microsoft(DSU)
- การปกป้องผู้คนจากการโจมตีทางไซเบอร์ล่าสุด | Microsoft On the Issues

อิหร่านก้าวร้าวมากขึ้นหลังจากการเปลี่ยนผ่านอำนาจ

Microsoft ได้สังเกตว่ากลุ่มรัฐของอิหร่านและผู้เกี่ยวข้องเพิ่มความเร็วและขอบเขตของการโจมตีทางไซเบอร์ต่ออิสราเอล ขยายการโจมตีด้วยแรนซัมแวร์นอกเหนือจากศัตรูในระดับภูมิภาคไปยังเหยื่อของสหรัฐฯ และสหภาพยุโรป และกำหนดเป้าหมายโครงสร้างพื้นฐานที่สำคัญของสหรัฐฯ เป็นอย่างน้อยเพื่อเตรียมพร้อมสำหรับการโจมตีทางไซเบอร์ที่อาจทำลายล้าง

การรุกรานทางไซเบอร์ที่เพิ่มขึ้นของผู้ดำเนินการของรัฐอิหร่านได้ติดตามการเปลี่ยนแปลงอำนาจของประธานาธิบดีในช่วงฤดูร้อนปี 2021 ประธานาธิบดีอิบราฮิม ไรซี สายแข็งได้เข้ามาแทนที่ประธานาธิบดีฮัสซัน โรฮานีสายกลาง ตรงกันข้ามกับ Raisi ซึ่งเป็นลูกบุญธรรมของผู้นำสูงสุดและเป็นพันธมิตรที่ใกล้ชิดของกองกำลังพิทักษ์การปฏิวัติอิสลาม (IRGC) อดีตประธานาธิบดี Rouhani ชื่นชอบการทูต มักทำให้เขาขัดแย้งกับผู้นำสูงสุดและผู้นำระดับสูงของ IRGC[29] ความเห็นอันเฉียบขาดของคณะบริหาร Raisi ดูเหมือนจะทำให้ความตึงใจของผู้ดำเนินการชาวอิหร่านมีท่าทีที่กล้าแสดงออกมากขึ้นกับอิสราเอลและชาติตะวันตก โดยเฉพาะอย่างยิ่งสหรัฐอเมริกา แม้ว่าการสู้รบทางการทูตจะเริ่มต้นใหม่อีกครั้ง รื้อฟื้นข้อตกลงนิวเคลียร์กับอิหร่าน

การก้าวเพิ่มขึ้นและขอบเขตของการโจมตีทางไซเบอร์ของอิหร่านต่ออิสราเอล

ภายในไม่กี่สัปดาห์หลังจากที่ Raisi ก่อตั้งทีมนโยบายต่างประเทศของเขาเสร็จสิ้น[30] ผู้มีบทบาทของรัฐอิหร่านก็กลับมาโจมตีทางไซเบอร์แบบทำลายล้างต่ออิสราเอลอีกครั้งอย่างรวดเร็วกว่าปีก่อนหน้า แรนซัมแวร์และการโจมตีแบบแฮ็กและรั่วเหล่านี้ดำเนินการทุกสองสามสัปดาห์ตั้งแต่เดือนกันยายน และเกี่ยวข้องกับผู้ที่เกี่ยวข้องกับอิหร่านอย่างน้อยสามคน บ่งชี้ว่าการโจมตีอาจเป็นส่วนหนึ่งของการรณรงค์ตอบโต้อิสราเอลทั่วประเทศ ในกรณีอย่างน้อยหนึ่งกรณี Microsoft ประเมินว่าการโจมตีด้วยแรนซัมแวร์ต่อองค์กรของอิสราเอลในช่วงปลายปี 2021 มีวัตถุประสงค์เพื่อปกปิดการโจมตีเพื่อลบข้อมูลพื้นฐาน การวิเคราะห์มัลแวร์ของ Microsoft ระบุว่าแรนซัมแวร์ที่ส่งไปยังเหยื่อนั้นได้รับการตั้งโปรแกรมให้รันมัลแวร์ไวเปอร์ตามการเข้ารหัส

ภายในปี 2022 การโจมตีทางไซเบอร์ของอิหร่านได้ทวีความรุนแรงขึ้นทั้งการเลือกเป้าหมายและรูปแบบการโจมตี ในเดือนกุมภาพันธ์ DEV-0198 พยายามโจมตีทำลายโครงสร้างพื้นฐานที่สำคัญของอิสราเอล Microsoft ยังประเมินว่านักแสดงในสังกัดของอิหร่านน่าจะเป็นผู้รับผิดชอบการโจมตีทางไซเบอร์ที่ซับซ้อนซึ่งทำให้เกิดไซเรนจรวดฉุกเฉินในอิสราเอลในเดือนมิถุนายน โดยอาจใช้ซอฟต์แวร์ที่ปรับแต่งเสียงผ่านเครือข่าย IP

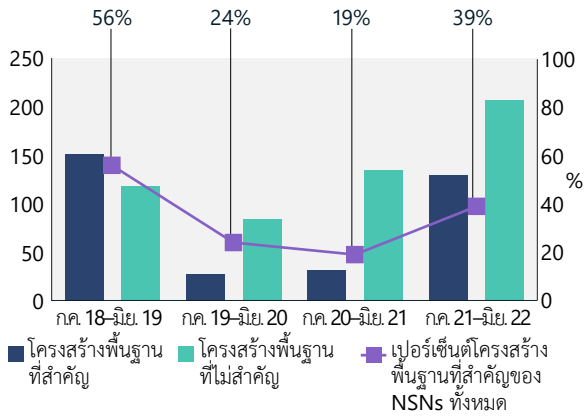
ภัยคุกคามของอิหร่านต่อโครงสร้างพื้นฐานที่สำคัญของสหรัฐฯ และอิสราเอลเพิ่มขึ้นตลอดทั้งปี

ผู้มีบทบาทของรัฐอิหร่านที่ Microsoft ประเมินนั้นมีความเกี่ยวข้องกับ IRGC (PHOSPHORUS และ DEV-0198) ที่กำหนดเป้าหมายโครงสร้างพื้นฐานที่สำคัญของสหรัฐฯ และอิสราเอลตั้งแต่ปลายปี 2021 ถึงกลางปี 2022 เป้าหมายที่เป็นไปได้คือเพื่อให้เตหะรานมีทางเลือกในการตอบโต้ภาคส่วนที่เจ้าหน้าที่ IRGC อาวุโสกล่าวโทษสหรัฐฯ และอิสราเอลว่าก่อกวนในอิหร่าน[31] เราประเมินว่ากิจกรรมนี้เชื่อมโยงกัน ถ้อยแถลงเมื่อปลายเดือนตุลาคม 2021 โดยนายพล Gholamreza Jalali ของ IRGC หัวหน้าองค์กรป้องกันเชิงรับของอิหร่าน ซึ่งสะท้อนข้อกล่าวหาจากบุคคลผู้ทรงอิทธิพลอื่นๆ ภายในระบอบการปกครองที่ว่าสหรัฐอเมริกาและอิสราเอลทำการโจมตีทางไซเบอร์บนท่าเรือ ทางรถไฟ และสถานีเติมน้ำมันของอิหร่าน[32] Jalali กล่าวข้อกล่าวหานี้เป็นครั้งที่สองในคำพูดที่เตรียมไว้ระหว่างการปราศรัยในวันศุกร์ที่เว็บไซต์ปราศรัยบนโพเดียมโดยมีภาพของขีปนาวุธกระทบคำว่า "USA" โดยแนะนำว่าผู้อาวุโสของเขามีมุมมองเดียวกัน[33]

PHOSPHORUS เริ่มทำการสแกนอย่างกว้างขวางในองค์กรของสหรัฐฯ ในเดือนตุลาคม 2021 เพื่อหาช่องโหว่ของ Fortinet และ ProxyShell ที่ยังไม่ได้แพตช์ เมื่อถูกบุกรุก ระบบที่ไม่ได้แพตช์เหล่านี้จะถูกใช้เพื่อดำเนินการโจมตีแรนซัมแวร์ ในหลายกรณีกับโครงสร้างพื้นฐานที่สำคัญในสหรัฐอเมริกาและประเทศตะวันตกอื่นๆ สิ่งเหล่านี้ถือเป็นกรณีแรกที่ได้รับการยืนยันจากการโจมตีแรนซัมแวร์ในเครือรัฐของอิหร่านนอกตะวันออกกลาง หลังจากการโจมตีทางไซเบอร์กับสถานีเติมน้ำมันของอิหร่านในปลายเดือนตุลาคม Microsoft สังเกตเห็นการโจมตีด้วยแรนซัมแวร์ของอิหร่านที่พุ่งสูงขึ้นกับบริษัทของสหรัฐฯ ซึ่งบ่งบอกถึงความสัมพันธ์ที่เป็นไปได้

ในเวลาเดียวกัน PHOSPHORUS ได้ย้ายเข้าสู่การกำหนดเป้าหมายโดยตรง ซึ่งมักจะใช้การฟิชชิงแบบสเปียร์ของบริษัทโครงสร้างพื้นฐานที่สำคัญที่มีชื่อเสียงของสหรัฐฯ ซึ่งรวมถึงท่าเรือและสนามบินหลัก ระบบขนส่งมวลชน บริษัทสาธารณูปโภค และบริษัทน้ำมันและก๊าซ การกำหนดเป้าหมายนี้ซึ่งมักดำเนินการผ่านฟิชชิงแบบสเปียร์ มีผลจนถึงกลางปี 2022 เป้าหมายที่สอดคล้องโดยตรงกับภาคส่วนต่างๆ เตหะรานกล่าวโทษสหรัฐฯ และอิสราเอลสำหรับการโจมตีในอิหร่าน และมีแนวโน้มว่าจะทำให้อิหร่านมีทางเลือกในการตอบโต้ การประนีประนอมกับเป้าหมายที่ใกล้เคียงกันจะเปิดโอกาสให้ยับยั้งการโจมตีดังกล่าวในอนาคต ในขณะเดียวกันก็พยายามหลีกเลี่ยงการบานปลายด้วยการส่งสัญญาณถึงสาเหตุของการโจมตีโดยไม่ยอมรับความผิด

การฟื้นตัวของการกำหนดเป้าหมายโครงสร้างพื้นฐานของอิหร่าน



การกำหนดเป้าหมายโครงสร้างพื้นฐานที่สำคัญของอิหร่านเพิ่มขึ้นเป็นระดับสูงสุดที่สังเกตได้ตั้งแต่ช่วงปลายปี 2018 ถึงต้นปี 2019 เราใช้คำสั่งนโยบายประธานาธิบดีสหรัฐฯ 21 (PPD-21) เพื่อพิจารณาว่าบริษัทมีคุณสมบัติตรงตามเกณฑ์ของโครงสร้างพื้นฐานที่สำคัญหรือไม่ (กรกฎาคม 2021–มิถุนายน 2022)

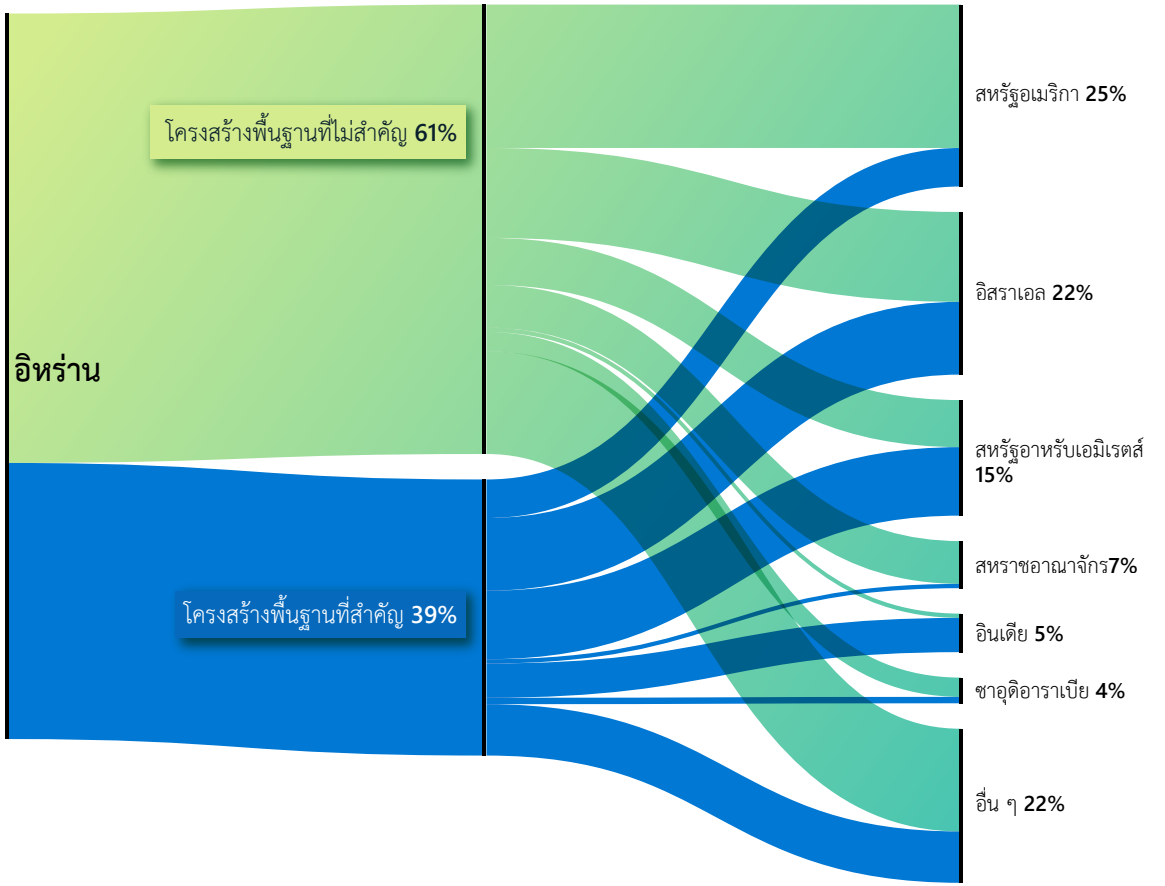
อิหร่านก้าวร้าวมากขึ้นหลังจากการเปลี่ยนผ่านอำนาจ

ต่อไป

ในอิสราเอล DEV-0198 กำหนดเป้าหมายไปที่การรถไฟของอิสราเอล บริษัทโลจิสติกส์ ผู้ให้บริการซอฟต์แวร์ของบริษัทโลจิสติกส์ และบริษัทเชื้อเพลิงโดยเน้นที่สถานีบริการน้ำมัน ในช่วงต้นปี 2022 กลุ่มดังกล่าวได้ทำการโจมตีเครือข่ายของบริษัทโลจิสติกส์รายใหญ่ของอิสราเอล ซึ่งทำให้บริษัทต้องปิดคอมพิวเตอร์และการดำเนินงานบางส่วนเพื่อยับยั้งการโจมตี ในอีกกรณีหนึ่ง เราสังเกตเห็นว่ากลุ่มพยายามเข้าถึงเครือข่ายของผู้ให้บริการขนส่งรายใหญ่ของอิสราเอลผ่านข้อมูลประจำตัวที่ถูกขโมยหรือใช้ซ้ำ ในขณะเดียวกัน DEV-0343 นักแสดงชาวอิหร่านอีกคนซึ่งมีเป้าหมายในการป้องกันประเทศ การขนส่งทางทะเล และบริษัทภาพถ่ายดาวเทียมได้แนะนำการเชื่อมโยงไปยัง IRGC ซึ่งเป็นบัญชีที่ถูกบุกรุกที่การขนส่งของอิสราเอลและหน่วยงานที่เกี่ยวข้องกับท่าเรือตลอดช่วงต้นปี 2021

กลุ่มภัยคุกคามจากอิหร่านมีแนวโน้มที่จะยังคงเป็นภัยคุกคามต่อบริษัทขนส่งและพลังงานของสหรัฐฯ และอิสราเอล โดยเฉพาะอย่างยิ่งเมื่อความพยายามทางการทูตในการฟื้นฟูข้อตกลงนิวเคลียร์ของอิหร่านและวอชิงตันเทลอาวีฟ และเตหะรานแสวงหาวิธีการบีบบังคับทางเลือกอื่นเพื่อใช้ประโยชน์จากข้อตกลง

โครงสร้างพื้นฐานที่สำคัญของอิหร่านกำหนดเป้าหมายตามประเทศ



การกำหนดเป้าหมายโครงสร้างพื้นฐานที่สำคัญของอิหร่านเกิดขึ้นอย่างชัดเจนที่สุดต่อองค์กรของอิสราเอล สหรัฐอาหรับเอมิเรตส์ และสหรัฐ

ผู้ดำเนินการชาวอิหร่านมีแนวโน้มที่จะยังคงเป็นภัยคุกคามต่อบริษัทขนส่งและพลังงานของสหรัฐฯ และอิสราเอลในปีหน้า

กลุ่มชาวอิหร่านได้ขยายการโจมตีด้วยแรนซัมแวร์เกินกว่าศัตรูระดับภูมิภาค และมุ่งเป้าไปที่เป้าหมายโครงสร้างพื้นฐานที่สำคัญของสหรัฐฯ และอิสราเอล

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ปรับปรุงสุขอนามัยทางไซเบอร์โดยรวมขององค์กรของคุณด้วยการเปิดใช้งานโซลูชันที่ไม่ต้องใช้รหัสผ่าน เช่น MFA และบังคับใช้สำหรับการเชื่อมต่อระยะไกลทั้งหมดเพื่อลดข้อมูลประจำตัวที่อาจถูกบุกรุก
2. ประเมินความถูกต้องของการรับส่งข้อมูลอีเมลขาเข้าทั้งหมดเพื่อให้แน่ใจว่าที่อยู่ผู้ส่งถูกต้องตามกฎหมาย
3. แพทช์เร็วและบ่อย[34]
4. ตรวจทานและตรวจสอบความสัมพันธ์ของคู่ค้าแต่ละรายกับผู้ให้บริการเพื่อลดการอนุญาตที่ไม่จำเป็นระหว่างองค์กรของคุณกับผู้ให้บริการ อัปสตรีม Microsoft แนะนำให้ลบสิทธิ์การเข้าถึงสำหรับความสัมพันธ์ของคู่ค้าที่ดูไม่คุ้นเคยหรือยังไม่ได้ตรวจสอบโดยทันที [35]

ลิงค์ไปยังข้อมูลเพิ่มเติม

- การกำหนดเป้าหมายของอิหร่านในภาคไอทีที่เพิ่มขึ้น | ศูนย์ข่าวกรองภัยคุกคามของ Microsoft (MSTIC), หน่วยรักษาความปลอดภัยแบบดิจิทัล Microsoft (DSU)
- DEV-0343 ที่เชื่อมโยงกับอิหร่านโดยกำหนดเป้าหมายการป้องกัน, GIS และภาคการเดินเรือ | ศูนย์ข่าวกรองภัยคุกคามของ Microsoft (MSTIC), หน่วยรักษาความปลอดภัยดิจิทัลของ Microsoft (DSU)

กลุ่มที่มีฐานอยู่ในเลบานอนและเชื่อมโยงกับอิหร่านที่กำหนดเป้าหมายไปยังอิสราเอล

Microsoft ตรวจสอบกิจกรรมการคุกคามทางไซเบอร์โดยไม่คำนึงถึงแพลตฟอร์ม เหยื่อที่เป็นเป้าหมาย หรือภูมิภาคทางภูมิศาสตร์ เรารักษาการมองเห็นและการตามล่าภัยคุกคามทั่วโลกเพื่อเขียนการตรวจจับที่ดีขึ้นสำหรับลูกค้าของเรา

แม้ว่าภัยคุกคามจากรัสเซีย จีน อิหร่าน และเกาหลีเหนือจะเป็นตัวแทนของกิจกรรมตัวแสดงของรัฐชาติส่วนใหญ่ที่เราสังเกต แต่เรายังติดตามและสื่อสารเกี่ยวกับภัยคุกคามจากประเทศสมาชิก NATO และประเทศประชาธิปไตยและประเทศประชาธิปไตย ปีที่แล้ว เราได้นำเสนอกิจกรรมโดยนักแสดงจากตุรกี (SILICON) และนักแสดงจากเวียดนาม (BISMUTH) ในปีนี้ เรากำลังขยายรายละเอียดของกลุ่มที่มีฐานอยู่ในเลบานอนที่เราเปิดเผยต่อสาธารณะก่อนหน้านี้[36]

Microsoft ค้นพบกลุ่มฐานในเลบานอนที่ไม่มีเอกสารก่อนหน้านี้ ซึ่งเราประเมินด้วยความมั่นใจในระดับปานกลางที่ดำเนินการโดยประสานงานกับผู้ดำเนินการที่สังกัดกระทรวงข่าวกรองและความมั่นคงของอิหร่าน (MOIS) ความร่วมมือหรือทิศทางดังกล่าวจากเตหะรานจะสอดคล้องกับการเปิดเผยตั้งแต่ช่วงปลายปี 2020 ที่รัฐบาลอิหร่านกำลังใช้บุคคลที่สามเพื่อดำเนินการทางไซเบอร์ ซึ่งมีแนวโน้มที่จะเพิ่มความน่าเชื่อถือที่ปฏิเสธได้ของอิหร่าน

ในกิจกรรมที่สังเกตได้ POLONIUM กำหนดเป้าหมายหรือประนีประนอมองค์กรในอิสราเอลสองโหลและ IGO หนึ่งแห่งที่ดำเนินงานในเลบานอนระหว่างเดือนกุมภาพันธ์ถึงพฤษภาคม 2022 ก่อนที่ Microsoft จะหยุดชะงักและเปิดเผยกิจกรรมต่อสาธารณะ เกือบครึ่งหนึ่งขององค์กรในอิสราเอลเป็นส่วนหนึ่งของอุตสาหกรรมการป้องกันประเทศของอิสราเอลหรือมีความเชื่อมโยงกับบริษัทด้านการป้องกันของอิสราเอล ซึ่งบ่งชี้ว่ากลุ่มนี้มีความสนใจคล้ายกับอิหร่านในการรวบรวมข้อมูลข่าวกรองและ/หรือตอบโต้อิสราเอลโดยตรง[37]

การเชื่อมโยงที่ได้รับการประเมินของ POLONIUM ไปยังกลุ่ม MOIS นั้นขึ้นอยู่กับการทับซ้อนของเหยื่อที่สังเกตได้และความเหมือนกันของเครื่องมือและเทคนิคต่างๆ

- เหยื่อที่ทับซ้อนกัน: กลุ่มรัฐของอิหร่านที่เชื่อมโยงกับ MOIS ของอิหร่าน ซึ่ง Microsoft ติดตามว่าเป็น MERCURY ซึ่งก่อนหน้านี้ได้ประนีประนอมเหยื่อหลายรายของ POLONIUM ซึ่งบ่งชี้ถึงการบรรจบกันของข้อกำหนดในภารกิจหรือการ “ส่งต่อ” เหยื่อระหว่างกลุ่ม
- เครื่องมือและเทคนิคทั่วไป: คล้ายกับ POLONIUM, MSTIC สังเกต DEV-0588 (หรือที่เรียกว่า CopyKittens) มักใช้ AirVPN สำหรับการดำเนินการ และ DEV-0133 (หรือที่เรียกว่า Lyceum[38]) ใช้ OneDrive สำหรับ C2 และการกรอง POLONIUM ใช้ผู้ให้บริการระบบคลาวด์เพื่อประนีประนอมกับบริษัทการบินและสำนักงานกฎหมายของอิสราเอล เช่นเดียวกับผู้มีบทบาทของรัฐอิหร่าน[39]

POLONIUM ใช้ชุดของรากเทียมแบบกำหนดเองโดยใช้บริการคลาวด์สำหรับ C2 และการกรองข้อมูล โดยเฉพาะ OneDrive และ DropBox POLONIUM มักจะสร้างแอปพลิเคชัน OneDrive เฉพาะสำหรับเป้าหมาย ซึ่งมีแนวโน้มที่จะหลบเลี่ยงการตรวจจับ

ในเดือนมิถุนายน 2022 Microsoft ระงับแอปพลิเคชัน OneDrive ที่สร้างโดย POLONIUM มากกว่า 20 รายการ แจ้งเตือนองค์กรที่ได้รับผลกระทบ และปรับใช้ชุดข้อมูลอัปเดตด้านความปลอดภัยเพื่อกักกันเครื่องมือที่พัฒนาโดย POLONIUM

Microsoft ตรวจพบและปิดการใช้งาน OneDrive ในทางที่ผิดของ POLONIUM เป็น C2 ได้สำเร็จ

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. อัปเดตเครื่องมือป้องกันไวรัส[40] และตรวจสอบว่าการป้องกันระบบคลาวด์[41] เปิดอยู่เพื่อตรวจหาตัวบ่งชี้ที่เกี่ยวข้อง
2. สำหรับลูกค้าที่มีความสัมพันธ์กับผู้ให้บริการให้ตรวจสอบและตรวจสอบความสัมพันธ์ของคู่ค้าทั้งหมดเพื่อลดการอนุญาตที่ไม่จำเป็นระหว่างองค์กรของคุณและผู้ให้บริการต้นทาง[2] ลบสิทธิ์การเข้าถึงสำหรับความสัมพันธ์ของคู่ค้าที่ไม่คุ้นเคยหรือไม่ได้รับการตรวจสอบทันที

ลิงค์ไปยังข้อมูลเพิ่มเติม

- เปิดเผยกิจกรรมและโครงสร้างพื้นฐานของ POLONIUM ที่กำหนดเป้าหมายองค์กรของอิสราเอล | ศูนย์ข่าวกรองภัยคุกคามของ Microsoft (MSTIC), หน่วยรักษาความปลอดภัยดิจิทัลของ Microsoft (DSU)
- MERCURY ใช้ประโยชน์จากช่องโหว่ Log4j 2 ในระบบที่ไม่ได้แพตช์เพื่อกำหนดเป้าหมายองค์กรในอิสราเอล | ศูนย์ข่าวกรองภัยคุกคามของ Microsoft (MSTIC), ทีมวิจัย Microsoft 365 Defender, ข่าวกรองภัยคุกคามของ Microsoft Defender

ความสามารถทางไซเบอร์ของเกาหลีเหนือใช้เพื่อบรรลุเป้าหมายหลักสามประการของระบอบการปกครอง

ลำดับความสำคัญทางไซเบอร์ของเกาหลีเหนือในปีที่ผ่านมาสะท้อนให้เห็นถึงลำดับความสำคัญระดับโลกที่ระบุไว้ของรัฐบาล Kim Jong Un เน้นความสำคัญสามประการของการสร้างขีดความสามารถในการป้องกัน หนุนเศรษฐกิจที่กำลังดิ้นรนของประเทศ และประกันเสถียรภายในประเทศในประเด็นสำคัญหลายประการ[43] การดำเนินการของผู้มีบทบาทในเกาหลีเหนืออย่างชัดเจน แสดงว่ามีการใช้ไซเบอร์เพื่อบรรลุเป้าหมายทั้งสามนี้

ผู้มีบทบาทของรัฐเกาหลีเหนือใช้กลวิธีที่หลากหลายเพื่อพยายามเจาะกลุ่มบริษัทการบินและอวกาศทั่วโลก

กลุ่มภัยคุกคามของรัฐเกาหลีเหนือ โดยหลักคือ CERIUM และ ZINC ใช้กลวิธีที่หลากหลายเพื่อพยายามเจาะเครือข่ายบริษัทด้านการป้องกันและอวกาศทั่วโลก ในขณะที่เกาหลีเหนือเริ่มต้นการทดสอบขีปนาวุธในช่วงเวลาที่ดุเดือดที่สุดเท่าที่เคยมีมาในช่วงครึ่งแรกของปี 2022 เกาหลีเหนือได้ใช้หน่วยสืบราชการลับทางไซเบอร์เพื่อช่วยให้นักวิจัยของเกาหลีเหนือมีความได้เปรียบในการพัฒนาระบบป้องกันของชนพื้นเมืองและมาตรการตอบโต้เพื่อความก้าวหน้าของศัตรู

เราสังเกตเห็นว่า COPERNICIUM กำหนดเป้าหมายบริษัทที่เกี่ยวข้องกับสกุลเงินดิจิทัลหลายแห่งทั่วโลก ซึ่งมักจะประสบความสำเร็จ เพื่อช่วยสนับสนุนเศรษฐกิจที่กำลังดิ้นรนของเกาหลีเหนือ แม้ว่าเราไม่สามารถยืนยันได้ว่ากลุ่มสามารถถอนเงินออกไปได้หรือไม่หลังจากการประนีประนอม แต่เราสังเกตเห็นว่า COPERNICIUM แพร่ระบาดในเครื่องนับสิบเครื่องโดยส่งเอกสารที่เป็นอันตรายซึ่งปลอมแปลงเป็นข้อเสนอจากบริษัทคริปโตเคอเรนซีอื่นๆ

ในที่สุด กลุ่ม Microsoft ติดตามในขณะที่ DEV-0215 ทำงานเพื่อรักษาเสถียรภาพและความภักดีในเกาหลีเหนือ โดยกำหนดเป้าหมายไปที่องค์กรข่าวที่รายงานปัญหาเกาหลีเหนือ หน่วยงานเหล่านี้มีแหล่งที่มาทั้งในเกาหลีเหนือและในชุมชนของผู้แปรพักตร์ ซึ่งเปียงยางมองว่าเป็นภัยคุกคามที่มีอยู่ นอกจากนี้ กลุ่มยังทำงานเพื่อเข้าถึงเครือข่ายของกลุ่มคริสเตียนที่พูดภาษาเกาหลี ซึ่งมีแนวโน้มที่จะเปิดเผยต่อต้านเกาหลีเหนือและทำงานอย่างแข็งขันกับผู้แปรพักตร์ชาวเกาหลีเหนือ

การกำหนดเป้าหมายของบริษัทป้องกันและการบินและอวกาศ

ผู้มีบทบาทของรัฐเกาหลีเหนือที่นำโดย CERIUM และ ZINC ใช้ความพยายามอย่างมากในการพัฒนากลยุทธ์ที่มุ่งเจาะกลุ่มบริษัทด้านการป้องกันประเทศและการบินและอวกาศ CERIUM ตรวจสอบเครือข่ายส่วนตัวเสมือน (VPN) ของเกาหลีใต้ซ้ำๆ โดยการดาวน์โหลดไคลเอ็นต์และมองหาจุดอ่อน นอกจากนี้ยังดาวน์โหลดแอปพลิเคชันทั่วไปที่ใช้โดยลูกค้าทางทหารและรัฐบาลของเกาหลีใต้ ซึ่งน่าจะมองหาช่องโหว่ กลุ่มติดตามเหตุการณ์ปัจจุบันอย่างใกล้ชิดและเขียนเอกสารล่อใหม่ซึ่งใช้หัวข้อที่มีรายละเอียดสูงเป็นเหยื่อล่อเพื่อกระตุ้นให้เป้าหมายคลิกที่โปรแกรมปฏิบัติการและลิงก์มัลแวร์

ทั้ง ZINC และ CERIUM ใช้สื่อสังคมออนไลน์และวิศวกรรมสังคมในแคมเปญ ZINC มีความเชี่ยวชาญเป็นพิเศษในการสร้างโปรไฟล์ปลอมบน LinkedIn และเว็บไซต์โซเชียลมีเดียระดับมืออาชีพอื่นๆ โดยผู้ดำเนินการได้สวมรอยเป็นนายหน้าให้กับบริษัทด้านการป้องกันประเทศและการบินและอวกาศรายใหญ่ เมื่อใช้โปรไฟล์เหล่านี้ พวกเขาส่งลิงก์หรือไฟล์แนบที่เป็นอันตรายไปยังผู้ที่อาจตกเป็นเหยื่อโดยใช้ข้อความโดยตรงบนโซเชียลมีเดียหรืออีเมล

นอกเหนือจากพนักงานของบริษัทแล้ว CERIUM ยังกำหนดเป้าหมายไปยังสมาชิกของกองทัพเกาหลีใต้ในวงกว้าง โดยแสดงความสนใจเป็นพิเศษทั้งในสถาบันการทหารของเกาหลีใต้และสมาชิกกองทัพที่ทำงานด้านวิชาการ

กำหนดเป้าหมายสกุลเงินดิจิทัลเพื่อรักษาสมดุลของการสูญเสีย

ตั้งแต่สหประชาชาติคว่ำบาตรในปี 2016 เศรษฐกิจของเกาหลีเหนือยังคงหดตัว บวกกับภัยธรรมชาติ เช่น น้ำท่วม[44] และภัยแล้ง[45] ตลอดจนการปิดพรมแดนเพื่อนำเข้าสินค้าเกือบทั้งหมดนับตั้งแต่เกิดการระบาดของโควิด-19 ในต้นปี 2020[46] แม้ว่าเกาหลีเหนือจะเปิดพรมแดนเพื่อการค้ากับจีนช่วงสั้นๆ ในต้นปี 2022 ไม่นานพวกเขาก็ปิดอีกครั้ง[47] ในช่วงกลางเดือนพฤษภาคม เกาหลีเหนือรายงานผู้ป่วยโควิด-19 ภายในประเทศรายแรก[48] ตั้งแต่นั้นเป็นต้นมา ได้ใช้กลยุทธ์ “ศูนย์โควิด” แบบจีนในการปิดล้อมจำนวนมากเพื่อต่อสู้กับไวรัสซึ่งส่งผลกระทบในทางลบต่อเศรษฐกิจที่เปราะบางอยู่แล้วของเกาหลีเหนือ

กลุ่มรัฐของเกาหลีเหนือ COPERNICIUM พยายามชดเชยรายได้บางส่วนที่สูญเสียไปด้วยการขโมยเงิน—โดยทั่วไปจะอยู่ในรูปของสกุลเงินดิจิตอล—จากบริษัทใดๆ ที่สามารถเจาะเครือข่ายได้ เราเห็นเครื่องหลายสิบเครื่องถูกบุกรุกซึ่งเป็นของบริษัทที่เกี่ยวข้องกับสกุลเงินดิจิทัลในสหรัฐอเมริกา แคนาดา ยุโรป และทั่วเอเชีย COPERNICIUM ยังทำลายเครื่องจักรของบริษัทที่เกี่ยวข้องกับสกุลเงินดิจิทัลภายในจีน ซึ่งเป็นพันธมิตรที่แข็งแกร่งที่สุดของเกาหลีเหนือ ทั้งในแผ่นดินใหญ่และในฮ่องกง กลุ่มพึ่งพาสื่อสังคมออนไลน์อย่างมากในการลาดตระเวนและเข้าหาเป้าหมายในระยะแรก ผู้ดำเนินการจะสร้างโปรไฟล์ที่แสร้งทำเป็นนักพัฒนาหรือเจ้าหน้าที่อาวุโสในธุรกิจที่เกี่ยวข้องกับสกุลเงินดิจิทัล จากนั้นพวกเขาจะสร้างความสัมพันธ์กับผู้ที่อยู่ในอุตสาหกรรม โดยส่งลิงก์หรือไฟล์ที่เป็นอันตรายเมื่อพวกเขาสร้างสายสัมพันธ์แล้ว

ความสามารถทางไซเบอร์ของเกาหลีเหนือใช้เพื่อบรรลุเป้าหมายหลักสามประการของระบอบการปกครอง

ต่อไป

กลุ่มที่เกี่ยวข้องกับ PLUTONIUM พัฒนาและปรับใช้แรนซัมแวร์

กลุ่มผู้มีบทบาทที่มาจากเกาหลีเหนือที่ Microsoft ติดตามว่า DEV-0530 เริ่มพัฒนาและใช้แรนซัมแวร์ในการโจมตีในเดือนมิถุนายน 2021 กลุ่มนี้ซึ่งเรียกตัวเองว่า H0lyGh0st ใช้เพย์โหลดแรนซัมแวร์ที่มีชื่อเดียวกันสำหรับแคมเปญและประสบความสำเร็จในการบุกรุกธุรกิจขนาดเล็กในหลายประเทศอย่างเร็วที่สุดในเดือนกันยายน 2021

Microsoft ประเมินว่า DEV-0530 มีการเชื่อมต่อกับกลุ่มอื่นในเกาหลีเหนือที่ถูกติดตามในชื่อ PLUTONIUM (หรือที่เรียกว่า DarkSeoul หรือ Andariel) แม้ว่าการใช้แรนซั่มแวร์ H0lyGh0st ในแคมเปญจะไม่ซ้ำกับ DEV-0530 แต่ MSTIC สังเกตการสื่อสารระหว่างสองกลุ่มเช่นเดียวกับ DEV-0530 โดยใช้เครื่องมือที่สร้างขึ้นโดย PLUTONIUM โดยเฉพาะ

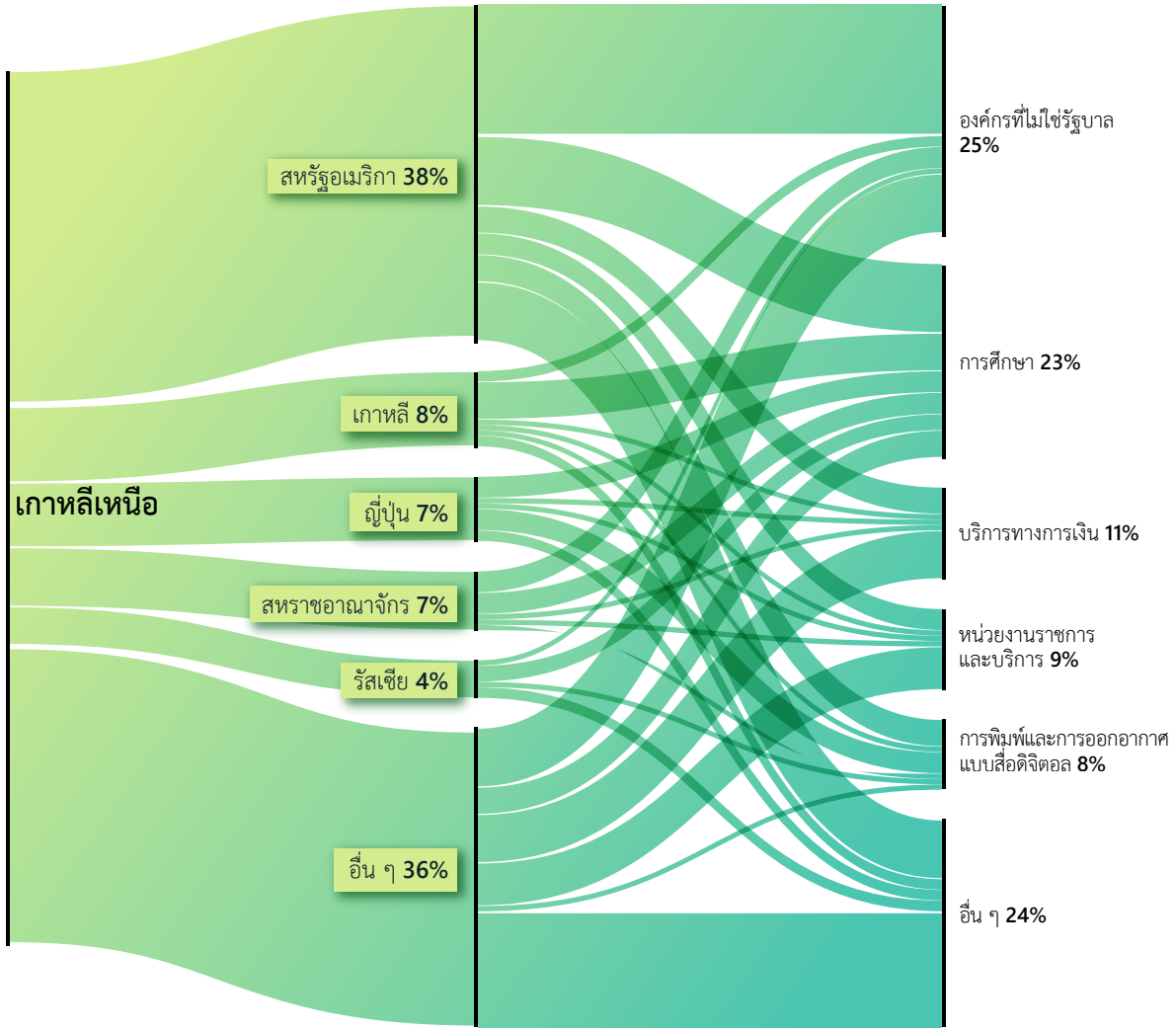
ไม่แน่ใจว่ากิจกรรม DEV-0530 ได้รับการสนับสนุนจากรัฐบาล แม้ว่ารัฐบาลจะสั่งการโจมตีแรนซัมแวร์ด้วยเหตุผลเดียวกับที่สนับสนุนการโจรกรรมจากบริษัทสกุลเงินดิจิทัล แต่ก็เป็นไปได้ว่าผู้อยู่เบื้องหลัง DEV-0530 นั้นทำงานอย่างอิสระเพื่อหารายได้ให้กับตัวเอง หากเป็นแฮ็กเกอร์ชาวเกาหลีเหนือที่ทำงานโดยอิสระ นั่นจะอธิบายได้ว่าทำไมกิจกรรมดังกล่าวถึงไม่แพร่หลายเมื่อเทียบกับการดำเนินการโจรกรรมที่สนับสนุนโดยรัฐบาลต่อบริษัทสกุลเงินดิจิทัล

กำหนดเป้าหมายสำนักข่าวเกาหลีเหนือ ผู้แปรพักตร์ กลุ่มศาสนา และองค์กรช่วยเหลือ

ในปีที่แล้ว ผู้นำสูงสุดคิมจองอึนให้ความสำคัญกับความมั่นคงภายในและความจงรักภักดีต่อสาธารณชนมากกว่าขีปนาวุธและอาวุธนิวเคลียร์ สะท้อนให้เห็นถึงความหมกมุ่นกับปัญหาภายในประเทศ กลุ่มรัฐเกาหลีเหนืออย่างน้อยสองกลุ่มมุ่งความสนใจไปที่แง่มุมที่รัฐบาลจะมองว่าเป็นภัยคุกคามภายในประเทศ

กลุ่มแรกคือกลุ่มที่ Microsoft ติดตามในชื่อ DEV-0215 ซึ่งกำหนดเป้าหมายองค์กรสื่อที่ติดตามข่าวเกาหลีเหนืออย่างใกล้ชิด เหตุผลหนึ่งที่เป็นไปได้สำหรับการกำหนดเป้าหมายนี้คือสื่อเหล่านี้ได้รับข่าวจากผู้แปรพักตร์ชาวเกาหลีเหนือ ชาวจีนที่ทำงานใกล้ชิดกับเกาหลีเหนือ และแม้แต่ชาวเกาหลีเหนือบางคนที่อาศัยอยู่ในประเทศ โดยใช้วิธีต่างๆ เพื่อสื่อสารกับโลกภายนอก รัฐบาลเกาหลีเหนือมองว่ากลุ่มเหล่านี้เป็นภัยคุกคามต่อความอยู่รอด โดยเฉพาะพลเมืองในเกาหลีเหนือที่จะถูกมองว่าเป็นคนทรยศและเป็นสายลับ DEV-0215 มีแนวโน้มที่จะพยายามระบุแหล่งที่มาของหน่วยงานเหล่านี้ เพื่อให้สามารถแก้การรั่วไหลของข้อมูลที่อาจเกิดขึ้นได้

เกาหลีเหนือ: ประเทศเป้าหมายสูงสุดและภาคอุตสาหกรรม



เกาหลีเหนือถือว่าสหรัฐอเมริกา เกาหลีใต้ และญี่ปุ่นเป็นศัตรูตัวฉกาจ ในขณะที่รัสเซียเป็นพันธมิตรมายาวนาน ผู้คุกคามเกาหลีเหนือมุ่งเป้าไปที่สถาบันคลังสมอง นักวิชาการ และเจ้าหน้าที่ทางการทูตของรัสเซียเพื่อรับข้อมูลข่าวกรองเกี่ยวกับมุมมองของรัสเซียเกี่ยวกับกิจการระดับโลก

ความสามารถทางไซเบอร์ของเกาหลีเหนือใช้เพื่อบรรลุเป้าหมายหลักสามประการของระบอบการปกครอง

ต่อไป

Microsoft ยังเห็นหลักฐานของ DEV-0215 ที่กำหนดเป้าหมายชุมชนคริสเตียนที่พูดภาษาเกาหลี คริสตจักรเกาหลีที่นับถือศาสนาคริสต์นิกายอีแวนเจลิคัลมักจะวิจารณ์ทั้งรัฐบาลเกาหลีเหนือและเกาหลีใต้ที่สนับสนุนการมีส่วนร่วมกับเกาหลีเหนือ คริสตจักรเหล่านี้มีแนวโน้มที่จะดำเนินการเข้าถึงผู้แปรพักตร์ และบางแห่งมีส่วนร่วมในงานด้านมนุษยธรรมกับเกาหลีเหนือ เกาหลีเหนือมองว่าพวกเขาเป็นภัยคุกคาม เพราะในขณะที่กระแสของผู้แปรพักตร์ที่มาจากเกาหลีเหนือเกือบจะเหือดหายไปในช่วงการระบาดใหญ่[49] กลุ่มคริสเตียนเหล่านี้มักมีบทบาทสำคัญในการช่วยเหลือผู้แปรพักตร์หนี DEV-0215 ได้สร้างเอกสารปลอมเกี่ยวกับการประชุมคริสเตียนสำหรับผู้พูดภาษาเกาหลีเพื่อล่อเป้าไปที่กลุ่มและค้นหาว่าใครเป็นคนช่วยจัดระเบียบการแปรพักตร์

ในที่สุด กลุ่มรัฐ OSMIUM แสดงความสนใจอย่างต่อเนื่องในองค์กรช่วยเหลือระหว่างประเทศตลอดทั้งปี รวมถึงองค์กรที่เคยช่วยเหลือเกาหลีเหนือในอดีต แม้ว่าโดยทั่วไปแล้วเกาหลีเหนือจะหลีกเลี่ยงข้อเสนอความช่วยเหลือจากภายนอกประเทศ โดยเฉพาะอย่างยิ่งตั้งแต่เกิดการระบาดของโควิด-19 แต่[50] เป็นไปได้ว่าเกาหลีเหนือกำลังพิจารณารับข้อเสนอความช่วยเหลือ แต่ก็ระมัดระวังเรื่องความปลอดภัยในการอนุญาตให้เจ้าหน้าที่ช่วยเหลือชาวต่างชาติเข้ามาในประเทศ เกาหลีเหนืออาจเจาะเครือข่ายองค์กรช่วยเหลือทั่วโลกเพื่อพิจารณาว่าจะให้ความช่วยเหลือดังกล่าวในประเทศของตนหรือไม่

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ผู้มีบทบาททางการเมืองของเกาหลีเหนือมีทักษะไม่ย่อท้อ และมีความคิดสร้างสรรค์ แต่องค์กรต่างๆ สามารถปกป้องพวกเขาได้
2. การโจมตีที่ประสบความสำเร็จส่วนใหญ่สามารถหยุดได้ด้วยสุขอนามัยพื้นฐานทางไซเบอร์ เช่น การยืนยันตัวตนแบบสองปัจจัยหรือการไม่เปิดไฟล์แนบจากบุคคลที่ไม่รู้จักในสภาพแวดล้อมเสมือนจริง

ลิงค์ไปยังข้อมูลเพิ่มเติม

- ผู้คุกคามชาวเกาหลีเหนือกำหนดเป้าหมายธุรกิจขนาดเล็กและขนาดกลางด้วยแรนซัมแวร์ H0lyGh0st | ศูนย์ข่าวกรองภัยคุกคามของ Microsoft (MSTIC), หน่วยรักษาความปลอดภัยดิจิทัลของ Microsoft (DSU)



ในบรรดาผู้เชี่ยวชาญของเกาหลีเหนือมีการถกเถียงกันมานานแล้วว่ารัฐบาลเกาหลีเหนือจริงจังกับแถลงการณ์ต่อสาธารณะหรือไม่ การโจมตีทางไซเบอร์ที่สอดคล้องกับลำดับความสำคัญของการประกาศของเกาหลีเหนือเป็นการยืนยันความเชื่อที่ว่าเกาหลีเหนือหมายถึงสิ่งที่พูดเมื่อพูดถึงเป้าหมายอย่างเปิดเผยต่อสาธารณะ

ทหารรับจ้างไซเบอร์คุกคามความมั่นคงของไซเบอร์สเปซ

มีอุตสาหกรรมที่กำลังเติบโตของบริษัทเอกชนที่พัฒนาและขายเครื่องมือ เทคนิค และบริการที่ช่วยให้ลูกค้าของพวกเขา ซึ่งมักจะเป็นรัฐบาล สามารถเจาะเข้าไปในเครือข่าย คอมพิวเตอร์ โทรศัพท์ และอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตได้ สินทรัพย์สำหรับผู้ดำเนินการในระดับชาติ หน่วยงานเหล่านี้มักเป็นอันตรายต่อผู้เห็นต่าง นักปกป้องสิทธิมนุษยชน นักข่าว ผู้สนับสนุนภาคประชาสังคม เราเรียกคนเหล่านี้ว่าทหารรับจ้างในโลกไซเบอร์หรือผู้ดำเนินการที่ไม่เหมาะสมในภาคเอกชน

โลกที่บริษัทเอกชนสร้างและขายอาวุธไซเบอร์นั้นอันตรายมากขึ้นสำหรับผู้บริโภค ธุรกิจทุกขนาด และรัฐบาล เครื่องมือที่ไม่เหมาะสมเหล่านี้สามารถใช้ในลักษณะที่ไม่สอดคล้องกับบรรทัดฐานและค่านิยมของธรรมาภิบาลและประชาธิปไตย Microsoft เชื่อว่าการคุ้มครองสิทธิมนุษยชนเป็นภาระหน้าที่ขั้นพื้นฐาน และเราดำเนินการอย่างจริงจังโดยการลด “การเฝ้าระวังในฐานะบริการ” ทั่วโลก

ไมโครซอฟต์ได้ประเมินผู้มีบทบาทของรัฐบางคนในระบอบประชาธิปไตยและเผด็จการจากภายนอกในการพัฒนาหรือการใช้เทคโนโลยี “การสอดแนมเป็นบริการ” นี่คือวิธีที่พวกเขาหลีกเลี่ยงความรับผิดชอบและการกำกับดูแล ตลอดจนได้รับความสามารถที่ยากต่อการพัฒนาโดยกำเนิด

> อาวุธไซเบอร์เหล่านี้ทำให้รัฐชาติมีความสามารถในการสอดแนม ซึ่งพวกเขาจะไม่สามารถพัฒนาได้โดยลำพัง

ตลาดที่ทหารรับจ้างไซเบอร์ดำเนินการนั้นไม่ชัดเจน อย่างไรก็ตาม เรายังคงเฝ้าสังเกตกลุ่มเหล่านี้โดยใช้ช่องโหว่แบบ Zero-day และแม้แต่ช่องโหว่แบบ Zero-click ที่ไม่ต้องการปฏิสัมพันธ์ของเหยื่อเลย ทำให้สามารถเฝ้าระวังได้ในฐานะบริการ

Microsoft เพิ่งประกาศตัวรุกภาคเอกชนในยุโรปที่เราเรียกว่า KNOTWEED ซึ่งเป็น PSOA ในออสเตรีย ที่เรียกว่า DSIRF รายงานข่าวหลายฉบับเชื่อมโยงบริษัทกับการพัฒนาและพยายามขายชุดเครื่องมือมัลแวร์ที่เรียกว่า Subzero[51] เหยื่อรวมถึงสำนักงานกฎหมาย ธนาคาร และที่ปรึกษาเชิงกลยุทธ์ในประเทศต่างๆ เช่น ออสเตรีย สหราชอาณาจักร และปานามา[52]

เนื่องจากความสามารถในการสอดแนมเชิงรุกเหล่านี้ไม่ได้ถูกจัดประเภทโดยหน่วยงานป้องกันและหน่วยข่าวกรองอีกต่อไป แต่ปัจจุบันเป็นผลิตภัณฑ์เชิงพาณิชย์ที่นำเสนอแก่บริษัทและบุคคลทั่วไป กฎระเบียบใดๆ สำหรับอาวุธไซเบอร์จำเป็นต้องก้าวข้ามการควบคุมการส่งออก ผลกระทบของอาวุธไซเบอร์เหล่านี้สามารถทำลายล้างได้เมื่อทหารรับจ้างไซเบอร์ใช้ประโยชน์จากช่องโหว่ในผลิตภัณฑ์หรือบริการ พวกเขาทำให้ระบบนิเวศคอมพิวเตอร์ทั้งหมดตกอยู่ในความเสี่ยง เมื่อมีการระบุช่องโหว่ต่อสาธารณะ บริษัทต่างๆ จะต้องแข่งกับเวลาเพื่อปล่อยการป้องกันก่อนที่การโจมตีในวงกว้างจะตามมา (ดูการสนทนาก่อนหน้านี้เกี่ยวกับการหาช่องโหว่จากช่องโหว่) นี่เป็นวัฏจักรที่อันตรายและยากลำบากสำหรับทั้งซัพพลายเออร์ซอฟต์แวร์ (ซึ่งต้องพัฒนาแพตช์อย่างเร่งด่วน) และผู้บริโภคผลิตภัณฑ์ (ที่ต้องติดตั้งแพตช์ทันที)

ในฐานะสมาชิกผู้ก่อตั้ง Cybersecurity Tech Accord[53] ซึ่งเป็นพันธมิตรชั้นนำที่รวบรวมบริษัทเทคโนโลยีมากกว่า 150 แห่ง Microsoft ให้คำมั่นสัญญาที่จะไม่มีส่วนร่วมในการกระทำที่ไม่เหมาะสมทางออนไลน์ เรายึดมั่นในคำมั่นสัญญาดังกล่าวและด้วยความรับผิดชอบด้านสิทธิมนุษยชนของเราในด้านนี้ เรามีส่วนร่วมในการหยุดชะงักทางเทคนิคและความท้าทายทางกฎหมายเพื่อเน้นย้ำถึงผลกระทบด้านลบที่เกิดจากบริการของทหารรับจ้างในโลกไซเบอร์ และจะปกป้องลูกค้าของเราต่อไปเมื่อเราพบเห็นการละเมิด

> ทหารรับจ้างไซเบอร์สร้างและให้บริการความสามารถด้าน “การเฝ้าระวังในฐานะบริการ” ที่มีความซับซ้อนทางเทคโนโลยีและพร้อมใช้งานในวงกว้าง รวมถึงมัลแวร์ขั้นสูงและเทคนิคต่างๆ

ข้อมูลเชิงลึกที่นำไปใช้ได้จริงสำหรับรัฐบาล

1. ใช้ข้อกำหนดด้านความโปร่งใสและการกำกับดูแลสำหรับการสอดแนมในฐานะบริการ โดยเฉพาะอย่างยิ่งในการจัดซื้อจัดจ้าง รวมถึงการห้ามผู้กระทำการที่ไม่เหมาะสมเหล่านี้ ดังเช่นที่สหรัฐฯ ดำเนินการกับกระทรวงพาณิชย์ในการจดทะเบียนบริษัทในรายการเอนทิตี
2. กำหนดข้อจำกัดหลังออกจากงานสำหรับอดีตพนักงานในภาคส่วนนี้
3. มุ่งมั่นที่จะดำเนินการตามข้อผูกพัน “รู้จักลูกค้าของคุณ” และสนับสนุนให้บริษัทต่างๆ ปฏิบัติตามข้อผูกพันด้านสิทธิมนุษยชน

ลิงค์ไปยังข้อมูลเพิ่มเติม

- แกะ KNOTWEED: ตัวรุกของภาคเอกชนยุโรปโดยใช้การหาประโยชน์ 0 วัน | Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), RiskIQ (Microsoft Defender Threat Intelligence)
- การต่อสู้ต่อเนื่องกับอาวุธไซเบอร์ของภาคเอกชน | Microsoft เกี่ยวกับปัญหา

ดำเนินการตามบรรทัดฐานความปลอดภัยทางไซเบอร์เพื่อสันติภาพและความปลอดภัยในโลกไซเบอร์

เราต้องการกรอบสากลที่สอดคล้องกันอย่างเร่งด่วน ซึ่งให้ความสำคัญกับสิทธิมนุษยชนและปกป้องผู้คนจากพฤติกรรมของรัฐที่ประมาทในโลกออนไลน์ ไม่มีที่ใดที่จะแสดงให้เห็นอย่างชัดเจนมากไปกว่าสงครามที่กำลังดำเนินอยู่ในยูเครน นอกเหนือจากความพยายามเชิงกลยุทธ์ระดับโลกแล้ว รัฐบาลสามารถดำเนินการในขณะนี้เพื่อสร้างผลกระทบเชิงบวกในทันที

เมื่อห้าปีที่แล้ว Microsoft เรียกร้องให้มี “อนุสัญญาเจนีวาดิจิทัล" เพื่อยกระดับความรับผิดชอบและภาระหน้าที่ในภาคส่วนต่างๆ เพื่อปกป้องสันติภาพและความปลอดภัยทางออนไลน์ โลกไซเบอร์กำลังเกิดขึ้นในฐานะขอบเขตความขัดแย้งและการแข่งขันระหว่างรัฐที่แตกต่างกันและผันผวน โดยการโจมตีกลายเป็นเรื่องธรรมดามากขึ้น แม้ในยามสงบสุข

ทุกวันนี้ ยังคงมีความจำเป็นที่ชัดเจนสำหรับกรอบการทำงานดังกล่าว ซึ่งเห็นได้จากการโจมตีทางไซเบอร์ของรัสเซียต่อยูเครน ซึ่งเป็นส่วนหนึ่งของการรุกรานของรัสเซีย สงครามครั้งนี้ได้สร้างแนวรบใหม่ที่แตกต่างจากที่เราเคยรู้จักมาก่อนอย่างมาก

การนำเสถียรภาพมาสู่โลกไซเบอร์จะต้องสร้างความแข็งแกร่งและปรับเปลี่ยนสถาบันการกำกับดูแลระดับโลกใหม่เพื่อให้เหมาะสมกับวัตถุประสงค์ โลกไซเบอร์โดยพื้นฐานแล้วแตกต่างจากโดเมนอื่นๆ โดยพื้นฐานแล้วมันไร้พรมแดน สังเคราะห์ และดูแลโดยอุตสาหกรรมส่วนตัวเป็นส่วนใหญ่ ซึ่งหมายถึงการขอให้อุตสาหกรรมเทคโนโลยีรับผิดชอบมากขึ้นทั้งความปลอดภัยของผลิตภัณฑ์และบริการและระบบนิเวศดิจิทัลที่กว้างขึ้น แม้ว่าจะมีความก้าวหน้าอย่างเห็นได้ชัดในทุกด้าน แต่ความท้าทายก็เพิ่มขึ้นอย่างมาก

เราต้องเพิ่มความพยายามร่วมกันเป็นสองเท่าเพื่อปกป้องความปลอดภัยของโลกไซเบอร์ เราไม่สามารถถือเอาสิทธิและเสรีภาพที่เราคาดว่าจะได้รับในโลกออนไลน์ ในขณะที่เราต่อสู้เพื่อจัดการกับความท้าทาย ผู้ประสงค์ร้ายกำลังวางแผนว่าจะโจมตีอย่างไรและที่ไหนต่อไปโดยใช้ AI ใช้ประโยชน์จากข้อมูลที่บิดเบือน และค้นหาวิธีบ่อนทำลายเมตาเวิร์สที่ยังใหม่อยู่ นักปกป้องสิทธิมนุษยชน อุตสาหกรรมเทคโนโลยี และรัฐบาลที่เคารพสิทธิต้องทำงานร่วมกันเพื่อบรรลุวิสัยทัศน์ที่ยืนยันถึงโลกออนไลน์ที่ปลอดภัยและมั่นคง หนทางข้างหน้ายังอีกยาวไกล แต่มีสิ่งที่รัฐบาลสามารถทำได้ในขณะนี้เพื่อปรับปรุงระบบนิเวศความปลอดภัยทางไซเบอร์ในทันที:

- อ้างอิงบรรทัดฐาน กฎหมาย และผลที่ตามมาในการระบุแหล่งที่มา การปรับปรุงที่สำคัญอย่างหนึ่งในช่วงห้าปีที่ผ่านมาคือความเร็วและการประสานงานของการโจมตีทางไซเบอร์ของรัฐบาล นอกเหนือจากการตั้งชื่อและทำให้อับอายแล้ว ข้อความเหล่านี้จำเป็นต้องเน้นย้ำว่ากฎหมายหรือบรรทัดฐานระหว่างประเทศใดบ้างที่ถูกละเมิด และผลที่ตามมาจะถูกกำหนดในลักษณะใดเพื่อช่วยเสริมสร้างการรับรู้ถึงความคาดหวังระหว่างประเทศ
- ชี้แจงการตีความกฎหมายระหว่างประเทศออนไลน์ แม้ว่ารัฐบาลจะยอมรับว่ากฎหมายระหว่างประเทศมีผลบังคับใช้ทางออนไลน์ แต่คำถามยังคงมีอยู่เกี่ยวกับวิธีการบังคับใช้ในบางกรณี สิ่งนี้มีความเกี่ยวข้องอย่างยิ่งในผลพวงของการรุกรานของยูเครน รัฐบาลสามารถดำเนินการได้ไกลในการกำหนดความคาดหวัง หลีกเลี่ยงความเข้าใจผิด และสร้างความไว้วางใจโดยระบุว่าพวกเขาเข้าใจพันธกรณีภายใต้กฎหมายระหว่างประเทศอย่างไร
- ปรึกษากับผู้มีส่วนได้ส่วนเสียอื่นๆ ในขณะที่ฟอรัมระหว่างประเทศยังคงค้นพบวิธีที่ดีที่สุดในการอำนวยความสะดวกในการรวมผู้มีส่วนได้ส่วนเสียหลายกลุ่มที่แข็งแกร่ง รัฐบาลสามารถสนับสนุนการสนทนาที่มีข้อมูลโดยปรึกษากับชุมชนผู้มีส่วนได้ส่วนเสียหลายกลุ่ม โดยเฉพาะอุตสาหกรรมเทคโนโลยี เพื่อให้แน่ใจว่าได้รับประโยชน์จากการสนทนาจากผู้ที่มีความเชี่ยวชาญที่ขาดไม่ได้
- สร้างองค์กรที่ยืนหยัดเพื่อสนับสนุนพฤติกรรมของรัฐที่มีความรับผิดชอบในโลกไซเบอร์ การทำงานของเวทีทางการทูตระหว่างประเทศเพื่อพัฒนาพฤติกรรมของรัฐที่มีความรับผิดชอบทางออนไลน์นั้นมีความสำคัญมากกว่าที่เคย มีความจำเป็นที่ชัดเจนสำหรับกลไกถาวรของสหประชาชาติในการจัดการกับไซเบอร์สเปซที่เป็นโดเมนของความขัดแย้ง
- กำหนดบรรทัดฐานใหม่สำหรับภัยคุกคามที่กำลังพัฒนา ภัยคุกคามทางโลกไซเบอร์มีการพัฒนาอย่างต่อเนื่อง ควบคู่ไปกับนวัตกรรมทางเทคโนโลยี แม้ว่าบรรทัดฐานระหว่างประเทศควรเป็นกลางทางเทคโนโลยี แต่ก็จำเป็นต้องได้รับการปรับปรุงและลดทอนตามการเปลี่ยนแปลงของแนวภัยคุกคามและวิธีที่เราใช้เทคโนโลยี แม้กระทั่งทุกวันนี้ เราเห็นช่องว่างในกรอบระหว่างประเทศที่มีอยู่ถูกละเมิด รัฐควรให้คำมั่นอย่างชัดเจนในการปกป้องกระบวนการหลักที่สนับสนุนระบบนิเวศดิจิทัลที่ไม่ได้รับการคุ้มครองในปัจจุบัน เช่น กระบวนการอัปเดตซอฟต์แวร์ นอกจากนี้ พื้นที่เฉพาะควรได้รับการคุ้มครองเพิ่มเติม ตัวอย่างเช่น ดังที่เราได้เรียนรู้ท่ามกลางการแพร่ระบาด บรรทัดฐานในการปกป้องสุขภาพเป็นสิ่งสำคัญ

ผู้ดำเนินการและการโจมตีในระดับชาติเพิ่มปริมาณและความซับซ้อนมากขึ้น สร้างสถานการณ์ที่ไม่สามารถป้องกันได้

การดำเนินการในทันทีเป็นสิ่งจำเป็น—มีหลายสิ่งที่รัฐบาลสามารถทำได้ในขณะนี้เพื่อปรับปรุงระบบนิเวศความปลอดภัยทางไซเบอร์ในทันที รวมถึงการดำเนินการตามบรรทัดฐานและกฎที่ตกลงร่วมกันสำหรับพฤติกรรมของรัฐในโลกไซเบอร์ และการทำงานร่วมกับชุมชนผู้มีส่วนได้ส่วนเสียที่กว้างขึ้นเพื่อจัดการกับช่องว่างที่เกิดขึ้น

สถาบันพหุภาคีต้องได้รับการพิจารณาใหม่เพื่อจัดการกับความท้าทายเร่งด่วนของการโจมตีทางไซเบอร์ของรัฐชาติ

ลิงค์ไปยังข้อมูลเพิ่มเติม

- ช่วงเวลาแห่งการพิจารณา: ความต้องการการตอบสนองด้านความปลอดภัยในโลกไซเบอร์ที่แข็งแกร่งและทั่วโลก | Microsoft เกี่ยวกับปัญหา
- การโจมตีทางไซเบอร์ที่กำหนดเป้าหมายการดูแลสุขภาพต้องหยุด | Microsoft เกี่ยวกับปัญหา
- บทต่อไปของการทูตไซเบอร์ที่สหประชาชาติ | Microsoft On the Issues

อ้างอิงท้ายเอกสาร

1. https://www.microsoft.com/en-us/cybersecurity/content-hub/cloud-security
2. https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
3. โครงสร้างพื้นฐานที่สำคัญในบทนี้กำหนดโดย Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience (กุมภาพันธ์ 2013)
4. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
5. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
6. https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/
7. https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-passwordless-authentication
8. https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
9. https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release
10. https://reliefweb.int/report/ukraine/unicef-ukraine-humanitarian-situation-report-no-13-10-17-may-2022
11. https://news.un.org/en/story/2022/06/1119672
12. https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r ; https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
13. https://www.cnn.com/2022/03/14/economy/china-jan-feb-economy-challenges-ahead-intl-hnk/index.html
14. https://www.wsj.com/articles/russias-vladimir-putin-meets-with-chinese-leader-xi-jinping-in-beijing-11643966743
15. https://www.washingtonpost.com/world/2022/04/01/china-eu-summit/
16. https://twitter.com/MoNDefense
17. https://news.usni.org/2022/01/24/2-u-s-aircraft-carriers-now-in-south-china-sea-as-chinese-air-force-flies-39-aircraft-near-taiwan
18. https://ec.europa.eu/trade/policy/in-focus/eu-china-agreement/; https://www.usnews.com/news/world/articles/2022-02-28/eu-plans-summit-with-china-on-april-1-to-address-tensions
19. https://www.wsj.com/articles/u-s-on-sidelines-as-china-and-other-asia-pacific-nations-launch-trade-pact-11641038401
20. https://greenfdc.org/chinas-two-sessions-2022-what-it-means-for-economy-climate-biodiversity-green-finance-and-the-belt-and-road-initiative-bri/
21. https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea
22. https://www.theguardian.com/world/2022/apr/30/the-china-solomons-security-deal-has-been-signed-time-to-move-on-from-megaphone-diplomacy
23. https://www.fmprc.gov.cn/eng/zxxx_662805/202205/t20220531_10694928.html
24. https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/; https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
25. https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/
26. https://attack.mitre.org/techniques/T1053/
27. https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
28. https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/
29. https://www.timesofisrael.com/in-rare-criticism-of-irgc-rouhani-slams-anti-israel-slogans-on-test-missiles/; https://www.theguardian.com/world/2017/may/05/iran-president-hassan-rouhani-nuclear-agreement-sabotaged; https://d2071andvip0wj.cloudfront.net/184-iran-s-priorities-in-a-turbulent-middle-east_1.pdf; https://www.aljazeera.com/news/2016/3/9/iran-launches-ballistic-missiles-during-military-drill; https://www.usatoday.com/story/news/world/2015/04/25/iran-yemen-weapons/26367493/; https://www.armscontrol.org/blog/ArmsControlNow/2016-03-14/The-Iranian-Ballistic-Missile-Launches-That-Didnt-Happen; https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/;
30. https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/; https://www.france24.com/en/live-news/20210825-iran-s-parliament-approves-president-s-cabinet-choices

อ้างอิงท้ายเรื่องต่อ

31. https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-inintelligence-operations; https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential; https://miburo.substack.com/p/iran-disinfo-privatized?s=r.
32. https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/
33. https://www.tasnimnews.com/en/news/2021/11/05/2602361/us-military-action-off-the-table-iranian-general
34. โดยเฉพาะอย่างยิ่ง แก้ไขเซิร์ฟเวอร์ Exchange สำหรับช่องโหว่ ProxyShell (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 และ CVE-2021-27065, CVE-2021-34473) นอกจากนี้ อย่าลืมแก้ไขอุปกรณ์ Fortinet FortiOS SSL VPN เพื่อหาช่องโหว่
35. https://docs.microsoft.com/en-us/microsoft-365/commerce/manage-partners?view=o365-worldwide
36. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
37. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
38. https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
39. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
40. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-baselines-microsoft-defender-antivirus?view=o365-worldwide
41. https://docs.microsoft.com/microsoft-365/security/defender-endpoint/cloud-protection-microsoft-defender-antivirus
42. https://docs.microsoft.com/microsoft-365/commerce/manage-partners?view=o365-worldwide
43. https://www.marketwatch.com/story/kim-jong-un-calls-for-improved-living-conditions-in-north-korea-01633920099
https://www.bbc.com/news/world-asia-59845636
https://kcnawatch.org/newstream/1650963237-449932111/respected-comrade-kim-jong-un-makes-speech-at-military-parade-held-in-celebration-of-90th-founding-anniversary-of-kpra/
44. https://www.theguardian.com/world/2021/aug/06/north-korea-homes-wreckeddamaged-and-and-bridges-washed-away-in-floods
45. https://www.reuters.com/world/asia-pacific/nkorea-mobilises-office-workers-fight-drought-amid-food-shortages-2022-05-04/
46. https://www.washingtonpost.com/world/asia_pacific/north-korea-kim-pandemic/2021/09/08/31adfd74-ff53-11eb-87e0-7e07bd9ce270_story.html
47. https://news.yahoo.com/china-halts-freight-train-traffic-102451425.html
48. https://www.cnn.com/2022/05/11/asia/north-korea-covid-omicron-coronavirus-intl-hnk/index.html
49. https://www.csis.org/analysis/number-north-korean-defectors-drops-lowest-level-two-decades
50. https://www.aljazeera.com/economy/2022/5/20/north-korea-shuns-outside-help-as-covid-catastrophe-looms
51. Jan-Philipp Hein, In the mystery of creepy spy software, the trail leads via Wirecard to the Kremlin, FOCUS Online, (2022), https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html; Sugar Mizzy, We unveil the “Subzero” state trojan from Austria, Europe-cities (2021), https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/; Andre Meister, We unveil the state Trojan “Subzero” from Austria, Netzpolitik.org (2022), https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich
52. ตามที่ระบุไว้ในบล็อกทางเทคนิคของเรา การระบุเป้าหมายในประเทศไม่ได้แปลว่าลูกค้าของ DSIRF อาศัยอยู่ในประเทศเดียวกัน เนื่องจากการกำหนดเป้าหมายระหว่างประเทศเป็นเรื่องปกติ
53. หน้าแรก | Cybersecurity Tech Accord (cybertechaccord.org)

เครื่องมือและโครงสร้างพื้นฐาน

ด้วยการเร่งความเร็วของการเปลี่ยนแปลงทางดิจิทัล
ความปลอดภัยของโครงสร้างพื้นฐานทางดิจิทัล
จึงมีความสำคัญมากกว่าที่เคย

ภาพรวมของอุปกรณ์และโครงสร้างพื้นฐาน 57
ข้อมูลเบื้องต้น 58
รัฐบาลดำเนินการเพื่อปรับปรุงความปลอดภัย และความยืดหยุ่นของโครงสร้างพื้นฐานที่สำคัญ 59
IoT และ OT เปิดเผย: แนวโน้มและการโจมตี 62
ห่วงโซ่อุปทานและการแฮ็คเฟิร์มแวร์ 65
สปอตไลท์เกี่ยวกับช่องโหว่ของเฟิร์มแวร์ 66
การโจมตี OT ตามการลาดตระเวน 68
ภาพรวมของการปฏิบัติการอิทธิพลทางไซเบอร์ 72

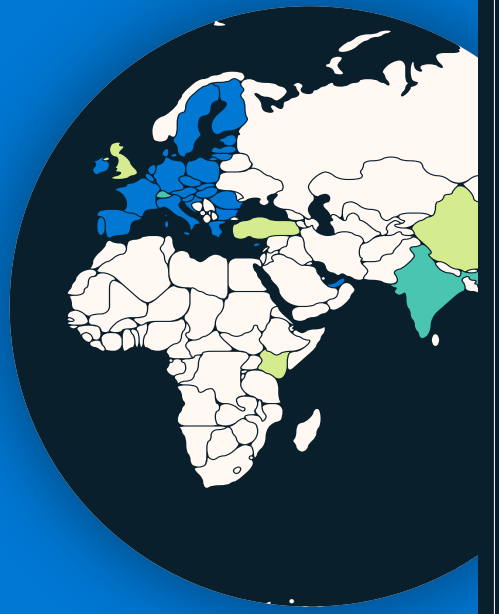
ภาพรวมของ

อุปกรณ์และโครงสร้างพื้นฐาน

การระบาดใหญ่ควบคู่ไปกับการนำอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตทุกประเภทมาใช้อย่างรวดเร็ว เป็นองค์ประกอบในการเร่งการเปลี่ยนแปลงทางดิจิทัลได้เพิ่มพื้นผิวการโจมตีของโลกดิจิทัลอย่างมาก

อาชญากรไซเบอร์และประเทศกำลังฉวยโอกาสอย่างรวดเร็ว แม้ว่าความปลอดภัยของฮาร์ดแวร์และซอฟต์แวร์ด้านไอทีจะแข็งแกร่งขึ้นในช่วงไม่กี่ปีที่ผ่านมา แต่ความปลอดภัยของอุปกรณ์ Internet of Things (IoT) และเทคโนโลยีการดำเนินงาน (OT) กลับไม่ก้าวทัน ผู้คุกคามกำลังใช้ประโยชน์จากอุปกรณ์เหล่านี้เพื่อสร้างการเข้าถึงบนเครือข่ายและเปิดใช้งานการเคลื่อนไหวด้านข้าง เพื่อสร้างหลักในห่วงโซ่อุปทาน หรือขัดขวางการดำเนินงาน OT ขององค์กรเป้าหมาย

รัฐบาลทั่วโลกกำลังเคลื่อนไหวเพื่อปกป้องโครงสร้างพื้นฐานที่สำคัญโดยการปรับปรุงความปลอดภัยของ IoT และ OT

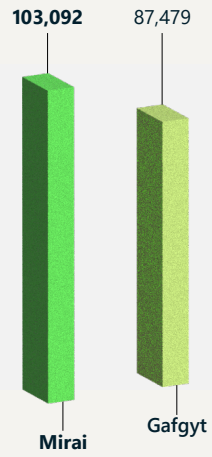


ค้นหาข้อมูลเพิ่มเติมหน้า 59

นโยบายความปลอดภัยที่สอดคล้องกันทั่วโลกและทำงานร่วมกันได้เป็นสิ่งจำเป็นเพื่อให้แน่ใจว่าจะมีการนำไปใช้อย่างกว้างขวาง

ค้นหาข้อมูลเพิ่มเติมหน้า 59

มัลแวร์ในฐานะบริการได้ย้ายเข้าสู่การดำเนินการขนาดใหญ่เพื่อต่อต้าน IoT และ OT ที่เปิดเผยในโครงสร้างพื้นฐานและยูทิลิตี้ เช่นเดียวกับเครือข่ายองค์กร



ค้นหาข้อมูลเพิ่มเติมหน้า 63

การโจมตีอุปกรณ์การจัดการระยะไกลเพิ่มสูงขึ้น โดยมีการโจมตีมากกว่า 100 ล้านครั้งในเดือนพฤษภาคม 2022 ซึ่งเพิ่มขึ้น 5 เท่าในปีที่ผ่านมา

ค้นหาข้อมูลเพิ่มเติมหน้า 62



ผู้โจมตีใช้ประโยชน์จากช่องโหว่ในเฟิร์มแวร์อุปกรณ์ IoT มากขึ้นเรื่อยๆ เพื่อแทรกซึมเครือข่ายองค์กรและเปิดการโจมตีทำลายล้าง

ค้นหาข้อมูลเพิ่มเติมหน้า 65

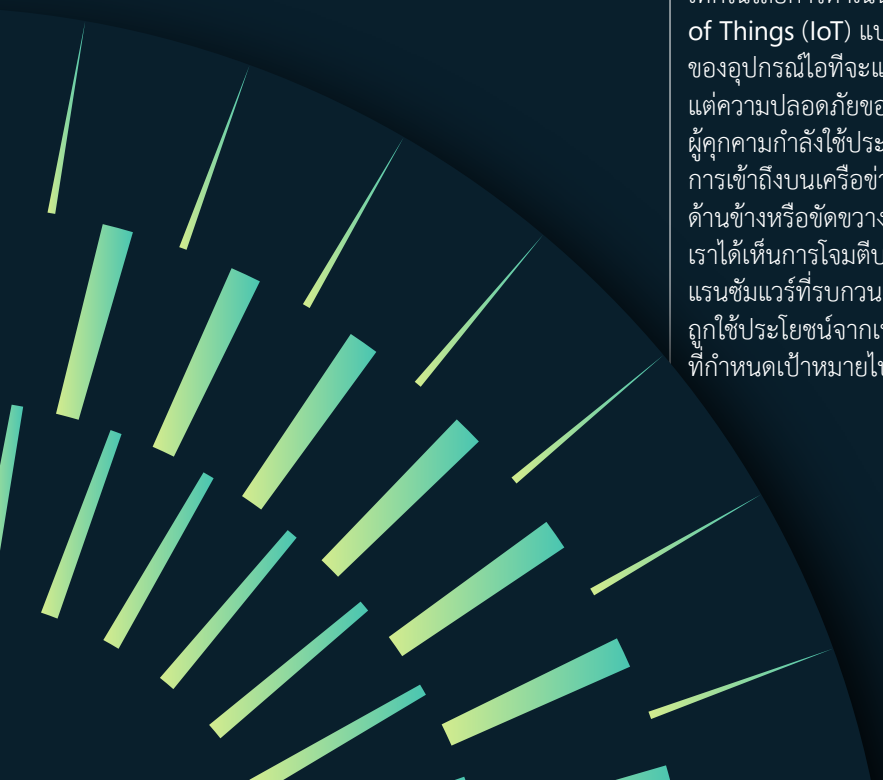
ภาพเฟิร์มแวร์ 32% ที่วิเคราะห์มีช่องโหว่ร้ายแรงที่รู้จักอย่างน้อย 10 รายการ



ค้นหาข้อมูลเพิ่มเติมหน้า 66

ข้อมูลเบื้องต้น

การเร่งการเปลี่ยนแปลงทางดิจิทัลได้เพิ่มความเสี่ยงด้านความปลอดภัยทางไซเบอร์ให้กับโครงสร้างพื้นฐานที่สำคัญและระบบทางกายภาพทางไซเบอร์



หลายปีที่ผ่านมามีการเปลี่ยนแปลงที่ไม่เคยเกิดขึ้นมาก่อนในโลกดิจิทัล องค์กรต่างๆ กำลังพัฒนาเพื่อใช้ประโยชน์จากความก้าวหน้าในความสามารถในการประมวลผลจากทั้งคลาวด์อัจฉริยะและเอดจ์อัจฉริยะ อันเป็นผลมาจากการแพร่ระบาดทำให้หน่วยงานต่างๆ ต้องแปลงเป็นดิจิทัลเพื่อความอยู่รอด และอัตราที่อุตสาหกรรมต่างๆ ทั่วโลกหันมาใช้อุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตได้ พื้นผิวการโจมตีของโลกดิจิทัลจึงเพิ่มขึ้นอย่างทวีคูณ

การโยกย้ายที่รวดเร็วนี้แซงหน้าความสามารถของชุมชนความปลอดภัยในการตามให้ทัน ในปีที่ผ่านมา เราสังเกตเห็นภัยคุกคามที่ใช้ประโยชน์จากอุปกรณ์ในทุกส่วนขององค์กร ตั้งแต่อุปกรณ์ไอทีแบบดั้งเดิมไปจนถึงตัวควบคุมเทคโนโลยีการดำเนินงาน (OT) หรือเซ็นเซอร์ Internet of Things (IoT) แบบธรรมดา แม้ว่าความปลอดภัยของอุปกรณ์ไอทีจะแข็งแกร่งขึ้นในช่วงไม่กี่ปีที่ผ่านมา แต่ความปลอดภัยของอุปกรณ์ IoT และ OT ก็ยังไม่ก้าวทัน ผู้คุกคามกำลังใช้ประโยชน์จากอุปกรณ์เหล่านี้เพื่อสร้างการเข้าถึงบนเครือข่ายและเปิดใช้งานการเคลื่อนไหวด้านข้างหรือขัดขวางการปฏิบัติงาน OT ขององค์กร เราได้เห็นการโจมตีบนกริดพลังงาน การโจมตีด้วยแรนซัมแวร์ที่รบกวนการทำงานของ OT เราเตอร์ IoT ถูกใช้ประโยชน์จากเพื่อเพิ่มความทนทาน และการโจมตีที่กำหนดเป้าหมายไปที่ช่องโหว่ในเฟิร์มแวร์

แม้ว่าช่องโหว่ IoT และ OT ที่แพร่หลายจะเป็นความท้าทายสำหรับทุกองค์กร แต่โครงสร้างพื้นฐานที่สำคัญกลับมีความเสี่ยงเพิ่มขึ้น เนื่องจากผู้คุกคามได้เรียนรู้ว่าการปิดใช้งานบริการที่สำคัญนั้นเป็นกลไกที่มีประสิทธิภาพ การโจมตีด้วยแรนซัมแวร์ในปี 2021 ต่อบริษัท Colonial Pipeline แสดงให้เห็นว่าอาชญากรสามารถขัดขวางบริการที่สำคัญได้อย่างไร เพื่อเพิ่มโอกาสในการจ่ายค่าไถ่ และการโจมตีทางไซเบอร์ของรัสเซียต่อยูเครนแสดงให้เห็นว่าบางประเทศมองว่าการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานที่สำคัญเป็นการก่อวินาศกรรมที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์ทางทหาร

อย่างไรก็ตาม ยังคงมีความหวังอยู่ ผู้กำหนดนโยบายและผู้ปกป้องเครือข่ายกำลังทำหน้าที่ปรับปรุงความปลอดภัยทางไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญ รวมถึงอุปกรณ์ IoT และ OT ที่พวกเขาพึ่งพา ผู้กำหนดนโยบายกำลังเร่งการพัฒนากฎหมายและระเบียบข้อบังคับเพื่อสร้างความไว้วางใจของสาธารณะในความปลอดภัยทางไซเบอร์ของโครงสร้างพื้นฐานและอุปกรณ์ที่สำคัญ

Microsoft กำลังร่วมมือกับรัฐบาลทั่วโลกเพื่อคว้าโอกาสนี้ในการปรับปรุงความปลอดภัยทางไซเบอร์ และเรายินดีต้อนรับการมีส่วนร่วมเพิ่มเติม อย่างไรก็ตาม เรากังวลว่าข้อกำหนดที่ไม่สอดคล้องกัน ตามความต้องการ หรือซับซ้อนอาจมีผลกระทบที่ไม่ได้ตั้งใจ รวมถึงการลดความปลอดภัยในบางกรณีโดยการโอนทรัพยากรด้านความปลอดภัยที่หายากไปสู่การปฏิบัติตามการรับรองที่ทำซ้ำหลายรายการ

จากจุดยืนของการดำเนินการด้านความปลอดภัย ผู้ปกป้องเครือข่ายใช้แนวทางต่างๆ เพื่อปรับปรุงท่าทางการรักษาความปลอดภัย IoT/OT ขององค์กรของตน แนวทางหนึ่งคือการใช้การตรวจสอบอุปกรณ์ IoT และ OT อย่างต่อเนื่อง อีกประการหนึ่งคือ "shift-left" ซึ่งหมายถึงความต้องการและนำแนวทางปฏิบัติด้านความปลอดภัยทางไซเบอร์ที่ดีขึ้นสำหรับอุปกรณ์ IoT และ OT เอง แนวทางที่สามคือการใช้โซลูชันการตรวจสอบความปลอดภัยซึ่งครอบคลุมทั้งเครือข่าย IT และ OT แนวทางแบบองค์รวมนี้มีประโยชน์เพิ่มเติมอย่างมากในการมีส่วนร่วมในกระบวนการที่สำคัญขององค์กร เช่น "การทำลายไซโล" ระหว่าง OT และ IT ซึ่งจะทำให้องค์กรบรรลุมาตรการรักษาความปลอดภัยที่ได้รับการปรับปรุงในขณะที่บรรลุวัตถุประสงค์ทางธุรกิจ

Michal Braverman-Blumenstyk
รองประธานองค์กร ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยีความปลอดภัยบนคลาวด์และ AI

รัฐบาลดำเนินการเพื่อปรับปรุงความปลอดภัยและความยืดหยุ่นของโครงสร้างพื้นฐานที่สำคัญ

รัฐบาลทั่วโลกกำลังพัฒนาและพัฒนานโยบายเพื่อจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญ หลายแห่งกำลังออกนโยบายเพื่อปรับปรุงความปลอดภัยของอุปกรณ์ IoT และ OT การริเริ่มนโยบายทั่วโลกที่เพิ่มขึ้นกำลังสร้างโอกาสมหาศาลในการปรับปรุงความปลอดภัยทางไซเบอร์ แต่ยังก่อให้เกิดความท้าทายต่อผู้มีส่วนได้ส่วนเสียทั่วทั้งระบบนิเวศ

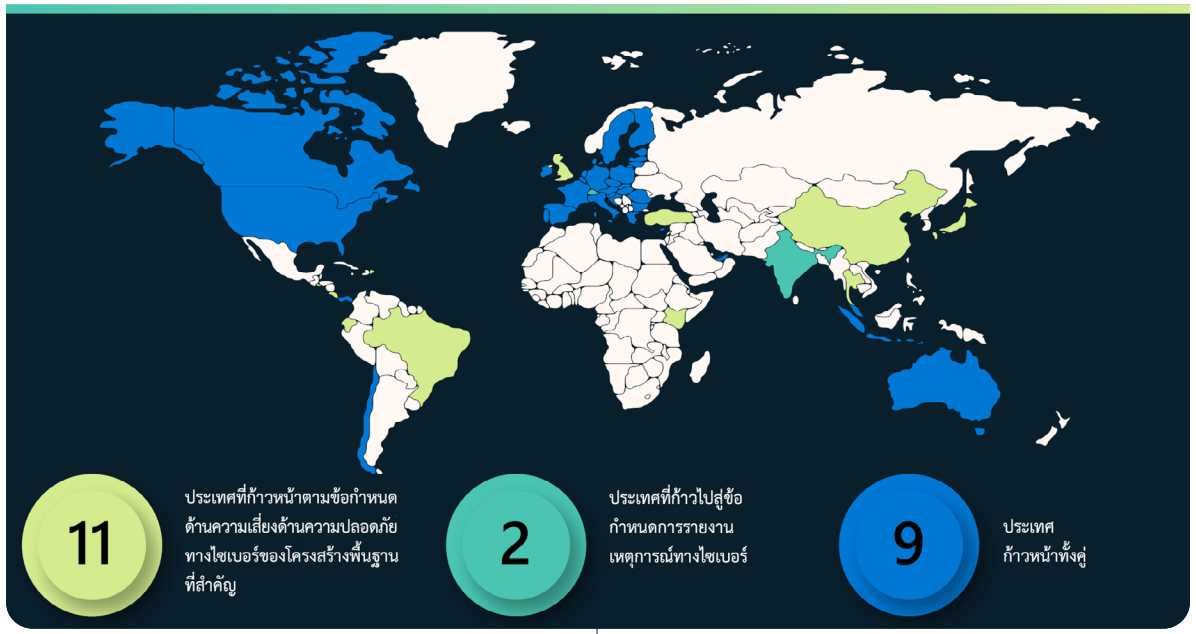
การพัฒนาวิสัยทัศน์แบบองค์รวมสำหรับการจัดการความเสี่ยงทางไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญเป็นสิ่งสำคัญ แต่ก็มีความซับซ้อน โดยเฉพาะอย่างยิ่งเมื่อพิจารณาจากระดับของการเชื่อมต่อระหว่างเทคโนโลยีและซัพพลายเออร์ทั่วโลก การใช้เทคโนโลยีที่หลากหลายและความเสี่ยงที่เกี่ยวข้อง และความจำเป็นในการลงทุนทั้งในระยะสั้นและระยะยาว กลยุทธ์ นโยบายที่กำหนดขอบเขตอย่างมีประสิทธิภาพที่ขับเคลื่อนการเรียนรู้และการปรับปรุงซ้ำๆ และสนับสนุนการทำงานร่วมกันข้ามภาคส่วนทั่วโลก สามารถช่วยจัดการความซับซ้อนและเปิดใช้งานการแปลงทางดิจิทัลที่คำนึงถึงความปลอดภัยมากขึ้น อย่างไรก็ตาม แนวทางการออกกฎหมายที่กระจัดกระจายอาจนำไปสู่ข้อกำหนดด้านกฎระเบียบที่ทับซ้อนกันและไม่สอดคล้องกัน สิ่งนี้อาจส่งผลกระทบต่อทรัพยากรและทำลายวัตถุประสงค์ด้านความปลอดภัย ในที่สุด ตัวอย่างเช่น องค์กรสามารถโอนทรัพยากรจากนวัตกรรมและความปลอดภัยไปสู่การปฏิบัติตามกฎอย่างเป็นทางการ

Microsoft พยายามที่จะเป็นพันธมิตรกับรัฐบาลทั่วโลกในการปฏิบัติตามนโยบายความปลอดภัยทางไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญอย่างมีประสิทธิภาพ เพิ่มความเข้าใจในความท้าทายและโอกาส และสนับสนุนความพยายามในการยกระดับสถานะความเสี่ยงโดยรวม

การพัฒนานโยบายในโครงสร้างพื้นฐานที่สำคัญในการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์

ในช่วงปีที่ผ่านมา เขตอำนาจศาลหลายแห่ง ได้แก่ ออสเตรเลีย ชิลี สหภาพยุโรป (EU) ญี่ปุ่น สิงคโปร์ สหราชอาณาจักร (UK) และสหรัฐอเมริกา ได้พัฒนาปรับปรุง หรือดำเนินการรักษาความปลอดภัยทางไซเบอร์ข้ามภาคส่วนหรือเฉพาะภาคส่วน ข้อกำหนด[1] รัฐบาลเหล่านี้หลายแห่ง—และอื่นๆ เช่น อินเดีย[2] และสวิตเซอร์แลนด์[3]—ออกแล้วหรือกำลังพัฒนาข้อกำหนดการรายงานเหตุการณ์ด้านความปลอดภัยทางไซเบอร์สำหรับโครงสร้างพื้นฐานที่สำคัญและผู้ให้บริการที่จำเป็น[4]

การพัฒนานโยบายที่โดดเด่นบางอย่างเกิดขึ้นในออสเตรเลีย สหภาพยุโรป อินโดนีเซีย และสหรัฐอเมริกาในช่วงปีที่แล้ว ออสเตรเลียออกกฎหมายสองฉบับเพื่อช่วยจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญข้ามภาคส่วน เหนือสิ่งอื่นใด กฎหมายกำหนดภาคส่วนโครงสร้างพื้นฐานที่สำคัญใหม่ กำหนดให้มีการพัฒนาแผนการจัดการความเสี่ยง กำหนดให้มีการรายงานเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ และให้อำนาจรัฐบาลในการเข้าแทรกแซง หากพิจารณาแล้วว่าผู้ดำเนินการโครงสร้างพื้นฐานที่สำคัญไม่เต็มใจหรือไม่สามารถตอบสนองต่อเหตุการณ์ได้อย่างเพียงพอ



สหภาพยุโรปทำงานเพื่อปรับปรุงข้อกำหนด NIS ประจำปี 2016 ซึ่งเป็นกรอบสำหรับประเทศสมาชิกสหภาพยุโรปในการควบคุมบริการและผลิตภัณฑ์เทคโนโลยีที่ถือว่ามีความสำคัญต่อเศรษฐกิจและการทำงานของสังคม NIS 2 ที่เสนอรวมถึงการแก้ไขที่จะสร้างหมวดหมู่ใหม่ของโครงสร้างพื้นฐานดิจิทัลที่สำคัญ เพิ่มข้อกำหนดสำหรับการรายงานเหตุการณ์ทางไซเบอร์ และกำหนดข้อกำหนดการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์เพิ่มเติม สหภาพยุโรปยังได้พัฒนาการปรับปรุงที่เสนอสำหรับ Digital Operational Resilience Act (DORA) ข้อกำหนดใหม่สำหรับเทคโนโลยีการสื่อสารข้อมูลที่ใช้ในภาคบริการทางการเงิน

ในเดือนพฤษภาคม อินโดนีเซียออกกฎระเบียบประธานาธิบดีว่าด้วยการคุ้มครองโครงสร้างพื้นฐานข้อมูลสำคัญ (“IIV”) ซึ่งจะมีผลบังคับใช้ในเดือนพฤษภาคม 2024 และครอบคลุมภาคส่วนต่างๆ เช่น พลังงาน การขนส่ง การเงิน สุขภาพ และอื่นๆ วัตถุประสงค์ของอินโดนีเซียตามกฎระเบียบคือเพื่อปกป้องความต่อเนื่องของการนำ IIV ไปใช้ ป้องกันการโจมตีทางไซเบอร์ และเพิ่มการเตรียมพร้อมในการจัดการกับเหตุการณ์ทางไซเบอร์ ผู้ให้บริการ IIV จะรับผิดชอบในการดำเนินการป้องกันที่ปลอดภัยและเชื่อถือได้ ใช้การจัดการความเสี่ยงทางไซเบอร์ที่มีประสิทธิภาพ และรายงานผลลัพธ์ความเสี่ยงทางไซเบอร์ไปยังหน่วยงานรัฐบาลที่เกี่ยวข้อง กฎระเบียบรวมถึงข้อกำหนดในการรายงานเหตุการณ์ทางไซเบอร์ภายใน 24 ชั่วโมง

รัฐบาลดำเนินการเพื่อปรับปรุงความปลอดภัยและความยืดหยุ่นของโครงสร้างพื้นฐานที่สำคัญ

ต่อไป

รัฐสภาสหรัฐฯแห่งสหรัฐอเมริกาผ่านกฎหมายที่อนุญาตให้หน่วยงานความมั่นคงปลอดภัยไซเบอร์และโครงสร้างพื้นฐาน (CISA) ออกข้อบังคับเพื่อกำหนดให้ต้องรายงานเหตุการณ์ทางไซเบอร์จากผู้ให้บริการโครงสร้างพื้นฐานที่สำคัญ และหน่วยงานรักษาความปลอดภัยด้านการขนส่งของสหรัฐฯ (TSA) ได้ออกข้อกำหนดใหม่เกี่ยวกับความปลอดภัยทางไซเบอร์เฉพาะภาคส่วนในภาคการขนส่ง ในปี 2021 TSA ได้ออกคำสั่งด้านความปลอดภัย 2 ฉบับให้กับผู้ปฏิบัติงานท่อส่งของเหลวและก๊าซธรรมชาติที่เป็นอันตรายเพื่อตอบสนองต่อการโจมตีของแรนซัมแวร์ในบริษัท Colonial Pipeline:

- คำสั่งแรกกำหนดให้ผู้ปฏิบัติงานกำหนดผู้ประสานงานด้านความปลอดภัยทางไซเบอร์ รายงานเหตุการณ์ทางไซเบอร์ภายใน 12 ชั่วโมง และดำเนินการประเมินช่องโหว่ของระบบ
- คำสั่งที่สองซึ่ง TSA แก้ไขในปี 2022 กำหนดให้ใช้มาตรการลดผลกระทบเฉพาะเพื่อป้องกันการโจมตีจากแรนซัมแวร์และภัยคุกคามอื่นๆ ที่ทราบต่อระบบ IT และ OT พัฒนาและดำเนินการแผนฉุกเฉินด้านความปลอดภัยทางไซเบอร์และแผนรับมือภายใน 30 วัน และผ่านการรักษาความปลอดภัยทางไซเบอร์ประจำปี ทบทวนการออกแบบสถาปัตยกรรม

จากข้อบังคับสำหรับท่อส่ง TSA ได้ออกคำสั่งด้านความปลอดภัยเพิ่มเติม 2 คำสั่งในภายหลังในปี 2021 ซึ่งประกาศใช้ข้อกำหนดด้านความปลอดภัยทางไซเบอร์สำหรับรถไฟบรรทุกสินค้า ผู้ให้บริการรถไฟโดยสารหรือระบบขนส่งทางราง คำสั่งกำหนดให้ผู้ปฏิบัติงานที่ครอบคลุมกำหนดผู้ประสานงานความปลอดภัยทางไซเบอร์ รายงานเหตุการณ์ความปลอดภัยทางไซเบอร์ภายใน 24 ชั่วโมง พัฒนาและดำเนินการแผนตอบสนองต่อเหตุการณ์ความปลอดภัยทางไซเบอร์ และทำการประเมินช่องโหว่ด้านความปลอดภัยทางไซเบอร์ TSA ประกาศพร้อมกันว่าได้ปรับปรุงโปรแกรมการรักษาความปลอดภัยด้านการบินเพื่อกำหนดให้ผู้ให้บริการสนามบินและสายการบินปฏิบัติตามข้อกำหนด 2 ข้อแรก โดยกำหนดผู้ประสานงานและรายงานเหตุการณ์ภายใน 24 ชั่วโมง

การพัฒนานโยบายด้านความปลอดภัยของอุปกรณ์ IoT และ OT

ในหลายสิบประเทศ รัฐบาลกำลังกระตือรือร้นในการพัฒนาข้อกำหนดเพื่อพัฒนาความปลอดภัยทางไซเบอร์ของผลิตภัณฑ์และบริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) รวมถึงอุปกรณ์ IoT และ OT ในบริบทของผลิตภัณฑ์และบริการ ICT ข้อกังวลที่ใหญ่ที่สุดคือความปลอดภัยของห่วงโซ่อุปทานของซอฟต์แวร์และความปลอดภัยของ IoT

- คณะกรรมาธิการยุโรปเสนอกฎหมาย Cyber Resilience Act ซึ่งจะกำหนดข้อกำหนดด้านความปลอดภัยทางไซเบอร์สำหรับซอฟต์แวร์แบบสแตนด์อโลนและอุปกรณ์ที่เชื่อมต่อและบริการเสริม[5] แนวปฏิบัติที่เกี่ยวข้องสำหรับผู้จำหน่ายซอฟต์แวร์ได้แก่ การใช้ประโยชน์จากวงจรชีวิตการพัฒนาซอฟต์แวร์ที่ปลอดภัย[6] และจัดทำรายการวัสดุซอฟต์แวร์[7] ข้อกำหนดด้านความปลอดภัยใหม่จะใช้กับอุปกรณ์ที่เชื่อมต่อและผู้ผลิตทุกรายจะได้รับมอบหมายให้ด้วยการจัดการการเปิดเผยช่องโหว่ที่ประสานกัน[8] กระบวนการสำหรับผลิตภัณฑ์ที่นำออกใช้

ผู้กำหนดนโยบายยังได้มุ่งความสนใจไปที่การเพิ่มจำนวนอย่างต่อเนื่องของอุปกรณ์ IoT และอุปกรณ์ OT บนเครือข่าย

- ในสหราชอาณาจักร ร่างกฎหมายความปลอดภัยผลิตภัณฑ์และโครงสร้างพื้นฐานโทรคมนาคมจะกำหนดให้ผู้ผลิตผลิตภัณฑ์เชื่อมต่อสำหรับผู้บริโภค เช่น สมาร์ททีวี หยุดใช้รหัสผ่านเริ่มต้นที่เป็นเป้าหมายง่ายสำหรับอาชญากรไซเบอร์ กำหนดนโยบายการเปิดเผยช่องโหว่ (เช่น วิธี เพื่อรับการแจ้งเตือนเกี่ยวกับข้อบกพร่องด้านความปลอดภัย) และเพื่อให้โปร่งใสเกี่ยวกับระยะเวลาขั้นต่ำที่พวกเขาจะอัปเดตความปลอดภัย[9]
- ในสหภาพยุโรป มีการบังคับใช้มาตรฐานหรือข้อกำหนดด้านความปลอดภัยใหม่ผ่านตราสารทางกฎหมายหลายฉบับ รวมถึงกฎหมายที่ได้รับมอบอำนาจจาก Radio Equipment Directive ที่ใช้กับอุปกรณ์ไร้สายและพยายามที่จะปรับปรุงความยืดหยุ่นของเครือข่าย ปกป้องความเป็นส่วนตัวของผู้บริโภค และลดความเสี่ยงของการฉ้อโกงทางการเงิน[10] นอกจากนี้การใช้รูปนอกจากนี้ การใช้แบบแผนการรับรองระบบคลาวด์[11] ที่กำลังอยู่ในระหว่างการพัฒนาซึ่งเป็นผลมาจากพระราชบัญญัติความปลอดภัยทางไซเบอร์ของสหภาพยุโรปปี 2019,[12] อาจจำเป็นต้องใช้

ความจำเป็นในความสอดคล้อง

ในหลายกรณี ขอบเขตของกิจกรรมทั่วทั้งภูมิภาค ภาคส่วน เทคโนโลยี และพื้นที่การจัดการความเสี่ยงด้านปฏิบัติการกำลังถูกติดตามไปพร้อมๆ กัน ส่งผลให้เกิดการทับซ้อนหรือไม่สอดคล้องกันในขอบเขต ข้อกำหนด และความซับซ้อน สำหรับองค์กรที่ต้องการใช้ประโยชน์จากคำแนะนำหรือแสดงการปฏิบัติตาม หากไม่มีคำจำกัดความของ IoT ที่เป็นที่ยอมรับในระดับสากล ขอบเขตจะเป็นสิ่งที่ท้าทายอย่างยิ่งสำหรับข้อบังคับด้านอุปกรณ์ IoT และ OT ตัวอย่างข้างต้นอาจนำไปใช้กับ “ผลิตภัณฑ์ที่เชื่อมต่อและบริการเสริม” “ผลิตภัณฑ์ที่เชื่อมต่อได้สำหรับผู้บริโภค” และ “อุปกรณ์ไร้สาย” ในขณะเดียวกัน รัฐบาลหลายแห่งตั้งเป้าที่จะใช้ระบบการประเมินที่มีประสิทธิภาพมากขึ้น เพื่อทำความเข้าใจว่าองค์กรและผลิตภัณฑ์ต่างๆ เป็นไปตามข้อกำหนดในปัจจุบัน ที่เกิดขึ้นใหม่ และที่กำลังพัฒนาหรือไม่ เมื่อแนวโน้มเหล่านี้รวมกัน ความซับซ้อนจะเพิ่มขึ้น ที่น่ายินดีคือคำถามที่เกิดขึ้นระหว่างการปรึกษาหารือเกี่ยวกับกฎหมายความยืดหยุ่นทางไซเบอร์ของสหภาพยุโรป (EU Cyber Resilience Act) ได้สำรวจว่ากฎระเบียบใหม่อาจโต้ตอบกับกฎระเบียบด้านความปลอดภัยในโลกไซเบอร์ที่มีอยู่ได้อย่างไร ซึ่งบ่งชี้ถึงเจตนาที่จะหลีกเลี่ยงข้อกำหนดด้านความปลอดภัยทางไซเบอร์ที่ขัดแย้งกัน

แนวทางซ้ำๆ ที่อิงตามความเสี่ยงและผลลัพธ์หรือเชิงกระบวนการ (เทียบกับการนำไปใช้เฉพาะ) สามารถส่งเสริมการรักษาความปลอดภัยทางไซเบอร์ที่ดีขึ้นและการปรับปรุงอย่างต่อเนื่อง ในทำนองเดียวกัน การมุ่งเน้นที่การเปิดใช้งานการทำงานร่วมกันข้ามภาคส่วน ภูมิภาค และด้านนโยบายสามารถเพิ่มความปลอดภัยทางไซเบอร์ได้อย่างสม่ำเสมอทั่วทั้งห่วงโซ่อุปทานทั่วโลกที่เชื่อมต่อถึงกัน

รัฐบาลดำเนินการเพื่อปรับปรุงความปลอดภัยและความยืดหยุ่นของโครงสร้างพื้นฐานที่สำคัญ

ต่อไป

มีการพัฒนานโยบายความปลอดภัยทางไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญซับซ้อนขึ้นเรื่อยๆ ทั่วทั้งภูมิภาค ภาคส่วนต่างๆ และหัวข้อต่างๆ กิจกรรมนี้นำมาซึ่งโอกาสและความท้าทายที่สำคัญ วิธีการดำเนินการของรัฐบาลจะมีความสำคัญต่ออนาคตของการเปลี่ยนแปลงทางดิจิทัลและการรักษาความปลอดภัยทั่วทั้งระบบนิเวศ

เร่งการลงทุนทั่วทั้งระบบนิเวศในการรักษาความปลอดภัยของห่วงโซ่อุปทานของซอฟต์แวร์และสถาปัตยกรรม Zero Trust

คำสั่งผู้บริหารสหรัฐ (EO) 14028 เรื่องการปรับปรุงการรักษาความปลอดภัยทางไซเบอร์เป็นตัวกระตุ้นเพื่อเร่งการริเริ่มอย่างต่อเนื่องของ Microsoft เพื่อลงทุนในความปลอดภัยในซัพพลายเชนของเราเองและทั่วทั้งระบบนิเวศ และเพื่อให้ลูกค้าของเราสามารถบรรลุวัตถุประสงค์ Zero Trust ได้

เราเชื่อมานานแล้วว่าการปรับปรุงห่วงโซ่อุปทานของซอฟต์แวร์ต้องมีการแบ่งปันการเรียนรู้และแนวทางปฏิบัติที่ดีที่สุด โดยเริ่มจากการเปิดตัววงจรการพัฒนาการรักษาความปลอดภัยของ Microsoft เมื่อประมาณ 15 ปีที่แล้ว

นอกจากนี้ เรายังร่วมมืออย่างใกล้ชิดกับ National Cybersecurity Center of Excellence เพื่อแสดงแนวทางของ Zero Trust Architecture ที่ประยุกต์ใช้กับทั้งในสถานที่และเทคโนโลยีคลาวด์ และสร้างความสามารถใหม่ๆ ของผลิตภัณฑ์ รวมถึงความสามารถในการบังคับใช้การพิสูจน์ตัวตนที่ป้องกันฟิชชิ่งสำหรับไฮบริดและมัลติ- สภาพแวดล้อมแบบคลาวด์

ในวันนี้ เราจะก้าวไปไกลกว่าข้อกำหนดของ EO เพื่อแสดงให้เห็นถึงความสอดคล้องกับข้อกำหนดด้านความปลอดภัยของห่วงโซ่อุปทานของซอฟต์แวร์ และให้ข้อมูลรายการวัสดุซอฟต์แวร์ (SBOM) ในสองวิธี:

1. อันดับแรก เรากำลังแชร์เครื่องมือสร้าง SBOM เวอร์ชันโอเพ่นซอร์ส ซึ่งเราสร้างขึ้นเพื่อให้ผสานรวมกับไปป์ไลน์ CI/CD ได้อย่างง่ายดาย ซึ่งรองรับการสร้างบนแพลตฟอร์ม Windows, Linux, Mac, iOS และ Android[13]
2. ประการที่สอง เรามีส่วนร่วมในการพัฒนามาตรฐานอุตสาหกรรมสำหรับความซื่อตรงของห่วงโซ่อุปทาน ความโปร่งใส และความน่าเชื่อถือ (SCITT) สิ่งนี้จะช่วยให้มีการแลกเปลี่ยนโดยอัตโนมัติของข้อมูลห่วงโซ่อุปทานที่ตรวจสอบได้ รวมถึงสิ่งประดิษฐ์ที่แสดงให้เห็นถึงความสอดคล้องกับข้อกำหนด เช่น สิ่งที่เป็นผลมาจากแนวทางห่วงโซ่อุปทานซอฟต์แวร์ของ EO

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. สถาบันพหุภาคีต้องได้รับการพิจารณาใหม่เพื่อจัดการกับความท้าทายเร่งด่วนของการโจมตีทางไซเบอร์ของรัฐชาติ
2. พัฒนานโยบายความปลอดภัยทางไซเบอร์ที่สอดคล้องและทำงานร่วมกันได้ทั่วทั้งภูมิภาค ภาคส่วนต่างๆ และหัวข้อต่างๆ

ลิงค์ไปยังข้อมูลเพิ่มเติม

- การลงทุนอย่างต่อเนื่องในการรักษาความปลอดภัยในห่วงโซ่อุปทานเพื่อสนับสนุนคำสั่งบริหารความปลอดภัยทางไซเบอร์ | ชุมชนเทคโนโลยีของ Microsoft
- US Government sets forth Zero Trust architecture strategy and requirements | บล็อกความปลอดภัยของ Microsoft
- CYBER EO | Microsoft Federal
- ความสมบูรณ์ของห่วงโซ่อุปทาน ความโปร่งใส และความน่าเชื่อถือ | github.com
- การใช้สถาปัตยกรรม Zero Trust | NCoE (nist.gov)

IoT และ OT เปิดเผย: แนวโน้มและการโจมตี

โลกดิจิทัลที่เชื่อมโยงกันมากขึ้นหมายความว่าอุปกรณ์กำลังออนไลน์อย่างรวดเร็ว สื่อสารกับระบบที่ใหญ่ขึ้น รวบรวมข้อมูล และสร้างการมองเห็นในพื้นที่ที่เคยถูกบดบัง สิ่งนี้นำมาซึ่งโอกาสสำหรับองค์กรและผู้คุกคาม โดยธุรกิจอาชญากรรมไซเบอร์กลายเป็นทั้งอุตสาหกรรมมูลค่าหลายพันล้านดอลลาร์และความเสี่ยง

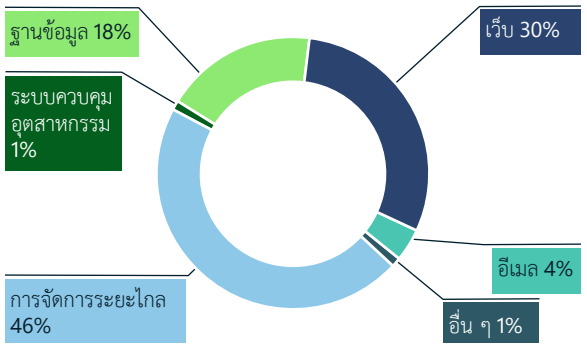
อุปกรณ์ IoT รวมถึงทุกอย่างตั้งแต่เครื่องพิมพ์ไปจนถึงกล้องเว็บ อุปกรณ์ควบคุมสภาพอากาศ และการควบคุมการเข้าถึงอาคาร ก่อให้เกิดความเสี่ยงด้านความปลอดภัยเฉพาะบุคคล องค์กร และเครือข่าย แม้จะมีความสำคัญต่อการดำเนินงานขององค์กรหลายแห่ง แต่ก็สามารถกลายเป็นความรับผิดชอบและความเสี่ยงด้านความปลอดภัยได้อย่างรวดเร็ว การนำโซลูชัน IoT มาใช้อย่างรวดเร็วในเกือบทุกอุตสาหกรรมได้เพิ่มจำนวนของเวกเตอร์การโจมตีและความเสี่ยงที่เปิดเผยขององค์กร

มัลแวร์ในฐานะบริการได้ย้ายเข้าสู่การดำเนินงานขนาดใหญ่กับโครงสร้างพื้นฐานและสาธารณูปโภคของพลเรือน (รวมถึงโรงพยาบาล น้ำมันและก๊าซ โครงข่ายไฟฟ้า บริการขนส่ง และโครงสร้างพื้นฐานที่สำคัญอื่นๆ) ตลอดจนเครือข่ายขององค์กร ผู้คุกคามต้องใช้ความพยายามในการวิจัยอย่างมากในการเปิดเผยและใช้ประโยชน์จากการกำหนดค่าของสภาพแวดล้อมการปฏิบัติงานและอุปกรณ์ IoT และ OT ที่ฝังอยู่

อุปกรณ์ IoT มีความเสี่ยงด้านความปลอดภัยเฉพาะในฐานะจุดเข้าและจุดหมุนในเครือข่าย อุปกรณ์ IoT หลายล้านเครื่องไม่ได้แพตช์หรือเปิดเผย

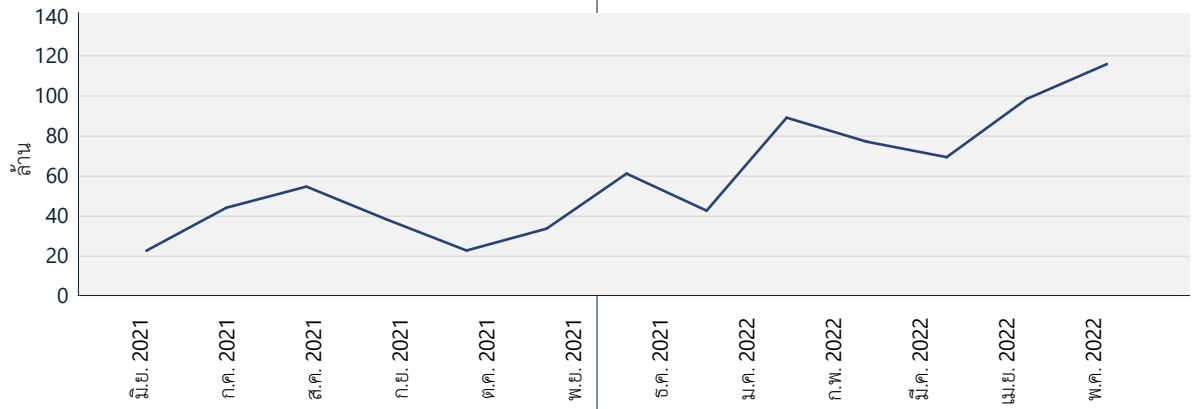
อุปกรณ์ที่เปิดเผยสามารถค้นพบได้ผ่านเครื่องมือค้นหาทางอินเทอร์เน็ตโดยการระบุบริการที่รับฟังบนพอร์ตเครือข่ายแบบเปิด พอร์ตเหล่านี้มักใช้สำหรับการจัดการอุปกรณ์จากระยะไกล หากไม่ได้รับการรักษาความปลอดภัยอย่างถูกต้อง อุปกรณ์ IoT ที่เปิดเผยสามารถใช้เป็นจุดหมุนในชั้นอื่นของเครือข่ายองค์กรได้ เนื่องจากผู้ใช้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงพอร์ตจากระยะไกลได้ เราสังเกตเห็นผู้คุกคามหลายรายที่พยายามใช้ประโยชน์จากช่องโหว่ในอุปกรณ์ที่เปิดเผยอินเทอร์เน็ต ตั้งแต่กล้องไปจนถึงเราเตอร์ไปจนถึงเทอร์โมสตัท อย่างไรก็ตาม แม้จะมีความเสี่ยง แต่อุปกรณ์นับล้านยังคงไม่ปะติดปะต่อหรือถูกเปิดเผย

สรุปประเภทการโจมตีบน IoT/OT



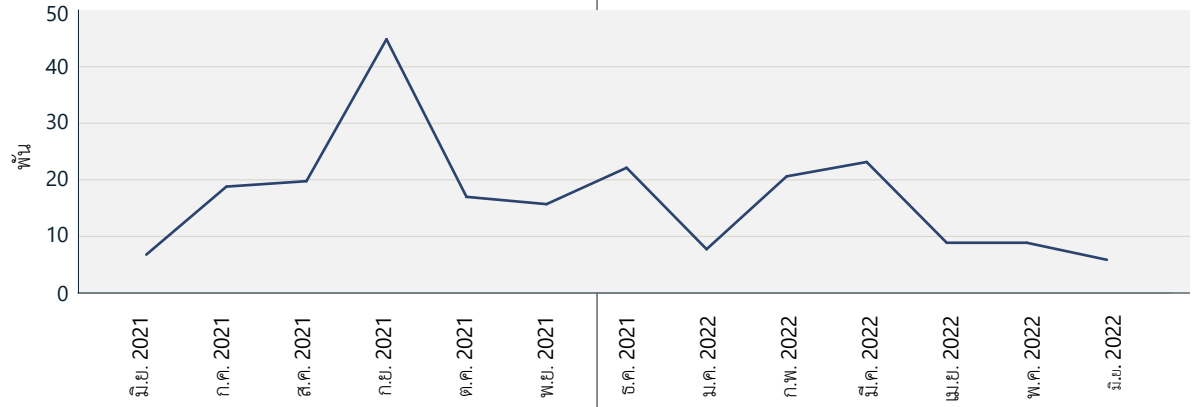
ประเภทการโจมตีที่สังเกตได้จากเครือข่ายเซ็นเซอร์ MSTIC การโจมตีที่แพร่หลายที่สุดคือการโจมตีอุปกรณ์การจัดการระยะไกล การโจมตีผ่านเว็บ และการโจมตีฐานข้อมูล (การใช้กำลังหรือการใช้ประโยชน์)

การโจมตีอุปกรณ์การจัดการระยะไกล



การโจมตีพอร์ตการจัดการระยะไกลเพิ่มขึ้นเมื่อเวลาผ่านไป ดังที่เห็นได้จากเครือข่ายเซ็นเซอร์ MSTIC

การโจมตีเว็บต่อ IoT และ OT



ปริมาณการโจมตีเว็บในช่วงเวลาหนึ่ง ดังที่เห็นได้จากเครือข่ายเซ็นเซอร์ MSTIC เนื่องจากจำนวนอุปกรณ์ที่เชื่อมต่อโดยตรงกับเว็บยังคงลดลง ในที่สุดผู้โจมตีอาจมีโอกาสน้อยที่จะตรวจสอบหาอุปกรณ์เหล่านั้น

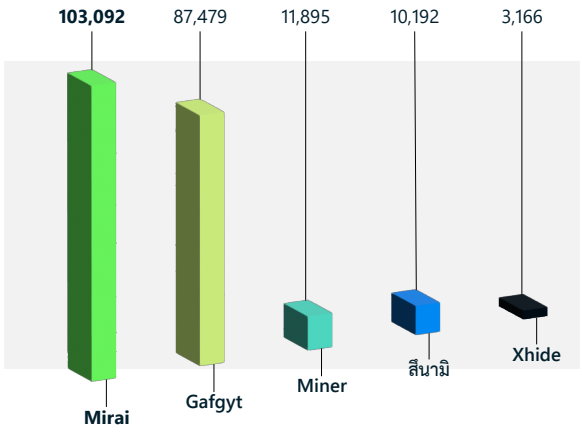
IoT และ OT เปิดเผย: แนวโน้มและการโจมตี

ต่อไป

ยูทิลิตี้มัลแวร์ปรับปรุงใหม่

ในขณะที่กลุ่มอาชญากรไซเบอร์มีการพัฒนา การติดตั้งมัลแวร์และตัวเลือกเป้าหมายก็เช่นกัน ในปีที่ผ่านมา เราสังเกตเห็นการโจมตีโปรโตคอล IoT ทั่วไป เช่น Telnet ลดลงอย่างมาก ในบางกรณีมากถึง 60 เปอร์เซ็นต์ ในขณะเดียวกัน บ็อตเน็ตก็ถูกนำมาใช้ใหม่โดยกลุ่มอาชญากรไซเบอร์และผู้มีบทบาทในระดับชาติ การคงอยู่ของมัลแวร์ เช่น Mirai เน้นย้ำถึงความเป็นโมดูลของการโจมตีเหล่านี้ และความสามารถในการปรับตัวของภัยคุกคามที่มีอยู่

มัลแวร์ IoT อันดับต้นๆ ที่ตรวจพบได้ทั่วไป

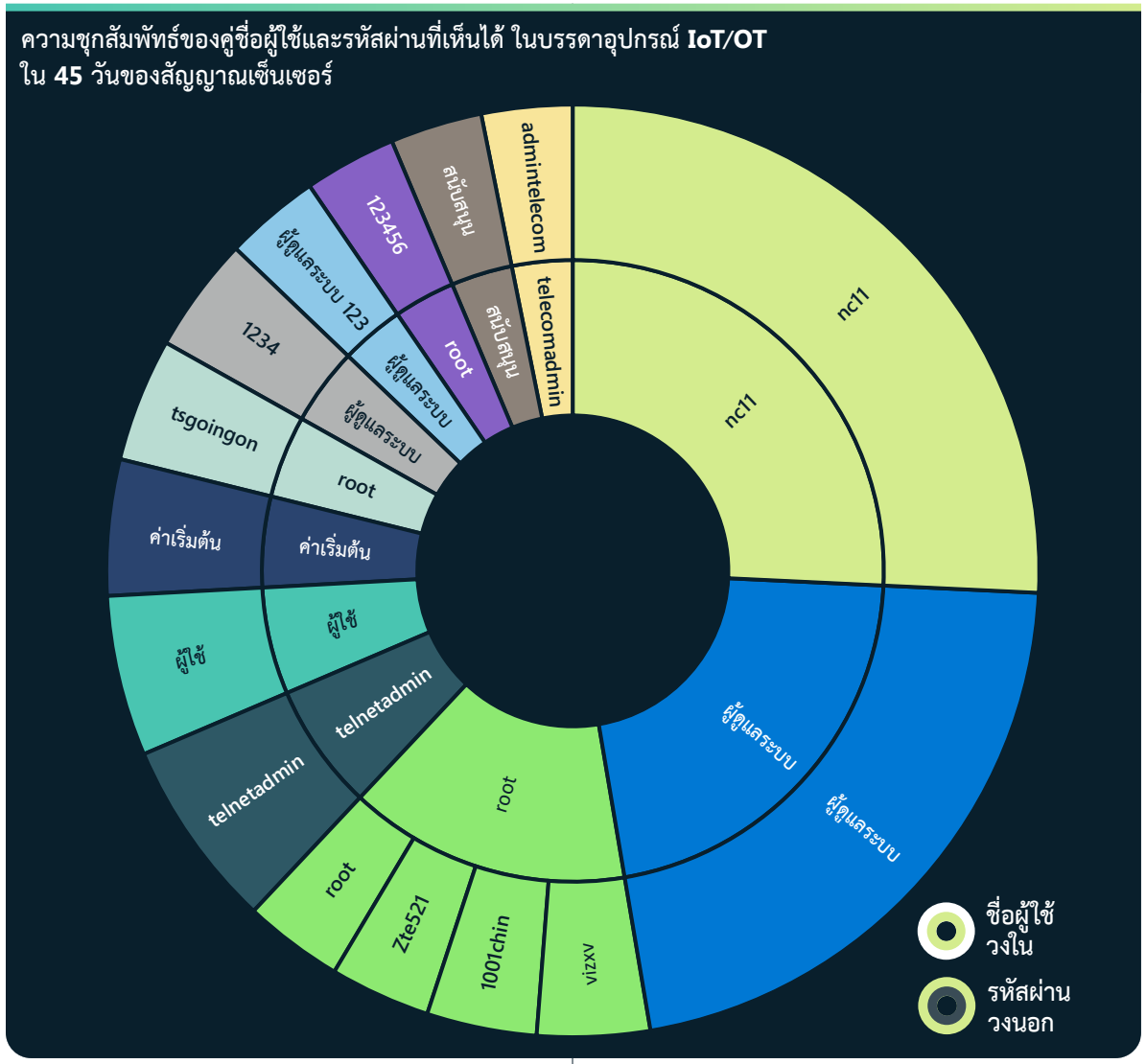


Mirai พัฒนาเพื่อแพร่เชื้อไปยังอุปกรณ์ IoT ที่หลากหลาย รวมถึงกล้องอินเทอร์เน็ตโปรโตคอล เครื่องบันทึกวิดีโอดิจิตอลของกล้องรักษาความปลอดภัย และเราเตอร์ เวกเตอร์การโจมตีข้ามการควบคุมความปลอดภัยแบบเดิม และก่อให้เกิดความเสี่ยงต่ออุปกรณ์ปลายทางภายในเครือข่ายโดยการใช้ประโยชน์จากช่องโหว่เพิ่มเติมและย้ายออกไปด้านข้าง Mirai ได้รับการออกแบบใหม่หลายครั้ง โดยมีรูปแบบต่างๆ ที่ปรับให้เข้ากับสถาปัตยกรรมที่แตกต่างกัน และใช้ประโยชน์จากช่องโหว่ทั้งที่รู้จักและช่องโหว่ Zero-day เพื่อประนีประนอมกับเวกเตอร์การโจมตีใหม่ๆ

การใช้งาน Mirai เพิ่มขึ้นระหว่างสถาปัตยกรรมซีพียู x86 ทั้งแบบ 32 และ 64 บิตในช่วงปีที่ผ่านมา และมัลแวร์ได้รับความสามารถใหม่ซึ่งนำไปใช้อย่างรวดเร็วโดยรัฐชาติและกลุ่มอาชญากร ผู้โจมตีระดับชาติใช้ประโยชน์จากรูปแบบใหม่ของบอตเน็ตที่มีอยู่แล้วในการโจมตีแบบกระจายการปฏิเสธการให้บริการ (DDoS) กับศัตรูต่างชาติ

เนื่องจากรายได้จากการโจมตีอุปกรณ์ IoT ลดลงในปี 2022 เราสังเกตเห็นกลุ่มผู้คุกคามหลายกลุ่มใช้ช่องโหว่ในทางที่ผิด เช่น Log4j และ Spring4Shell เพื่อส่งเพย์โหลดที่เป็นอันตรายไปยังอุปกรณ์ต่างๆ เช่น เซิร์ฟเวอร์ แพร่เชื้อ และคัดเลือกพวกเขาเข้าสู่บอตเน็ตขนาดใหญ่ที่ดำเนินการโจมตี DDoS ยูทิลิตี้ที่ปรับปรุงใหม่ของมัลแวร์ที่ออกแบบมาเพื่อกำหนดเป้าหมายอุปกรณ์ IoT ที่มีช่องโหว่มีผลกระทบร้ายแรงสำหรับทั้งองค์กรและประเทศชาติ เนื่องจากการเคลื่อนไหวด้านข้างอาจทำให้แบ็คดอร์เปิดเผยต่อเพย์โหลดเพิ่มเติมและอุปกรณ์อื่นๆ บนเครือข่าย

โปรโตคอลระบบควบคุมอุตสาหกรรมจำนวนมากไม่ได้รับการตรวจสอบ ดังนั้นจึงเสี่ยงต่อการโจมตี เฉพาะ OT นี่อาจหมายถึงความเสี่ยงที่เพิ่มขึ้นสำหรับโครงสร้างพื้นฐานที่สำคัญ



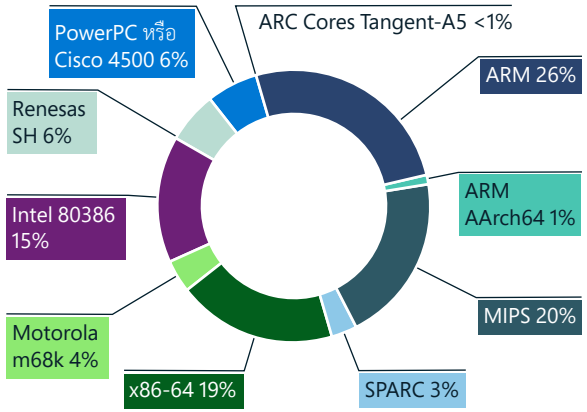
การใช้คู่ชื่อผู้ใช้และรหัสผ่านร่วมกันจะเพิ่มความเสี่ยงต่อการถูกประนีประนอม จากขนาดตัวอย่างของอุปกรณ์ IoT และ OT กว่า 39 ล้านชิ้น อุปกรณ์ที่ใช้ชื่อผู้ใช้และรหัสผ่านเหมือนกันคิดเป็นประมาณ 20 เปอร์เซ็นต์

IoT และ OT เปิดเผย: แนวโน้มและการโจมตี

ต่อไป

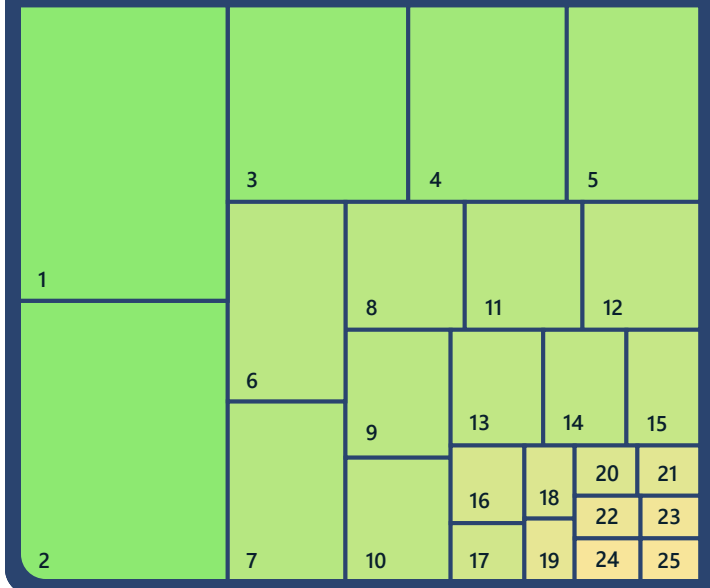
แม้ว่าการกำหนดค่าที่ไม่รัดกุมและข้อมูลประจำตัวที่เป็นค่าเริ่มต้นจะยังก่อให้เกิดความเสี่ยงต่อเครือข่าย แต่ Microsoft ก็สังเกตเห็นการแสวงหาผลประโยชน์บนเว็บจำนวนมากโดยใช้ HTTP เราสังเกตเห็นการโจมตีบริการบนเว็บที่เพิ่มขึ้นนี้โดยใช้บอตเน็ตรุ่นเก่า ในขณะเดียวกัน จำนวนพอร์ต telnet ที่เปิดอยู่บนอินเทอร์เน็ตก็ลดลง ซึ่งเป็นสัญญาณเชิงบวกสำหรับความปลอดภัยของเครือข่าย เนื่องจากบอทเน็ตซึ่งก่อให้เกิดความเสี่ยงในอดีตต่ออุปกรณ์กำลังสูญเสียความเกี่ยวข้อง แม้ว่าพอร์ต telnet ที่เปิดอยู่จะลดลง แต่เรายังคงสังเกตเห็นบ็อตเน็ตถาวรในเครือข่ายเซ็นเซอร์

การแพร่กระจายของมัลแวร์ IoT โดยสถาปัตยกรรม CPU



Microsoft สังเกตว่าอุปกรณ์ IoT ที่ทำงานบน ARM ตกเป็นเป้าหมายของมัลแวร์มากที่สุด ตามมาด้วย MIPS, X86-64 และ Intel 80386 CPU

ความแพร่หลายของโปรโตคอลระบบควบคุมอุตสาหกรรม



1. อีเทอร์เน็ต/IP
2. MODBUS
3. BACNet
4. Siemens S7
5. Profinet เรียลไทม์
6. Profinet DCP
7. Siemens S7 Plus
8. ชุดโค้ด
9. ตัวแทนของ Siemens WinCC
10. อีเทอร์เน็ต/IP O/O
11. การควบคุมการเข้าถึงข้อมูลของ Honeywell
12. MMS
13. IEC-60870
14. การวินิจฉัย Honeywell FDA
15. Suitelink
16. DeltaV
17. GSM
18. DNP3
19. AMS
20. SRTP
21. TwinCat
22. Emerson Roc
23. Bently Nevada
24. มิตซูบิชิ MELSEC
25. TriStation Tricon

ช่องโหว่ของโปรโตคอลระบบควบคุมอุตสาหกรรม

เราตรวจสอบข้อมูล OT จากเซ็นเซอร์ที่เชื่อมต่อกับระบบคลาวด์ของเรา ซึ่งเผยให้เห็นโปรโตคอลระบบควบคุมอุตสาหกรรม (ICS) ที่พบมากที่สุด โปรโตคอลเหล่านี้ให้ข้อมูลเชิงลึกเกี่ยวกับธรรมชาติของอุปกรณ์เหล่านี้และพื้นผิวการโจมตี สิ่งนี้เกี่ยวข้องอย่างยิ่งกับการรักษาความปลอดภัยของโครงสร้างพื้นฐานที่สำคัญ การเรียนรู้ที่สำคัญบางประการ ได้แก่:

1. โปรโตคอลส่วนใหญ่ที่แสดงเป็นกรรมสิทธิ์ ดังนั้นเครื่องมือตรวจสอบด้านไอทีมาตรฐานจึงไม่มีการมองเห็นความปลอดภัยที่เพียงพอในอุปกรณ์และโปรโตคอลเหล่านี้ ด้วยเหตุนี้ เครือข่ายจึงไม่มีการตรวจสอบ ดังนั้นจึงเสี่ยงต่อการถูกโจมตีเฉพาะ OT
2. มีโปรโตคอลเฉพาะของผู้ขายที่หลากหลาย ซึ่งหมายความว่าโซลูชันการรักษาความปลอดภัยเฉพาะของผู้จำหน่ายจะไม่สามารถครอบคลุมเครือข่ายทั้งหมดได้อย่างเพียงพอ Microsoft จัดลำดับความสำคัญของวิธีการที่ไม่เชื่อเรื่องพระเจ้าของผู้จำหน่าย เพื่อให้ความคุ้มครองด้านความปลอดภัยสำหรับอุปกรณ์ต่างๆ ที่หลากหลาย
3. องค์กรควรตรวจสอบให้แน่ใจว่าโปรโตคอลเหล่านี้ไม่ถูกเปิดเผยโดยตรงจากเครือข่ายของตนสู่อินเทอร์เน็ต การเปิดเผยนี้อาจก่อให้เกิดความเสี่ยงด้านความปลอดภัยที่สำคัญเนื่องจากช่องโหว่และลักษณะที่ไม่ปลอดภัยของโปรโตคอลเหล่านี้

มัลแวร์เช่น Mirai ยังคงมีอยู่โดยการพัฒนาความสามารถใหม่ๆ และกำลังถูกนำไปใช้โดยกลุ่มอาชญากรไซเบอร์และตัวแสดงของรัฐ โดยใช้ประโยชน์จากรูปแบบใหม่ของบอตเน็ตที่มีอยู่แล้วในการโจมตี DDoS กับศัตรูต่างชาติ

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ตรวจสอบให้แน่ใจว่าอุปกรณ์มีความทนทานโดยการใช้แพตช์ เปลี่ยนรหัสผ่านเริ่มต้น และพอร์ต SSH เริ่มต้น
2. ลดพื้นที่การโจมตีโดยกำจัดการเชื่อมต่ออินเทอร์เน็ตและพอร์ตเปิดที่ไม่จำเป็น จำกัดการเข้าถึงระยะไกลโดยการบล็อกพอร์ต ปฏิเสธการเข้าถึงระยะไกลและใช้บริการ VPN
3. ใช้โซลูชันการตรวจจับและตอบสนองเครือข่าย (NDR) ของ IoT/OT-aware และข้อมูลความปลอดภัยและการจัดการเหตุการณ์ (SIEM)/การจัดการความปลอดภัยและการตอบสนอง (SOAR) เพื่อตรวจสอบอุปกรณ์เพื่อหาพฤติกรรมที่ผิดปกติหรือไม่ได้รับอนุญาต เช่น การสื่อสารกับโฮสต์ที่ไม่คุ้นเคย
4. แบ่งกลุ่มเครือข่ายเพื่อจำกัดความสามารถของผู้โจมตีในการเคลื่อนที่ไปด้านข้างและประนีประนอมทรัพย์สินหลังจากการบุกรุกครั้งแรก อุปกรณ์ IoT และเครือข่าย OT ควรถูกแยกออกจากเครือข่ายไอทีขององค์กรโดยใช้ไฟร์วอลล์
5. ตรวจสอบให้แน่ใจว่าโปรโตคอล ICS จะไม่เปิดเผยสู่อินเทอร์เน็ตโดยตรง

ห่วงโซ่อุปทานและการแฮ็คเฟิร์มแวร์

อุปกรณ์เชื่อมต่ออินเทอร์เน็ตเกือบทุกเครื่องมีเฟิร์มแวร์ ซึ่งเป็นซอฟต์แวร์ที่ฝังอยู่ในฮาร์ดแวร์หรือแผงวงจรของอุปกรณ์ ในช่วงไม่กี่ปีที่ผ่านมา เราได้เห็นการกำหนดเป้าหมายเฟิร์มแวร์เพิ่มขึ้นเพื่อเริ่มการโจมตีทำลายล้าง เนื่องจากเฟิร์มแวร์มีแนวโน้มว่าจะยังคงเป็นเป้าหมายที่มีค่าสำหรับผู้คุกคามองค์กรต่างๆ จึงต้องป้องกันการแฮ็กเฟิร์มแวร์

เฟิร์มแวร์มีหน้าที่รับผิดชอบในการทำงานหลักของอุปกรณ์ เช่น การเชื่อมต่อกับเครือข่ายหรือการจัดเก็บข้อมูล พบเฟิร์มแวร์ได้ในเราเตอร์ กล้อง โทรทัศน์ และอุปกรณ์อื่นๆ ที่ใช้ในองค์กร (IoT) พร้อมกับอุปกรณ์ควบคุมอุตสาหกรรม (OT) ที่ใช้ในโครงสร้างพื้นฐานที่สำคัญ ในอดีต เฟิร์มแวร์ถูกเขียนขึ้นด้วยรหัสที่ไม่ปลอดภัย ทำให้เกิดช่องโหว่ที่สำคัญ ซึ่งสามารถใช้เพื่อครอบครองอุปกรณ์หรือใส่รหัสที่เป็นอันตรายลงในเฟิร์มแวร์ได้

ความเสี่ยงนี้จะทวีคูณเมื่อพูดถึงห่วงโซ่อุปทาน อุปกรณ์ส่วนใหญ่สร้างขึ้นโดยใช้ส่วนประกอบซอฟต์แวร์และฮาร์ดแวร์จากผู้ผลิตจำนวนมาก เช่นเดียวกับไลบรารีโอเพ่นซอร์ส ในหลายกรณี ผู้ให้บริการอุปกรณ์ไม่สามารถมองเห็นรายการวัสดุฮาร์ดแวร์และซอฟต์แวร์ (H/SBOM) เพื่อประเมินความเสี่ยงด้านห่วงโซ่อุปทานของอุปกรณ์ในเครือข่ายของตนได้ ในเดือนมิถุนายน 2020 มีการเปิดเผยช่องโหว่ในกลุ่มเครือข่ายที่ใช้โดยผู้ผลิตหลายรายซึ่งส่งผลกระทบต่ออุปกรณ์ IoT หลายร้อยล้านเครื่องในพื้นที่อุปกรณ์สำหรับผู้บริโภคและอุปกรณ์อุตสาหกรรม[14] ในบางกรณี Network Stack ถูกเปลี่ยนแบรนด์ใหม่โดยผู้ขายรายอื่น และไม่มีสัญญาณบ่งชี้ว่าอุปกรณ์มีช่องโหว่ เราเห็นภัยคุกคามที่เพิ่มมากขึ้นของผู้ไม่ประสงค์ดีที่กำหนดเป้าหมายซอฟต์แวร์และห่วงโซ่อุปทานฮาร์ดแวร์ของอุปกรณ์ IoT/OT นี้เพื่อประนีประนอมองค์กร

กระบวนการอัปเดตเฟิร์มแวร์จะแตกต่างกันไปในแต่ละอุปกรณ์ และความซับซ้อนและความท้าทายด้านลอจิสติกส์ในการดำเนินการจะส่งผลต่อความถี่ในการอัปเดต ไม่สามารถระบุได้เสมอไปว่าอุปกรณ์กำลังเรียกใช้เฟิร์มแวร์ล่าสุดหรือไม่ ทำให้ผู้เชี่ยวชาญด้านความปลอดภัยสามารถตรวจสอบและรับรองท่าทางความปลอดภัยในอุปกรณ์ IoT และ OT ของตนได้ยาก นอกจากนี้ อุปกรณ์บางอย่างมีเฟิร์มแวร์ที่ไม่ได้ลงนามด้วยการเข้ารหัส ทำให้สามารถอัปเดตได้โดยไม่ต้องมีการตรวจสอบจากผู้ใช้ จุดอ่อนเหล่านี้ยิ่งเปิดทางให้อุปกรณ์โจมตีห่วงโซ่อุปทานตลอดห่วงโซ่การผลิตและการกระจายสินค้า

เพื่อจัดการกับภัยคุกคามเหล่านี้ Microsoft ลงทุนอย่างมากในการรับรองความปลอดภัยและความสมบูรณ์ของเฟิร์มแวร์ในขณะที่เคลื่อนผ่านขั้นตอนต่างๆ ของห่วงโซ่อุปทาน และในการยืนยันว่าไม่มีการแก้ไขใดๆ ในระหว่างการนำเข้าหรือระหว่างทาง สิ่งนี้จะช่วยให้เราตรวจสอบความน่าเชื่อถือระหว่างส่วนไปป์ไลน์แต่ละส่วนและจัดหาห่วงโซ่การดูแลตั้งแต่ต้นจนจบที่ได้รับการรับรองและพิสูจน์ได้สำหรับส่วนประกอบทุกชิ้นที่เราจัดส่งให้กับลูกค้า เรากำลังทำงานร่วมกับพันธมิตรของเราเพื่อนำการรักษาความปลอดภัยแบบชิปไปสู่ระบบคลาวด์ไปยังอุปกรณ์ทั้งหมดในองค์กรและเครือข่าย OT

"ซัพพลายเออร์โครงสร้างพื้นฐานด้านไอซีทีกำลังตกเป็นเป้าหมายมากขึ้น เนื่องจากพวกเขาเปิดใช้การจำลองการโจมตีครั้งเดียวอย่างกว้างขวาง ในขณะเดียวกัน กฎหมาย ข้อบังคับทั่วโลก และความต้องการของลูกค้าสำหรับความปลอดภัยและความยืดหยุ่นของห่วงโซ่อุปทานก็เพิ่มสูงขึ้น ซึ่งมักจะทำให้ความต้องการของพวกเขาแตกต่างกัน

ทางออกคือการเป็นหุ้นส่วน เมื่อทำงานร่วมกับซัพพลายเออร์และรัฐบาลทั่วโลก Microsoft มุ่งมั่นที่จะจัดการกับความปลอดภัยในระบบนิเวศห่วงโซ่อุปทานของเรา ซึ่งเกินความต้องการจากลูกค้าและหน่วยงานกำกับดูแล ในการทำเช่นนี้ เรากำลังขับเคลื่อนแนวทางที่ครอบคลุมในการรักษาความปลอดภัยและความยืดหยุ่นในการปฏิบัติงานซึ่งปรับใช้อย่างยืดหยุ่นทั่วทั้งห่วงโซ่อุปทาน

การขับเคลื่อนความสมบูรณ์ของเฟิร์มแวร์ตั้งแต่การออกแบบจนถึงการทำงานของอุปกรณ์เป็นกุญแจสำคัญในแนวทางร่วมกันของเรา การรับรองกระบวนการ SDL ของซัพพลายเออร์และการปรับใช้รูทฮาร์ดแวร์ของนวัตกรรมที่เชื่อถือได้เป็นตัวอย่างของวิธีที่เราสามารถ 'สร้าง' ความสมบูรณ์ของห่วงโซ่อุปทานได้

ชุมชนของเราใช้ประโยชน์จากการวิจัยและพัฒนาโดยรวมซึ่งครอบคลุมถึงเทคนิคการต่อต้านการปลอมแปลงใหม่และกลไกการเข้ารหัส รวมกับการตรวจสอบอย่างต่อเนื่องและการตรวจจับความผิดปกติ เรากำลังดำเนินการร่วมกันในการลดแรงจูงใจของห่วงโซ่อุปทานให้เป็นพื้นผิวของการโจมตีให้เหลือน้อยที่สุด"

Edna Conway,
รองประธาน เจ้าหน้าที่ความปลอดภัยและความเสี่ยง โครงสร้างพื้นฐานระบบคลาวด์

สปอตไลท์เกี่ยวกับช่องโหว่ของเฟิร์มแวร์

ผู้โจมตีใช้ประโยชน์จากช่องโหว่ในเฟิร์มแวร์อุปกรณ์ IoT มากขึ้นเรื่อยๆ เพื่อแทรกซึมเครือข่ายองค์กร ซึ่งแตกต่างจากอุปกรณ์ปลายทางด้านไอทีแบบเดิมที่ใช้ตัวแทน XDR เพื่อระบุจุดอ่อน การระบุช่องโหว่ภายในอุปกรณ์ IoT/OT นั้นเข้าใจยากกว่ามาก

การสำรวจล่าสุดที่จัดทำโดย Microsoft และ Ponemon Institute เน้นทั้งโอกาสและความท้าทายด้านความปลอดภัยของอุปกรณ์ IoT/OT ในองค์กร[15] ในขณะที่ 68 เปอร์เซ็นต์ของผู้ตอบแบบสอบถามเชื่อว่าการนำ IoT/OT มีความสำคัญต่อการเปลี่ยนแปลงทางดิจิทัลเชิงกลยุทธ์ โดย 60 เปอร์เซ็นต์ตระหนักว่าการรักษาความปลอดภัยของ IoT/OT เป็นหนึ่งในด้านที่มีความปลอดภัยน้อยที่สุดของโครงสร้างพื้นฐานด้าน IT/OT

ตัวอย่างของผู้โจมตีที่ใช้ช่องโหว่ในเฟิร์มแวร์อุปกรณ์ IoT เพื่อแทรกซึมเครือข่ายคือโทรจัน Trickbot ซึ่งใช้รหัสผ่านเริ่มต้นและช่องโหว่ในเราเตอร์ Mikrotik[16] เพื่อเลี่ยงระบบป้องกันขององค์กร ความท้าทายพื้นฐานของเฟิร์มแวร์อุปกรณ์ IoT คือการขาดความสามารถในการมองเห็นท่าทางการรักษาความปลอดภัยและช่องโหว่ของอุปกรณ์

แม้ว่าจะมีโซลูชันในการสร้างอุปกรณ์ที่ปลอดภัย แต่ก็มีอุปกรณ์หลายพันล้านเครื่องในตลาดและปรับใช้ในองค์กร สิ่งเหล่านี้เรียกว่าอุปกรณ์บราวน์ฟิลด์ ในปี 2021 Microsoft ได้เข้าซื้อกิจการ ReFirm Labs เพื่อฉายแสงเกี่ยวกับความปลอดภัยของอุปกรณ์ในบราวน์ฟิลด์ และช่วยให้ผู้สร้างอุปกรณ์สามารถปรับปรุงความปลอดภัยของผลิตภัณฑ์ของตนได้ ReFirm Labs วิเคราะห์อิมเมจเฟิร์มแวร์ไบนารีของอุปกรณ์และสร้างรายงานโดยละเอียดเกี่ยวกับจุดอ่อนด้านความปลอดภัยที่อาจเกิดขึ้น[17] เทคโนโลยีนี้กำลังรวมเข้ากับ Microsoft Defender for IoT รุ่นอนาคต

ในปีที่ผ่านมา เราได้ตรวจสอบผลลัพธ์รวมของเฟิร์มแวร์เฉพาะที่ลูกค้าสแกน แม้ว่าจุดอ่อนทั้งหมดที่ค้นพบอาจไม่สามารถใช้ประโยชน์ได้ แต่ก็เน้นย้ำถึงความท้าทายพื้นฐานของการรักษาความปลอดภัยของเฟิร์มแวร์ของอุปกรณ์

โปรดทราบว่าประเภทของจุดอ่อนที่มีอยู่ในอุปกรณ์ IoT/OT จะไม่เป็นที่ยอมรับในอุปกรณ์ปลายทาง Windows หรือ Linux แบบดั้งเดิม

- รหัสผ่านที่ไม่รัดกุม: ยี่สิบเจ็ดเปอร์เซ็นต์ของอิมเมจเฟิร์มแวร์ที่สแกนมีบัญชีที่มีรหัสผ่านที่เข้ารหัสโดยใช้อัลกอริทึมที่อ่อนแอ (MD5/DES) ซึ่งผู้โจมตีสามารถทำลายได้ง่าย

วิเคราะห์จุดอ่อนด้านความปลอดภัยในภาพเฟิร์มแวร์



- ช่องโหว่ที่ทราบ: เช่นเดียวกับระบบอื่นๆ เฟิร์มแวร์อุปกรณ์ IoT/OT ใช้ประโยชน์จากไลบรารีโอเพ่นซอร์สอย่างกว้างขวาง อย่างไรก็ตาม อุปกรณ์มักมาพร้อมกับส่วนประกอบเหล่านี้ในเวอร์ชันที่ล้าสมัย ในการวิเคราะห์ของเรา 32 เปอร์เซ็นต์ของรูปภาพมีช่องโหว่ที่รู้จัก (CVE) อย่างน้อย 10 รายการซึ่งได้รับการจัดอันดับว่าวิกฤต (9.0 หรือสูงกว่า) สี่เปอร์เซ็นต์มีช่องโหว่ร้ายแรงอย่างน้อย 10 รายการที่มีอายุมากกว่าหกปี
- ใบรับรองที่หมดอายุ: ใบรับรองจะใช้ในการตรวจสอบความถูกต้องของการเชื่อมต่อและข้อมูลประจำตัว รวมถึงปกป้องข้อมูลที่ละเอียดอ่อน แต่ 13 เปอร์เซ็นต์ของภาพที่วิเคราะห์มีใบรับรองอย่างน้อย 10 รายการที่หมดอายุมากกว่าสามปีที่ผ่านมา
- ส่วนประกอบของซอฟต์แวร์: สามสิบหกเปอร์เซ็นต์ของรูปภาพมีส่วนประกอบของซอฟต์แวร์ที่ Microsoft แนะนำให้ไม่รวมอยู่ในอุปกรณ์ IoT เช่น เครื่องมือดักจับแพ็กเก็ต (tcpdump, libpcap) ซึ่งสามารถใช้ประโยชน์จากการสำรวจเครือข่ายโดยเป็นส่วนหนึ่งของห่วงโซ่การโจมตี

การโจมตีเฟิร์มแวร์มีอยู่ทั่วไป

Viasat: การใช้ช่องโหว่ของเฟิร์มแวร์เพื่อกำหนดเป้าหมายการสื่อสารผ่านดาวเทียม

ในเดือนกุมภาพันธ์ 2022 เหตุการณ์เครือข่ายดาวเทียมได้ตัดการเชื่อมต่อเครือข่ายการสื่อสารเชิงกลยุทธ์ซึ่งส่งผลกระทบทั่วยุโรป ระบบ KA-SAT ของ Viasat ได้รับทราฟฟิกจำนวนมากที่ตัดการเชื่อมต่อโมเด็มจำนวนมาก และการโจมตีแบบปฏิเสธบริการได้เริ่มขึ้นกับเครือข่าย เนื่องจากบรอดแบนด์แบบคงที่หยุดชะงัก กังหันลมหลายพันเครื่องไม่สามารถเข้าถึงได้จากระยะไกลสำหรับผู้ให้บริการ และมัลแวร์ไวเปอร์ที่เป็นอันตรายถูกนำไปใช้กับโมเด็มที่ได้รับผลกระทบ การหยุดชะงักส่งผลกระทบต่อสถานีรับสัญญาณดาวเทียมมากกว่า 30,000 แห่งที่บริษัทและองค์กรต่างๆ ใช้ในการติดต่อสื่อสาร

Cyclops Blink: ใช้การโจมตีซัพพลายเชนของเฟิร์มแวร์เพื่อกำหนดเป้าหมายเกตเวย์ไฟร์วอลล์

สำหรับผู้ก่อภัยคุกคาม การพัฒนาและการขยายของคำสั่งและการควบคุม (C2) และโครงสร้างพื้นฐานการโจมตีเป็นองค์ประกอบสำคัญของความสำเร็จ เนื่องจากความต้องการโครงสร้างพื้นฐาน C2 ที่มีความเสถียรมีมากขึ้น เราเตอร์จึงกลายเป็นเวกเตอร์การโจมตีที่พึงปรารถนาเนื่องจากการแพทช์ที่ไม่บ่อยนักและการขาดโซลูชันการรักษาความปลอดภัย ที่ครอบคลุม

> Microsoft กำลังร่วมมือกับรัฐบาลและอุตสาหกรรมในเทคโนโลยีการวิเคราะห์เฟิร์มแวร์เพื่อนำการมองเห็นที่ลึกกว่ามาใช้กับการรักษาความปลอดภัยอุปกรณ์ และ ให้การรักษาความปลอดภัยที่ครอบคลุมตลอดทั้งวงจรชีวิตสำหรับผู้สร้างอุปกรณ์และผู้ประกอบการ

ตั้งแต่เดือนมิถุนายน 2019 กลุ่มภัยคุกคามแบบต่อเนื่องขั้นสูง (APT) ในเครือรัฐใช้มัลแวร์โมดูลาร์ Cyclops Blink เพื่อมุ่งเป้าไปที่อุปกรณ์ไฟร์วอลล์ WatchGuard และเราเตอร์ ASUS ที่มีช่องโหว่ โดยดำเนินการอัปเดตเฟิร์มแวร์ที่เป็นอันตรายและเลือกไปเป็นบอทเน็ตขนาดใหญ่ มัลแวร์ทำให้อุปกรณ์ติดไวรัสได้สำเร็จโดยการใช้ประโยชน์จากช่องโหว่ที่รู้จักกันดีซึ่งช่วยยกระดับสิทธิ์การใช้งาน ช่วยให้ผู้ก่อภัยคุกคามสามารถจัดการอุปกรณ์ได้ เมื่อติดไวรัสแล้ว มัลแวร์จะช่วยให้โมดูลอื่นๆ ได้รับการติดตั้งและหลบเลี่ยงการอัปเดตเฟิร์มแวร์ อุปกรณ์ที่ถูกบุกรุกได้รับการตรวจพบว่าเชื่อมต่อไปยังเซิร์ฟเวอร์ C2 ที่โฮสต์บนอุปกรณ์ WatchGuard อื่นๆ การออกใบรับรอง SSL จำนวนมากสำหรับ C2 บนพอร์ต TCP ต่างๆ ผู้ปฏิบัติงาน Cyclops Blink ได้รับสิทธิ์การเข้าถึงระยะไกลไปยังเครือข่ายโดยการดำเนินการอัปเดตเฟิร์มแวร์ที่เป็นอันตรายและหลบเลี่ยงวิธีการรักษาความปลอดภัยแบบดั้งเดิม เช่น การสแกน

วิธีการที่ Microsoft มีการปรับปรุงการรักษาความปลอดภัยห่วงโซ่อุปทาน

Microsoft กำลังร่วมมือกับรัฐบาลและอุตสาหกรรมเพื่อแก้ไขปัญหาด้านความปลอดภัยของอุปกรณ์ IoT และ OT เหล่านี้ (ดูการสนทนาในหน้า 66) การสนับสนุนของเราจะรวมถึงการใช้ประโยชน์จากเทคโนโลยีการวิเคราะห์เฟิร์มแวร์เพื่อให้ผู้ควบคุมอุปกรณ์สามารถมองเห็นรูปแบบการรักษาความปลอดภัยของอุปกรณ์บนเครือข่ายของตน ซึ่งจะช่วยให้ลูกค้าสามารถระบุและจัดลำดับความสำคัญของอุปกรณ์ที่ต้องการการป้องกัน การอัปเกรด หรือการทดแทนเพิ่มเติม และกระตุ้นความต้องการสำหรับผู้สร้างอุปกรณ์ในการลงทุนในการรักษาความปลอดภัยของอุปกรณ์ ในขณะเดียวกัน เรากำลังสนับสนุนผู้สร้างด้วยโซลูชันที่ครอบคลุมในการออกแบบอุปกรณ์ที่ปลอดภัยและการนำวงชีวิตการพัฒนาที่ปลอดภัยมาใช้

องค์ประกอบที่สำคัญอีกองค์ประกอบหนึ่งคือการจัดเตรียมโครงสร้างพื้นฐานที่แข็งแกร่งให้ผู้สร้างและผู้ควบคุมเพื่อให้เฟิร์มแวร์ของอุปกรณ์สามารถอัปเดตได้เมื่อมีการค้นพบและแก้ไขปัญหาด้านความปลอดภัย Microsoft กำลังนำการวิเคราะห์เฟิร์มแวร์และ Defender สำหรับ IoT มารวมกัน ด้วย Device Update สำหรับ IoT Hub เพื่อมอบโซลูชันในการแก้ไขปัญหาการรักษาความปลอดภัยของอุปกรณ์ IoT และ OT ตลอดวงจรชีวิต สิ่งเหล่านี้เป็นขั้นตอนสำคัญในการทำให้วิสัยทัศน์ของเราบรรลุผลสำหรับลูกค้าในการรักษาความปลอดภัยโครงสร้างพื้นฐานโดยการนำอุปกรณ์ที่สนับสนุนแนวทาง Zero Trust มาใช้กับโซลูชัน IoT และ OT ของพวกเขา[18]

> ผู้โจมตีกำหนดเป้าหมายไปที่ช่องโหว่ในเฟิร์มแวร์อุปกรณ์ IoT มากขึ้นเรื่อยๆ เพื่อแทรกซึมเครือข่ายองค์กร

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. รับการมองเห็นที่ลึกขึ้นเกี่ยวกับอุปกรณ์ IoT/OT บนเครือข่ายของคุณ และจัดลำดับความสำคัญตามความเสี่ยงต่อองค์กรหากถูกบุกรุก
2. ใช้เครื่องมือสแกนเฟิร์มแวร์เพื่อทำความเข้าใจจุดอ่อนด้านความปลอดภัยที่อาจเกิดขึ้น และทำงานร่วมกับผู้จำหน่ายเพื่อระบุวิธีลดความเสี่ยงสำหรับอุปกรณ์ที่มีความเสี่ยงสูง
3. มีอิทธิพลเชิงบวกต่อความปลอดภัยของอุปกรณ์ IoT/OT โดยกำหนดให้ผู้ขายของคุณยอมรับแนวทางปฏิบัติที่ดีที่สุดในวงจรการพัฒนาที่ปลอดภัย

ลิงค์ไปยังข้อมูลเพิ่มเติม

- การประเมินห่วงโซ่อุปทานที่สำคัญที่สนับสนุนอุตสาหกรรมเทคโนโลยีสารสนเทศและการสื่อสารของสหรัฐอเมริกา

การโจมตี OT ตามการลาดตระเวน

ห่วงโซ่อุปทานที่ซับซ้อนใช้ข้อมูลการออกแบบที่เฉพาะเจาะจงเพื่อวางแผนระบบจริง ในบรรดาทรัพย์สินมากมายที่ประกอบเป็นข้อมูลการออกแบบนี้ สิ่งที่สำคัญที่สุดคือไฟล์โครงการซึ่งกำหนดสภาพแวดล้อมและสินทรัพย์ของตน ไฟล์นี้เป็นเป้าหมายเชิงกลยุทธ์ที่สำคัญสำหรับผู้ก่อภัยภัยคุกคามที่ต้องการเข้าถึงและปรับใช้การโจมตีที่ประสบความสำเร็จที่ปรับให้เหมาะสมกับสภาพแวดล้อมทั้งหมด

การกำหนดเป้าหมายระบบอุตสาหกรรมเพื่อขัดขวางกระบวนการดำเนินงาน เกี่ยวข้องกับขั้นตอนสองขั้นตอน

1. ขั้นแรก ผู้โจมตีจะต้องเข้าถึงเครือข่าย OT ซึ่งสามารถทำได้โดยการป้อนผ่านอุปกรณ์ IoT ในฝั่งองค์กรของเครือข่าย (Purdue Model Level 4) และข้ามขอบเขต IT-OT ซึ่งปกติจะแยกจากกันโดยไฟร์วอลล์และและอุปกรณ์ระบบเครือข่าย ไปสู่ระดับปฏิบัติการและการควบคุม
2. ขั้นที่สอง อุปกรณ์เครือข่ายต้องได้รับการระบุ ระบบอุตสาหกรรมใช้อุปกรณ์และส่วนประกอบมาตรฐานในสถาปัตยกรรมที่กำหนดเองซึ่งได้รับการออกแบบมาโดยเฉพาะสำหรับสภาพแวดล้อมของตน หนึ่งในอุปกรณ์มาตรฐานเหล่านี้คือตัวควบคุม logic (PLC) ที่ตั้งโปรแกรมได้ ผู้ผลิตทุกรายพัฒนาอินเทอร์เฟซและฟังก์ชันที่ไม่ซ้ำกันสำหรับ PLCs ซึ่งเป็นองค์ประกอบสำคัญของระบบอุตสาหกรรม และอุปกรณ์เหล่านี้ได้รับการกำหนดค่าเพิ่มเติมด้วยแบบแผนที่กำหนดเองซึ่งได้รับการออกแบบโดยเฉพาะสำหรับสภาพแวดล้อมของลูกค้า การกำหนดค่าเฉพาะของแต่ละ PLC ได้รับการอธิบายไว้ในไฟล์โครงการ ซึ่งประกอบด้วยคำจำกัดความของสภาพแวดล้อมและสินทรัพย์ แลดเดอร์ลอจิกและอื่นๆ

ในสภาพแวดล้อมส่วนใหญ่ที่แสดงหลักฐานของการโจมตี การวิเคราะห์จะแสดงไทม์ไลน์ก่อนหน้าการโจมตีที่มีมากเกินกว่าความยาวของการโจมตีนั้นเอง ผู้คุกคามมักใช้เวลาหลายเดือนในการจำลองสภาพแวดล้อมและสินทรัพย์จากระยะไกล พยายามทำหลายอย่างเพื่อการสร้างโมเดลและเตรียมความพร้อมในการโจมตีเป้าหมายของตน ในขณะที่สภาพแวดล้อมมีการเปลี่ยนแปลงอย่างต่อเนื่องและรวมอุปกรณ์ใหม่เข้าด้วยกัน ช่องโหว่จะถูกสร้างขึ้นโดยเฉพาะในข้อมูลในโครงการและไฟล์การกำหนดค่า การโจรกรรมไฟล์โครงการสามารถทำให้การโจมตีเร็วขึ้นได้หลายสัปดาห์หรือหลายเดือนและช่วยให้ผู้โจมตีสามารถจำลองสภาพแวดล้อมเป้าหมายได้อย่างรวดเร็วและแม่นยำมากขึ้น เพิ่มความยากในการตรวจจับกิจกรรมที่เป็นอันตราย

Industroyer และ Incontroller

เราได้สังเกตเห็นการโจมตีองค์กร โครงสร้างพื้นฐานที่สำคัญและการตั้งเป้าหมายไปที่รัฐบาลโดยผู้คุกคามที่ได้รับการสนับสนุนจากรัฐชาติเพิ่มมากขึ้น โดยการใช้มัลแวร์โมดูลาร์และกรอบงานการโจมตี ความพยายามครั้งใหม่ที่จะแทรกแซงการดำเนินงานที่สำคัญในยูเครนเน้นย้ำถึงภัยคุกคามที่เพิ่มขึ้นของการโจมตี OT ตามตามการสอดแนมที่มีการปรับให้เหมาะกับสภาพแวดล้อมเป้าหมายของตนอย่างมาก ระยะตามการสอดแนมและการวิจัยที่ขยายออกไปซึ่งดำเนินการโดยผู้ดำเนินการทางไซเบอร์ระดับชาติที่สำคัญชี้ให้เห็นถึงกลยุทธ์ของการใช้สงครามไซเบอร์เพื่อทำลายโครงสร้างพื้นฐานจากระยะไกลเพื่อตอบสนองเป้าหมายเชิงกลยุทธ์หรือการดำเนินงานที่เฉพาะเจาะจงในการดำเนินงานที่มีการเคลื่อนไหวทางไซเบอร์



เราได้สังเกตเห็นภัยคุกคามที่เพิ่มขึ้นจากการโจมตี OT ตามตามการสอดแนม ซึ่งมีการปรับให้เหมาะสมกับสภาพแวดล้อมเป้าหมายอย่างมาก

การโจมตี OT ตามการลาดตระเวน

ต่อไป

ในช่วงต้นปี 2022 การโจมตี OT ที่สำคัญแบบปรับเปลี่ยนได้สองครั้งได้รับการระบุ การโจมตีทางไซเบอร์-กายภาพในสถานีไฟฟ้าย่อยและรีเลย์การป้องกันในยูเครนดำเนินการโดยใช้มัลแวร์ที่กำหนดเองซึ่งรวมถึงตัวแปรของ Industroyer มัลแวร์ที่ทราบกันดีว่าเป็นสาเหตุทำให้เกิดไฟดับในยูเครนหลังจากมีการใช้งานในปี 2016

Industroyer2 เป็นการปรับใช้มัลแวร์โจมตี OT ที่เป็นอันตรายในเป้าหมายใหม่ครั้งแรกที่เป็นที่รู้จักกันดี ซึ่งใช้ปลั๊กอินโพรโทคอล IEC104 (โพรโทคอลมาตรฐานสำหรับการตรวจสอบและควบคุมระบบไฟฟ้าและการควบคุม) ที่พัฒนาขึ้นสำหรับ Industroyer และกำหนดเป้าหมายเป็นหน่วยเทอร์มินัลระยะไกลที่มีลักษณะคล้าย PLC เป็นส่วนใหญ่โดยมีหมายเลขโมเดล ABB RTU540/560 ผู้เขียนมัลแวร์นี้ใช้ความรู้เกี่ยวกับสภาพแวดล้อมของเหยื่อเพื่อออกคำสั่งซ้ำๆ ไปยังเอาต์พุตที่กำหนดไว้ล่วงหน้าเพื่อให้แน่ใจว่าไม่สามารถเปิดใช้งานด้วยตนเองได้ ซึ่งทำให้มั่นใจว่าไฟจะดับยาวนานและส่งผลกระทบที่สร้างความเสียหายได้มากขึ้น

Incontroller หรือกรอบการโจมตีแบบโมดูลาร์ที่ระบุในช่วงระยะเวลาเดียวกัน คือชุดเครื่องมือแบบโมดูลาร์ที่ช่วยลดระยะเวลารอคอยในการเจาะและโจมตีอุปกรณ์ OT ลงอย่างมาก โดยไม่ต้องผ่านโซลูชันความมั่นคงปลอดภัยแบบเก่า ชุดเครื่องมือที่ใช้งานทั่วไปมีความสามารถในการเก็บข้อมูล ตามการสอดแนม และความสามารถในการโจมตีที่สามารถปรับแต่งได้สูงในสภาพแวดล้อมที่แตกต่างกันและสามารถส่งผลกระทบต่อระยะการวิจัยสำหรับการโจมตีของ OT อย่างมาก ลดเวลาที่จำเป็นต้องใช้ในการดำเนินตามการสอดแนม สนับสนุนการจำลองของสภาพแวดล้อมโดยการดึงข้อมูลเกี่ยวกับอุปกรณ์และการกำหนดค่า

เฟรมเวิร์ก Incontroller รองรับโปรโตคอลสำหรับ Schneider Electric and Omron PLCs และรวบรวมข้อมูล เช่น เวอร์ชันเฟิร์มแวร์ ประเภทโมเดล และอุปกรณ์ที่เชื่อมต่อ ชุดเครื่องมือสามารถออกคำสั่งเพื่อเปลี่ยนการกำหนดค่ารวมถึงเปิดและปิดเอาท์พุทได้ เมื่อมีการเข้าถึงสภาพแวดล้อมแล้ว เฟรมเวิร์กจะสนับสนุนการฝังรูรั่วในอุปกรณ์เพื่อส่งเพย์โหลดที่มากขึ้น ออกช่องโหว่ที่จะเพิ่มจุดการเข้าถึง อัปโหลดแลดเดอร์ลอจิกและความสามารถในการเริ่มต้นการโจมตี DoS ลักษณะทั่วไปของชุดเครื่องมือช่วยให้ผู้ก่อภัยคุกคามสามารถโจมตีสภาพแวดล้อมได้อย่างรวดเร็วโดยไม่จำเป็นต้องเขียนการโจมตีใหม่สำหรับทุกๆ PLC หรือตำแหน่งที่ตั้ง ซึ่งจะช่วยให้ผู้ก่อภัยคุกคามสามารถโต้ตอบกับเครื่องจักรประเภทต่างๆ ในอุตสาหกรรมต่างๆ ได้อย่างง่ายดาย



ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. หลีกเลี่ยงการถ่ายโอนไฟล์ที่มีคำจำกัดความของระบบผ่านช่องทางที่ไม่ปลอดภัยหรือไปยังบุคลากรที่ไม่จำเป็น
2. เมื่อการถ่ายโอนไฟล์ดังกล่าวหลีกเลี่ยงไม่ได้ ตรวจสอบให้แน่ใจว่าได้ตรวจสอบกิจกรรมบนเครือข่ายและให้แน่ใจว่าสินทรัพย์มีความปลอดภัย
3. ปกป้องสถานีวิศวกรรมโดยการตรวจสอบด้วยโซลูชัน EDR
4. ดำเนินการตอบสนองต่อเหตุการณ์ในเชิงรุกสำหรับเครือข่าย OT
5. ปรับใช้การตรวจสอบอย่างต่อเนื่อง เช่น Defender สำหรับ IoT

อ้างอิงท้ายเอกสาร

1. ดูที่ เช่น Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe's digital future (europa.eu); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1; Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (homeaffairs.gov.au); ชิลี: Bill for cybersecurity and critical information infrastructure introduced in Senate | News post | DataGuidance; Japan passes economic security bill to guard sensitive technology | The Japan Times; Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs (csa.gov.sg); Proposal for legislation to improve the UK's cyber resilience—GOV.UK (www.gov.uk); Telecommunications (Security) Act 2021 (legislation.gov.uk); Updating the NIST Cybersecurity Framework—Journey To CSF 2.0 | NIST
2. Cert-In—หน้าแรก
3. การเริ่มต้นการปรึกษาเกี่ยวกับข้อผูกพันในการรายงานการโจมตีทางไซเบอร์ (admin.ch)
4. ดูที่ เช่น ไม่มีชื่อ (house.gov)
5. พระราชบัญญัติความยืดหยุ่นทางไซเบอร์ | สร้างอนาคตดิจิทัลของยุโรป (europa.eu)
6. ดูที่ เช่น วงจรการพัฒนาการรักษาความปลอดภัยของ Microsoft
7. ดูที่ เช่น การสร้าง Software Bills of Materials (SBOMs) ด้วย SPDX ที่ Microsoft—Engineering@Microsoft; ดู เช่น องค์ประกอบขั้นต่ำสำหรับ Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. ดูที่ เช่น https://www.microsoft.com/en-us/msrc/cvd
9. ร่างพระราชบัญญัติการรักษาความปลอดภัยผลิตภัณฑ์และโครงสร้างพื้นฐานโทรคมนาคม (PSTI) (Product Security and Telecommunications Infrastructure (PSTI))—เอกสารด้านความปลอดภัยของผลิตภัณฑ์—GOV.UK (www.gov.uk)
10. คณะกรรมาธิการเสริมสร้างความปลอดภัยทางไซเบอร์ของอุปกรณ์และผลิตภัณฑ์ไร้สาย (europa.eu)
11. แผนการรับรองระบบคลาวด์: สร้างบริการระบบคลาวด์ที่เชื่อถือได้ทั่วทั้งยุโรป — ENISA (europa.eu)
12. การรับรอง — ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool" GitHub - microsoft/sbom-tool: เครื่องมือ SBOM เป็นเครื่องมือที่ปรับขนาดได้สูงและพร้อมใช้งานสำหรับองค์กรเพื่อสร้าง SBOM ที่เข้ากันได้กับ SPDX 2.2 สำหรับอาร์ทิแฟกต์ต่างๆ
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come
15. นวัตกรรม IoT/OT สำคัญแต่มาพร้อมกับความเสี่ยงที่สูง (ธ.ค. 2021): https://www.microsoft.com/security/blog/2021/12/08/new-research-shows-iot-and-ot-innovation-is-critical-to-business-but-comes-with-significant-risks/
16. เปิดเผยการใช้อุปกรณ์ IoT ของ Trickbot ในโครงสร้างพื้นฐาน C2 (มี.ค. 2022): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. IoT แสดงใน Channel 9 ตอนในการสแกนเฟิร์มแวร์ IoT (พ.ค. 2022): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. วิธีการใช้แนวทาง Zero Trust กับโซลูชัน IoT ของคุณ (พ.ค. 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

ปฏิบัติการมีอิทธิพลทางไซเบอร์

การดำเนินงานที่มีอิทธิพลจากต่างประเทศในปัจจุบันใช้วิธีการและเทคโนโลยีใหม่ๆ ทำให้แคมเปญของพวกเขาออกแบบมาเพื่อทำลายความไว้วางใจอย่างมีประสิทธิภาพและมีประสิทธิภาพมากขึ้น

ข้อมูลเบื้องต้น 73

แนวโน้มของการปฏิบัติการด้านอิทธิพลทางไซเบอร์ 74

จับตาการปฏิบัติการด้านอิทธิพลในช่วงโควิด-19 และการรุกรานยูเครนของรัสเซีย 76

การติดตามดัชนีโฆษณาชวนเชื่อของรัสเซีย 78

สื่อสังเคราะห์ 80

แนวทางแบบองค์รวมเพื่อป้องกันการปฏิบัติการด้านอิทธิพลทางไซเบอร์ 83

ภาพรวมของความยืดหยุ่นทางไซเบอร์ 87

ภาพรวมของ

การปฏิบัติการอิทธิพลทางไซเบอร์

การดำเนินงานที่มีอิทธิพลจากต่างประเทศในปัจจุบันใช้วิธีการและเทคโนโลยีใหม่ๆ ทำให้แคมเปญของพวกเขาออกแบบมาเพื่อทำลายความไว้วางใจอย่างมีประสิทธิภาพและมีประสิทธิภาพมากขึ้น

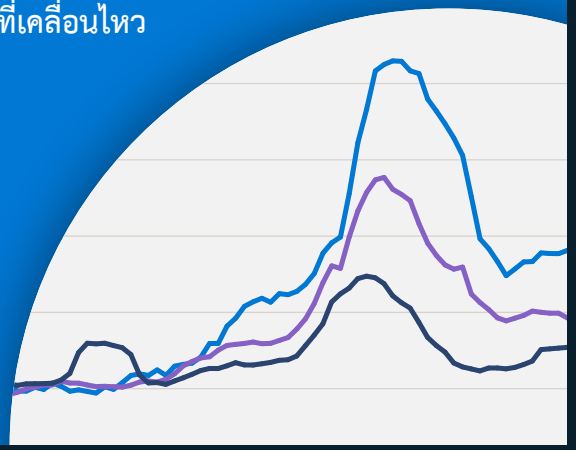
รัฐชาติกำลังใช้อิทธิพลที่ซับซ้อนมากขึ้นเพื่อเผยแพร่โฆษณาชวนเชื่อและส่งผลกระทบต่อความคิดเห็นของประชาชนทั้งในประเทศและต่างประเทศ แคมเปญเหล่านี้บั่นทอนความไว้วางใจ เพิ่มการแบ่งขั้ว และคุกคามกระบวนการประชาธิปไตย นักบงการขั้นสูงที่มีทักษะขั้นสูงกำลังใช้สื่อดั้งเดิมร่วมกับอินเทอร์เน็ตและโซเชียลมีเดียเพื่อเพิ่มขอบเขต ขนาด และประสิทธิภาพของแคมเปญของพวกเขาอย่างมหาศาล รวมถึงผลกระทบที่เกินขอบเขตที่พวกเขามีต่อระบบนิเวศข้อมูลทั่วโลก ในปีที่ผ่านมา เราได้เห็นปฏิบัติการเหล่านี้ถูกใช้เป็นส่วนหนึ่งของสงครามลูกผสมของรัสเซียในยูเครน แต่ยังเห็นรัสเซียและประเทศอื่นๆ รวมถึงจีนและอิหร่าน ใช้ปฏิบัติการโฆษณาชวนเชื่อที่ขับเคลื่อนโดยสื่อสังคมออนไลน์มากขึ้นเพื่อขยายอิทธิพลไปทั่วโลก

การปฏิบัติการด้านอิทธิพลทางไซเบอร์มีความซับซ้อนมากขึ้นเนื่องจากรัฐบาลและรัฐชาติจำนวนมากขึ้นกำลังใช้การดำเนินการเหล่านี้ในการสร้างความคิดเห็น ทำลายชื่อเสียงฝ่ายตรงข้ามและส่งเสริมความไม่ลงรอยกัน



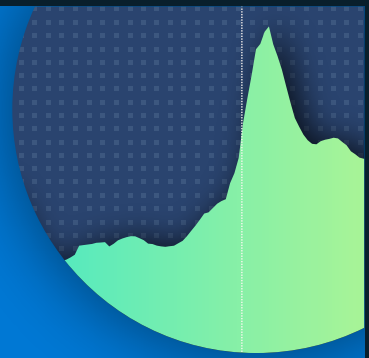
ค้นหาข้อมูลเพิ่มเติมหน้า 74

การบุกครองยูเครนของรัสเซียแสดงให้เห็นถึงการปฏิบัติการด้านอิทธิพลทางไซเบอร์ที่รวมกับการโจมตีทางไซเบอร์แบบดั้งเดิมและการดำเนินงานทางทหารที่เคลื่อนไหวเพื่อเพิ่มผลกระทบ



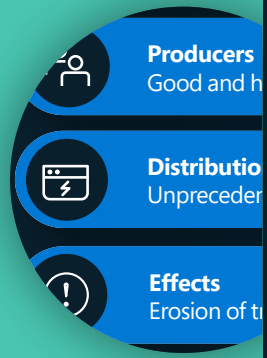
ค้นหาข้อมูลเพิ่มเติมหน้า 76

รัสเซีย อิหร่าน และจีนได้ใช้การโฆษณาชวนเชื่อและแคมเปญสร้างอิทธิพลตลอดการแพร่ระบาดของโควิด-19 บ่อยครั้งในฐานะอุปกรณ์เชิงกลยุทธ์เพื่อให้บรรลุวัตถุประสงค์ทางการเมืองที่กว้างขึ้น



ค้นหาข้อมูลเพิ่มเติมหน้า 76

สื่อสังเคราะห์จะแพร่หลายมากขึ้นเนื่องจากการเพิ่มจำนวนของเครื่องมือที่สามารถสร้างและเผยแพร่รูปภาพ วิดีโอ และเสียงเทียมที่เหมือนจริงสูงได้อย่างง่ายดาย เทคโนโลยีแหล่งที่มาดิจิทัลที่รับรองแหล่งที่มาของเนื้อหาสื่อถือเป็นคำมั่นสัญญาในการต่อสู้กับการใช้งานในทางที่ผิด



ค้นหาข้อมูลเพิ่มเติมหน้า 80

แนวทางแบบองค์รวมเพื่อป้องกันการปฏิบัติการด้านอิทธิพลทางไซเบอร์

Microsoft กำลังสร้างโครงสร้างพื้นฐานข่าวกรองด้านภัยคุกคามทางไซเบอร์ซึ่งมีความพร้อมอย่างเต็มที่อยู่แล้วเพื่อต่อสู้กับการปฏิบัติการด้านอิทธิพลทางไซเบอร์ กลยุทธ์ของเราคือการตรวจสอบ ขัดขวาง ปกป้อง และยับยั้งการโฆษณาชวนเชื่อโดยผู้รุกรานที่ไม่คุ้นเคย

ค้นหาข้อมูลเพิ่มเติมหน้า 83

ข้อมูลเบื้องต้น

ประชาธิปไตยต้องการข้อมูลที่น่าเชื่อถือเพื่อการเจริญเติบโต พื้นที่สำคัญของการมุ่งเน้นสำหรับ Microsoft คือการดำเนินการที่มีอิทธิพลต่อการพัฒนาและความสามารถในการพัฒนาโดยรัฐชาติ แคมเปญเหล่านี้บั่นทอนความไว้วางใจ เพิ่มการแบ่งขั้ว และคุกคามกระบวนการประชาธิปไตย

การปฏิบัติการด้านอิทธิพลต่างประเทศเป็นภัยคุกคามต่อระบบนิเวศของข้อมูลมาโดยตลอด อย่างไรก็ตาม สิ่งที่แตกต่างในยุคของอินเทอร์เน็ตและโซเชียลมีเดียคือ ขอบเขต ขนาด และประสิทธิภาพของแคมเปญที่เพิ่มขึ้นอย่างมาก และผลกระทบที่เกินขอบเขตที่แคมเปญดังกล่าวสามารถมีต่อความสมบูรณ์ของระบบนิเวศข้อมูลทั่วโลก

ภาษิตเก่าที่ว่า "ความเท็จสามารถเดินทางไปได้ครึ่งโลกแล้วก่อนที่ความจริงจะมีโอกาสสวมรองเท้า" กำลังได้รับการยืนยันด้วยข้อมูล การศึกษาโดยสถาบันเทคโนโลยีแมสซาชูเซตส์ (MIT) พบว่าความเท็จมีแนวโน้มที่จะถูกรีทวีตมากกว่าความจริงถึง 70 เปอร์เซ็นต์ และเข้าถึงผู้คน 1,500 คนแรกได้เร็วกว่าถึงหกเท่า ระบบนิเวศข้อมูลมีความคลุมเครือมากขึ้นเนื่องจากแคมเปญโฆษณาชวนเชื่อแพร่หลายบนอินเทอร์เน็ตและโซเชียลมีเดีย และทำลายความน่าเชื่อถือของข่าวแบบดั้งเดิม ในการศึกษาในปี 2021[2] มีเพียงเจ็ดเปอร์เซ็นต์ของผู้ใหญ่ในสหรัฐฯ ที่กล่าวว่าตนมีความไว้วางใจและความมั่นใจ “อย่างมาก” ในการรายงานข่าวของหนังสือพิมพ์ โทรทัศน์ และวิทยุ ในขณะที่ 34 เปอร์เซ็นต์รายงานว่า “ไม่ไว้วางใจเลย ”

Microsoft ได้ทำงานเพื่อระบุผู้ดำเนินการหลัก ภัยคุกคามและกลยุทธ์ต่างๆ ในพื้นที่ที่มีอิทธิพลทางไซเบอร์ต่างประเทศและเพื่อแบ่งปันบทเรียนที่เรียนรู้ ในเดือนมิถุนายนปีนี้ เราได้ตีพิมพ์รายงานที่ครอบคลุมเกี่ยวกับบทเรียนที่ได้เรียนรู้จากยูเครนซึ่งมีรายละเอียดเกี่ยวกับการปฏิบัติการด้านอิทธิพลทางไซเบอร์ของรัสเซีย[3]

นอกจากนี้ เรายังศึกษาวิธีการที่เทคโนโลยีขั้นสูง เช่น การปลอมแปลงเชิงลึก สามารถนำมาปรับใช้เป็นอาวุธ และทำลายความน่าเชื่อถือของนักข่าว และเรากำลังทำงานร่วมกับอุตสาหกรรม รัฐบาล และสถาบันการศึกษาเพื่อพัฒนาวิธีการที่ดีกว่าในการตรวจสอบสื่อสังเคราะห์และฟื้นฟูความน่าเชื่อถือ—เช่น ระบบปัญญาประดิษฐ์ (AI) ที่สามารถตรวจจับการปลอมได้

ลักษณะที่เปลี่ยนแปลงอย่างรวดเร็วของระบบนิเวศข้อมูลและการโฆษณาชวนเชื่อทางออนไลน์ของรัฐชาติ รวมทั้งการผสมผสานการโจมตีทางไซเบอร์แบบดั้งเดิมเข้ากับปฏิบัติการด้านอิทธิพลและการแทรกแซงการเลือกตั้งที่เป็นประชาธิปไตย จำเป็นต้องใช้แนวทางที่ทุกภาคส่วนในสังคมมีส่วนร่วมเพื่อบรรเทาภัยคุกคามทั้งทางออนไลน์และออฟไลน์ต่อประชาธิปไตย

Microsoft ทุ่มเทให้กับการสนับสนุนระบบนิเวศข้อมูลที่สมบูรณ์ซึ่งข่าวสารที่เชื่อถือได้และข้อมูลสามารถเติบโต เรากำลังพัฒนาเครื่องมือและความสามารถในการตรวจจับภัยคุกคามเพื่อต่อสู้กับความเสี่ยงที่กำลังพัฒนาและขยายตัวของปฏิบัติการด้านอิทธิพลที่ขับเคลื่อนโดยรัฐชาติ เพื่อให้งานดังกล่าวดำเนินการไปได้ เราเพิ่งเข้าซื้อกิจการ Miburo Solutions เราร่วมมือกับผู้ตรวจสอบบุคคลที่สาม เช่น Global Disinformation Index และ NewsGuard และเราเข้าร่วมและบางครั้งก็เป็นผู้นำในการเป็นพันธมิตรกับผู้มีส่วนได้ส่วนเสียหลายฝ่าย รวมถึง Coalition for Content Provenance and Authenticity (C2PA) การทำงานร่วมกันเท่านั้นที่จะทำให้เราประสบความสำเร็จในการดำเนินการกับผู้ที่พยายามที่จะทำลายกระบวนการประชาธิปไตยและสถาบัน

เทเรซ่า ฮัทสัน

รองประธาน ฝ่ายเทคโนโลยีและความรับผิดชอบขององค์กร

แนวโน้มของการปฏิบัติการด้านอิทธิพลทางไซเบอร์

การปฏิบัติการด้านอิทธิพลทางไซเบอร์กำลังมีความซับซ้อนมากขึ้นเมื่อเทคโนโลยีพัฒนาขึ้นอย่างรวดเร็ว เรากำลังพบกับการทับซ้อนและการขยายตัวของเครื่องมือที่ใช้ในการโจมตีทางไซเบอร์แบบดั้งเดิมที่ถูกนำไปใช้กับปฏิบัติการด้านอิทธิพลทางไซเบอร์ นอกจากนี้ เรายังพบการประสานงานและการขยายตัวที่เพิ่มขึ้นในหมู่รัฐชาติ

Microsoft ลงทุนในการต่อสู้กับการปฏิบัติการด้านอิทธิพลจากต่างประเทศในปีนี้โดยการซื้อกิจการของ Miburo Solutions บริษัทที่เชี่ยวชาญในการวิเคราะห์การปฏิบัติการด้านอิทธิพลจากต่างประเทศ เมื่อรวมนักวิเคราะห์เหล่านี้เข้ากับนักวิเคราะห์บริบทภัยคุกคามของ Microsoft Microsoft จึงได้ก่อตั้งศูนย์กลางการวิเคราะห์ภัยคุกคามทางดิจิทัล (DTAC) DTAC วิเคราะห์และรายงานเกี่ยวกับภัยคุกคามระดับชาติ รวมทั้งการโจมตีทางไซเบอร์และการปฏิบัติการด้านอิทธิพล ผสมผสานข้อมูลและข้อมูลภัยคุกคามเข้ากับการวิเคราะห์ภูมิรัฐศาสตร์เพื่อให้ข้อมูลเชิงลึกและรายงานการตอบสนองและการป้องกันที่มีประสิทธิภาพ

ผู้คนมากกว่าสามในสี่จากทั่วโลกกล่าวว่ากังวลเกี่ยวกับการใช้ข้อมูลเป็นอาวุธ[4] และข้อมูลของเราสนับสนุนข้อกังวลเหล่านี้ Microsoft และพันธมิตรได้ติดตามวิธีการที่ผู้ดำเนินการในระดับชาติใช้การปฏิบัติการด้านอิทธิพลเพื่อให้บรรลุวัตถุประสงค์เชิงกลยุทธ์และเป้าหมายทางการเมือง นอกเหนือจากการโจมตีทางไซเบอร์ที่มีผลร้ายกาจและความพยายามในการจารกรรมไซเบอร์แล้ว ระบอบเผด็จการกำลังใช้ปฏิบัติการด้านอิทธิพลทางไซเบอร์มากขึ้นเรื่อยๆ เพื่อกำหนดความคิดเห็น ทำลายชื่อเสียงฝ่ายตรงข้าม ยุยงให้เกิดความกลัว ส่งเสริมความขัดแย้ง และบิดเบือนความเป็นจริง

โดยทั่วไปการปฏิบัติการด้านอิทธิพลทางไซเบอร์ต่างประเทศเหล่านี้ มักจะมีสามขั้นตอน:

การวางตำแหน่งล่วงหน้า

เช่นเดียวกับการวางตำแหน่งล่วงหน้าของมัลแวร์ภายในเครือข่ายคอมพิวเตอร์ขององค์กร การปฏิบัติการด้านอิทธิพลทางไซเบอร์ต่างประเทศจะวางตำแหน่งเรื่องเล่าที่เป็นเท็จในโดเมนสาธารณะบนอินเทอร์เน็ตไว้ล่วงหน้า กลยุทธ์การวางตำแหน่งล่วงหน้าช่วยให้กิจกรรมทางไซเบอร์แบบดั้งเดิมมีมายาวนาน โดยเฉพาะอย่างยิ่งหากผู้ดูแลระบบไอทีสแกนกิจกรรมเครือข่ายล่าสุดของตน มัลแวร์ที่วางไว้ตลอดเวลาที่ใช้งานบนเครือข่ายสามารถทำให้การใช้งานในภายหลังมีประสิทธิภาพมากขึ้น เรื่องเล่าที่เป็นเท็จที่ไม่มีใครสังเกตเห็นบนอินเทอร์เน็ตสามารถทำให้การอ้างอิงในภายหลังดูเหมือนน่าเชื่อถือมากขึ้น

เริ่มใช้งาน

บ่อยครั้งในเวลาที่เป็นประโยชน์มากที่สุดในการบรรลุเป้าหมายของผู้ดำเนินการ แคมเปญประสานงานถูกใช้งานเพื่อเผยแพร่เรื่องเล่าผ่านทางสื่อและช่องทางโซเชียลมีเดียที่ได้รับการสนับสนุนและได้รับอิทธิพลจากรัฐบาล

การขยาย

ประการสุดท้าย สื่อที่ควบคุมโดยรัฐและผู้ที่รับมอบฉันทะจะขยายการเล่าเรื่องภายในกลุ่มเป้าหมาย บ่อยครั้ง ผู้เปิดใช้งานเทคโนโลยีขยายขอบเขตการเข้าถึงเรื่องเล่าโดยไม่รู้ตัว ตัวอย่างเช่น การโฆษณาออนไลน์สามารถช่วยเหลือกิจกรรมด้านการเงินและระบบการจัดส่งเนื้อหาแบบประสานสามารถทำให้เครื่องมือค้นหาหลั่งไหลเข้ามามากมาย

วิธีการสามขั้นตอนนี้ถูกนำมาใช้ในปลายปี 2021 เพื่อสนับสนุนเรื่องเล่าเท็จของรัสเซียเกี่ยวกับอาวุธชีวภาพและห้องปฏิบัติการชีวภาพที่ถูกกล่าวหาในยูเครน เรื่องราวนี้ได้รับการอัปโหลดลงใน YouTube เป็นครั้งแรกเมื่อวันที่ 29 พฤศจิกายน 2021 โดยเป็นส่วนหนึ่งของรายการภาษาอังกฤษประจำ โดยชาวอเมริกันที่อาศัยอยู่ในมอสโกว ที่อ้างว่าห้องปฏิบัติการชีวภาพที่ได้รับทุนสนับสนุนจากสหรัฐฯ ในยูเครนมีความเชื่อมโยงกับอาวุธชีวภาพ เรื่องราวส่วนใหญ่ไม่มีใครสังเกตเห็นเป็นเวลาหลายเดือน ในวันที่ 24 กุมภาพันธ์ 2022 ขณะที่รถถังรัสเซียข้ามพรมแดน เรื่องราวก็ถูกส่งเข้าสู่สนามรบ ทีมวิเคราะห์ข้อมูลที่ Microsoft ระบุว่าเว็บไซต์ข่าวที่มีการควบคุมได้รับอิทธิพลจากรัสเซียมากถึง10 รายการ ซึ่งเผยแพร่รายงานพร้อมกันในวันที่ 24 กุมภาพันธ์ โดยชี้กลับไปที่ “รายงานของปีที่แล้ว” และพยายามทำให้น่าเชื่อถือ นอกจากนี้ เจ้าหน้าที่กระทรวงการต่างประเทศของของสหพันธรัฐรัสเซียได้จัดแถลงข่าวโดยสร้างข้อกล่าวหาเพิ่มเติมเกี่ยวกับห้องปฏิบัติการชีวภาพของสหรัฐฯ ในสภาพแวดล้อมข้อมูล จากนั้นทีมที่ได้รับการสนับสนุนจากรัสเซียได้ทำงานเพื่อขยายการเล่าเรื่องบนโซเชียลมีเดียและเว็บไซต์อินเทอร์เน็ตให้กว้างขึ้น

เรากำลังพบกับระบอบเผด็จการทั่วโลกที่ทำงานร่วมกันเพื่อสร้างมลพิษให้กับระบบนิเวศของข้อมูลเพื่อประโยชน์ร่วมกันของตน ตัวอย่างเช่น ตลอดช่วงการระบาดของโควิด-19 รัสเซีย อิหร่าน และจีนใช้การปฏิบัติการด้านโฆษณาชวนเชื่อและโน้มน้าว โดยใช้การผสมผสานระหว่างวิธีการเผยแพร่ที่เปิดเผย กึ่งปกปิด และแอบแฝง เพื่อกำหนดเป้าหมายไปที่ประชาธิปไตยและเป้าหมายทางภูมิรัฐศาสตร์อื่นๆ (รายละเอียดเพิ่มเติมในหน้า 76) ระบอบการปกครองทั้งสามแบบได้เล่นกับระบบการรับส่งข้อความและข้อมูลของกันและกันเพื่อส่งเสริมการเล่าเรื่องที่ต้องการ การรายงานข่าวนี้ส่วนใหญ่ประกอบด้วยการวิพากษ์วิจารณ์หรือทฤษฎีสมคบคิดเกี่ยวกับสหรัฐอเมริกาและพันธมิตรที่เผยแพร่โดยบุคคลสำคัญของรัฐบาลในแถลงการณ์อย่างเป็นทางการ ในขณะเดียวกันก็ส่งเสริมวัคซีนของตนเองและการตอบสนองต่อ COVID-19 ว่าเหนือกว่าสหรัฐอเมริกาและประเทศประชาธิปไตยอื่นๆ โดยขยายความซึ่งกันและกันสื่อที่ดำเนินการโดยรัฐ สร้างระบบนิเวศที่การรายงานข่าวเชิงลบเกี่ยวกับระบอบประชาธิปไตยหรือการรายงานข่าวเชิงบวกของรัสเซีย อิหร่าน และจีน ซึ่งผลิตโดยสื่อของรัฐแห่งหนึ่งได้รับการเสริมกำลังจากสื่ออื่นๆ



การทำให้เห็นภาพถึงวิธีการที่การเล่าเรื่องเกี่ยวกับห้องปฏิบัติการชีวภาพและอาวุธชีวภาพของสหรัฐฯ แพร่กระจายผ่านสามขั้นตอนกว้างๆ ในการปฏิบัติการด้านอิทธิพลจากต่างประเทศมากมาย ได้แก่ การวางตำแหน่งล่วงหน้า การเริ่ม และการขยาย

แนวโน้มของการปฏิบัติการด้านอิทธิพลทางไซเบอร์

ต่อไป

เพื่อเพิ่มความท้าทาย หน่วยงานด้านเทคโนโลยีภาคเอกชนอาจเปิดใช้แคมเปญเหล่านี้โดยไม่เจตนา ผู้เปิดใช้งานอาจรวมถึงบริษัทที่ลงทะเบียนโดเมนอินเทอร์เน็ต โฮสต์เว็บไซต์ โปรโมตเนื้อหาบนสื่อสังคมออนไลน์และไซต์การค้นหา ช่องทางการเข้าชม และช่วยจ่ายค่าดำเนินการเหล่านี้ผ่านการโฆษณาดิจิทัล องค์กรต้องตระหนักถึงเครื่องมือและวิธีการที่ถูกใช้โดยระบอบเผด็จการในการปฏิบัติการด้านอิทธิพลทางไซเบอร์เพื่อให้สามารถตรวจจับและป้องกันการแพร่กระจายของแคมเปญได้ นอกจากนี้ยังมีความต้องการที่เพิ่มขึ้นในการช่วยให้ผู้บริโภคพัฒนาความสามารถที่ซับซ้อนยิ่งขึ้นในการระบุการปฏิบัติการด้านอิทธิพลจากต่างประเทศและจำกัดการมีส่วนร่วมกับเรื่องเล่าหรือเนื้อหาของตน

การปฏิบัติการด้านอิทธิพลทางไซเบอร์ซึ่งรวมถึงการโฆษณาชวนเชื่อของเผด็จการเป็นภัยคุกคามต่อระบอบประชาธิปไตยทั่วโลก เนื่องจากสิ่งเหล่านี้กัดกร่อนความไว้วางใจ เพิ่มการแบ่งขั้ว และคุกคามกระบวนการประชาธิปไตย

การประสานงานและการแบ่งปันข้อมูลระหว่างภาครัฐ ภาคเอกชน และภาคประชาสังคมที่มากขึ้นเป็นสิ่งจำเป็นเพื่อเพิ่มความโปร่งใสและเปิดเผยและขัดขวางการแคมเปญที่มีอิทธิพลเหล่านี้

ผู้คนมากกว่าสามในสี่จากทั่วโลกกังวลเกี่ยวกับวิธีการนำข้อมูลไปใช้เป็นอาวุธ



จับตาการปฏิบัติการด้านอิทธิพลในช่วงโควิด-19 และการรุกรานยูเครนของรัสเซีย

รัฐชาติที่พยายามควบคุมสภาพแวดล้อมของข้อมูลตลอดช่วงการแพร่ระบาดและระหว่างการรุกรานยูเครนของรัสเซีย เป็นตัวอย่างที่ชัดเจนว่าระบอบเผด็จการผสมผสานการปฏิบัติการทางไซเบอร์และข้อมูลอย่างไร

โฆษณาชวนเชื่อ COVID-19

รัสเซีย อิหร่าน และจีนใช้การโฆษณาชวนเชื่อและแคมเปญด้านอิทธิพลตลอดช่วงการระบาดของ COVID-19 COVID-19 แสดงให้เห็นอย่างเด่นชัดในแคมเปญเหล่านี้ในสองแนวทางหลัก:

1. การเป็นตัวแทนของการระบาดเอง
2. แคมเปญที่ใช้โควิด-19 เป็นเครื่องมือเชิงกลยุทธ์เพื่อให้บรรลุวัตถุประสงค์ทางการเมืองที่กว้างขึ้น

วัตถุประสงค์กว้างๆ ของแคมเปญประเภทนี้มีอยู่ 2 ประการ ประการแรก เพื่อบ่อนทำลายระบอบประชาธิปไตย สถาบันประชาธิปไตย และภาพลักษณ์ของสหรัฐอเมริกาและพันธมิตรในเวทีโลก และประการที่สองเพื่อหนุนจุดยืนของตนเองทั้งในและต่างประเทศ

ตัวอย่างนี้สามารถเห็นได้ในการส่งข้อความโดยบัญชีรัสเซียและองค์กรสื่อที่เป็นที่รู้จักซึ่งกำหนดเป้าหมายไปที่ผู้อ่านภาษาอังกฤษ เทียบกับวิธีที่รัฐบาลรัสเซียสื่อสารกับประชาชนของตนเองเกี่ยวกับวัคซีนและความรุนแรงของโควิด-19

หัวข้อที่ครอบคลุมถึงเรื่องราวเกี่ยวกับไวรัสโคโรนาที่มีผู้ชมมากที่สุด 10 อันดับแรกบน RT.com
(ตุลาคม 2021–เมษายน 2022)

การโฆษณาชวนเชื่อต่อต้านวัคซีนมุ่งเป้าไปที่ผู้อ่านที่ไม่ใช่ชาวรัสเซีย

รัสเซีย (แปลด้านล่างเป็นภาษาอังกฤษ)	อังกฤษ
"การล็อกดาวน์และบูสเตอร์ป้องกันการแพร่เชื้อ"	"การฉีดวัคซีนไม่สามารถควบคุมการแพร่เชื้อได้และไม่มีผลกับเชื้อสายพันธุ์ใหม่"
"บุคคลสาธารณะของรัสเซียติดโควิด"	"วัคซีนไฟเซอร์มีผลข้างเคียงที่เป็นอันตราย"
"ผู้ติดเชื้อและผู้เสียชีวิตเพิ่มขึ้นในรัสเซีย"	"การฉีดวัคซีนในประชากรจำนวนมากมาจากแรงจูงใจทางการเมือง"
"วัคซีนสปุตนิก วี มีประสิทธิภาพสูง"	"ไฟเซอร์และโมเดอโรนาดำเนินการทดลองที่ไม่ได้ควบคุม"
"จำเป็นต้องมีหลักฐานวัคซีนในการขนส่งสาธารณะ"	

การส่งข้อความ COVID-19 รัสเซียแตกต่างกันไปตามภาษา

แคมเปญที่พยายามปิดบังที่มาของไวรัส COVID-19 นำเสนออีกตัวอย่างหนึ่ง ตั้งแต่เริ่มเกิดโรคระบาด โฆษณาชวนเชื่อเกี่ยวกับ COVID-19 ของรัสเซีย อิหร่าน และจีนได้เพิ่มความครอบคลุมจากสื่ออื่นๆ เพื่อขยายประเด็นหลักเหล่านี้ การรายงานข่าวนี้ส่วนใหญ่ประกอบด้วยการส่งเสริมการวิพากษ์วิจารณ์หรือทฤษฎีสมคบคิดเกี่ยวกับสหรัฐอเมริกา โดยการขยายความซึ่งกันและกันอย่างสม่ำเสมอ สื่อของรัฐได้พัฒนาระบบนิเวศซึ่งการรายงานข่าวเชิงลบเกี่ยวกับประชาธิปไตยหรือการรายงานข่าวเชิงบวกของรัสเซีย อิหร่าน และจีนโดยสื่อของรัฐหนึ่งได้รับการเสริมแรงโดยสื่ออื่นๆ ครั้งแล้วครั้งเล่า

ตัวอย่างหนึ่งคือข้อเสนอแนะในช่วงต้นของสื่อของรัฐรัสเซียและอิหร่านว่าโควิด-19 อาจเป็นอาวุธชีวภาพที่สร้างโดยสหรัฐอเมริกา การกล่าวอ้างดังกล่าวแพร่กระจายไปทั่วเว็บไซต์สมรู้ร่วมคิดช่วงต้นของการแพร่ระบาดหลังจากการสัมภาษณ์ศาสตราจารย์ด้านกฎหมายที่อ้างว่าเขาเชื่อว่า COVID-19 ถูกสร้างขึ้นมาเพื่อใช้เป็นอาวุธ[6] หลังจากการสัมภาษณ์ได้รับการเผยแพร่บนเว็บไซต์บางแห่งโดยมีการเข้าถึงที่จำกัด แล้วเรื่องดังกล่าวจึงถูกหยิบขึ้นมาโดยสื่อของรัฐ PressTV สื่อภาษาอังกฤษและภาษาฝรั่งเศสของอิหร่านที่ได้รับการสนับสนุนจากรัฐบาลอิหร่าน[7] เผยแพร่เรื่องราวเป็นภาษาอังกฤษในเดือนกุมภาพันธ์ 2020 ในหัวข้อ “ไวรัสโคโรนาเป็นอาวุธสงครามชีวภาพของสหรัฐฯ อย่างที่ฟรานซิส บอยล์เชื่อหรือไม่” บทความดังกล่าวชี้ให้เห็นว่าสหรัฐอเมริกาอยู่เบื้องหลังการแพร่ระบาดของโควิด-19 โดยเขียนว่า "ในทุกสงครามของสหรัฐฯ มีการใช้อาวุธกัมมันตภาพรังสี สารเคมี ชีวภาพ และอาวุธต้องห้ามอื่นๆ ซึ่งก่อให้เกิดความเสียหายร้ายแรงต่อผู้คนในพื้นที่เป้าหมาย”[8] สื่อของรัฐรัสเซียและบัญชีของรัฐบาลจีนได้กล่าวซ้ำถึงความคิดเห็นดังกล่าว Russia Today (RT) ซึ่งเป็นหน่วยงานของรัฐที่เป็นที่รู้จักจากบทบาทในการเผยแพร่โฆษณาชวนเชื่อของเครมลิน[9] ได้เผยแพร่เรื่องราวอย่างน้อยหนึ่งเรื่องที่สนับสนุนคำกล่าวของเจ้าหน้าที่อิหร่านที่อ้างว่า COVID-19 อาจเป็น “ผลิตภัณฑ์ของสหรัฐฯ 'การโจมตีทางชีวภาพ' ที่มุ่งเป้าไปที่อิหร่านและจีน”[10] และผลักดันโพสต์สื่อสังคมออนไลน์ที่ชี้นำข้อมูลดังกล่าวออกไป ตัวอย่างเช่น ทวีต RT จากวันที่ 27 กุมภาพันธ์ 2020 อ่านว่า "ยกมือขึ้น ใครบ้างจะไม่แปลกใจถ้ามีการเปิดเผยว่า #coronavirus เป็นอาวุธชีวภาพหรือไม่"[11]

สงครามในยูเครน การโฆษณาชวนเชื่อในฐานะอาวุธสงคราม

การรุกรานยูเครนของรัสเซียเป็นตัวอย่างที่ชัดเจนว่าการปฏิบัติการด้านอิทธิพลทางไซเบอร์ สามารถผสมผสานกับการโจมตีทางไซเบอร์แบบดั้งเดิมและการปฏิบัติการทางทหารภาคพื้นดินเพื่อเพิ่มผลกระทบสูงสุดได้อย่างไร

ก่อนการบุกยูเครน นักวิเคราะห์ข่าวกรองด้านภัยคุกคามของ Microsoft เห็นว่าผู้มีส่วนในแนวร่วมรัสเซียอย่างน้อยหกคนทำการโจมตีทางไซเบอร์ต่อยูเครนมากกว่า 237 ครั้ง แคมเปญเหล่านี้พยายามลดระดับบริการและสถาบันขัดขวางการเข้าถึงข้อมูลที่น่าเชื่อถือของชาวยูเครน และตั้งข้อสงสัยเกี่ยวกับความเป็นผู้นำของประเทศ

จับตาการปฏิบัติการด้านอิทธิพลในช่วงโควิด-19 และการรุกรานยูเครนของรัสเซีย

ต่อไป

ในรายงาน Microsoft ที่เผยแพร่ในเดือนเมษายน 2022 เราแสดงให้เห็นถึงความพยายามอย่างชัดเจนในการควบคุมสภาพแวดล้อมข้อมูลในเคียฟ รัสเซียเปิดตัวขีปนาวุธโจมตีหอส่งสัญญาณโทรทัศน์ในเคียฟในวันเดียวกับที่เปิดตัวมัลแวร์ทำลายล้างบริษัทสื่อรายใหญ่ของยูเครน[12]

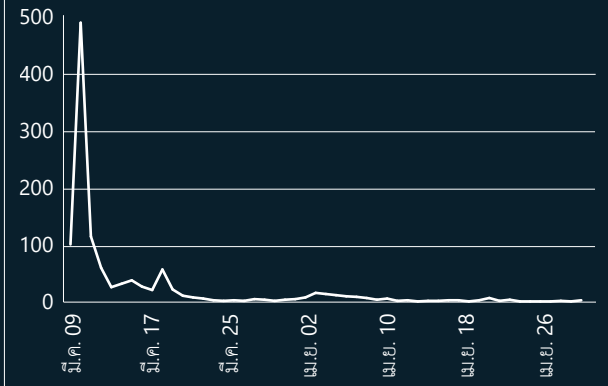
อีกตัวอย่างหนึ่งของการที่การโจมตีทางไซเบอร์และปฏิบัติการด้านอิทธิพลมาบรรจบกัน ผู้ก่อภัยคุกคามชาวรัสเซียส่งอีเมลถึงพลเมืองยูเครนโดยอ้างว่ามาจากชาวเมือง Mariupol กล่าวโทษรัฐบาลยูเครนที่ทำให้สงครามรุนแรงขึ้นและเรียกร้องให้เพื่อนร่วมชาติของพวกเขาต่อต้านรัฐบาล อีเมลเหล่านี้ถูกส่งไป (ตามชื่อ) ให้กับผู้ที่ได้รับอีเมลโดยเฉพาะ ซึ่งบ่งชี้ว่าพวกเขาอาจเคยถูกขโมยข้อมูลในการโจมตีทางไซเบอร์ที่เกี่ยวข้องกับการจารกรรมก่อนหน้านี้ ไม่มีการใส่ลิงก์ที่เป็นอันตรายซึ่งบ่งชี้ว่าเจตนาคือการปฏิบัติการด้านอิทธิพลอย่างแท้จริง

การมีเนื้อหาที่ถูกแฮ็ก รั่วไหล หรือเนื้อหาที่ละเอียดอ่อนเป็นกลวิธีทั่วไปที่ผู้ดำเนินการชาวรัสเซียใช้ในการปฏิบัติการด้านอิทธิพล ตลอดช่วงสงครามในยูเครน ช่องทางสื่อสังคมออนไลน์ที่สนับสนุนรัสเซียได้โปรโมตสิ่งที่พวกเขาอ้างว่ารั่วไหลหรือเป็นเนื้อหาที่ละเอียดอ่อนอื่นๆ จากแหล่งข่าวของยูเครน เนื้อหาที่รั่วไหลหรือละเอียดอ่อนถูกใช้โดยช่องทางและสื่อสังคมออนไลน์ที่ฝักใฝ่รัสเซีย ซึ่งเป็นส่วนหนึ่งของกลยุทธ์การโน้มน้าวที่กว้างขึ้น เพื่อลดทอนความไว้วางใจในสถาบันและทำให้เกิดข้อสงสัยต่อเรื่องเล่ากระแสหลัก ข้อมูลนี้สามารถจัดการได้เพื่อสร้างการโฆษณาชวนเชื่อโดยกำหนดเป้าหมายไปที่ยูเครนและตะวันตก ลดความน่าเชื่อถือในการรักษาความปลอดภัยดิจิตอลและการสนับสนุนการทำลายความช่วยเหลือจากทางตะวันตกไปยังยูเครน

รัสเซียใช้การโจมตีข้อมูลอื่นๆ เพื่อกำหนดความคิดเห็นของประชาชนหลังจากเหตุการณ์ในพื้นที่เพื่อปิดบังหรือบั่นทอนข้อเท็จจริง ตัวอย่างเช่น เมื่อวันที่ 7 มีนาคม รัสเซียได้เสนอเรื่องราวที่วางตำแหน่งไว้ล่วงหน้าผ่านการยื่นฟ้องต่อองค์การสหประชาชาติ (UN) ว่าโรงพยาบาลสำหรับคนท้องในเมือง Mariupol ประเทศยูเครน ถูกปล่อยทิ้งร้างและถูกใช้เป็นสถานที่ทางทหาร ในวันที่ 9 มีนาคม รัสเซียระเบิดโรงพยาบาล หลังจากข่าวการทิ้งระเบิดสิ้นสุดลง Dmitry Polyanskiy ตัวแทนของรัสเซียจากสหประชาชาติได้ทวีตว่าการรายงานข่าวของการทิ้งระเบิดนั้นเป็น "ข่าวปลอม" และอ้างถึงคำกล่าวอ้างก่อนหน้านี้ของรัสเซียเกี่ยวกับการถูกกล่าวหาว่าใช้เป็นที่ตั้งทางทหาร จากนั้นรัสเซียได้เผยแพร่เรื่องราวนี้ในวงกว้างในเว็บไซต์ที่ควบคุมโดยรัสเซียเป็นเวลาสองสัปดาห์หลังจากการโจมตีโรงพยาบาล



โดเมนที่มีการเข้าชม
(9 มีนาคม 2022-30 เมษายน 2022)



เว็บไซต์โฆษณาชวนเชื่อเผยแพร่เรื่องราวเกี่ยวกับโรงพยาบาลสำหรับคนท้องเป็นเวลาประมาณสองสัปดาห์โดยมีการฟื้นฟูในช่วงสั้นๆ เริ่มในวันที่ 1 เมษายน 2022 ที่มา: Microsoft AI for Good Lab

ภาพถ่ายดาวเทียมของโรงพยาบาลปริกำเนิดใน Mariupol ในเดือนกุมภาพันธ์และมีนาคม 2022



การวิเคราะห์ภาพจากดาวเทียมของ Microsoft เองแสดงให้เห็นว่าโรงพยาบาลปริกำเนิดถูกวางระเบิด ภาพแรกคือวันที่ 24 กุมภาพันธ์ 2022 และภาพที่สองคือวันที่ 24 มีนาคม 2022 แหล่งที่มาของรูปภาพ: Planet Labs

การล้างบาปความโหดร้ายของรัสเซียมีความก้าวหน้าอย่างต่อเนื่องในขณะที่สงครามประสบความสำเร็จ ตัวอย่างเช่น ในปลายเดือนมิถุนายนปี 2022 สื่อและผู้มีอิทธิพลของรัสเซียนำเสนอภาพการระเบิดห้างสรรพสินค้าว่าสมเหตุสมผลและจำเป็น โดยอ้างว่าห้างดังกล่าวไม่ได้ใช้เป็นห้างสรรพสินค้า แต่ใช้เป็นคลังอาวุธสำหรับกองกำลังป้องกันดินแดนของยูเครน[13] บล็อกเกอร์ที่ฝักใฝ่เครมลินหลายคนบน Telegram โพสต์และขยายเนื้อหาที่สนับสนุนการเล่าเรื่อง "การจัดฉาก" โดยบล็อกเกอร์ชี้ให้เห็นถึงตัวบ่งชี้ที่ถูกกล่าวหาว่าถูกปลอมขึ้นมา ซึ่งรวมถึงการปรากฏคนในเครื่องแบบทหารในวิดีโอจากที่เกิดเหตุ[14] และการไม่มีผู้หญิงในฟุตเทจ[15] รัสเซียเปิดตัวแคมเปญโดยอาศัยระบบผู้ส่งสารและสื่อโฆษณาชวนเชื่อที่สร้างขึ้นเอง การขยายเรื่องราวเหล่านี้ทางออนไลน์ทำให้รัสเซียสามารถหันเหความผิดในเวทีระหว่างประเทศและหลีกเลี่ยงความรับผิดชอบได้

รัฐชาติ เช่น รัสเซีย เข้าใจถึงคุณค่าของการใช้ข้อมูลที่ได้รับจากแหล่งที่มาที่ปิดเพื่อให้มีอิทธิพลต่อการรับรู้ของประชาชนโดยใช้แคมเปญ "แฮ็กและรั่วไหล" เพื่อกระจายเรื่องเล่าตอบโต้และสร้างความไม่ไว้วางใจ

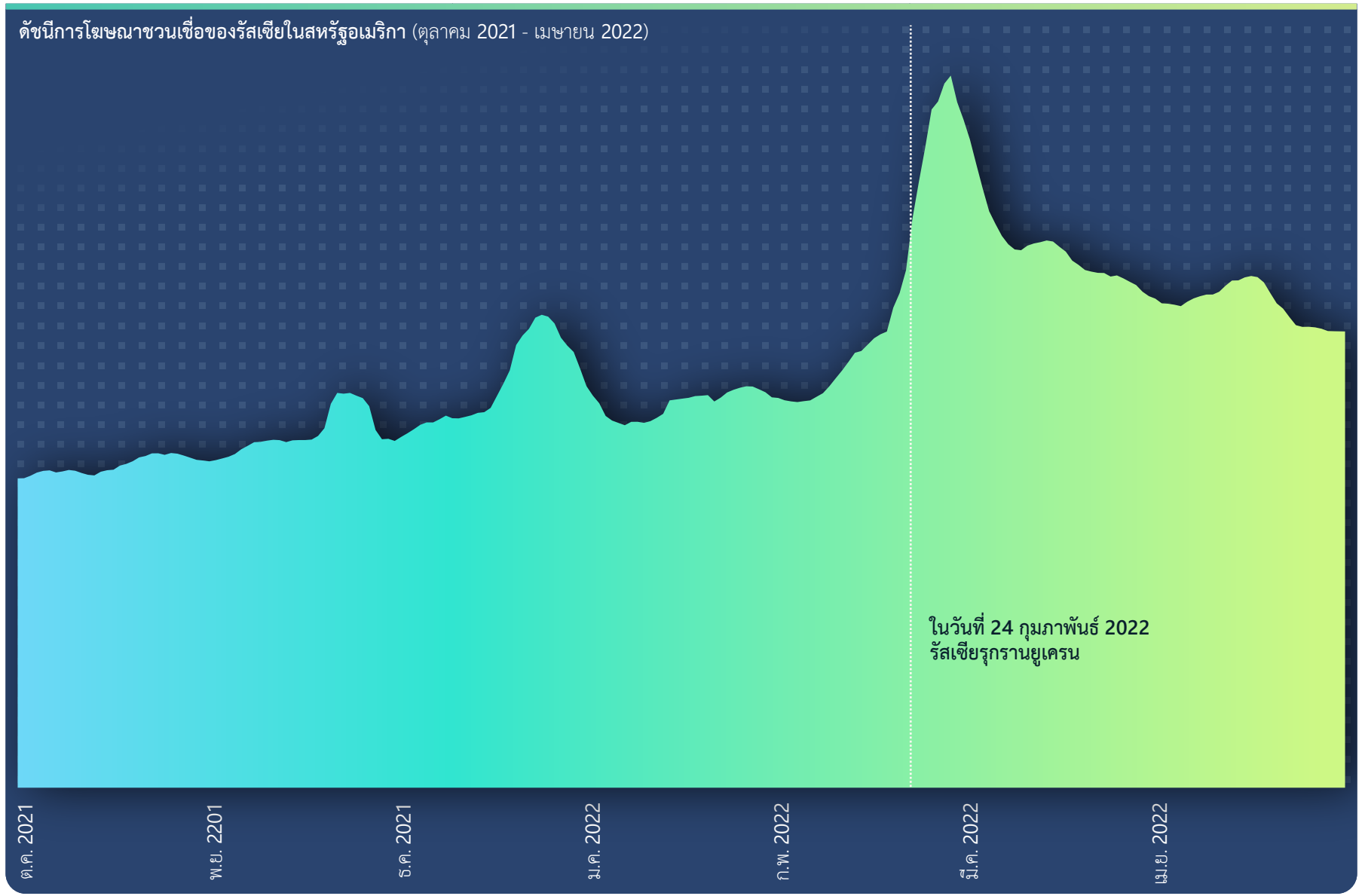
ลิงค์ไปยังข้อมูลเพิ่มเติม

- การปกป้องยูเครน: บทเรียนแรกจากสงครามไซเบอร์ | Microsoft On the Issues
- ภาพรวมของกิจกรรมการโจมตีทางไซเบอร์ของรัสเซียในประเทศยูเครน | รายงานพิเศษ Microsoft
- การรบกวนการโจมตีทางไซเบอร์ที่กำหนดเป้าหมายไปที่ยูเครน | Microsoft On the Issues

การติดตามดัชนีโฆษณาชวนเชื่อของรัสเซีย

ในเดือนมกราคม 2022 เว็บไซต์ในสหรัฐอเมริกาเกือบหนึ่งพันแห่งอ้างอิงการเข้าชมเว็บไซต์ของรัสเซียที่มีการโฆษณาชวนเชื่อ หัวข้อที่พบมากที่สุดสำหรับเว็บไซต์โฆษณาชวนเชื่อของรัสเซียที่กำหนดเป้าหมายผู้ชมสหรัฐอเมริกา คือ สงครามในยูเครน การเมืองในประเทศของสหรัฐฯ (ไม่ว่าจะสนับสนุนทรัมป์หรือไบเดน) และ COVID-19 และเรื่องที่เกี่ยวข้องกับวัคซีน

ดัชนีโฆษณาชวนเชื่อของรัสเซีย (RPI) ตรวจสอบการไหลของข่าวสารจากช่องทางข่าวสารที่มีการควบคุมโดยรัฐของรัสเซียและผู้สนับสนุนและการขยายโดยคิดเป็นสัดส่วนของปริมาณการใช้งานข่าวสารโดยรวมบนอินเทอร์เน็ต RPI สามารถใช้เพื่อสร้างแผนภูมิการบริโภคโฆษณาชวนเชื่อของรัสเซียผ่านอินเทอร์เน็ตและในภูมิภาคที่ต่างกันบนไทม์ไลน์ที่แม่นยำ อย่างไรก็ตาม Microsoft ตั้งข้อสังเกตว่าเราจะสามารถสังเกตได้เฉพาะโฆษณาชวนเชื่อของรัสเซียที่โพสต์ไปยังเว็บไซต์ที่ระบุไว้ก่อนหน้านี้เท่านั้น เราไม่ได้มีข้อมูลเชิงลึกเกี่ยวกับการโฆษณาชวนเชื่อเกี่ยวกับเว็บไซต์ประเภทอื่นๆ รวมถึงเว็บไซต์ข่าวที่เชื่อถือได้ เว็บไซต์ที่ไม่ปรากฏชื่อ และกลุ่มเครือข่ายทางสังคม



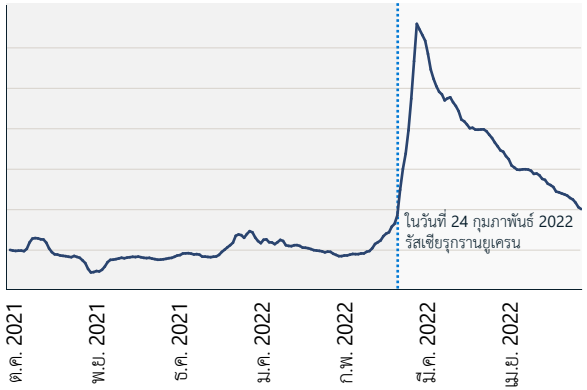
การติดตามดัชนีโฆษณาชวนเชื่อของรัสเซีย

ต่อไป

ดัชนีโฆษณาชวนเชื่อของรัสเซีย: ยูเครน

เมื่อสงครามยูเครนเริ่มขึ้น เราพบโฆษณาชวนเชื่อของรัสเซียเพิ่มขึ้น 216 เปอร์เซ็นต์ โดยสูงสุดในวันที่ 2 มีนาคม แผนภูมิด้านล่างแสดงให้เห็นถึงวิธีการที่การเพิ่มขึ้นอย่างกะทันหันนี้เกิดขึ้นพร้อมกับการรุกราน กราฟทั้งสองแสดงให้เห็นว่าการโฆษณาชวนเชื่อของรัสเซียเพิ่มขึ้นอย่างรวดเร็วหลังจากการรุกรานเริ่มต้นขึ้น

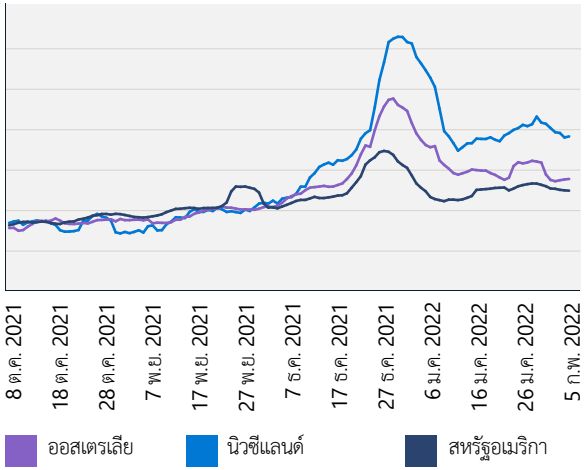
RPI ยูเครน
(7 ตุลาคม 2021-30 เมษายน 2022)



ดัชนีโฆษณาชวนเชื่อของรัสเซีย: นิวซีแลนด์กับออสเตรเลียและสหรัฐอเมริกา

การประเมินผลของ RPI ในนิวซีแลนด์แสดงให้เห็นถึงการพุ่งสูงขึ้นในช่วงปลายปี 2021 ซึ่งเกี่ยวข้องกับการโฆษณาชวนเชื่อที่เกี่ยวกับ COVID-19 การบริโภคโฆษณาชวนเชื่อของรัสเซียที่พุ่งสูงขึ้นอย่างรวดเร็วในนิวซีแลนด์นี้ เกิดขึ้นก่อนที่จะมีการประท้วงสาธารณะที่เพิ่มขึ้นในช่วงต้น 2022 ในเมืองเวลลิงตัน การพุ่งสูงขึ้นครั้งที่สองมีความเกี่ยวข้องกับการบุกรุกของรัสเซียอย่างชัดเจนและเกินสูงกว่า RPIs ของออสเตรเลียและสหรัฐอเมริกา

RPI, นิวซีแลนด์เทียบกับออสเตรเลียและสหรัฐอเมริกา



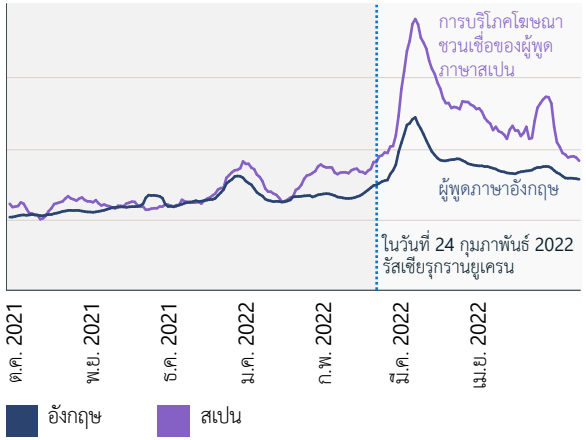
การบริโภคโฆษณาชวนเชื่อของรัสเซียในนิวซีแลนด์คล้ายกับออสเตรเลียจนถึงสัปดาห์แรกของเดือนธันวาคม 2021 หลังจากเดือนธันวาคม การบริโภคโฆษณาชวนเชื่อของรัสเซียในนิวซีแลนด์เพิ่มขึ้นมากกว่า 30 เปอร์เซ็นต์เมื่อเทียบกับการบริโภคในออสเตรเลียและสหรัฐอเมริกา

ดัชนีการโฆษณาชวนเชื่อของรัสเซียในสหรัฐอเมริกา: ภาษาอังกฤษและภาษาสเปน

นอกจากนี้ RPI ยังติดตามการโฆษณาชวนเชื่อทั่วทุกภาษาสื่อต่างๆ รวมถึง RT และ Sputnik News มีภาษารองรับมากกว่า 20 ภาษา ซึ่งได้แก่ ภาษาอังกฤษ, สเปน, เยอรมัน, ฝรั่งเศส, กรีก, อิตาลี, เช็ก, โปแลนด์, เซอร์เบีย, ลัตเวีย, ลิทัวเนีย, มอลโดวา, เบลารุส, อาร์มีเนีย, Ossetian, จอร์เจีย, อาเซอร์ไบจาน, อาหรับ, ตุรกี, เปอร์เซีย, และภาษาดารี

กราฟต่อไปนี้แสดงให้เห็นว่า RPI ข่าวภาษาสเปนในสหรัฐอเมริกาสูงกว่าข่าวภาษาอังกฤษมาก

การบริโภคโฆษณาชวนเชื่อของชาวรัสเซียอยู่ใน ระดับที่สูงขึ้น 2เท่าของตัวในหมู่ผู้ที่พูดภาษาสเปน



การบริโภคโฆษณาชวนเชื่อของรัสเซียในสหรัฐอเมริกาจะสูงขึ้นสองเท่าในหมู่ผู้ที่พูดภาษาสเปน

โฆษณาชวนเชื่อของรัสเซียมีมากในลาตินอเมริกา



RT ในภาษาสเปนเป็นสื่อต่างประเทศที่มีจำนวนการเพจและจำนวนการเข้าชมบน Facebook สูงสุด

แหล่งที่มา: Microsoft AI for Good Research Lab

สื่อสังเคราะห์

เรากำลังเข้าสู่ยุคทองสำหรับการสร้างและการจัดการสื่อที่เปิดใช้งาน AI นักวิเคราะห์ Microsoft ตั้งข้อสังเกตว่าเรื่องนี้มีสาเหตุมาจากแนวโน้มสำคัญสองประการ ได้แก่ การเพิ่มจำนวนของเครื่องมือและบริการที่ใช้งานง่าย สำหรับการสร้างภาพ วิดีโอ เสียง และข้อความสังเคราะห์ที่สมจริงสูงและความสามารถในการเผยแพร่เนื้อหาที่ปรับให้เหมาะสมกับผู้ชมที่เฉพาะเจาะจงได้อย่างรวดเร็ว

การพัฒนาเหล่านี้ไม่ใช่สิ่งที่เป็นปัญหาอย่างแท้จริงในตัวเอง เทคโนโลยีที่ใช้ AI สามารถนำมาใช้ในการสร้างเนื้อหาดิจิตอลที่สนุกสนานและน่าตื่นเต้น ไม่ว่าจะเป็นการสร้างเนื้อหาที่สังเคราะห์ทั้งหมดหรือการเสริมสร้างเนื้อหาที่มีอยู่แล้ว เครื่องมือเหล่านี้ถูกใช้กันอย่างแพร่หลายโดยองค์กรสำหรับการโฆษณาและการสื่อสาร และโดยบุคคลต่างๆ เพื่อสร้างเนื้อหาที่มีส่วนร่วมสำหรับผู้ติดตามของพวกเขา อย่างไรก็ตาม เมื่อสร้างและกระจายสื่อสังเคราะห์ด้วยเจตนาที่จะสร้างอันตราย จะมีศักยภาพในการทำความเสียหายร้ายแรงต่อบุคคล บริษัท สถาบันการเงิน และสังคม Microsoft เป็นแรงผลักดันในการพัฒนาเทคโนโลยีและการปฏิบัติทั้งภายในและทั่วทั้งระบบนิเวศสื่อที่กว้างขึ้นเพื่อจำกัดอันตรายนี้

ส่วนนี้สำรวจข้อมูลเชิงลึกจากการวิเคราะห์ของ Microsoft เกี่ยวกับสถานะปัจจุบันของเทคโนโลยีที่เป็นศิลปะสำหรับการสร้างเนื้อหาสังเคราะห์ที่สร้างความเสียหาย อันตรายที่อาจเกิดขึ้นได้หากเนื้อหานี้ได้รับการเผยแพร่อย่างกว้างขวาง และการบรรเทาทางเทคนิคที่สามารถป้องกันภัยคุกคามทางไซเบอร์จากสื่อสังเคราะห์

การสร้างสื่อสังเคราะห์

ในส่วนของข้อความและสื่อสังเคราะห์กำลังก้าวหน้าไปอย่างรวดเร็วอย่างไม่น่าเชื่อ จากเทคนิคที่เคยทำได้โดยใช้ทรัพยากรคอมพิวเตอร์จำนวนมหาศาลของสตูดิโอภาพยนตร์ขนาดใหญ่เท่านั้น แต่ตอนนี้เทคนิคดังกล่าวได้รวมเข้ากับแอพโทรศัพท์แล้ว ในเวลาเดียวกัน เครื่องมือต่างๆ จะใช้งานได้ง่ายขึ้นและสามารถสร้างเนื้อหาที่มีระดับความสมจริงที่สามารถหลอกได้แม้แต่ผู้เชี่ยวชาญด้านการสื่อสารทางนิติวิทยาศาสตร์ เราใกล้ถึงจุดที่ทุกคนสามารถสร้างวิดีโอสังเคราะห์ของใครก็ตามให้พูดหรือทำอะไรก็ได้ มันไม่ใช่เรื่องที่ไม่สมเหตุสมผลเลยที่จะเชื่อว่าเรากำลังเข้าสู่ยุคที่เนื้อหาจำนวนมากที่เราเห็นทางออนไลน์ถูกสังเคราะห์ขึ้นทั้งหมดหรือบางส่วนโดยใช้เทคนิค AI

> ด้วยความพร้อมใช้งานของเครื่องมือที่มีความซับซ้อนมากขึ้น ใช้งานง่าย และมีความพร้อมใช้งานอย่างกว้างขวาง การสร้างเนื้อหาสังเคราะห์จึงเพิ่มขึ้นเรื่อยๆ และในไม่ช้าก็จะแยกไม่ออกจากความเป็นจริง

มีเครื่องมือแก้ไขรูปภาพ วิดีโอ และเสียงคุณภาพสูงฟรีและเชิงพาณิชย์มากมาย เครื่องมือเหล่านี้สามารถใช้เพื่อทำให้การเปลี่ยนแปลงเนื้อหาดิจิทัลเป็นเรื่องง่ายแต่อาจทำให้เกิดความเสียหาย เช่น การเพิ่มข้อความที่ทำให้เข้าใจผิด การสลับหน้า และการลบหรือดัดแปลงบริบท ดังนั้น "การปลอมแบบไม่เนียน" มีการใช้กันอย่างแพร่หลายเพื่อกระจายเนื้อหาที่ชั่วร้าย ส่งเสริมอุดมการณ์ทางการเมือง และสร้างความเสียหายต่อชื่อเสียง ตัวอย่างที่รู้จักกันดีคือ[16] วิดีโอในปี 2019 ของแนนซี เปโลซี ประธานสภาผู้แทนราษฎรสหรัฐฯ พูดจาอ้อแอ้และดูเหมือนมึนเมา แม้ว่าจะมีการระบุได้อย่างรวดเร็วว่าวิดีโอถูกทำให้ช้าลงเพื่อสร้างเอฟเฟ็กต์ แต่ "การปลอมแบบไม่เนียน" แพร่กระจายไปทั่วก่อนที่วิดีโอต้นฉบับและบริบทจะปรากฏขึ้น

วิธีการที่ซับซ้อนมากขึ้นในการดัดแปลงเนื้อหาสื่อรวมถึงการประยุกต์ใช้เทคนิค AI ขั้นสูงเพื่อ (ก) สร้างสื่อสังเคราะห์ล้วน และ (ข) ทำการแก้ไขที่สื่อที่มีอยู่แล้วให้มีความซับซ้อนมากขึ้น คำว่า การปลอมแปลงเชิงลึก มักจะใช้สำหรับสื่อสังเคราะห์ที่ได้รับการสร้างขึ้นโดยใช้เทคนิค AI ที่ล้ำสมัย (ชื่อมาจากเครือข่ายประสาทเทียมเชิงลึกที่บางครั้งใช้อยู่) เทคโนโลยีเหล่านี้ได้รับการพัฒนาเป็นแอปพลิเคชันแบบสแตนด์อโลน เครื่องมือ และบริการ และรวมอยู่ในเครื่องมือการแก้ไขเชิงพาณิชย์และโอเพนซอร์ส

เทคโนโลยีดังกล่าวถูกนำมาใช้เป็นอาวุธโดยผู้ประสงค์ร้ายซึ่งหวังที่จะสร้างความเสียหายต่อบุคคลและสถาบัน ตัวอย่างของเทคนิคการปลอมแปลงเชิงลึก ได้แก่:

- **การสลับใบหน้า (วิดีโอ รูปภาพ)** —แทนที่ใบหน้าในวิดีโอด้วยอีกใบหน้าหนึ่ง เทคนิคนี้สามารถนำมาใช้เพื่อพยายามแบล็กเมล์บุคคล บริษัท หรือสถาบัน หรือเพื่อให้บุคคลอยู่ในสถานที่หรือสถานการณ์ที่น่าอับอาย
- **การเชิดหุ่น (วิดีโอ ภาพ)** —การใช้วิดีโอเพื่อทำให้ภาพนิ่งหรือวิดีโอที่สองมีความเคลื่อนไหว ซึ่งจะทำให้ดูเหมือนว่าใครคนหนึ่งพูดอะไรที่น่าอายหรือทำให้เข้าใจผิดได้
- **โครงข่ายประสาทเทียมก่อกำเนิดแบบมีคู่ปรปักษ์ (วิดีโอรูปภาพ)** —ชุดเทคนิคสำหรับการสร้างภาพที่สมจริง
- **โมเดลการปลอมแปลง (วิดีโอ รูปภาพ ข้อความ)** —การสร้างภาพที่หลากหลายจากคำอธิบายที่เป็นข้อความ

เทคนิคที่ใช้ AI ขั้นสูงดังกล่าวยังไม่ได้ใช้กันอย่างแพร่หลายในแคมเปญด้านอิทธิพลทางไซเบอร์ในปัจจุบัน แต่เราคาดว่าปัญหาจะเพิ่มขึ้นเมื่อเครื่องมือใช้งานง่ายขึ้นและพร้อมใช้งานอย่างกว้างขวางมากขึ้น

ผลกระทบของการจัดการสื่อสังเคราะห์

การใช้การดำเนินการข้อมูลเพื่อทำให้เกิดอันตรายหรือขยายอิทธิพลไม่ใช่เรื่องใหม่ อย่างไรก็ตาม ความเร็วในการที่ข้อมูลสามารถแพร่กระจายได้และและการที่เราไม่สามารถแยกแยะข้อเท็จจริงจากเรื่องแต่งได้อย่างรวดเร็วหมายถึงผลกระทบและอันตรายที่เกิดจากการปลอมและสื่อที่เป็นอันตรายอื่นๆ ที่มีการสังเคราะห์ขึ้นอาจรุนแรงมากกว่าเดิม ดังที่แสดงไว้ในตัวอย่าง Pelosi

มีอันตรายหลายประเภทที่เราได้พิจารณา: การจัดการตลาด การฉ้อโกงการชำระเงิน วิชชิ่ง การแอบอ้างบุคคลอื่น ความเสียหายต่อแบรนด์ ความเสียหายต่อชื่อเสียง และบ็อตเน็ต หลายหมวดหมู่จากหมวดหมู่ดังกล่าวมีการรายงานอย่างกว้างขวางถึงตัวอย่างที่เกิดในโลกแห่งความเป็นจริง ซึ่งอาจบั่นทอนความสามารถของเราในการแยกของจริงออกจากของที่แต่งขึ้น

ภัยคุกคามระยะยาวและร้ายกาจกว่าคือการทำความเข้าใจว่าอะไรคือความจริง ถ้าเราไม่สามารถไว้วางใจในสิ่งที่เราเห็นและได้ยินได้อีกต่อไป ด้วยเหตุนี้ รูปภาพ เสียง หรือวิดีโอที่ประนีประนอมของบุคคลสาธารณะหรือส่วนตัวจึงถูกปฏิเสธได้ว่าเป็นของปลอม ซึ่งเป็นผลลัพธ์ที่เรียกว่า The Liar's Dividend[17] การวิจัยล่าสุด[18] แสดงให้เห็นว่ามีการใช้เทคโนโลยีในทางที่ผิดเพื่อโจมตีระบบการเงินอยู่แล้ว แม้ว่าสถานการณ์การละเมิดอื่นๆ อีกมากมายจะมีเหตุผลก็ตาม

สื่อสังเคราะห์

ต่อไป

การตรวจหาสื่อสังเคราะห์

ความพยายามกำลังดำเนินการในอุตสาหกรรม รัฐบาล และสถาบันการศึกษาเพื่อพัฒนาวิธีที่ดีกว่าในการตรวจจับและลดความน่าเชื่อถือของสื่อสังเคราะห์และฟื้นฟูความไว้วางใจ มีหลายหนทางข้างหน้าที่ดูมีหวัง เช่นเดียวกับอุปสรรคที่ต้องได้รับการพิจารณา

วิธีหนึ่งคือการสร้างระบบที่ใช้ AI ซึ่งสามารถตรวจจับการปลอมได้ โดยพื้นฐานแล้วคือระบบ AI ที่ “ป้องกัน” เพื่อตอบโต้กับระบบ AI ที่ไม่เหมาะสม นี่คือหัวข้อของการวิจัยที่มีการใช้งานอยู่ ซึ่งระบบปัจจุบันจะทิ้งอาร์ทิแฟกต์ที่บอกเล่าเรื่องราวสำหรับการสร้างเสียงสังเคราะห์และวิดีโอ ซึ่งนักวิเคราะห์ทางนิติวิทยาศาสตร์สื่อที่ผ่านการฝึกอบรม และเครื่องมืออัตโนมัติสามารถตรวจจับได้

แต่น่าเสียดายในปัจจุบันการปลอมได้เปิดเผยให้เห็นถึงข้อบกพร่อง อาร์ทิแฟกต์ที่แม่นยำมักจะมีความเฉพาะเจาะจงกับเครื่องมือหรืออัลกอริทึมเฉพาะ ซึ่งหมายความว่าโดยปกติแล้วการฝึกอบรมเกี่ยวกับการปลอมที่รู้จัก มักไม่ได้นำไปใช้กับอัลกอริทึมอื่นๆ ตามที่แสดงให้เห็นในการแข่งขันแบบเปิดในปี 2020 เพื่อสร้างเครื่องตรวจจับภาพที่ปลอมแปลงเชิงลึก[19] เป็นสิ่งที่ดึงดูดให้เพิ่มการลงทุนในการพัฒนาตัวตรวจจับที่ทันสมัยมากขึ้นแต่ Microsoft มีความสงสัยอย่างสูงว่าจะส่งผลให้มีการปรับปรุงที่สำคัญ ด้วยเหตุผลสองประการ:

ประการแรก เรามีโมเดลทางกายภาพที่ยอดเยี่ยมที่สะท้อนถึงโลกแห่งความเป็นจริง ตัวสร้างเนื้อหาปลอมในปัจจุบันทำแบบชุ่ยๆ ส่งผลให้เกิดอาร์ทิแฟกต์ที่ตรวจจับได้ แต่โมเดลที่ใหม่กว่าจะเหมือนจริงมากขึ้น ไม่มีอะไรพิเศษอย่างแท้จริงเกี่ยวกับฉากที่มีอยู่จริงในโลกที่ถ่ายโดยกล้องที่ไม่สามารถจำลองโดยคอมพิวเตอร์ได้

ประการที่สอง อัลกอริธึมการสร้างปลอมขั้นสูงใช้เทคนิคที่เรียกว่า Generative Adversarial Networks (GANs) เป็นส่วนหนึ่งของกระบวนการสร้าง GAN ใช้ระบบ AI สองระบบเพื่อให้ค้านกันโดยใช้ตัวสร้างเพื่อสร้างเนื้อหาปลอมและตัวแยกเพื่อตรวจจับภาพปลอมและฝึกตัวสร้าง การลงทุนใดๆ ในการพัฒนาเครื่องตรวจจับที่ดีขึ้นเพียงแต่จะทำให้ตัวสร้างสามารถปรับปรุงคุณภาพในการสร้างของปลอมได้



สื่อสังเคราะห์

ต่อไป

แหล่งที่มาของสินทรัพย์ดิจิทัล

หากการตรวจจับของปลอมไม่น่าเชื่อถือ จะทำอย่างไรเพื่อป้องกันการใช้สื่อสังเคราะห์ที่เป็นอันตราย เทคโนโลยีเกิดใหม่ที่สำคัญอย่างหนึ่งคือแหล่งที่มาทางดิจิทัล ซึ่งเป็นกลไกที่ช่วยให้ผู้สร้างสื่อดิจิทัลสามารถรับรองเนื้อหาและช่วยให้ผู้บริโภคระบุได้ว่าเนื้อหาดิจิทัลนั้นถูกแก้ไขหรือไม่ แหล่งที่มาทางดิจิทัลมีความสำคัญอย่างยิ่งในบริบทของเครือข่ายโซเชียลมีเดียในปัจจุบัน เนื่องจากความเร็วที่เนื้อหาสามารถเดินทางบนอินเทอร์เน็ตและโอกาสสำหรับผู้ไม่หวังดีที่จะจัดการกับเนื้อหาได้อย่างง่ายดาย

เทคโนโลยีแหล่งที่มาดิจิทัลคือการลงนามในเอกสารเข้ารหัสเวอร์ชันทันสมัย ซึ่งออกแบบมาเพื่อบันทึกแหล่งที่มา ประวัติการแก้ไข และข้อมูลเมตาดาต้าของอ็อบเจ็กต์ที่ส่งผ่านเว็บในปัจจุบัน วิสัยทัศน์และวิธีการทางเทคนิคสำหรับการเปิดใช้งานการรับรองแบบครบวงจรของสื่อนี้ได้รับการพัฒนาโดยทีมนักวิจัยและนักวิทยาศาสตร์ที่ทำงานร่วมกันระหว่างทีมที่ Microsoft เรามีส่วนร่วมเป็นผู้นำในการเป็นหุ้นส่วนระหว่างอุตสาหกรรมที่มุ่งนำเทคโนโลยีแหล่งที่มาของสื่อมาใช้ใน Project Origin (ก่อตั้งโดย Microsoft, BBC, CBC/Radio-Canada และ New York Times) และมีส่วนร่วมใน Content Authenticity Initiative (ก่อตั้งโดย Adobe) นอกจากนี้ Microsoft ยังทำงานร่วมกับคู่ค้าด้านบริการด้านเทคโนโลยีและสื่อเพื่อจัดตั้ง Coalition for Content Provenance and Authenticity (C2PA) C2PA เป็นองค์กรมาตรฐานที่เพิ่งเผยแพร่ข้อกำหนดเกี่ยวกับแหล่งที่มาทางดิจิทัลขั้นสูงสุดเพื่อใช้กับเนื้อหาสื่อต่างๆ รวมถึงรูปภาพ วิดีโอ เสียง และข้อความ

ออบเจ็กต์ที่เปิดใช้งาน C2PA มีรายการที่ช่วยปกป้องวัตถุและเมตาดาต้าจากการแทรกแซงและใบรับรองที่ประกอบด้วยจะระบุผู้เผยแพร่

> เดิมทีสื่อสังเคราะห์ไม่ถูกออกแบบมาเพื่อทำให้เกิดอันตราย แต่จะถูกนำมาปรับใช้เป็นอาวุธโดยผู้ประสงค์ร้ายเพื่อทำลายความไว้วางใจในบุคคลและสถาบัน

> แหล่งที่มาทางดิจิทัลเป็นเทคโนโลยีใหม่ที่มีแนวโน้มว่าจะมีศักยภาพในการช่วยฟื้นความเชื่อมั่นของผู้คนต่อเนื้อหาสื่อออนไลน์โดยการรับรองแหล่งที่มาของเนื้อหาสื่อ

โซลูชันที่เผยแพร่สู่สาธารณะตามข้อกำหนด C2PA จะถูกปรับให้เป็นคุณลักษณะใหม่ในผลิตภัณฑ์ที่มีอยู่หรือแอปและบริการแบบสแตนด์อโลนใหม่ เราคาดว่าเครื่องมือที่ใช้ในการสร้าง การแก้ไข และการเขียนที่ใช้กันทั่วไปส่วนใหญ่จะเปิดใช้งาน C2PA ในอีกไม่กี่ปีข้างหน้า ซึ่งเป็นโอกาสสำหรับองค์กรในการกำหนดความต้องการและการใช้งานของตนสำหรับแหล่งที่มาทางดิจิทัลในปัจจุบัน และในการบังคับใช้การป้องกันอีกชั้นเพิ่มเติมในเครื่องมือที่ใช้ในเวิร์กโฟลว์ที่มีอยู่

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ใช้ขั้นตอนเชิงรุกเพื่อปกป้ององค์กรของคุณจากภัยคุกคามจากข้อมูลที่ผิดผ่านการพิจารณาจากการตอบสนองต่อการทำงานของ PR และการสื่อสารของคุณ
2. ใช้เทคโนโลยีแหล่งที่มา เพื่อปกป้องการสื่อสารอย่างเป็นทางการ

ลิงค์ไปยังข้อมูลเพิ่มเติม

- ก้าวต่อไปของการบิดเบือนข้อมูล | Microsoft On the Issues
- บรรลุเป้าหมายสำคัญ, 31 มกราคม 2022
- Project Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- ดูรายละเอียดทางเทคนิคเกี่ยวกับ Project Origin ของระบบที่ใช้สำหรับการรับรองความถูกต้องของสื่อ | Microsoft ALT Innovation

900%

การแพร่กระจายของการปลอมแปลงเชิงลึกเพิ่มขึ้นทุกปีตั้งแต่ 2019[20]

แนวทางแบบองค์รวมเพื่อป้องกันการปฏิบัติการด้านอิทธิพลทางไซเบอร์

Microsoft กำลังสร้างโครงสร้างพื้นฐานด้านข่าวกรองภัยคุกคามทางไซเบอร์ที่ที่พัฒนาเต็มที่แล้วเพื่อพัฒนามุมมองการปฏิบัติการด้านอิทธิพลทางไซเบอร์ที่กว้างขึ้นและครอบคลุมมากขึ้น

เราใช้กรอบงานสำหรับกลยุทธ์การตอบสนองและบรรเทาผลกระทบที่ได้รับการแนะนำเพื่อต่อสู้กับภัยคุกคามที่เกิดจากการดำเนินงานซึ่งสามารถแบ่งออกเป็นสี่เสาหลัก: ตรวจหา ทำลาย ป้องกัน และยับยั้ง

นอกจากนี้ Microsoft ได้นำหลักการสี่ประการมาใช้เพื่อยึดหลักการทำงานของเราในด้านนี้ ประการแรก เป็นความมุ่งมั่นที่จะเคารพเสรีภาพในการแสดงออกและรักษาความสามารถของลูกค้าของเราในการสร้าง เผยแพร่ และค้นหาข้อมูลผ่านแพลตฟอร์ม ผลิตภัณฑ์ และบริการของเรา ประการที่สอง เราทำงานเชิงรุกเพื่อป้องกันไม่ให้แพลตฟอร์มและผลิตภัณฑ์ของเราถูกใช้เพื่อขยายเว็บไซต์และเนื้อหาด้านอิทธิพลทางไซเบอร์ต่างประเทศ ประการที่สาม เราจะไม่รับผลกำไรโดยเจตนาจากการใช้เนื้อหาหรือผู้ดำเนินการด้านอิทธิพลทางไซเบอร์ต่างประเทศ ประการสุดท้าย เราจะจัดลำดับความสำคัญของเนื้อหาเพื่อรับมือกับการปฏิบัติการด้านอิทธิพลทางไซเบอร์ต่างประเทศโดยใช้ข้อมูลของบุคคลที่สามซึ่งเป็นข้อมูลภายในและเชื่อถือได้ในผลิตภัณฑ์ของเรา

ตรวจหา

เช่นเดียวกับการป้องกันไซเบอร์ ขั้นตอนแรกในการรับมือกับการปฏิบัติการด้านอิทธิพลทางไซเบอร์ต่างประเทศคือการพัฒนาขีดความสามารถในการตรวจหา ไม่มีบริษัทหรือองค์กรใดๆ ที่สามารถคาดหวังว่าจะทำให้เรื่องนี้คืบหน้าได้ด้วยตัวคนเดียว ความร่วมมือใหม่ที่กว้างขึ้นในภาคเทคโนโลยีจะเป็นสิ่งที่สำคัญ ด้วยความคืบหน้าในการวิเคราะห์และรายงานการปฏิบัติการด้านอิทธิพลทางไซเบอร์ต่างประเทศซึ่งพึ่งพาบทบาทของภาคประชาสังคมรวมถึงสถาบันการศึกษาและองค์กรที่ไม่แสวงหาผลกำไรเป็นหลัก

เมื่อตระหนักถึงบทบาทนี้ นักวิจัย Jake Shapiro และ Alicia Wanless จาก Princeton University และ Carnegie Endowment for International Peace ตามลำดับ จึงได้วางแผนเปิดตัว “Institute for Research on the Information Environment” (IRIE) แห่งใหม่ด้วยการสนับสนุนจาก Microsoft Knight Foundation และ Craig Newmark Philanthropies IRIE จะสร้างสถาบันวิจัยแบบรวมผู้มีส่วนได้ส่วนเสียหลายกลุ่ม โดยมีต้นแบบมาจาก European Organization for Nuclear Research (CERN) ซึ่งจะรวมความเชี่ยวชาญในการประมวลผลและวิเคราะห์ข้อมูลเพื่อเพิ่มความเร็วและปรับขนาดการพบข้อมูลใหม่ในด้านนี้ การค้นพบจะถูกแบ่งปันเพื่อแจ้งไปยังผู้กำหนดนโยบาย บริษัทเทคโนโลยี และผู้บริโภคในวงกว้างมากขึ้น

Defend

เสาหลักเชิงกลยุทธ์ที่สองคือการเสริมแนวป้องกันประชาธิปไตย ซึ่งมีความสำคัญมาอย่างยาวนานในความต้องการการลงทุนและนวัตกรรม ควรคำนึงถึงความท้าทายที่เทคโนโลยีสร้างขึ้นต่อประชาธิปไตย และโอกาสที่เทคโนโลยีสร้างขึ้นเพื่อปกป้องสังคมประชาธิปไตยอย่างมีประสิทธิภาพมากขึ้น

> กรอบงานกลยุทธ์ของ Microsoft มีจุดมุ่งหมายเพื่อช่วยให้ผู้มีส่วนได้ส่วนเสียร่วมตรวจหา ขัดขวาง ปกป้อง และขัดขวางการโฆษณาชวนเชื่อโดยเฉพาะอย่างยิ่งแคมเปญโดยการรุกรานจากต่างประเทศ

เป็นการเหมาะสมที่จะเริ่มต้นด้วยหนึ่งในความท้าทายทางเทคโนโลยีที่ยิ่งใหญ่ในยุคของเรา นั่นคือผลกระทบของอินเทอร์เน็ตและการโฆษณาดิจิทัลที่มีต่อสื่อสารมวลชนแบบดั้งเดิม ตั้งแต่ทศวรรษ 1700 สื่ออิสระมีบทบาทพิเศษในการสนับสนุนระบอบประชาธิปไตยทุกแห่งในโลก เปิดโปงการทุจริต จัดทำเอกสารเกี่ยวกับสงคราม และชี้ให้เห็นถึงความท้าทายทางสังคมครั้งใหญ่ที่สุดในครั้งนี้และทุกครั้ง อย่างไรก็ตาม อินเทอร์เน็ตได้ทำลายข่าวท้องถิ่นด้วยการกินรายได้จากการโฆษณาและล่อลวงให้สมาชิกแบบชำระเงินหนังสือพิมพ์ท้องถิ่นจำนวนมากได้ปิดตัวลง หนึ่งในข้อมูลเชิงลึกมากมายจากงานล่าสุดของเรา คือเมืองที่ไม่มีหนังสือพิมพ์ได้รับโฆษณาชวนเชื่อจากต่างประเทศในปริมาณที่มากกว่าค่าเฉลี่ยโดยไม่รู้ตัวและหลีกเลี่ยงไม่ได้ ด้วยเหตุผลเหล่านี้ ฝ่ายป้องกันที่สำคัญประการหนึ่งของระบอบประชาธิปไตยจะต้องเพิ่มความแข็งแกร่งให้กับการสื่อสารมวลชนแบบดั้งเดิมและสื่อเสรี โดยเฉพาะอย่างยิ่งในระดับท้องถิ่น ซึ่งจำเป็นต้องมีการลงทุนและนวัตกรรมอย่างต่อเนื่อง ซึ่งจะต้องสะท้อนถึงความต้องการในท้องถิ่นของประเทศและทวีปต่างๆ ปัญหาเหล่านี้ไม่ใช่เรื่องง่าย และจำเป็นต้องใช้แนวทางของผู้มีส่วนได้ส่วนเสียหลายฝ่าย ซึ่ง Microsoft และบริษัทด้านเทคโนโลยีอื่นๆ กำลังให้การสนับสนุนมากขึ้นเรื่อยๆ

นอกจากนี้ เรายังจำเป็นต้องมีนวัตกรรมใหม่ๆ ในนโยบายสาธารณะ ซึ่งจำเป็นต้องให้ความสำคัญกับสาธารณะเป็นอันดับแรก ซึ่งสามารถรวมถึงกฎหมายที่ช่วยให้ผู้เผยแพร่โฆษณาสามารถเจรจารายได้จากการโฆษณาโดยรวมร่วมกับบริษัทด้านเทคโนโลยีและกฎหมายที่ให้เครดิตภาษีเพื่อบรรเทาข้อมูลภายในท้องถิ่นของภาษีเงินเดือนของพวกเขาสำหรับนักข่าวที่พวกเขาใช้งาน นักข่าวต้องการเครื่องมืออื่นๆ อีกมากมายสำหรับงานฝีมือของพวกเขา รวมถึงความสามารถในการแยกเนื้อหาที่ถูกต้องตามกฎหมายออกจากแหล่งที่มาที่ฉ้อฉล

นอกจากนี้ยังมีความต้องการที่เพิ่มขึ้นอย่างรวดเร็วในการช่วยให้ผู้บริโภคพัฒนาความสามารถที่มีความซับซ้อนมากขึ้นในการระบุการดำเนินการด้านข้อมูลของประเทศที่ขับเคลื่อนโดยรัฐ แม้อาจดูเหมือนว่ายุ่งยาก แต่ก็มีลักษณะคล้ายกับงานที่ภาคเทคโนโลยีดำเนินการมาอย่างยาวนานเพื่อต่อสู้กับภัยคุกคามทางไซเบอร์อื่นๆ ลองพิจารณาการศึกษาของผู้บริโภคในการดูที่อยู่อีเมลอย่างรอบคอบมากขึ้น เพื่อช่วยตรวจจับสแปมหรือการสื่อสารที่ฉ้อฉลอื่นๆ โครงการริเริ่มในสหรัฐอเมริกา เช่น โครงการ News Literacy และ Trusted Journalism

ภัยคุกคามระยะยาวและร้ายกาจกว่าคือการทำความเข้าใจว่าอะไรคือความจริง ถ้าเราไม่สามารถไว้วางใจในสิ่งที่เราเห็นและได้ยินได้อีกต่อไป

แนวทางแบบองค์รวมเพื่อป้องกันการปฏิบัติการด้านอิทธิพลทางไซเบอร์

ต่อไป

โปรแกรม กำลังช่วยพัฒนาให้ผู้บริโภคได้รับข่าวสารและข้อมูลที่ดียิ่งขึ้น เทคโนโลยีใหม่ทั่วโลก เช่น ปลั๊กอินของเบราว์เซอร์จาก NewsGuard สามารถช่วยให้ความพยายามนี้ก้าวหน้าเร็วขึ้นมาก

สิ่งนี้ควรเตือนเราว่าส่วนหนึ่งของรากฐานสำหรับประชาธิปไตยคือการศึกษาในหน้าที่พลเมือง เช่นเคย ความพยายามนี้จำเป็นต้องเริ่มต้นในโรงเรียน แต่เราอยู่ในโลกที่เราต้องได้รับการศึกษาด้านพลเมืองอย่างต่อเนื่องตลอดชีวิตของเรา คำปฏิญาณ The new Civics at Work นำโดย Center for Strategic and International Studies ซึ่ง Microsoft เป็นผู้ลงนามและพันธมิตรในครั้งแรก พยายามที่จะส่งเสริมความรู้ด้านพลเมืองภายในชุมชนองค์กร เป็นตัวอย่างที่ดีของโอกาสในการเสริมสร้างการป้องกันประชาธิปไตยของเรา

ทำลาย

ในช่วงไม่กี่ปีที่ผ่านมา หน่วยงานอาชญากรรมดิจิตอลของ Microsoft (dcu) ได้มีการปรับกลยุทธ์และเครื่องมือที่พัฒนาขึ้นเพื่อทำลายภัยคุกคามทางไซเบอร์ตั้งแต่แรนซัมแวร์ไปจนถึงการทำงานของบอทเน็ตและการโจมตีของรัฐ เราได้เรียนรู้บทเรียนที่สำคัญมากมาย โดยเริ่มต้นจากบทบาทของการหยุดชะงักในการทำงานในวงกว้างของการโจมตีทางไซเบอร์ที่หลากหลาย

ในขณะที่เราคิดเกี่ยวกับการรับมือกับการปฏิบัติการด้านอิทธิพลทางไซเบอร์ การหยุดชะงักอาจมีบทบาทที่สำคัญมากยิ่งขึ้นและแนวทางที่ดีที่สุดในการหยุดชะงักก็ชัดเจนขึ้น ยาแก้พิษที่มีประสิทธิภาพที่สุดของการหลอกลวงในวงกว้างคือความโปร่งใส นั่นคือเหตุผลที่ Microsoft เพิ่มขีดความสามารถในการตรวจหาและทำลายการดำเนินงานของรัฐที่มีอิทธิพลโดยการซื้อกิจการ Miburo Solutions ซึ่งเป็นบริษัทวิเคราะห์และวิจัยภัยคุกคามทางไซเบอร์ชั้นนำที่เชี่ยวชาญในการตรวจหาและตอบสนองต่อการปฏิบัติการด้านอิทธิพลทางไซเบอร์ต่างประเทศ

ประสบการณ์ของเราแสดงให้เห็นว่ารัฐบาล บริษัทเทคโนโลยี และองค์กรพัฒนาเอกชนควรระบุถึงการโจมตีทางไซเบอร์อย่างระมัดระวังและมีหลักฐานเพียงพอ การทำความเข้าใจผลกระทบของการหยุดชะงักดังกล่าวมีความสำคัญและอาจมีประโยชน์มากในการขัดขวางอิทธิพลทางไซเบอร์ ร่วมเป็นสักขีพยานในการแบ่งปันข้อมูลของรัฐบาลสหรัฐฯ ในการนำไปสู่การรุกรานยูเครนของรัสเซีย ซึ่งทำให้เกิดความโปร่งใสในการดำเนินการที่มีประสิทธิภาพ เช่น การเปิดโปงแผนการของรัสเซีย รวมถึงการรณรงค์บางอย่าง เช่น การวางแผนที่จะใช้วิดีโอปลอม

ดังที่แสดงในเอกสารเผยแพร่เมื่อฤดูร้อนปีที่แล้วจากสถาบัน CyberPeace ในเจนีวาเกี่ยวกับการโจมตีทางไซเบอร์อย่างต่อเนื่องทั้งในและนอกยูเครน มีโอกาสสำหรับภาคประชาสังคมและองค์กรภาคเอกชนในวงกว้างในการพัฒนาความโปร่งใสที่เกี่ยวข้องการปฏิบัติการด้านอิทธิพลทางไซเบอร์ รายงานที่เชื่อถือได้เกี่ยวกับการดำเนินการที่เพิ่งค้นพบและมีเอกสารครบถ้วนสามารถช่วยให้สาธารณชนประเมินสิ่งที่อ่าน ดู และได้ยินได้ดีขึ้น โดยเฉพาะอย่างยิ่งบนอินเทอร์เน็ต เพื่อจุดประสงค์นี้ Microsoft จะสร้างและขยายการรายงานทางไซเบอร์ที่มีอยู่ และจะเผยแพร่รายงาน ข้อมูล และการอัปเดตใหม่ๆ ที่เกี่ยวข้องกับสิ่งที่เราค้นพบเกี่ยวกับการปฏิบัติการด้านอิทธิพลทางไซเบอร์ รวมถึงข้อความแสดงที่มาตามความเหมาะสม เราจะเผยแพร่รายงานประจำปีที่ใช้แนวทางที่ขับเคลื่อนด้วยข้อมูลเพื่อตรวจดูความแพร่หลายของการดำเนินการด้านข้อมูลต่างประเทศทั่วทั้งบริษัทและขั้นตอนต่อไปเพื่อให้แน่ใจว่ามีการปรับปรุงที่เพิ่มขึ้น นอกจากนี้ เราจะพิจารณาขั้นตอนเพิ่มเติมที่สร้างจากความโปร่งใสในทำนองนี้

ตัวอย่างเช่น บทบาทของการโฆษณาดิจิทัลมีความสำคัญเป็นพิเศษ เนื่องจากการโฆษณาสามารถช่วยสนับสนุนเงินทุนในการดำเนินงานในต่างประเทศ ในขณะเดียวกันก็สร้างภาพลักษณ์ที่ถูกต้องตามกฎหมายสำหรับไซต์โฆษณาชวนเชื่อที่ได้รับการสนับสนุนจากต่างชาติ จำเป็นต้องมีความพยายามใหม่เพื่อขัดขวางกระแสการเงินเหล่านี้

ขัดขวาง

ประการสุดท้าย เราไม่สามารถคาดหวังให้ประเทศต่างๆ เปลี่ยนพฤติกรรมได้ หากไม่ต้องมีความรับผิดชอบใดๆ ต่อการละเมิดกฎระหว่างประเทศ การบังคับใช้ความรับผิดชอบดังกล่าวเป็นความรับผิดชอบของรัฐบาลโดยเฉพาะ แต่การกระทำของผู้มีส่วนได้ส่วนเสียหลายกลุ่มกำลังมีบทบาทสำคัญในการเสริมสร้างและขยายบรรทัดฐานระหว่างประเทศ แพลตฟอร์มออนไลน์ ผู้ลงโฆษณา และผู้เผยแพร่มากกว่า 30 ราย รวมถึง Microsoft ได้ลงนามในแนวทางปฏิบัติเกี่ยวกับการบิดเบือนข้อมูลของคณะกรรมาธิการยุโรปที่เพิ่งได้รับการปรับปรุงเมื่อเร็วๆ นี้ โดยตกลงที่จะเพิ่มความมุ่งมั่นเพื่อรับมือกับความท้าทายที่เพิ่มขึ้นนี้ เช่นเดียวกับ Paris Call Christchurch Call และ Declaration on the Future of the Internet การดำเนินการแบบพหุภาคีและผู้มีส่วนได้ส่วนเสียหลายฝ่ายสามารถรวบรวมรัฐบาลและประชาชนในหมู่ประเทศประชาธิปไตยได้ จากนั้นรัฐบาลสามารถสร้างบรรทัดฐานและกฎหมายเหล่านี้เพื่อพัฒนาความรับผิดชอบที่ประชาธิปไตยของโลกต้องการและสมควรได้รับ

ด้วยความโปร่งใสที่รุนแรงรวดเร็ว รัฐบาลและสังคมประชาธิปไตยสามารถทำให้แคมเปญที่มีอิทธิพลอ่อนลงได้อย่างมีประสิทธิภาพโดยระบุแหล่งที่มาของการโจมตีรัฐชาติ แจ้งประชาชน และสร้างความไว้วางใจในสถาบันต่างๆ

> เราได้เพิ่มขีดความสามารถทางเทคนิคในการตรวจหาและขัดขวางการปฏิบัติการด้านอิทธิพลต่างประเทศ และมุ่งมั่นที่จะรายงานการดำเนินการเหล่านี้อย่างโปร่งใส เช่น การรายงานของเราเกี่ยวกับการโจมตีทางไซเบอร์

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ใช้แนวทางปฏิบัติด้านสุขอนามัยดิจิทัลที่เข้มงวดทั่วทั้งองค์กรของคุณ
2. พิจารณาถึงวิธีลดการเปิดใช้แคมเปญด้านอิทธิพลทางไซเบอร์โดยไม่ได้ตั้งใจโดยพนักงานหรือการดำเนินธุรกิจของคุณ ซึ่งรวมถึงการลดอุปทานไปยังเว็บไซต์โฆษณาชวนเชื่อในต่างประเทศที่เป็นที่รู้จัก
3. สนับสนุนการรู้เท่าทันข้อมูลและแคมเปญการมีส่วนร่วมของพลเมืองเป็นองค์ประกอบหลักในการช่วยสังคมป้องกันการโฆษณาชวนเชื่อและอิทธิพลจากต่างประเทศ
4. มีส่วนร่วมโดยตรงกับกลุ่มที่เกี่ยวข้องกับอุตสาหกรรมของคุณที่ทำงานเพื่อจัดการกับการปฏิบัติการด้านอิทธิพล

อ้างอิงท้ายเอกสาร

1. https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections?msclkid=8dc75d6abcfe11ecad9946a058d581c9
2. https://news.gallup.com/poll/355526/americans-trust-media-dips-second-lowest-record.aspx
3. การปกป้องยูเครน: บทเรียนแรกจากสงครามไซเบอร์ (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. โฆษกกระทรวงต่างประเทศของรัสเซีย มาเรีย ซาคาโรวา: https://tass.com/politics/1401777; Lavrov: https://www.cnn.com/2022/05/05/opinions/sergey-lavrov-hitler-comments-ukraine-kauders/index.html,Kirill Kudryavtsev/Pool/AFP/Getty Images
6. https://apnews.com/article/conspiracy-theories-iran-only-on-ap-media-misinformation-bfca6d5b236a29d61c4dd38702495ffe
7. https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib
8. https://www.presstv.ir/Detail/2020/02/04/617877/Is-the-coronavirus-a-US-bioweapon
9. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf
10. https://www.rt.com/news/482405-iran-coronavirus-us-biological-weapon/
11. https://web.archive.org/web/20220319124125/https://twitter.com/RT_com/status/1233187558793924608?s=20
12. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
13. คำกล่าวอ้างของเครเมนชุกของรัสเซียกับหลักฐาน— bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. การตรวจสอบข้อเท็จจริง: "เมา" วิดีโอ Nancy Pelosi ถูกจัดการ | Reuters
17. https://lawcat.berkeley.edu/record/1136469
18. https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237
19. ผลลัพธ์ของ Deepfake Detection Challenge: ความคิดริเริ่มที่เปิดกว้างเพื่อพัฒนา AI (facebook.com)
20. การปลอมแปลงเชิงลึก 2020 จุดพลิกผัน Johannes Tammekänd John Thomas และ Kristjan Peterson ตุลาคม 2020

ความยืดหยุ่นทางไซเบอร์

การทำความเข้าใจความเสี่ยงและผลตอบแทนของการปรับปรุงให้ทันสมัยมีความสำคัญต่อแนวทางแบบองค์รวมเพื่อความยืดหยุ่น

ข้อมูลเบื้องต้น 88

ความยืดหยุ่นทางไซเบอร์: รากฐานที่สำคัญของสังคมที่มีการเชื่อมต่อ 89

ความสำคัญของการปรับปรุงระบบและสถาปัตยกรรมให้ทันสมัย 90

ท่าทางการรักษาความปลอดภัยขั้นพื้นฐานเป็นปัจจัยกำหนดประสิทธิภาพของโซลูชันขั้นสูง 92

การรักษาสุขภาพของเอกลักษณ์เป็นพื้นฐานของความเป็นอยู่ที่ดีขององค์กร 93

การตั้งค่าความปลอดภัยเริ่มต้นของระบบปฏิบัติการ 96

ศูนย์กลางห่วงโซ่อุปทานของซอฟต์แวร์ 97

การสร้างความยืดหยุ่นต่อการโจมตี DDoS, เว็บแอปพลิเคชันและเครือข่ายที่เกิดขึ้นใหม่ 98

การพัฒนาแนวทางที่สมดุลในการรักษาความปลอดภัยข้อมูลและความยืดหยุ่นทางไซเบอร์ 101

ความยืดหยุ่นต่อปฏิบัติการมีอิทธิพลทางไซเบอร์: มิติของมนุษย์ 102

การเสริมสร้างปัจจัยมนุษย์ด้วยทักษะ 103

ข้อมูลเชิงลึกจากโปรแกรมกำจัดแรนซัมแวร์ของเรา 104

ดำเนินการในขณะนี้เกี่ยวกับผลกระทบด้านความปลอดภัยควอนตัม 105

การผสานรวมธุรกิจ ความปลอดภัย และ IT เพื่อความยืดหยุ่นที่มากขึ้น 106

เส้นโค้งความยืดหยุ่นทางไซเบอร์ 108

ทีมงานที่มีส่วนร่วม 111

ภาพรวมของ

ความยืดหยุ่นทางไซเบอร์

การรักษาความปลอดภัยเป็นกุญแจสำคัญของความสำเร็จทางเทคโนโลยี นวัตกรรมและประสิทธิภาพที่เพิ่มขึ้นสามารถทำได้โดยการนำมาตรการรักษาความปลอดภัยที่ทำให้องค์กรมีความยืดหยุ่นมากที่สุดเท่าที่จะเป็นไปได้จากการโจมตีสมัยใหม่

โรคระบาดได้มีการท้าทายให้เราเปลี่ยนหลักปฏิบัติและเทคโนโลยีด้านความปลอดภัยเพื่อปกป้องพนักงานของ Microsoft ในทุกที่ที่พวกเขาทำงาน ในปีที่ผ่านมา ผู้ก่อภัยคุกคามยังคงใช้ประโยชน์จากช่องโหว่ที่เปิดเผยระหว่างการแพร่ระบาดและการเปลี่ยนไปใช้สภาพแวดล้อมการทำงานแบบผสมผสาน ตั้งแต่นั้นมา ความท้าทายหลักของเราคือการจัดการความแพร่หลายและความซับซ้อนของวิธีการโจมตีต่างๆ และกิจกรรมของรัฐชาติที่เพิ่มขึ้น

ความยืดหยุ่นทางไซเบอร์ที่มีประสิทธิภาพนั้นต้องการวิธีการแบบองค์รวมและปรับเปลี่ยนได้ เพื่อต้านทานภัยคุกคามที่พัฒนาต่อบริการหลักและโครงสร้างพื้นฐาน

ค้นหาข้อมูลเพิ่มเติมหน้า 89

ระบบและสถาปัตยกรรมที่ทันสมัยมีความสำคัญต่อการจัดการภัยคุกคามในโลกที่เชื่อมต่อถึงกัน

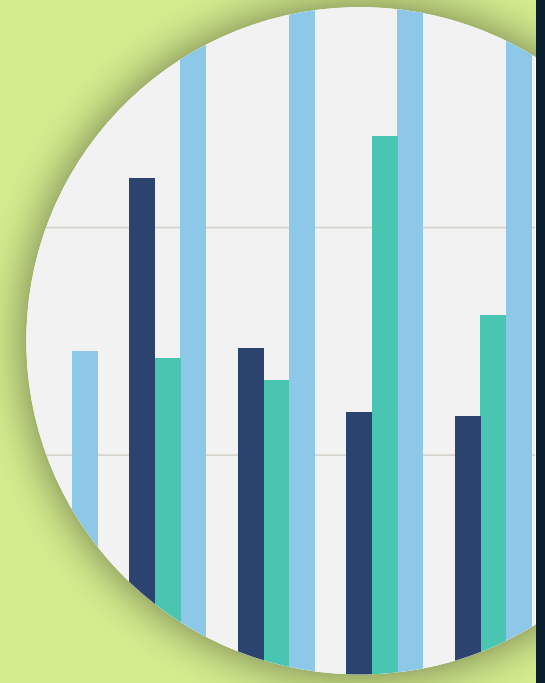


ค้นหาข้อมูลเพิ่มเติมหน้า 90

ท่าทางการรักษาความปลอดภัยขั้นพื้นฐานเป็นปัจจัยกำหนดประสิทธิภาพของโซลูชันขั้นสูง

ค้นหาข้อมูลเพิ่มเติมหน้า 92

แม้ว่าการโจมตีด้วยรหัสผ่านยังคงเป็นแหล่งที่มาหลักของการถูกบุกรุกข้อมูลประจำตัว แต่การโจมตีประเภทอื่นๆ ก็กำลังเกิดขึ้น



ค้นหาข้อมูลเพิ่มเติมหน้า 93

มิติของมนุษย์ในความยืดหยุ่นต่อการปฏิบัติการด้านอิทธิพลทางไซเบอร์คือความสามารถของเราในการทำงานร่วมกันและให้ความร่วมมือ

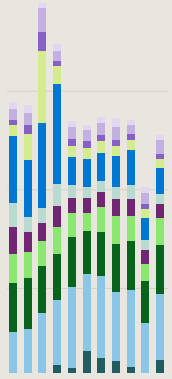
ค้นหาข้อมูลเพิ่มเติมหน้า 102

การโจมตีทางไซเบอร์ที่ประสบความสำเร็จส่วนใหญ่สามารถป้องกันได้โดยใช้ความปลอดภัยขั้นพื้นฐาน

ค้นหาข้อมูลเพิ่มเติมหน้า 108



ในช่วงปีที่ผ่านมา โลกประสบกับกิจกรรมของ DDoS ที่มีปริมาณ ความซับซ้อน และความถี่อย่างไม่เคยปรากฏมาก่อน



ค้นหาข้อมูลเพิ่มเติมหน้า 98

ข้อมูลเบื้องต้น

โรคระบาดได้ท้าทายให้เราเปลี่ยนหลักปฏิบัติและเทคโนโลยีด้านความปลอดภัยเพื่อปกป้องพนักงานของ Microsoft ในทุกที่ที่พวกเขาทำงาน ในปีที่ผ่านมา ผู้ก่อภัยคุกคามยังคงใช้ประโยชน์จากช่องโหว่ที่เปิดเผยระหว่างการแพร่ระบาดและการเปลี่ยนไปใช้สภาพแวดล้อมการทำงานแบบผสมผสาน ตั้งแต่นั้นมา ความท้าทายหลักของเราคือการจัดการความแพร่หลายและความซับซ้อนของวิธีการโจมตีต่างๆ และกิจกรรมของรัฐชาติที่เพิ่มขึ้น

กิจกรรมการคุกคามทางดิจิทัลและระดับความซับซ้อนของการโจมตีทางไซเบอร์สูงเป็นประวัติการณ์ การโจมตีที่ซับซ้อนจำนวนมากในปัจจุบันมุ่งเน้นไปที่การลดทอนประสิทธิภาพถาปัตยกรรมของข้อมูลประจำตัว ห่วงโซ่อุปทาน และบุคคลที่สามที่มีระดับการควบคุมความปลอดภัยที่แตกต่างกัน โดยเฉพาะอย่างยิ่ง เรามีการตรวจพบการโจมตีแบบฟิชชิงข้อมูลประจำตัวเป็นภัยคุกคามที่ชัดเจนและเป็นปัจจุบัน อย่างไรก็ตาม การโจมตีประเภทนี้มักไม่ประสบความสำเร็จ หากมีการจัดการข้อมูลประจำตัวที่ดี การควบคุมฟิชชิง และการจัดการปลายทาง ด้วยเหตุนี้ เราต้องจำข้อมูลพื้นฐาน: เก้าสิบแปดเปอร์เซ็นต์ของการโจมตีสามารถหยุดได้ด้วยมาตรการด้านสุขอนามัยขั้นพื้นฐาน ที่ Microsoft เราจะจัดการข้อมูลประจำตัวและอุปกรณ์โดยเป็นส่วนหนึ่งของแนวทาง Zero Trust ของเรา ซึ่งรวมถึงการเข้าถึงที่มีสิทธิ์น้อยที่สุดและข้อมูลประจำตัวที่มีความสามารถในการป้องกันฟิชชิง เพื่อหยุดผู้ก่อภัยคุกคามอย่างมีประสิทธิภาพและป้องกันข้อมูลของเรา

ปัจจุบัน แม้แต่ผู้ก่อภัยคุกคามที่ไม่มีทักษะด้านเทคนิคที่ซับซ้อนก็สามารถเปิดใช้การโจมตีที่ทำลายล้างได้อย่างไม่น่าเชื่อ เนื่องจากการเข้าถึงกลยุทธ์ขั้นสูง เทคนิค และกระบวนการต่างๆ มีอยู่อย่างกว้างขวางในเศรษฐกิจของอาชญากรรมไซเบอร์ สงครามในยูเครนแสดงให้เห็นว่าผู้ดำเนินการในระดับชาติได้เลื่อนระดับการดำเนินการทางไซเบอร์ที่ไม่เหมาะสมของตนผ่านการใช้แรนซัมแวร์ที่เพิ่มขึ้นได้อย่างไร ขณะนี้แรนซัมแวร์เป็นอุตสาหกรรมที่มีความซับซ้อน โดยมีผู้ก่อภัยคุกคามที่ใช้กลยุทธ์ขู่กรรโชกสองหรือสามครั้งเพื่อแยกการจ่ายเงินออกและนักพัฒนาเสนอแรนซัมแวร์เป็นบริการ (RaaS) ด้วย RaaS ผู้ก่อภัยคุกคามใช้เครือข่ายพันธมิตรเพื่อดำเนินการโจมตี ลดอุปสรรคในการเข้าถึงของอาชญากรไซเบอร์ที่มีทักษะน้อยกว่า และขยายกลุ่มผู้โจมตีในท้ายที่สุด

ด้วยเหตุนี้ Microsoft จึงออกแบบโปรแกรมกำจัดแรนซัมแวร์ เป้าหมายของโปรแกรมคือการแก้ไขปัญหาช่องว่างในการควบคุมและความครอบคลุม ช่วยในการปรับปรุงคุณสมบัติสำหรับบริการ และพัฒนาคู่มือการกู้คืนสำหรับศูนย์ปฏิบัติการด้านความปลอดภัยและทีมวิศวกรรมของเราในกรณีที่มีการโจมตีด้วยแรนซัมแวร์ ห่วงโซ่อุปทานล่าสุดและการโจมตีซัพพลายเออร์บุคคลที่สามแสดงให้เห็นถึงจุดการเปลี่ยนแปลงที่สำคัญในอุตสาหกรรม การหยุดชะงักของการโจมตีเหล่านี้ทำให้ลูกค้า คู่ค้า รัฐบาล และ Microsoft แสดงให้เห็นถึงความสำคัญของการให้ความสนใจที่มุ่งเน้นไปที่ความยืดหยุ่นทางไซเบอร์และการทำงานร่วมกันระหว่างผู้มีส่วนได้ส่วนเสียด้านความปลอดภัย เพิ่มขึ้นอย่างต่อเนื่อง นอกจากนี้ ฝ่ายตรงข้ามยังกำหนดเป้าหมายไปที่ระบบภายในองค์กร ตอกย้ำความจำเป็นที่องค์กรต้องจัดการช่องโหว่ที่เกิดจากระบบเดิมโดยการปรับปรุงให้ทันสมัยและย้ายโครงสร้างพื้นฐานไปยังระบบคลาวด์ที่ซึ่งการรักษาความปลอดภัยมีความแข็งแกร่งมากขึ้น

เราอยู่ในยุคที่การรักษาความปลอดภัยเป็นปัจจัยสำคัญของความสำเร็จทางเทคโนโลยี นวัตกรรมและประสิทธิภาพที่เพิ่มขึ้นสามารถทำได้โดยการนำมาตรการรักษาความปลอดภัยที่ทำให้องค์กรมีความยืดหยุ่นมากที่สุดเท่าที่จะเป็นไปได้จากการโจมตีสมัยใหม่ เมื่อภัยคุกคามทางดิจิทัลเพิ่มขึ้นและพัฒนาขึ้น สิ่งสำคัญคือต้องสร้างความยืดหยุ่นทางไซเบอร์ให้กับโครงสร้างของทุกองค์กร

เบรต อาร์เซนอลต์
ประธานด้านความปลอดภัยสารสนเทศ

ความยืดหยุ่นทางไซเบอร์: รากฐานที่สำคัญของสังคมที่มีการเชื่อมต่อ

การปฏิวัติเทคโนโลยีดิจิทัลได้เห็นว่าองค์กรเปลี่ยนแปลงไปเพื่อเชื่อมโยงกันมากขึ้นทั้งในด้านวิธีการทำงานและบริการที่ตนนำเสนอ เมื่อภัยคุกคามในโลกไซเบอร์เพิ่มมากขึ้น การสร้างความยืดหยุ่นทางไซเบอร์ในโครงสร้างขององค์กรจึงมีความสำคัญพอๆ กับความยืดหยุ่นทางการเงินและการดำเนินงาน

การเปลี่ยนแปลงด้านดิจิทัลได้เปลี่ยนแปลงวิธีที่องค์กรโต้ตอบกับลูกค้า คู่ค้า พนักงาน และผู้มีส่วนได้ส่วนเสียอื่นๆ ไปตลอดกาล เทคโนโลยีใหม่ๆ มอบโอกาสมหาศาลในการมีส่วนร่วมกับผู้คน เปลี่ยนแปลงผลิตภัณฑ์ และเพิ่มประสิทธิภาพการดำเนินงาน การระบาดเร่งการเปลี่ยนแปลงทางดิจิทัลโดยขับเคลื่อนเทคโนโลยีที่เป็นนวัตกรรมซึ่งช่วยให้ผู้คนทำงานร่วมกันในรูปแบบใหม่และจากทุกที่

เมื่อภัยคุกคามทางไซเบอร์กลายเป็นโรคเฉพาะถิ่น การป้องกันไม่ให้ส่งกระทบต่อประสิทธิภาพองค์กรกลายเป็นเรื่องยากขึ้นในโลกที่ “เชื่อมต่อกันตลอดเวลา” ของเรา ความยืดหยุ่นทางไซเบอร์แสดงถึงความสามารถขององค์กรในการดำเนินการต่อและคงไว้ซึ่งอัตราการเร่งการเติบโตแม้จะมีการโจมตีมากมาย การป้องกันต้องสมดุลกับความสามารถในการอยู่รอดและการกู้คืน รวมถึงรัฐบาลและองค์กรต่างๆ กำลังพัฒนาโมเดลที่ครอบคลุมซึ่งขยายออกไปนอกเหนือไปจากความปลอดภัยและความเป็นส่วนตัว เพื่อปกป้องทรัพย์สิน ข้อมูล และทรัพยากรอื่นๆ ซึ่งเป็นส่วนหนึ่งของความยืดหยุ่นในโลกไซเบอร์

การพัฒนาวิธีการแบบองค์รวมสำหรับความยืดหยุ่นในโลกไซเบอร์

ความยืดหยุ่นทางไซเบอร์ต้องใช้แนวทางแบบองค์รวม ปรับเปลี่ยนได้ และเป็นสากลที่ สามารถต้านทานภัยคุกคามที่พัฒนาต่อบริการหลักและโครงสร้างพื้นฐาน ซึ่งรวมถึง:

- ด้านสุขอนามัยไซเบอร์พื้นฐานตามที่อธิบายไว้ในเส้นโค้งความยืดหยุ่นทางไซเบอร์
- ทำความเข้าใจและจัดการการแลกเปลี่ยนความเสี่ยง/ผลตอบแทนของการเปลี่ยนแปลงทางดิจิทัล
- ความสามารถในการตอบสนองแบบเรียลไทม์ซึ่งเปิดใช้งานการตรวจหาภัยคุกคามและช่องโหว่แบบเชิงรุก
- การป้องกันการโจมตีและกิจกรรมเชิงป้องกันที่รู้จักกับเวกเตอร์การโจมตีใหม่และที่คาดไว้ ซึ่งรวมถึงความสามารถในการแก้ไขปัญหาโดยอัตโนมัติ
- ลดผลกระทบของการโจมตีและภัยพิบัติผ่านการแยกข้อบกพร่องและการแบ่ง
- การกู้คืนอัตโนมัติ และการสำรองข้อมูลในกรณีที่เกิดการหยุดชะงัก
- จัดลำดับความสำคัญของการทดสอบการดำเนินงานเพื่อค้นหาช่องว่างและทำความเข้าใจความรับผิดชอบที่ใช้ร่วมกันและการพึ่งพาทรัพยากรภายนอก เช่น โซลูชันการรักษาความปลอดภัยบนระบบคลาวด์

โปรแกรมความยืดหยุ่นทางไซเบอร์ที่มีประสิทธิภาพเริ่มต้นด้วยพื้นฐานของทรัพยากร เช่น การทำความเข้าใจกับบริการที่มีอยู่และการมีแคตตาล็อกทรัพยากรที่เชื่อถือได้ซึ่งสามารถเรียกใช้ได้ในกรณีที่เกิดการหยุดชะงัก จากพื้นฐานดังกล่าว โปรแกรมจะต้องสามารถประเมินประสิทธิภาพของตนเอง วัดประสิทธิภาพของบริการที่สำคัญและการพึ่งพา ทดสอบและตรวจสอบความสามารถทั่วทั้งองค์กรและบริการคลาวด์ และป้อนการปรับปรุงอย่างต่อเนื่องตลอดวงจรชีวิตดิจิทัลขององค์กร เพื่อนำเสนอวิธีการแบบองค์รวม เรากำลังร่วมมือกับองค์กรต่างๆ เพื่อระบุบริการภายในองค์กรและบริการออนไลน์ที่สำคัญที่สุด กระบวนการทางธุรกิจ การพึ่งพา บุคลากร ผู้ขาย และซัพพลายเออร์ นอกจากนี้ เรายังมองหาสินทรัพย์และทรัพยากรที่เกี่ยวข้องกับความคาดหวังของลูกค้าและตลาด ข้อบังคับและข้อผูกมัดตามสัญญา และการดำเนินงานภายใน เมื่อมีการระบุทรัพยากรที่สำคัญเหล่านี้แล้ว ความพยายามแบบคู่ขนานควรตรวจหาและติดตามภัยคุกคาม การหยุดชะงัก โอกาสโจมตีที่อาจเกิดขึ้น และระบบและกระบวนการที่มีช่องโหว่ ความสามารถในการทำเช่นนี้ภายใต้การขาดแคลนทักษะปัจจุบันจำเป็นต้องมีการจัดลำดับความสำคัญอย่างเข้มงวดโดยพิจารณาจากความเสี่ยงโดยรวมที่เกิดกับองค์กร

วิธีการแบบองค์รวมแบบองค์รวมประเภทนี้จำเป็นต้องปรับเปลี่ยนให้เข้ากับฉากหลังของภูมิทัศน์ภัยคุกคามที่มีการพัฒนาอย่างต่อเนื่องโดยมีเป้าหมายในการขับเคลื่อนการปรับปรุงประสิทธิภาพที่วัดได้ ลดเวลาในการตรวจหา การตอบสนองและการกู้คืน และลดรัศมีของผลกระทบในกรณีที่เกิดการหยุดชะงัก วิธีการยังต้องตระหนักถึงความเชื่อมโยงที่เพิ่มขึ้นของภัยคุกคาม ตัวอย่างเช่น เหตุการณ์ด้านความปลอดภัยอาจส่งผลให้เกิดการละเมิดข้อมูลที่มีผลกระทบด้านความเป็นส่วนตัวซึ่งต้องใช้ทีมงานภายในและภายนอกจำนวนมากเพื่อทำงานร่วมกันเพื่อตอบสนองได้อย่างรวดเร็วและลดผลกระทบ

> ความยืดหยุ่นในโลกไซเบอร์คือความสามารถขององค์กรในการดำเนินงานต่อไปและรักษาความเร่งการเติบโตอย่างไม่หยุดชะงัก ซึ่งรวมถึงการโจมตีทางไซเบอร์

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. สร้างและจัดการระบบเทคโนโลยีที่จำกัดผลกระทบของการละเมิดและช่วยให้ดำเนินการต่อได้อย่างปลอดภัยและมีประสิทธิภาพ แม้ว่าการละเมิดจะประสบความสำเร็จ มุ่งเน้นไปที่สินทรัพย์ที่สำคัญทั่วไป การสนับสนุนความคล่องตัว และการออกแบบเพื่อความสามารถในการปรับตัว (ตัวอย่างเช่น ไฮบริดและมัลติคลาวด์ หลายแพลตฟอร์ม) ลดพื้นผิวการโจมตี (ตัวอย่างเช่น ลบแอปพลิเคชันที่ไม่ได้ใช้และสิทธิ์การเข้าถึงที่จัดสรรเกิน) ถือว่าทรัพยากรถูกบุกรุก และคาดหวังว่าศัตรูจะมีวิวัฒนาการ
2. เมื่อวางแผนโครงการดิจิทัล ให้พิจารณาภัยคุกคามที่อาจเกิดขึ้นควบคู่ไปกับโอกาสต่างๆ และความรับผิดชอบร่วมกันสำหรับการยืดหยุ่นทั่วทั้งซัพพลายเชนเทคโนโลยีดิจิทัล รวมถึงโซลูชันการรักษาความปลอดภัยบนคลาวด์
3. สร้างระบบเพื่อฝังความปลอดภัยด้วยการออกแบบและดำเนินการตามขั้นตอนต่างๆ เพื่อคาดการณ์ ตรวจสอบ ต้านทาน ปรับตัว และตอบสนองต่อภัยคุกคามที่พัฒนาในอนาคต
4. ตรวจสอบให้แน่ใจว่าผู้นำทางธุรกิจได้ปรึกษาทีมรักษาความปลอดภัยตามความจำเป็นเพื่อทำความเข้าใจความเสี่ยงที่เกี่ยวข้องกับการพัฒนาใหม่ๆ ในทำนองเดียวกัน ทีมรักษาความปลอดภัยควรพิจารณาจุดมุ่งหมายทางธุรกิจและแนะนำผู้นำเกี่ยวกับเกี่ยวกับวิธีการติดตามเป้าหมายอย่างปลอดภัย
5. ตรวจสอบให้แน่ใจว่ามีแนวทางปฏิบัติและขั้นตอนการปฏิบัติงานที่ชัดเจนสำหรับความยืดหยุ่นขององค์กรสำหรับเหตุการณ์ทางไซเบอร์

ความสำคัญของการปรับปรุงระบบและสถาปัตยกรรมให้ทันสมัย

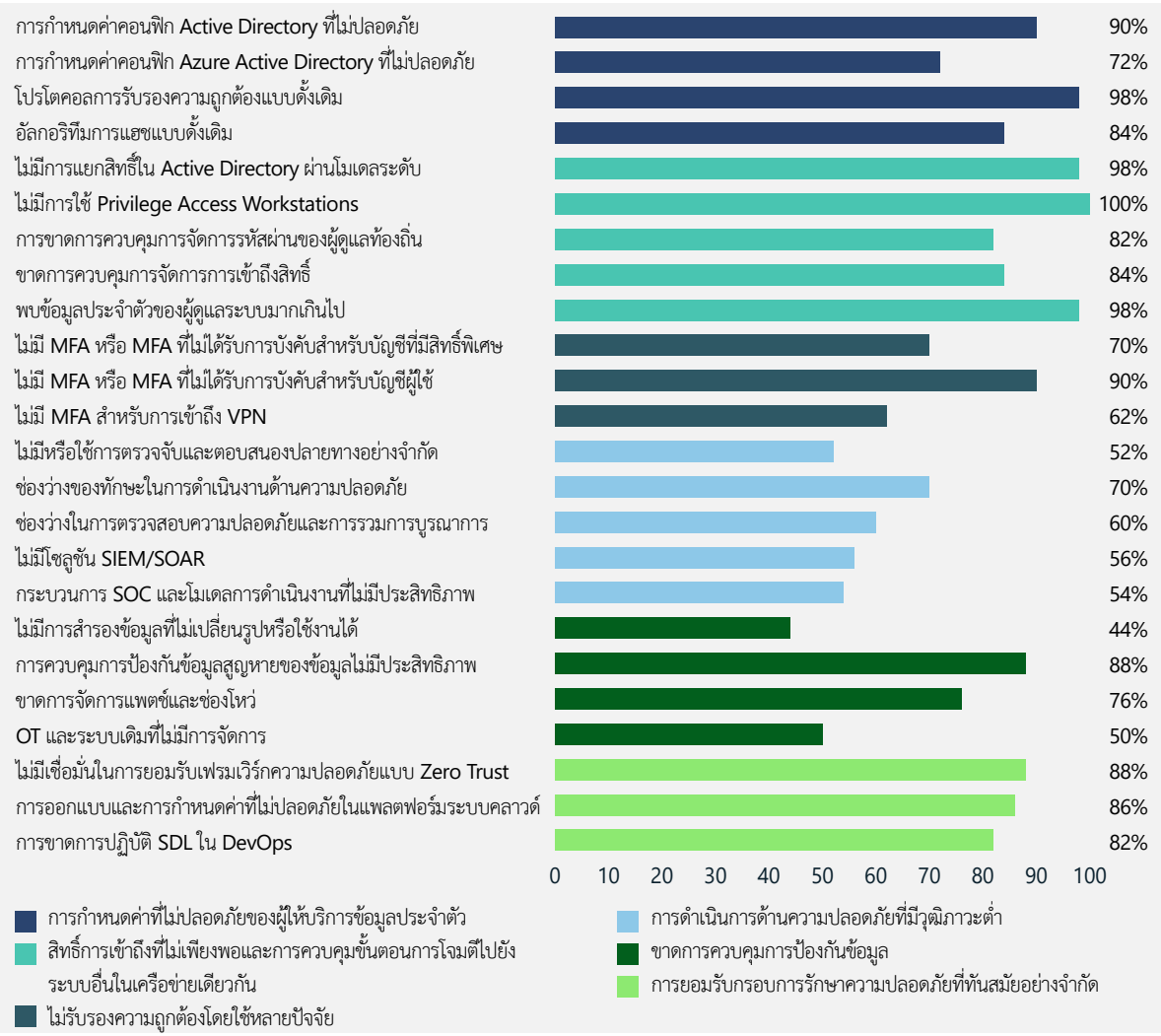
ในขณะที่เราพัฒนาความสามารถใหม่ๆ สำหรับโลกที่เชื่อมต่อกัน เราต้องจัดการภัยคุกคามที่เกิดจากระบบและซอฟต์แวร์รุ่นเก่า

ระบบรุ่นเก่า คือระบบที่พัฒนาขึ้นก่อนที่เครื่องมือการเชื่อมต่อสมัยใหม่ เช่น สมาร์ทโฟน แท็บเล็ต และบริการคลาวด์จะกลายเป็นบรรทัดฐาน ซึ่งแสดงถึงความเสี่ยงต่อองค์กรที่ยังคงใช้งานระบบเหล่านั้นอยู่ ความเสี่ยงนี้ได้รับการเน้นย้ำจากผลการศึกษาโดยทีม Microsoft Security Services for Incident Response ซึ่งเป็นกลุ่มผู้เชี่ยวชาญด้านความปลอดภัยที่ช่วยให้ลูกค้าตอบสนองและกู้คืนจากการโจมตี

ในช่วงปีที่ผ่านมา ปัญหาที่พบในลูกค้าที่กู้คืนจากการโจมตีนั้นเกี่ยวข้องกับหกหมวดหมู่ตามที่แสดงในแผนภูมิในหน้านี้ หน้าต่อไปนี้สรุปขั้นตอนที่สามารถดำเนินการได้เพื่อปรับปรุงความยืดหยุ่น

กว่า 80 เปอร์เซ็นต์ของเหตุการณ์ด้านความปลอดภัยสามารถติดตามไปยังองค์ประกอบบางอย่างที่ขาดหายไปซึ่งสามารถแก้ไขได้ด้วยแนวทางการรักษาความปลอดภัยที่ทันสมัย

ประเด็นสำคัญที่ส่งผลกระทบต่อความยืดหยุ่นทางไซเบอร์



แผนภูมินี้แสดงเปอร์เซ็นต์ของลูกค้าที่ได้รับผลกระทบซึ่งขาดการควบคุมความปลอดภัยขั้นพื้นฐาน ซึ่งมีความสำคัญต่อการเพิ่มความยืดหยุ่นทางไซเบอร์ขององค์กร ผลการวิจัยขึ้นอยู่กับการมีส่วนร่วมของ Microsoft ในช่วงปีที่ผ่านมา

"ผู้นำควรคิดถึงความยืดหยุ่นทางไซเบอร์เป็นแง่มุมที่สำคัญของความยืดหยุ่นทางธุรกิจ พวกเขาควรวางแผนสำหรับการหยุดชะงักทางไซเบอร์ในลักษณะเดียวกับที่เกิดภัยพิบัติทางธรรมชาติหรือเหตุการณ์ที่ไม่คาดฝันอื่นๆ และนำผู้มีส่วนได้ส่วนเสียภายในมารวมกัน เช่น การปฏิบัติการ การสื่อสาร กฎหมาย และอื่นๆ เพื่อกำหนดกลยุทธ์ การทำเช่นนี้จะช่วยให้องค์กรต่างๆ นำระบบธุรกิจที่สำคัญของตนกลับมาออนไลน์โดยเร็วที่สุดเท่าที่จะเป็นไปได้เพื่อกลับมาดำเนินธุรกิจตามปกติ

แต่นี่ไม่ใช่ทั้งหมด เนื่องจากหลายองค์กรพึ่งพาซัพพลายเออร์และผู้ให้บริการบุคคลที่สาม ผู้นำควรขยายการวางแผนความยืดหยุ่นทางไซเบอร์ไปยังห่วงโซ่คุณค่าแบบครบวงจร เพื่อให้แน่ใจว่าธุรกิจมีความต่อเนื่องและความยืดหยุ่น"

Ann Johnson,
รองประธานองค์กรด้านความปลอดภัย การปฏิบัติตามข้อกำหนด เอกลักษณ์ และการพัฒนาธุรกิจการจัดการ

ความสำคัญของการปรับปรุงระบบและสถาปัตยกรรมให้ทันสมัย

ต่อไป

มีหลายประเด็นที่ชัดเจนที่องค์กรสามารถแก้ไขได้เพื่อปรับปรุงวิธีการให้ทันสมัยและปกป้องจากภัยคุกคาม:

ปัญหา	ขั้นตอนที่ดำเนินการได้
การกำหนดค่าที่ไม่ปลอดภัยของผู้ให้บริการข้อมูลประจำตัว การกำหนดค่าที่ผิดพลาดและการเปิดเผยแพลตฟอร์มข้อมูลประจำตัวและส่วนประกอบต่างๆ เป็นเวกเตอร์ทั่วไปสำหรับการได้รับสิทธิ์การเข้าถึงระดับสูงโดยไม่ได้รับอนุญาต	ปฏิบัติตามพื้นฐานการกำหนดค่าความปลอดภัยและแนวทางปฏิบัติที่ดีที่สุดเมื่อปรับใช้และบำรุงรักษาระบบข้อมูลประจำตัว เช่น โครงสร้างพื้นฐาน AD และ Azure AD ใช้การจำกัดการเข้าถึงโดยบังคับใช้การแยกสิทธิ์ สิทธิ์การเข้าถึงขั้นต่ำ และการใช้สิทธิ์การเข้าถึงเวิร์กสเตชัน (PAW) สำหรับการจัดการระบบข้อมูลประจำตัว
สิทธิ์การเข้าถึงที่ไม่เพียงพอและการควบคุมขั้นตอนการโจมตีไปยังระบบอื่นในเครือข่ายเดียวกัน ผู้ดูแลระบบมีสิทธิ์มากเกินไปในสภาพแวดล้อมดิจิทัลและมักเปิดเผยข้อมูลประจำตัวของผู้ดูแลระบบบนเวิร์กสเตชันที่มีความเสี่ยงด้านอินเทอร์เน็ตและประสิทธิภาพการทำงาน	รักษาความปลอดภัยและจำกัดการเข้าถึงระดับผู้ดูแลระบบเพื่อทำให้สภาพแวดล้อมมีความยืดหยุ่นมากขึ้นและจำกัดขอบเขตของการโจมตี ใช้การควบคุมการจัดการการเข้าถึงสิทธิ์ เช่น การเข้าถึงแบบทันเวลา และการดูแลระบบแบบพอเพียง
ไม่รับรองความถูกต้องโดยใช้หลายปัจจัย (MFA) ผู้โจมตีในปัจจุบันไม่ได้เจาะระบบ แต่พวกเขาเข้าสู่ระบบ	MFA เป็นการควบคุมการเข้าถึงของผู้ใช้ที่สำคัญและเป็นพื้นฐานที่ทุกองค์กรควรเปิดใช้งานควบคู่กับการเข้าถึงแบบมีเงื่อนไข MFA มีประโยชน์อย่างมากในการต่อสู้กับภัยคุกคามทางไซเบอร์
การดำเนินการด้านความปลอดภัยที่มีวุฒิภาวะต่ำ องค์กรที่ได้รับผลกระทบส่วนใหญ่ใช้เครื่องมือตรวจจับภัยคุกคามแบบดั้งเดิมและไม่มีข้อมูลเชิงลึกที่เกี่ยวข้องสำหรับการตอบสนองและการแก้ไขอย่างทันท่วงที	กลยุทธ์การตรวจจับภัยคุกคามที่ครอบคลุมจำเป็นต้องมีการลงทุนในการตรวจจับและตอบสนองแบบขยาย (XDR) และเครื่องมือแบบเนทีฟบนคลาวด์สมัยใหม่ที่ใช้การเรียนรู้ของเครื่องเพื่อแยกสัญญาณรบกวนออกจากสัญญาณ ปรับปรุงเครื่องมือดำเนินการด้านความปลอดภัยให้ทันสมัยโดยผสมผสาน XDR ที่สามารถให้ข้อมูลเชิงลึกด้านความปลอดภัยเชิงลึกทั่วทั้งภูมิทัศน์ดิจิทัล
ขาดการควบคุมการป้องกันข้อมูล องค์กรต่างๆ ยังคงประสบปัญหาในการรวมเอาการควบคุมการป้องกันข้อมูลแบบองค์รวมที่ครอบคลุมทั่วทั้งตำแหน่งข้อมูลและยังคงมีประสิทธิภาพตลอดวงจรชีวิตของข้อมูลและสอดคล้องกับความสำคัญทางธุรกิจของข้อมูล	ระบุข้อมูลธุรกิจที่สำคัญของคุณและตำแหน่งที่ตั้ง ทบทวนกระบวนการวงจรชีวิตของข้อมูลและบังคับใช้การปกป้องข้อมูล ในขณะเดียวกันก็รับประกันความต่อเนื่องทางธุรกิจ
การยอมรับกรอบการรักษาความปลอดภัยที่ทันสมัยอย่างจำกัด ข้อมูลประจำตัวคือขอบเขตการรักษาความปลอดภัยใหม่ ทำให้สามารถเข้าถึงบริการดิจิทัลและสภาพแวดล้อมการประมวลผลที่แตกต่างกัน การผสานรวมหลักการ Zero trust ความปลอดภัยของโปรแกรมประยุกต์และเฟรมเวิร์กทางไซเบอร์สมัยใหม่อื่นๆ ช่วยให้องค์กรสามารถจัดการความเสี่ยงในเชิงรุก ซึ่งมิฉะนั้นองค์กรอาจประสบปัญหาในการมองเห็น	กรอบงาน Zero Trust บังคับใช้แนวคิดของสิทธิ์ขั้นต่ำ การตรวจสอบการเข้าถึงทั้งหมดอย่างชัดเจน และถือว่ามีการถูกบุกรุกเสมอ นอกจากนี้ องค์กรควรใช้การควบคุมความปลอดภัยและแนวทางปฏิบัติใน DevOps และกระบวนการวงจรชีวิตแอปพลิเคชันสำหรับระดับการรับประกันที่สูงขึ้นในระบบธุรกิจของตน

ท่าทางการรักษาความปลอดภัยขั้นพื้นฐานเป็นปัจจัยกำหนดประสิทธิภาพของโซลูชันขั้นสูง

จากการวิเคราะห์ของเรา เราค้นพบจุดบอดที่พบบ่อยในการป้องกันองค์กร ซึ่งทำให้ผู้โจมตีสามารถเข้าถึงเบื้องต้นได้ ตั้งหลัก และดำเนินการโจมตี แม้ว่าจะมีโซลูชันการรักษาความปลอดภัยขั้นสูงอยู่ก็ตาม

ในหลายกรณี ผลของการโจมตีทางไซเบอร์จะถูกกำหนดนานก่อนที่จะเริ่มการโจมตี ผู้โจมตีใช้ประโยชน์จากสภาพแวดล้อมที่มีช่องโหว่เพื่อเข้าถึงเบื้องต้น ดำเนินการเฝ้าระวัง และสร้างความหายนะด้วยการเคลื่อนไหวด้านข้างและการเข้ารหัสหรือการกรองข้อมูล การหยุดผู้โจมตีในระยะเริ่มต้นจะเพิ่มโอกาสในการลดผลกระทบโดยรวมอย่างมาก

Microsoft ศึกษาการกำหนดค่าเฉพาะในท่าทางการรักษาความปลอดภัยเพื่อระบุข้อบกพร่องที่พบบ่อยที่สุดในการปฏิบัติจริงในสภาพแวดล้อมเหล่านี้ สิ่งนี้ทำให้เราเห็นช่องโหว่ที่พบบ่อยที่สุดที่ถูกโจมตีระหว่างการโจมตีของแรนซัมแวร์ที่ดำเนินการโดยมนุษย์ ซึ่งทำให้ผู้คุกคามสามารถเข้าถึงและเดินทางผ่านเครือข่ายที่ตรวจไม่พบ

ต้องเปิดใช้งานการกำหนดค่าความปลอดภัยพื้นฐาน

อุปกรณ์ขององค์กรที่ไม่ได้ออนบอร์ดหรือล้าสมัย (ทั้งในส่วนที่เกี่ยวข้องกับช่องโหว่และสถานะตัวแทนความปลอดภัย) ทำหน้าที่เป็นจุดเริ่มต้นที่เป็นไปได้และเส้นทางการจัดตั้งการเข้าถึงสำหรับผู้โจมตี เราพบว่าในขณะที่มั่นใจว่าอุปกรณ์ขององค์กรได้รับการออนบอร์ดด้วยการตรวจหาและการตอบสนองปลายทางที่อัปเดต[1] (EDR) และแพลตฟอร์มการป้องกันปลายทาง[2] โซลูชัน 2 (EPP) เป็นขั้นตอนที่สำคัญ ไม่รับประกันว่าจะหยุดแรนซัมแวร์ได้

โซลูชันขั้นสูง เช่น EDR และ EPP มีความสำคัญอย่างยิ่งในการตรวจจับผู้โจมตีตั้งแต่เนิ่นๆ ของกระแสการโจมตี และเปิดใช้งานการแก้ไขและป้องกันโดยอัตโนมัติ อย่างไรก็ตาม เนื่องจากโซลูชันขั้นสูงเหล่านี้ใช้ความสามารถพื้นฐานในการตรวจจับการโจมตี จึงจำเป็นต้องเปิดใช้งานการกำหนดค่าความปลอดภัยพื้นฐาน ในความเป็นจริง เราสังเกตเห็นสถานการณ์ที่แพร่หลายด้วยโซลูชันขั้นสูงที่มีอยู่ ซึ่งถูกบั่นทอนโดยขาดการกำหนดค่าความปลอดภัยพื้นฐาน

แนวทางปฏิบัติที่ดีที่สุดในการกำหนดค่าการรักษาความปลอดภัยเป็นตัวบ่งชี้ความยืดหยุ่นที่มากกว่าเวลาตอบสนองของนักวิเคราะห์ศูนย์ปฏิบัติการความปลอดภัย (SOC)

เราสังเกตว่าเวลาที่นักวิเคราะห์ SOC ใช้ในการดูและดำเนินการกับการแจ้งเตือนที่เกี่ยวข้องลดลง 70 เปอร์เซ็นต์ในช่วงหกเดือนสำหรับลูกค้าและพันธมิตรของเรา การรับรู้ที่เพิ่มขึ้นนี้เป็นสัญญาณที่ดี อย่างไรก็ตาม ในขณะที่การมองเห็นการกำหนดค่าความปลอดภัยช่วยปรับปรุงประสิทธิภาพของนักวิเคราะห์ SOC การเปิดใช้งานการมองเห็นผลิตภัณฑ์โดยการออนบอร์ดและการอัปเดตอุปกรณ์ขององค์กรเป็นตัวทำนายที่ดีกว่าในการป้องกันที่ประสบความสำเร็จ

ความเสี่ยงที่เกิดจากอุปกรณ์ที่ไม่รู้จัก

ตรงกันข้ามกับเครือข่ายคลาวด์ที่ลูกค้าทราบว่าสินทรัพย์ใดกำลังทำงานบนระบบปฏิบัติการใด เครือข่ายภายในองค์กรสามารถมีอุปกรณ์ที่หลากหลาย เช่น IoT, เดสก์ท็อป, เซิร์ฟเวอร์ และอุปกรณ์เครือข่ายที่ไม่ได้รับการตรวจสอบหรือจัดการโดยองค์กร

เครือข่ายองค์กรโดยเฉลี่ยมีอุปกรณ์เชื่อมต่อมากกว่า 3,500 เครื่องที่ไม่ได้รับการปกป้องโดยตัวแทน EDR และอาจมีสิทธิ์เข้าถึงทรัพยากรขององค์กรหรือแม้แต่ทรัพย์สินที่มีมูลค่าสูง Microsoft Defender for Endpoint (MDE) ใช้การตรวจสอบเครือข่ายเพื่อค้นหาอุปกรณ์และให้ข้อมูลเกี่ยวกับการจัดประเภทอุปกรณ์สำหรับผู้ที่เชื่อมต่อกับเครือข่าย เช่น ชื่ออุปกรณ์ การกระจายระบบปฏิบัติการ และประเภทอุปกรณ์

3,500

จำนวนอุปกรณ์ที่เชื่อมต่อโดยเฉลี่ยในองค์กรที่ไม่ได้รับการป้องกันโดยตัวแทนการตรวจจับและตอบสนองปลายทาง

สำหรับอุปกรณ์ที่ไม่รองรับโดยตัวแทน EDR อย่างน้อยควรตระหนักถึงการมีอยู่ของอุปกรณ์และดำเนินการเพื่อปกป้องอุปกรณ์เหล่านั้นโดยการประเมินช่องโหว่ รวมถึงการจำกัดการเข้าถึงเครือข่าย

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. แม้แต่โซลูชันขั้นสูงก็อาจถูกทำลายได้หากไม่มีการกำหนดค่าความปลอดภัยพื้นฐาน
2. ลงทุนในแนวทางปฏิบัติที่ดีที่สุดในการกำหนดค่าท่าทางการรักษาความปลอดภัยเพื่อป้องกันการโจมตีในอนาคต การตั้งค่าพื้นฐานเหล่านี้สร้างผลตอบแทนจากการลงทุนจำนวนมากในแง่ของความสามารถขององค์กรในการป้องกันการโจมตี
3. ติดตั้งอุปกรณ์ที่เกี่ยวข้องทั้งหมดเข้ากับโซลูชัน EDR
4. ตรวจสอบให้แน่ใจว่าได้อัปเดตตัวแทนการรักษาความปลอดภัยและรับรองการป้องกันจากการปลอมแปลงเพื่อให้มองเห็นได้มากขึ้นและได้รับประโยชน์จากการป้องกันที่สมบูรณ์ยิ่งขึ้นของผลิตภัณฑ์

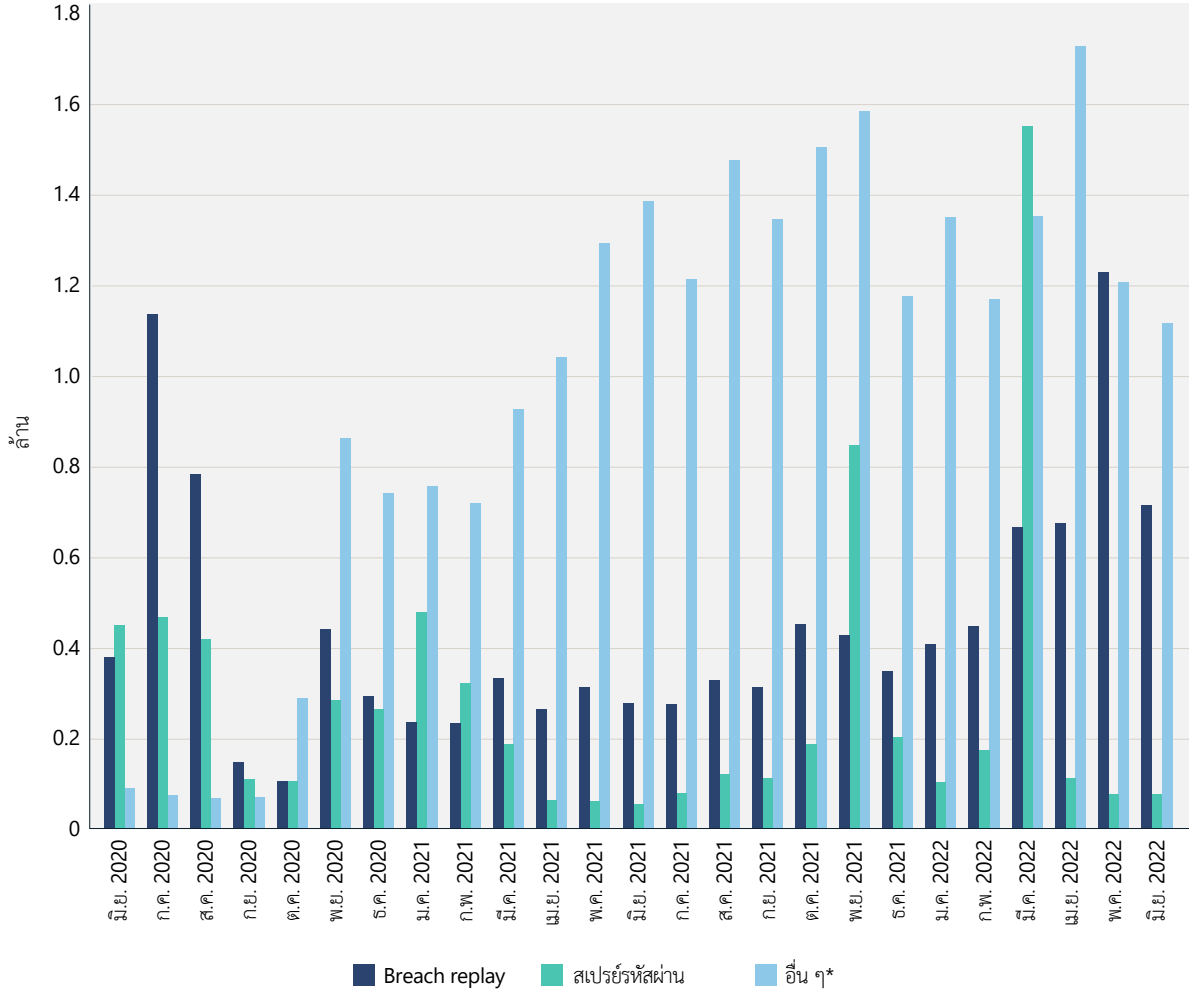
การรักษาสุขภาพของเอกลักษณ์เป็นพื้นฐานของความเป็นอยู่ที่ดีขององค์กร

การปกป้องข้อมูลประจำตัวสำคัญมากกว่าเคย แม้ว่าการโจมตีด้วยรหัสผ่านยังคงเป็นแหล่งที่มาหลักของการถูกบุกรุกข้อมูลประจำตัว แต่การโจมตีประเภทอื่นๆ ก็กำลังเกิดขึ้น ปริมาณของการโจมตีที่ซับซ้อนยังคงเพิ่มขึ้นเมื่อเทียบกับบรรทัดฐานก่อนหน้าของการพ่นรหัสผ่านและเล่นซ้ำการละเมิด

การโจมตีด้วยรหัสผ่านยังคงพบได้ทั่วไป และกว่า 90 เปอร์เซ็นต์ของบัญชีที่ถูกบุกรุกด้วยวิธีเหล่านี้ไม่ได้รับการป้องกันด้วยการรับรองความถูกต้องที่รัดกุม การตรวจสอบสิทธิ์ที่รัดกุมจะใช้การตรวจสอบสิทธิ์มากกว่าหนึ่งปัจจัย เช่น รหัสผ่าน + SMS และคีย์ความปลอดภัย FIDO2

เราได้เห็นการโจมตีด้วยสเปรย์รหัสผ่านแบบกำหนดเป้าหมายที่เพิ่มขึ้น โดยปริมาณการรับส่งข้อมูลของผู้โจมตีพุ่งสูงขึ้นอย่างมากกระจายไปทั่วที่อยู่ IP หลายพันรายการ

ผู้ใช้ที่ถูกบุกรุกตามหมวดหมู่การโจมตี



ผู้ใช้ที่ถูกบุกรุกรายเดือนแยกตามหมวดหมู่การโจมตี ปริมาณการโจมตีด้วยสเปรย์รหัสผ่านมีความผันผวนสูง ดังที่เห็นได้จากการพุ่งสูงขึ้นในเดือนพฤศจิกายน 2021 และมีนาคม 2022 พุ่งสูงขึ้นเหล่านี้เป็นตัวแทนของผู้ใช้หลายพันคนและที่อยู่ IP นับพันที่แตะต้อง
*"อื่นๆ" บ่งชี้ถึงการโจมตีที่แตกต่างจากสเปรย์รหัสผ่านและการเล่นซ้ำของการละเมิด รวมถึงฟิชชิง มัลแวร์ การถูกบุกรุกของผู้ออกโทเค็นภายในองค์กร และอื่นๆ ที่มา: Azure AD Identity Protection

4,500

ในเวลาที่ใช้ในการอ่านคำชี้แจงนี้ เราได้ป้องกันการโจมตีด้วยรหัสผ่าน 4,500 ครั้ง

การรักษาสุขภาพของเอกลักษณ์เป็นพื้นฐานของความเป็นอยู่ที่ดีขององค์กร

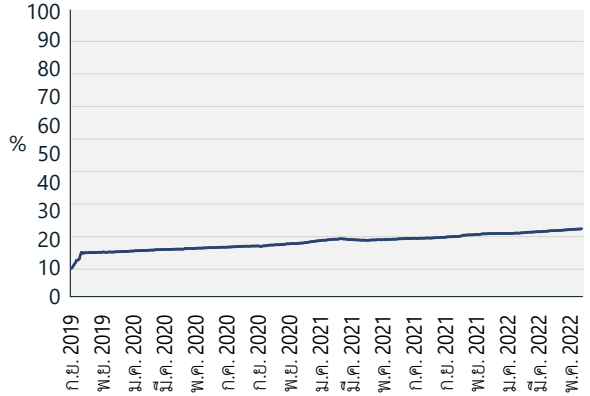
ต่อไป

การปรับใช้การรับรองความถูกต้องที่เข้มงวด

ในแง่บวก เราเห็นการเติบโตอย่างต่อเนื่องในการนำการรับรองความถูกต้องที่แข็งแกร่งมาใช้ในฐานลูกค้าองค์กร Azure Active Directory (Azure AD) สำหรับ Azure AD ผู้ใช้งานรายเดือนที่มีการตรวจสอบสิทธิ์ที่แข็งแกร่ง (MAU) เพิ่มขึ้นจาก 19 เปอร์เซ็นต์เป็น 26 เปอร์เซ็นต์ในปีที่แล้ว ในขณะที่ MAU การรับรองความถูกต้องที่แข็งแกร่งสำหรับบัญชีดูแลระบบเพิ่มขึ้นจาก 30 เป็นประมาณ 33 เปอร์เซ็นต์

แนวโน้มนี้เป็นไปในเชิงบวก แต่ยังต้องการการเติบโตอย่างมากเพื่อให้เข้าถึงการรับรองความถูกต้องที่เข้มงวดได้ครอบคลุมส่วนใหญ่ ลูกค้าที่ไม่ได้ใช้การพิสูจน์ตัวตนที่รัดกุมในสภาพแวดล้อมของพวกเขาควรเริ่มวางแผนและปรับใช้การรับรองความถูกต้องที่เข้มงวดเพื่อปกป้องผู้ใช้ของพวกเขา[3] ในขณะที่ออกแบบการปรับใช้การพิสูจน์ตัวตนที่รัดกุม ควรพิจารณาการรับรองความถูกต้องแบบไม่ใช้รหัสผ่านด้วย มอบประสบการณ์การใช้งานที่ปลอดภัยที่สุด ขจัดความเสี่ยงจากการโจมตีด้วยรหัสผ่าน

การใช้การรับรองความถูกต้องที่เข้มงวด
(กันยายน 2019–พฤษภาคม 2022)

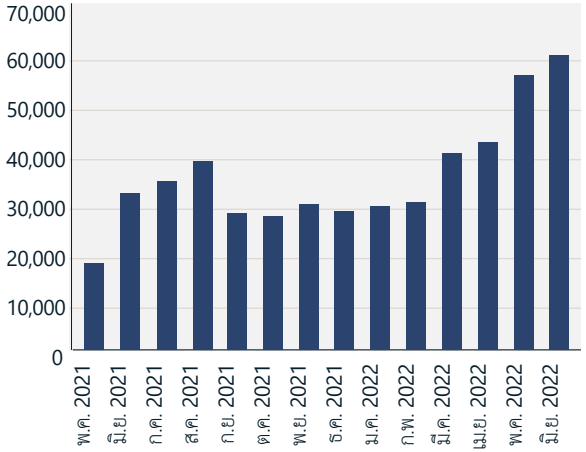


แม้ว่าการใช้การรับรองความถูกต้องที่แข็งแกร่งได้เพิ่มขึ้นเป็นสองเท่าตั้งแต่ปี 2019 แต่มีผู้ใช้เพียง 26 เปอร์เซ็นต์และผู้ดูแลระบบ 33 เปอร์เซ็นต์ที่ใช้การรับรองความถูกต้องที่แข็งแกร่ง ที่มา: Azure Active Directory

การโจมตีซ้ำด้วยโทเค็นเพิ่มขึ้นอย่างต่อเนื่อง

ส่วนแบ่งของการโจมตีรูปแบบอื่นๆ เพิ่มขึ้นในปี 2022 เราเห็นการเพิ่มขึ้นของการโจมตีแบบกำหนดเป้าหมายที่หลีกเลี่ยงการตรวจสอบสิทธิ์ด้วยรหัสผ่านโดยเฉพาะเพื่อลดโอกาสในการตรวจจับ การโจมตีเหล่านี้ใช้ประโยชน์จากคุกกี้การลงชื่อเข้าใช้ครั้งเดียว (SSO) ของเบราว์เซอร์หรือโทเค็นการรีเฟรชที่ได้รับจากมัลแวร์ ฟิชชิง และวิธีการอื่นๆ ในบางกรณี ผู้โจมตีเลือกโครงสร้างพื้นฐานในตำแหน่งที่ใกล้กับตำแหน่งทางภูมิศาสตร์ของผู้ใช้เป้าหมายเพื่อลดโอกาสในการตรวจจับ เราได้เห็นการโจมตีซ้ำด้วยโทเค็นที่เพิ่มขึ้นอย่างต่อเนื่อง เข้าถึงการตรวจจับมากกว่า 40,000 ครั้งต่อเดือนใน Azure AD Identity Protection การเล่นซ้ำของโทเค็นคือการใช้โทเค็นที่ออกให้แก่ผู้ใช้ที่ถูกต้องตามกฎหมายโดยผู้โจมตีที่มีโทเค็นดังกล่าวอยู่ในครอบครอง โดยปกติแล้วโทเค็นจะได้รับจากมัลแวร์ เช่น โดยการกรองคุกกี้ออกจากเบราว์เซอร์ของผู้ใช้หรือผ่านวิธีการฟิชชิ่งขั้นสูง

ปริมาณของการโจมตีซ้ำโทเค็นที่ตรวจพบ



การโจมตีซ้ำโทเค็นที่ตรวจพบต่อเดือน ที่มา: Azure AD Identity Protection เซสชันเฉพาะที่ถูกตั้งค่าสถานะโดยการตรวจหาโทเค็นที่ผิดปกติ

การรักษาสุขภาพของเอกลักษณ์เป็นพื้นฐานของความเป็นอยู่ที่ดีขององค์กร

ต่อไป

การแยกโทเค็น

มากกว่ามัลแวร์ ผู้โจมตีต้องการข้อมูลประจำตัวเพื่อให้บรรลุเป้าหมาย ในความเป็นจริง 100 เปอร์เซ็นต์ของการโจมตีด้วยแรนซัมแวร์ที่ดำเนินการโดยมนุษย์นั้นรวมถึงการขโมยข้อมูลประจำตัว การบุกรุกที่ซับซ้อนหลายอย่างรวมถึงข้อมูลประจำตัวที่ซื้อจากเว็บมืด ซึ่งเริ่มแรกถูกขโมยจากมัลแวร์ ขโมยข้อมูลประจำตัวที่ไม่ซับซ้อนและกระจายเป็นวงกว้าง มัลแวร์ประเภทนี้พัฒนาขึ้นเพื่อขโมยโทเค็น รวมถึงข้อมูลเซสชันและการอ้างสิทธิ์ MFA ซึ่งหมายความว่าการติดไวรัสบนระบบโฮม ซึ่งผู้ใช้ลงชื่อเข้าใช้สินทรัพย์ของบริษัท อาจนำไปสู่เหตุการณ์ร้ายแรงบนเครือข่ายขององค์กรได้

ผู้โจมตียังสามารถดึงโทเค็นจากอุปกรณ์ของเหยื่อผ่านการโจมตีแบบคนกลาง ซึ่งเหยื่อจะคลิกลิงก์ที่เป็นอันตรายในอีเมลฟิชชิ่งหรือข้อความโต้ตอบแบบทันที และถูกนำไปยังเว็บไซต์ที่มีลักษณะเหมือนหน้าลงชื่อเข้าใช้ที่ถูกต้องตามกฎหมายของ ผู้ให้บริการข้อมูลประจำตัว ในความเป็นจริงนี่เป็นบริการบนเว็บที่ผู้โจมตีปั่นขึ้นซึ่งถ่ายทอดและสกัดกั้นการรับส่งข้อมูลทั้งหมดระหว่างผู้ใช้และผู้ให้บริการข้อมูลประจำตัว ผู้โจมตีสามารถสกัดกั้นชื่อผู้ใช้และรหัสผ่านและถ่ายทอดความท้าทายของ MFA ได้ โทเค็นผลลัพธ์ที่ออกโดยผู้ให้บริการข้อมูลประจำตัวและสกัดกั้นโดยผู้โจมตีอาจมีการอ้างสิทธิ์ของ MFA ที่ผู้โจมตีสามารถใช้เพื่อให้เป็นไปตามข้อกำหนดของ MFA

Microsoft Defender for Cloud Apps ตรวจพบการโจมตีดังกล่าวโดยเฉลี่ย 895 ครั้งต่อเดือนตั้งแต่ต้นปี 2022 การโจมตีรูปแบบนี้สามารถป้องกันได้โดยใช้ปัจจัยป้องกันฟิชชิ่งของ MFA เช่น Certificate Based Authentication, Windows Hello for Business หรือคีย์ความปลอดภัย FIDO2

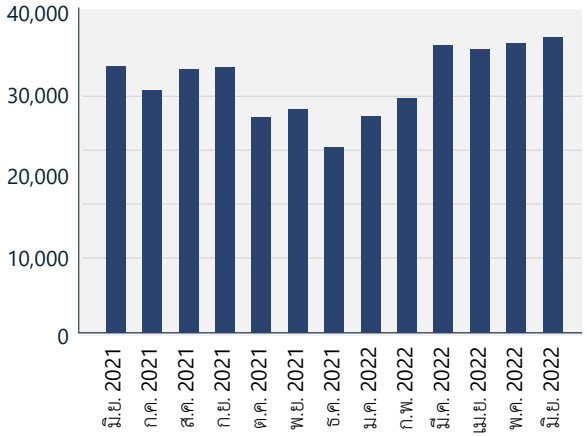
> การโจมตีด้วยรหัสผ่านเป็นวิธีการหลักที่ทำให้บัญชีถูกบุกรุก

ความเหนื่อยล้า MFA

การใช้แนวคิดของ “ความเหนื่อยล้าของ MFA” ผู้โจมตีสร้างคำขอหลายรายการสำหรับ MFA ไปยังอุปกรณ์ของเหยื่อ โดยหวังว่าเหยื่อจะยอมรับคำขอโดยไม่ตั้งใจหรือเป็นผลจากความเหนื่อยล้า การโจมตีนี้สามารถป้องกันได้โดยใช้แอปตัวรับรองความถูกต้องที่ทันสมัย เช่น Microsoft Authenticator รวมกับคุณลักษณะต่างๆ เช่นหมายเลขที่ตรงกัน[4] และเปิดใช้งานบริบทเพิ่มเติม[5] Azure AD Identity Protection ประมาณว่ามี 30,000 การโจมตีเมื่อยล้าของ MFA ต่อเดือน

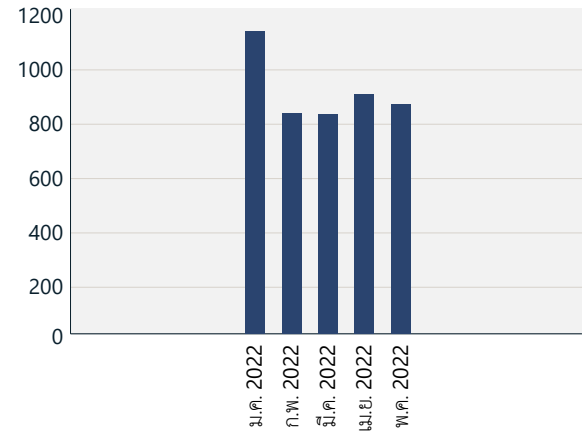
> การมีส่วนร่วมของการโจมตีที่ซับซ้อนยังคงเพิ่มขึ้นอย่างต่อเนื่อง เน้นย้ำถึงความจำเป็นของปัจจัยป้องกันฟิชชิ่งของการรับรองความถูกต้องหลายปัจจัย

อินสแตนซ์โดยประมาณของการโจมตี ความเหนื่อยล้า MFA



ที่มา: Azure AD Identity Protection

อินสแตนซ์ที่ตรวจพบของฟิชชิงที่ตามด้วยการโจมตีจากคนกลาง



ที่มา: แอป Microsoft Defender for Cloud

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ตรวจสอบให้แน่ใจว่าบัญชีทั้งหมดทั่วทั้งองค์กรของคุณได้รับการปกป้องด้วยมาตรการการรับรองความถูกต้องที่แข็งแกร่ง
2. การรับรองความถูกต้องแบบไม่ใช้รหัสผ่านมอบประสบการณ์ที่ปลอดภัยและเป็นมิตรกับผู้ใช้มากที่สุด ลดความเสี่ยงจากการโจมตีด้วยรหัสผ่าน
3. ปิดใช้งานการรับรองความถูกต้องแบบดั้งเดิมทั่วทั้งองค์กรของคุณ
4. ปกป้องบัญชีที่มีมูลค่าสูงและบัญชีดูแลระบบด้วยรูปแบบการรับรองความถูกต้องที่แข็งแกร่งที่ป้องกันฟิชชิ่ง
5. ปรับให้ทันสมัยจากผู้ให้บริการข้อมูลประจำตัวภายในองค์กรให้เป็นผู้ให้บริการข้อมูลประจำตัวบนระบบคลาวด์ และเชื่อมต่อแอปทั้งหมดของคุณกับผู้ให้บริการข้อมูลประจำตัวบนระบบคลาวด์เพื่อประสบการณ์ผู้ใช้และความปลอดภัยที่สอดคล้องกัน

ลิงค์ไปยังข้อมูลเพิ่มเติม

- วันรหัสผ่านโลกนี้พิจารณาการทิ้งรหัสผ่านทั้งหมด | Microsoft Security

การตั้งค่าความปลอดภัยเริ่มต้นของระบบปฏิบัติการ

ด้วยแนวภัยคุกคามด้านความปลอดภัยที่มีการพัฒนาอย่างต่อเนื่อง เรามองเห็นความต้องการที่เพิ่มขึ้นสำหรับการรักษาความปลอดภัยคอมพิวเตอร์ที่กำหนดค่าตามค่าเริ่มต้นเพื่อปรับปรุงความยืดหยุ่นทางไซเบอร์ แม้ว่าความปลอดภัยของระบบปฏิบัติการจะเป็นเรื่องเร่งด่วน ซับซ้อน และมีความสำคัญต่อธุรกิจมากกว่าที่เคยเป็นมา แต่การทำให้ถูกต้องและจัดการอาจเป็นเรื่องยาก

ในอดีต การรักษาความปลอดภัยของคอมพิวเตอร์และอุปกรณ์รวมถึงคุณลักษณะการรักษาความปลอดภัยในตัวที่ลูกค้าหรือผู้เชี่ยวชาญด้านไอทีต้องกำหนดค่าให้อยู่ในระดับที่ต้องการ วิธีการนี้ไม่เพียงพออีกต่อไป เนื่องจากผู้โจมตีใช้เครื่องมือขั้นสูงในระบบอัตโนมัติ โครงสร้างพื้นฐานระบบคลาวด์ และเทคโนโลยีการเข้าถึงระยะไกลเพื่อให้บรรลุเป้าหมาย ซึ่งกลายเป็นเรื่องสำคัญที่การรักษาความปลอดภัยทุกชั้น ตั้งแต่ชิปไปจนถึงระบบคลาวด์ได้รับการกำหนดค่าตามค่าเริ่มต้น Microsoft ได้พัฒนาเพื่อกำหนดค่าความปลอดภัยของระบบปฏิบัติการ Windows ตามค่าเริ่มต้น[6]

ลูกค้าที่ใช้การป้องกัน—เชิงลึกรวมถึงท่าทางการรักษาความปลอดภัยแบบหลายชั้น ฟีเจอร์การรักษาความปลอดภัยใหม่ๆ การแพตช์และการอัปเดตอย่างสม่ำเสมอและสม่ำเสมอ ตลอดจนการฝึกอบรมด้านความปลอดภัยและการรับรู้เพื่อรายงานฟิชชิงและการหลอกลวงอื่นๆ สามารถคาดหวังมัลแวร์น้อยลง

เพื่อลดความซับซ้อนในการป้องกันในเชิงลึก Windows 11 ได้รวมการป้องกันฮาร์ดแวร์และซอฟต์แวร์ไว้อย่างแน่นแฟ้น โดยเปิดใช้งานตามค่าเริ่มต้น รวมถึงความสมบูรณ์ของหน่วยความจำ Secure Boot และ Trusted Platform Module 2.0 ผู้ใช้ Windows 10 บนฮาร์ดแวร์ที่มีความสามารถสามารถเปิดคุณลักษณะเหล่านี้ได้ในแอปการตั้งค่า Windows หรือในเมนู BIOS

โดยทั่วไปแล้วอุปกรณ์รุ่นเก่ามักจะไม่มีความสอดคล้องกันระหว่างความปลอดภัยของฮาร์ดแวร์และเทคนิคการรักษาความปลอดภัยของซอฟต์แวร์ สำหรับอุปกรณ์ที่ไม่ได้เปิดใช้งานการรักษาความปลอดภัยตามค่าเริ่มต้น ให้กำหนดค่าด้วยตนเองในการตั้งค่าหากเป็นไปได้[7]

สำหรับอุปกรณ์ที่ไม่ได้เปิดใช้งานการรักษาความปลอดภัยตามค่าเริ่มต้น Microsoft แนะนำให้กำหนดค่าด้วยตนเองในการตั้งค่าหากเป็นไปได้

ดำเนินการเชิงรุกเกี่ยวกับการใช้การอัปเดตระบบปฏิบัติการอย่างต่อเนื่องและแพตช์ความปลอดภัยที่ช่วยป้องกันตลอดวงจรชีวิตของฮาร์ดแวร์และซอฟต์แวร์

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ใช้โซลูชันที่ไม่ต้องใช้รหัสผ่านซึ่งผูกข้อมูลรับรองการลงชื่อเข้าใช้ใน Trusted Platform Module โดยเฉพาะ ให้มองหาโซลูชันที่ไม่ต้องใช้รหัสผ่านซึ่งตรงตามมาตรฐานอุตสาหกรรม[8] Faster Identity Online (FIDO) Alliance
2. ดำเนินการล้างไฟล์ปฏิบัติการที่ไม่ได้ใช้งานและค้างอยู่ในอุปกรณ์ขององค์กรอย่างทันท่วงที
3. ป้องกันการโจมตีเฟิร์มแวร์ขั้นสูงด้วยการเปิดใช้งานความสมบูรณ์ของหน่วยความจำ Secure Boot และ Trusted Platform Module 2.0 หากไม่ได้เปิดใช้งานตามค่าเริ่มต้น ซึ่งจะทำให้การบูตแข็งแกร่งขึ้นโดยใช้ความสามารถที่มีอยู่ใน CPU สมัยใหม่
4. เปิดการเข้ารหัสข้อมูลและการป้องกันข้อมูลประจำตัว
5. เปิดใช้งานการควบคุมแอปพลิเคชันและเบราว์เซอร์เพื่อเพิ่มการป้องกันจากแอปพลิเคชันที่ไม่น่าเชื่อถือและการป้องกันช่องโหว่ในตัวอื่นๆ
6. เปิดใช้งานการป้องกันการเข้าถึงหน่วยความจำเพื่อช่วยป้องกันการโจมตีทางกายภาพทั่วไป เช่น การเสียบอุปกรณ์ที่เป็นอันตรายเข้ากับพอร์ตที่เข้าถึงได้จากภายนอก

ลิงค์ไปยังข้อมูลเพิ่มเติม

- สมุดความปลอดภัยของ Windows | พาณิชย์
- คุณลักษณะด้านความปลอดภัยใหม่สำหรับ Windows 11 จะช่วยป้องกันการทำงานแบบไฮบริด | บล็อก Microsoft Security

ศูนย์กลางห่วงโซ่อุปทานของซอฟต์แวร์

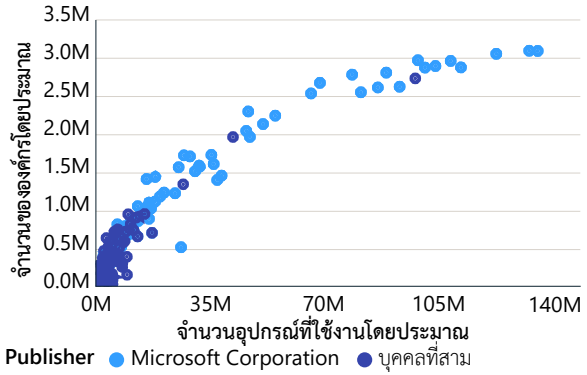
การโจมตีแอป ปลั๊กอิน และส่วนขยายของบุคคลที่สามสามารถทำลายความไว้วางใจของลูกค้าที่มีต่อซัพพลายเออร์ที่มีบทบาทสำคัญในระบบนิเวศการจัดหา การใช้ทฤษฎีเครือข่ายเพื่อดูการเป็นศูนย์กลางของซอฟต์แวร์ช่วยให้เห็นความสำคัญของแพตช์ โดยเฉพาะอย่างยิ่งสำหรับแอปส่วนกลาง

มีการติดตั้งและใช้งาน Windows App Network ของแอปพลิเคชัน 18 ล้านรายการในองค์กร 5 ล้านแห่ง ซึ่งให้มุมมองระดับบนสุดของระบบนิเวศซอฟต์แวร์ของเรา จากแอปพลิเคชันที่ใช้มากที่สุด 100,000 รายการ ร้อยละ 97 ผลิตโดยองค์กรบุคคลที่สามซึ่งอัปเดตและแพตช์ความปลอดภัยได้รับการดูแลโดยพวกเขา สิ่งนี้แสดงให้เห็นลักษณะสำคัญสองประการของระบบนิเวศแอปพลิเคชันเชิงพาณิชย์ของเรา

ประการแรก มีศูนย์กลางในระบบนิเวศของแอปพลิเคชันเชิงพาณิชย์ของ Windows เฉพาะแอปพลิเคชัน 100,000 อันดับแรก (จาก 18 ล้าน) เท่านั้นที่ใช้บนอุปกรณ์ 1,000 เครื่องขึ้นไป กล่าวอีกนัยหนึ่งคือ มากกว่าครึ่งหนึ่งของ 1 เปอร์เซ็นต์ของแอปพลิเคชันเหล่านี้มีผลกระทบในวงกว้างเช่นนี้ในระบบนิเวศของอุปกรณ์

ประการที่สอง ความสามารถในการจัดการแอปพลิเคชันเหล่านั้นมีความหลากหลาย โดยซัพพลายเออร์แอปพลิเคชันชั้นนำ 10,000 รายจัดการการอัปเดตและแพตช์ความปลอดภัยของแอปพลิเคชันเชิงพาณิชย์ที่ใช้มากที่สุดเหล่านี้ สิ่งนี้แสดงให้เห็นถึงการพึ่งพาซึ่งกันและกันที่บริษัทมีต่อชุดความปลอดภัย การปฏิบัติตามข้อกำหนด และการควบคุมการจัดการของซัพพลายเออร์ซอฟต์แวร์ที่หลากหลาย

การเจาะเชิงพาณิชย์ของแอปพลิเคชันที่ใช้มากที่สุด



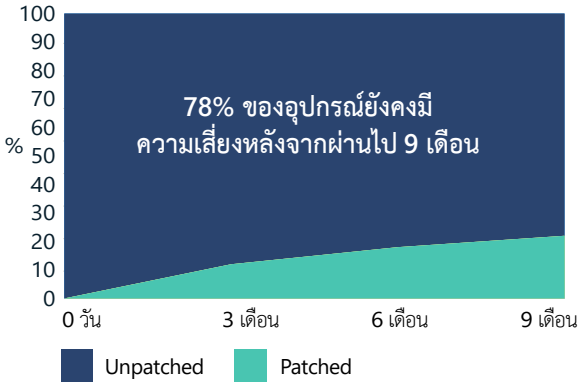
แอปพลิเคชันยอดนิยมถูกใช้โดยองค์กรหลายล้านแห่งและอุปกรณ์หลายสิบล้านเครื่อง เนื่องจากเกือบจะมีอยู่ทุกหนทุกแห่ง ผู้ไม่หวังดีจึงคอยมองหาช่องโหว่ในแอปพลิเคชันยอดนิยมเหล่านี้อย่างต่อเนื่อง ซึ่งอาจส่งผลกระทบต่ออุปกรณ์หลายล้านเครื่องในฐานผู้ใช้

เราสังเกตว่าอุปกรณ์เชิงพาณิชย์หลายล้านเครื่องยังคงใช้เวอร์ชันแอปพลิเคชันที่มีช่องโหว่หลายเดือนหลังจากปล่อยแพตช์ หรือแม้แต่หลายปีหลังจากสิ้นสุดการสนับสนุนผลิตภัณฑ์ ตัวอย่างเช่น มีอุปกรณ์ Windows เชิงพาณิชย์มากกว่าหนึ่งล้านเครื่องที่ใช้งานโปรแกรมอ่าน PDF เวอร์ชันที่ไม่รองรับมาตั้งแต่ปี 2017

แอปพลิเคชันเวอร์ชันเก่าที่ไม่ได้รับการสนับสนุนยังคงใช้งานอยู่ในอุปกรณ์เชิงพาณิชย์หลายล้านเครื่อง ส่งผลให้องค์กรต่างๆ มีความเสี่ยงที่จะเกิดช่องโหว่ที่ไม่ได้รับการแก้ไข

สำหรับเวอร์ชันแอปพลิเคชันที่สนับสนุน เราเห็นว่าความเร็วของการนำแพตช์ที่สำคัญไปใช้ที่ราบสูง ซึ่งตรงกันข้ามกับแนวโน้มที่จะขับเคลื่อนความยืดหยุ่น เส้นโค้งควรแสดงการใช้แพตช์เพิ่มขึ้นแบบทวีคูณในเดือนต่อเดือน เพื่อให้ได้ความยืดหยุ่นที่จำเป็น

อัตราการปรับใช้แพตช์ที่สำคัญ



หลังจากตรวจสอบช่องโหว่ร้ายแรงที่ส่งผลกระทบต่อเบราว์เซอร์ 134 เวอร์ชัน เราพบว่า 78 เปอร์เซ็นต์หรืออุปกรณ์หลายล้านเครื่องยังคงใช้หนึ่งในเวอร์ชันที่ได้รับผลกระทบ 9 เดือนหลังจากออกแพตช์

เราใช้ชุดเครื่องมือ[9] InterpretML เพื่อระบุคุณลักษณะที่เกี่ยวข้องกับองค์กรที่มีแนวโน้มที่จะมีอุปกรณ์ที่มีแอปเวอร์ชันเก่า สิ่งที่สำคัญที่สุดของตัวทำนายเหล่านี้ ได้แก่ การมีส่วนร่วมกับอุปกรณ์ในเวลาน้อย พื้นที่ทางภูมิศาสตร์ เช่น เอเชียแปซิฟิกและละตินอเมริกา และอุตสาหกรรมต่างๆ เช่น ยานยนต์ เคมีภัณฑ์ โทรคมนาคม การขนส่งและลอจิสติกส์ ผู้จ่ายค่ารักษาพยาบาล (ผู้จัดการสินไหมทดแทน) และการประกันภัย

การบำรุงรักษาความยืดหยุ่นของซอฟต์แวร์ควรรวมถึงการปิดใช้งานหรือถอนการติดตั้งแอปพลิเคชันที่ไม่ได้ใช้งานเป็นประจำ

ความปลอดภัยและการปฏิบัติตามกฎระเบียบขององค์กรขึ้นอยู่กับความพยายามขององค์กรและซัพพลายเออร์ซอฟต์แวร์

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ดำเนินการอัปเดตแอปพลิเคชันและจุดสิ้นสุดทั้งหมดอย่างทันท่วงทีผ่านองค์กรของคุณ
2. ดำเนินการล้างไฟล์ปฏิบัติการที่ไม่ได้ใช้งานและค้างอยู่ในอุปกรณ์ขององค์กรอย่างทันท่วงที

ลิงค์ไปยังข้อมูลเพิ่มเติม

- คู่มือ Microsoft Intune | Microsoft Docs
- จัดการแอป | Microsoft Docs
- Microsoft Defender for Endpoint | Microsoft Security
- OSS Secure Supply Chain Framework | วิศวกรรมความปลอดภัยของ Microsoft
- Microsoft Open Source Software Secure Supply Chain Framework | GitHub

การสร้างความยืดหยุ่นต่อการโจมตี DDoS, เว็บแอปพลิเคชัน และเครือข่ายที่เกิดขึ้นใหม่

การเปลี่ยนแปลงทางดิจิทัลแบบเร่งรัดได้ทำให้เครือข่ายแบบเดิมและรูปแบบขอบเขตความปลอดภัยสิ้นสุดลง การย้ายไปยังระบบคลาวด์หมายความว่าองค์กรต่างๆ ต้องใช้การรักษาความปลอดภัยเครือข่ายแบบคลาวด์เนทีฟเพื่อปกป้องทรัพย์สินดิจิทัล

ความซับซ้อน ความถี่ และปริมาณการโจมตียังคงเพิ่มขึ้นและไม่จำกัดเฉพาะช่วงเทศกาลวันหยุดอีกต่อไป ซึ่งบ่งชี้ถึงการเปลี่ยนแปลงไปสู่การโจมตีตลอดทั้งปี สิ่งนี้เน้นย้ำถึงความสำคัญของการป้องกันอย่างต่อเนื่องนอกเหนือจากช่วงที่มีการจราจรหนาแน่นแบบดั้งเดิม

การโจมตีของการปฏิเสธการให้บริการแบบกระจาย (DDoS)

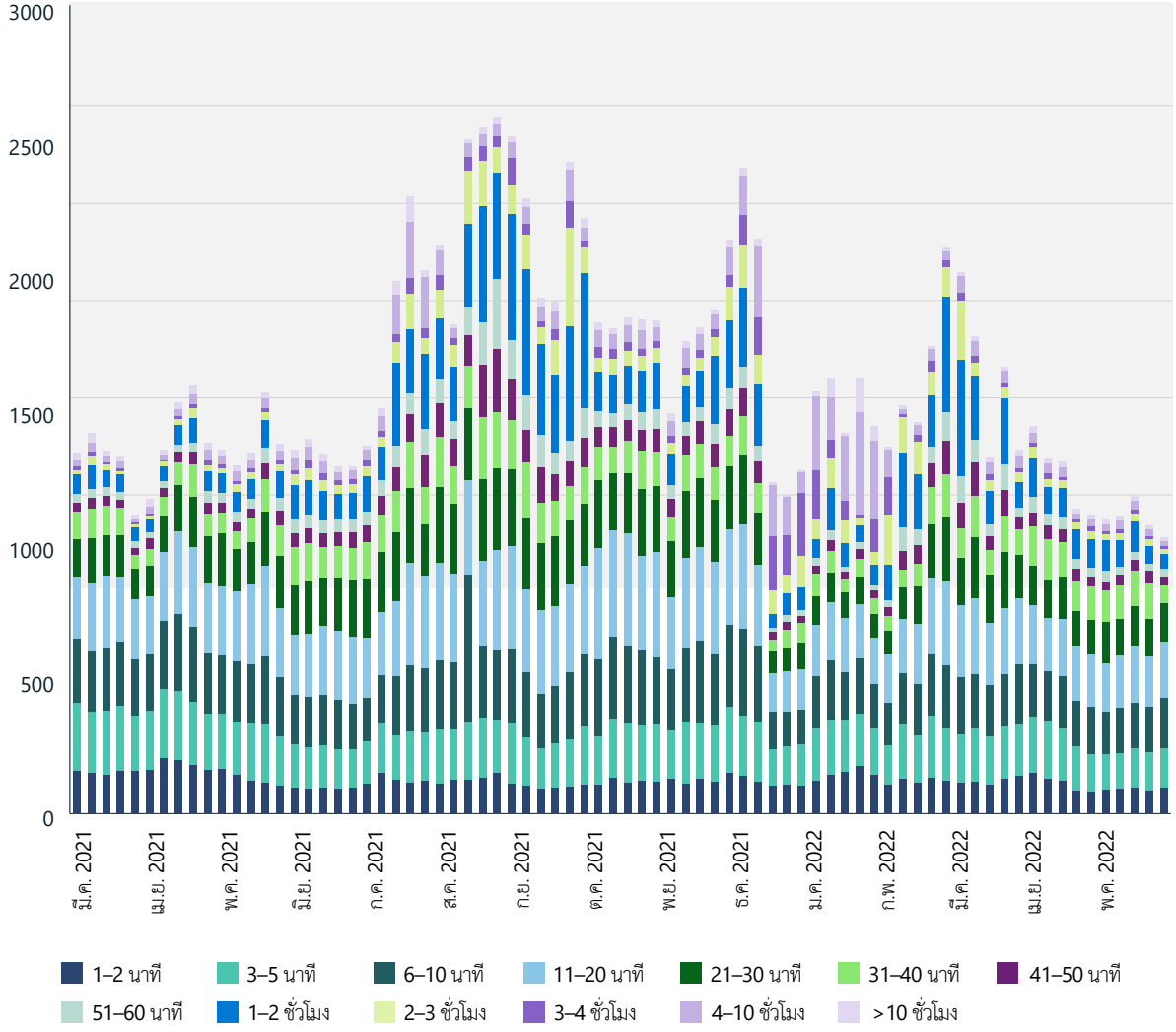
ในช่วงปีที่ผ่านมา โลกประสบกับกิจกรรมของ DDoS ที่มีปริมาณ ความซับซ้อน และความถี่อย่างไม่เคยปรากฏมาก่อน การระเบิดของ DDoS นี้ได้รับแรงหนุนจากการโจมตีของรัฐในประเทศที่เพิ่มขึ้นอย่างมากและการขยายตัวอย่างต่อเนื่องของบริการเช่า DDoS ที่มีต้นทุนต่ำ Microsoft ลดการโจมตีเฉลี่ย 1,955 ครั้งต่อวัน เพิ่มขึ้น 40 เปอร์เซ็นต์จากปีก่อนหน้า ก่อนหน้านี้ จำนวนการโจมตีสูงสุดมักเกิดขึ้นในช่วงเทศกาลวันหยุดสิ้นปี อย่างไรก็ตาม ในปีนี้มีการบันทึกมากที่สุดในหนึ่งวันคือวันที่ 10 สิงหาคม 2021 ซึ่งอาจบ่งชี้ถึงการเปลี่ยนไปสู่การโจมตีตลอดทั้งปี และเน้นย้ำถึงความสำคัญของการป้องกันอย่างต่อเนื่องนอกเหนือจากช่วงที่มีการจราจรคับคั่งแบบดั้งเดิม

ในเดือนพฤศจิกายน 2021 Microsoft ขัดขวางการโจมตี DDoS เชิงปริมาตรด้วยทรูพุต 3.4 เทราบิตต่อวินาที (Tbps) จากแหล่งที่มาประมาณ 10,000 แห่งในหลายประเทศ การโจมตีแบบปริมาณสูงที่คล้ายกันที่สูงกว่า 2+Tbps ลดลงในปี 2022 โดยเน้นว่าไม่ใช่แค่ความซับซ้อน ความถี่ของการโจมตีที่เพิ่มขึ้น แต่ยังรวมถึงปริมาณ (แบนด์วิธ) ของการโจมตีด้วย

ระยะเวลา การโจมตี

การโจมตีส่วนใหญ่ที่สังเกตได้ในปีที่ผ่านมานี้เป็นเพียงช่วงสั้นๆ ประมาณ 28 เปอร์เซ็นต์ของการโจมตีใช้เวลาน้อยกว่า 10 นาที 26 เปอร์เซ็นต์ใช้เวลา 10–30 นาที และ 14 เปอร์เซ็นต์ใช้เวลา 31–60 นาที สามสิบสองเปอร์เซ็นต์ของการโจมตีมีระยะเวลานานกว่าหนึ่งชั่วโมง

จำนวนการโจมตี DDoS และการกระจายระยะเวลา
(มีนาคม 2021-พฤษภาคม 2022)



การโจมตีส่วนใหญ่ในปีที่แล้วมีระยะสั้น ประมาณ 28 เปอร์เซ็นต์ของการโจมตีใช้เวลาน้อยกว่า 10 นาที

การสร้างความยืดหยุ่นต่อการโจมตี DDoS, เว็บแอปพลิเคชัน และเครือข่ายที่เกิดขึ้นใหม่

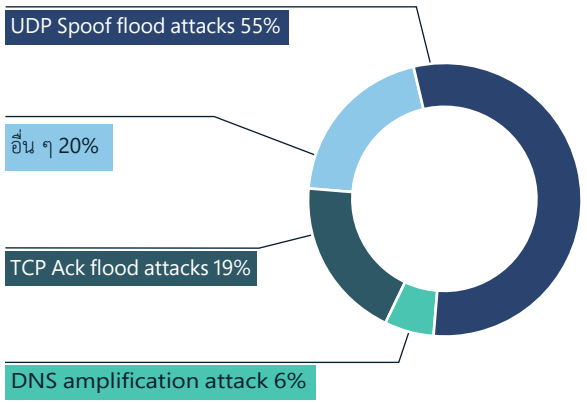
ยังคงดำเนินต่อไป

เวกเตอร์การโจมตี DDoS

ในปีที่ผ่านมา เวกเตอร์การโจมตีที่ใช้โดยทั่วไปคือการสะท้อน User Datagram Protocol (UDP) บนพอร์ต 80 โดยใช้โปรโตคอลการค้นหาบริการอย่างง่าย (SSDP) โปรโตคอลการเข้าถึงไดเรกทอรีน้ำหนักเบาแบบไร้การเชื่อมต่อ (CLDAP) ระบบชื่อโดเมน (DNS) และโปรโตคอลเวลาเครือข่าย (NTP) ประกอบด้วยพีคเดียว นอกจากนี้ เรายังเห็นการเพิ่มขึ้นของการโจมตี DDoS ในชั้นแอปพลิเคชันที่กำหนดเป้าหมายเว็บไซต์ด้วย RPS สูงสุด 16.3 ล้านครั้ง (คำขอต่อวินาที) และการจราจรสูงสุด 9.89 Tbps

ในปี 2022 Microsoft ลดการโจมตี DDoS เกือบ 2,000 ครั้งต่อวัน และขัดขวางการโจมตี DDoS ที่ใหญ่ที่สุดเท่าที่เคยมีรายงานมาในประวัติศาสตร์

เวกเตอร์การโจมตี DDoS



การโจมตี UDP Spoof flood เพิ่มขึ้นเป็นเวกเตอร์สูงสุดในช่วงครึ่งแรกของปี 2022 จาก 16 เปอร์เซ็นต์เป็น 55 เปอร์เซ็นต์ การโจมตี TCP Ack flood ลดลงจาก 54 เปอร์เซ็นต์เป็น 19 เปอร์เซ็นต์

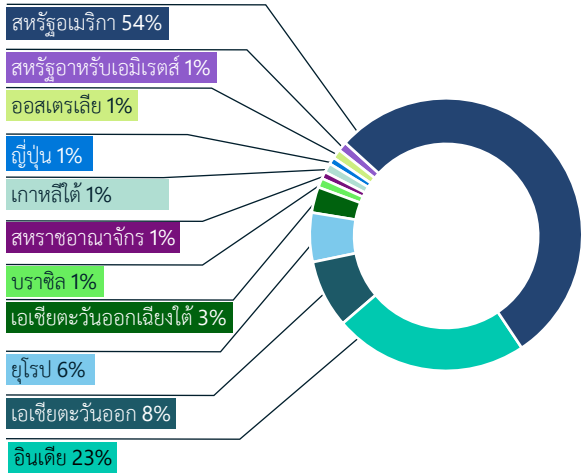


อุตสาหกรรมเกมยังคงเป็นเป้าหมายสูงสุดของการโจมตี DDoS ส่วนใหญ่มาจากการกลายพันธุ์ของบอทเน็ต Mirai และการโจมตีโปรโตคอล UDP ปริมาณต่ำ เนื่องจาก UDP ถูกใช้โดยทั่วไปในแอปพลิเคชันเกมและสตรีมมิ่ง การโจมตีส่วนใหญ่ที่มากคือ UDP spoof ในขณะที่ส่วนน้อยคือการโจมตีการสะท้อนและการขยาย UDP

ภูมิภาคเป้าหมายทางภูมิศาสตร์

จากการโจมตี DDoS ที่ตรวจพบในปีที่ผ่านมา 54 เปอร์เซ็นต์ดำเนินการกับเป้าหมายในสหรัฐอเมริกา แนวโน้มที่อาจอธิบายได้บางส่วนจากข้อเท็จจริงที่ว่าลูกค้า Azure และ Microsoft ส่วนใหญ่อยู่ในสหรัฐอเมริกา นอกจากนี้ เรายังเห็นการโจมตีอินเดียเพิ่มขึ้นอย่างรวดเร็ว จากเพียง 2 เปอร์เซ็นต์ของการโจมตีทั้งหมดในช่วงครึ่งหลังของปี 2021 เป็น 23 เปอร์เซ็นต์ในครึ่งแรกของปี 2022 โดยเฉพาะเอเชียตะวันออก ฮ่องกง ยังคงเป็นเป้าหมายยอดนิยมที่ 8 เปอร์เซ็นต์ สำหรับยุโรป เราเห็นความเข้มข้นของการโจมตีต่อภูมิภาคอัมสเตอร์ดัม เวียนนา ปารีส และแฟรงก์เฟิร์ต

ปลายทางการโจมตี DDoS

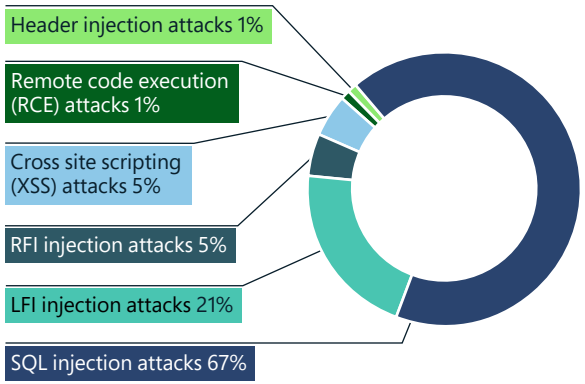


เราระบุว่าการโจมตีจำนวนมากในเอเชียเป็นผลมาจากเกมขนาดใหญ่ในภูมิภาคนี้ โดยเฉพาะในจีน ญี่ปุ่น เกาหลีใต้ และอินเดีย รอยเท้านี้จะขยายต่อไปเนื่องจากการเจาะตลาดสมาร์ทโฟนที่เพิ่มขึ้นผลักดันความนิยมของเกมบนมือถือ บ่งชี้ว่าเป้าหมายทางภูมิศาสตร์นี้จะเติบโตต่อไปเท่านั้น

การหาประโยชน์จากเว็บแอปพลิเคชัน

ไฟร์วอลล์ของเว็บแอปพลิเคชัน (WAF) ร่วมกับการป้องกัน DDoS เป็นส่วนสำคัญของกลยุทธ์การป้องกันเชิงลึกสำหรับการปกป้องเว็บและทรัพย์สินส่วนต่อประสานการเขียนโปรแกรมแอปพลิเคชัน (API) Microsoft สังเกตกฎ WAF มากกว่า 300 พันล้านรายการที่เรียกใช้ต่อเดือนผ่าน Azure WAFs

การกระจายประเภทการโจมตีที่แพร่หลายที่สุด



Azure WAF ตรวจพบการโจมตี Open Web Application Security Project (OWASP) 10 อันดับแรก[10] นับพันล้านรายการทุกวัน ตามสัญญาณของเรา ผู้โจมตีพยายามโจมตีด้วยการแทรก SQL มากที่สุด ตามด้วยการแทรกไฟล์ในเครื่องและการโจมตีด้วยการแทรกไฟล์จากระยะไกล ซึ่งสอดคล้องกับรายการ OWASP Top Ten ที่แสดงการโจมตีแบบฉีดเป็นประเภทการโจมตีทางเว็บที่พบมากเป็นอันดับสาม

นอกจากนี้ยังมีการโจมตีบอทกับเว็บแอปพลิเคชัน Azure เพิ่มขึ้น โดยมีคำขอบอทเฉลี่ย 1.7 พันล้านคำขอต่อเดือน และ 4.6 เปอร์เซ็นต์ของการจราจรนั้นประกอบด้วยบอทที่ไม่ดี

การสร้างความยืดหยุ่นต่อการโจมตี DDoS, เว็บแอปพลิเคชัน และเครือข่ายที่เกิดขึ้นใหม่

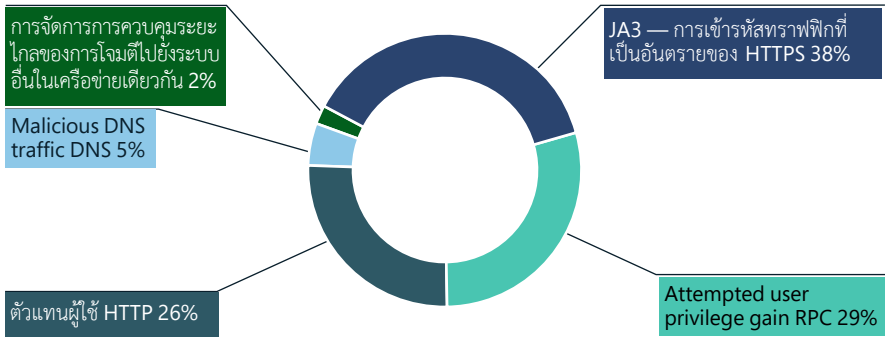
ต่อไป

เนื่องจากการเพิ่มจำนวนของบอทที่ทำการโจมตีเพื่อยัดข้อมูลประจำตัว การฉ้อโกงบัตรเครดิต แคมเปญที่มีอิทธิพลทางไซเบอร์ และการโจมตีห่วงโซ่อุปทาน เราคาดว่าจะเห็นการโจมตีของบอทกับเว็บแอปพลิเคชันเพิ่มขึ้นอย่างต่อเนื่อง

การบุกรุกเครือข่าย: การตรวจจับและการป้องกัน

เราสังเกตว่าการใช้ประโยชน์จากเลเยอร์เครือข่ายเพิ่มขึ้นอย่างมาก โดยเฉพาะมัลแวร์ในปี 2022 ระบบตรวจจับและป้องกันการบุกรุกของ Azure Firewall (IDPS) บล็อกการเชื่อมต่อมากกว่า 150 ล้านครั้งในเดือนมิถุนายนเพียงเดือนเดียว

IDPS ปฏิเสธเหตุผลการรับส่งข้อมูล



IDPS เหตุผลในการแจ้งเตือนการจราจร



การวิเคราะห์การแจ้งเตือนและปฏิเสธการรับส่งข้อมูลของ IDPS แสดงแนวทางต่อไปนี้ที่ผู้โจมตีใช้ในการปฏิเสธการรับส่งข้อมูล เราเห็นผู้โจมตีใช้ SSL เพื่อซ่อนกิจกรรมของพวกเขา และการโจมตีแบบสั่งการระยะไกลกำลังกลายเป็นเรื่องธรรมดามากขึ้น ในการรับส่งข้อมูลการแจ้งเตือน เราเห็นโปรโตคอล SMB/SMB2 ที่ใช้ในการดำเนินการโจมตีระยะไกล

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ตรวจสอบการรับส่งข้อมูลทั้งหมดระหว่างระบบภายในศูนย์ข้อมูลหรือบริการระบบคลาวด์ และการรับส่งข้อมูลที่ต้องการเข้าถึง
2. พัฒนากลยุทธ์การตอบสนองด้านความปลอดภัยเครือข่ายที่แข็งแกร่งตลอดทั้งปี
3. ใช้บริการรักษาความปลอดภัยระบบคลาวด์เนทีฟเพื่อใช้มาตรการรักษาความปลอดภัย Zero Trust ที่แข็งแกร่ง

ลิงค์ไปยังข้อมูลเพิ่มเติม

- ปรับปรุงการป้องกันความปลอดภัยของคุณสำหรับการโจมตีแรนซัมแวร์ด้วย Azure Firewall | บล็อก Azure และการอัปเดต | Microsoft Azure
- ศาสตร์ของการโจมตีด้วยการขยาย DDoS | บล็อก Microsoft Security
- การป้องกันแอปพลิเคชันอัจฉริยะจากขอบสู่ระบบคลาวด์ด้วย Azure Web Application Firewall | บล็อก Azure และการอัปเดต | Microsoft Azure

การพัฒนาแนวทางที่สมดุลในการรักษาความปลอดภัยข้อมูลและความยืดหยุ่นทางไซเบอร์

การเปลี่ยนแปลงทางดิจิทัลได้กระตุ้นการขยายตัวของสินทรัพย์ข้อมูลและความเสี่ยงด้านความปลอดภัย การปฏิบัติตามข้อกำหนด และความเป็นส่วนตัวที่เพิ่มขึ้น องค์กรที่มีความยืดหยุ่นทางไซเบอร์ต้องสร้างสมดุลระหว่างการลงทุนในการปกป้องข้อมูล การปฏิบัติตามข้อกำหนด และความสามารถในการกู้คืนข้อมูล และผสานรวมสิ่งเหล่านี้เข้ากับกระบวนการตอบสนองด้านกฎระเบียบเฉพาะเพื่อจัดการกับการละเมิดประเภทต่างๆ

การละเมิดข้อมูลไม่ได้ขึ้นอยู่กับว่าจะเกิดขึ้นหรือไม่ แต่จะเกิดขึ้นเมื่อใด การศึกษา “ต้นทุนของการละเมิดข้อมูลในปี 2021” ของ IBM และ Ponemon Institute รายงานต้นทุนการละเมิดข้อมูลโดยเฉลี่ยทั่วโลกอยู่ที่ 4.24 ล้านดอลลาร์สหรัฐ (เพิ่มขึ้น 10 เปอร์เซ็นต์จากปีที่แล้ว) และ 9.05 ล้านดอลลาร์สหรัฐในสหรัฐอเมริกา ความล้มเหลวในการปฏิบัติตามข้อบังคับพบว่าเป็นปัจจัยขยายต้นทุนสูงสุด ในทางกลับกัน การลดต้นทุนการละเมิดข้อมูลนั้นเกี่ยวข้องกับแนวทางปฏิบัติที่ดีที่สุด เช่น การวางแผนการตอบสนองต่อเหตุการณ์ (IR) วุฒิภาวะในการปรับใช้ Zero Trust การรักษาความปลอดภัย AI และระบบอัตโนมัติ และการใช้การเข้ารหัส

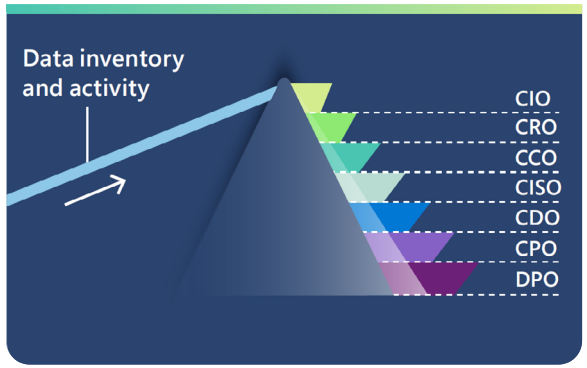
การละเมิดข้อมูลเป็นสิ่งที่หลีกเลี่ยงไม่ได้ องค์กรที่ใช้แนวทางการคืนสภาพที่สมดุลจะลดความถี่ ผลกระทบ และต้นทุนของการละเมิด

การกำกับดูแลข้อมูล ความปลอดภัย การปฏิบัติตามข้อกำหนด และความเป็นส่วนตัวนั้นพึ่งพาซึ่งกันและกัน

เราได้เห็นความโดดเด่นของการรับข้อมูลในช่วงไม่กี่ปีที่ผ่านมาในฐานะเครื่องมือสร้างมูลค่าที่สำคัญสำหรับองค์กร ในขณะเดียวกัน การเพิ่มขึ้นของกฎระเบียบด้านความเป็นส่วนตัวที่กำหนดให้ทั้งการกำกับดูแลข้อมูลและความปลอดภัยได้ทำให้เส้นแบ่งระหว่างบทบาทความเสี่ยงไม่ชัดเจน ในขณะที่บทบาทระดับ C ที่ใหม่กว่า เช่น Chief Data Officer (CDO) หรือ Chief Privacy Officers (CPO) มีส่วนได้ส่วนเสียในด้านความปลอดภัยและการปฏิบัติตามกฎระเบียบ การดำเนินการและการดำเนินงานของการปกป้องข้อมูลมักอาศัยทีมที่นำโดย Chief Information Officers (CIO) และ/หรือ Chief Information Security Officer (CISO) นี่เพียงเท่านั้น เนื่องจากการริเริ่มการกำกับดูแลข้อมูลที่นำโดย CDOs ก็มีประโยชน์ด้านความปลอดภัยเช่นกัน ผลจากการเชื่อมต่อระหว่างกันนี้ ทีมไอที การกำกับดูแลข้อมูล ความปลอดภัย การปฏิบัติตามกฎระเบียบ และความเป็นส่วนตัวจำเป็นต้องทำงานอย่างใกล้ชิดมากขึ้นเพื่อให้ได้ประสิทธิภาพและจัดการความเสี่ยง

แพลตฟอร์มการจัดการความเสี่ยงด้านข้อมูลแบบครบวงจรสำหรับพื้นที่ข้อมูลทั้งองค์กรคืออนาคต

การจัดระบบ IT การกำกับดูแลข้อมูล ความปลอดภัย การปฏิบัติตามข้อกำหนด และกระบวนการจัดการความเป็นส่วนตัวเป็นเรื่องยากในสภาพแวดล้อมของแอปพลิเคชันเฉพาะสำหรับแต่ละกฎระเบียบ และการครอบคลุมที่ไม่สอดคล้องกันทั่วทั้งองค์กรแบบไฮบริดทั่วไป การแผ่ขยายข้อมูลแบบมัลติคลาวด์ เราเชื่อว่าองค์กรต่างๆ ต้องการกระจกเพียงบานเดียวเพื่อค้นหาและรู้จักข้อมูล ปกป้องข้อมูล ควบคุมการเข้าถึง การใช้งาน และวงจรชีวิตของข้อมูล และป้องกันข้อมูลสูญหายทั่วทั้งพื้นที่เก็บข้อมูล การทำงานจากรายการข้อมูลเดียวกันและข้อมูลกิจกรรมช่วยให้กระบวนการระหว่างทีมง่ายขึ้น ให้ภาพความเสี่ยงที่ครอบคลุมมากขึ้น และช่วยให้องค์กรสามารถเตรียมการและเพิ่มประสิทธิภาพการตอบสนองต่อการละเมิดได้ดีขึ้น



“บานหน้าต่างที่ครอบคลุมเพียงบานเดียว” ควรทำหน้าที่เป็นปริซึม ทีมที่มีส่วนในการรักษาความปลอดภัยข้อมูล การปฏิบัติตามข้อกำหนด และความเป็นส่วนตัวต้องการมุมมองที่แตกต่างกันแต่สอดคล้องกันของรายการข้อมูลและกิจกรรมเดียวกันเพื่อให้สอดคล้องและทำงานร่วมกัน กิจกรรมข้อมูลรวมถึงการเข้าถึงข้อมูล การแก้ไข และเหตุการณ์การเคลื่อนไหว ซึ่งเป็นส่วนสำคัญของสมการความปลอดภัยของข้อมูล

การกำกับดูแลข้อมูลที่มีประสิทธิภาพ ความปลอดภัย การปฏิบัติตามข้อกำหนด และความเป็นส่วนตัวนั้นพึ่งพาซึ่งกันและกัน และต้องการความร่วมมือระหว่างทีม

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. สร้างความสมดุลระหว่างการป้องกันกับการกู้คืนและลดผลกระทบจากการละเมิดข้อมูลโดยการลงทุนในการปฏิบัติตามข้อกำหนด การปกป้องข้อมูล และความสามารถในการตอบสนอง
2. พัฒนาและปรับใช้กระบวนการและเครื่องมือที่ตัดความเสี่ยงของข้อมูลและครอบคลุมพื้นที่ข้อมูลทั้งหมด

ลิงค์ไปยังข้อมูลเพิ่มเติม

- Microsoft Purview—โซลูชันการปกป้องข้อมูล | Microsoft Security
- อนาคตของการปฏิบัติตามกฎระเบียบและการกำกับดูแลข้อมูลอยู่ที่นี่: ขอแนะนำ Microsoft Purview | บล็อก Microsoft Security

ความยืดหยุ่นต่อปฏิบัติการมีอิทธิพลทางไซเบอร์: มิติของมนุษย์

ในช่วงห้าปีที่ผ่านมา ความก้าวหน้าด้านกราฟิกและแมชชีนเลิร์นนิงได้นำเสนอเครื่องมือที่ใช้งานง่าย ซึ่งสามารถสร้างเนื้อหาคุณภาพสูงที่เหมือนจริงได้อย่างรวดเร็ว ซึ่งสามารถแพร่กระจายไปทั่วอินเทอร์เน็ตได้อย่างกว้างขวางภายในเวลาไม่กี่วินาที

เมื่อพูดถึงเหตุการณ์ที่รายงานผ่านเนื้อหาข้อความ เสียง และภาพ เราได้มาถึงจุดที่ทั้งมนุษย์และอัลกอริทึมไม่สามารถแยกแยะข้อเท็จจริงจากเรื่องแต่งได้อย่างน่าเชื่อถือ การเพิ่มจำนวนของเครื่องมือเหล่านี้และผลลัพธ์ทำให้เกิดข้อสงสัยเกี่ยวกับความน่าเชื่อถือของสื่อดิจิทัลทั้งหมด ขัดขวางความเข้าใจของเราเกี่ยวกับเหตุการณ์ในท้องถิ่นและโลก รูปแบบใหม่ของการดำเนินการสร้างอิทธิพลที่เกิดจากความก้าวหน้าทางเทคโนโลยีมีนัยยะสำคัญต่อกระบวนการประชาธิปไตย[11]

คำถามเกิดขึ้นเกี่ยวกับสิ่งที่เราสามารถทำได้เพื่อเตรียมพร้อมสำหรับอนาคตที่ยืดหยุ่นมากขึ้นในการต่อต้านการดำเนินการที่มีอิทธิพลทางไซเบอร์เหล่านี้ เทคโนโลยีเป็นเพียงส่วนหนึ่งของปริศนา ต้องใช้ความพยายามหลายด้าน รวมถึงการศึกษาที่มุ่งเป้าไปที่การรู้เท่าทันสื่อ การตระหนักรู้ และการระแวดระวัง การลงทุนด้านสื่อสารมวลชนที่มีคุณภาพ โดยมีผู้รายงานที่เชื่อถือได้ในเหตุการณ์ เครือข่ายระดับท้องถิ่น ระดับชาติ และระดับนานาชาติในการแบ่งปันและแจ้งเตือนเกี่ยวกับปฏิบัติการใช้อิทธิพล และรูปแบบใหม่ๆ ของกฎระเบียบที่ลงโทษผู้ประสงค์ร้ายที่สร้างหรือดัดแปลงสื่อดิจิทัลโดยมีวัตถุประสงค์เพื่อหลอกลวง



นอกจากนี้ เรายังตระหนักดีว่าการฟื้นฟูความไว้วางใจในเนื้อหาดิจิทัลเป็นเป้าหมายที่ทะเยอทะยานซึ่งต้องการมุมมองและการมีส่วนร่วมที่หลากหลาย ไม่มีบริษัท สถาบัน หรือรัฐบาลแห่งใดที่สามารถแก้ไขภัยคุกคามเหล่านี้ได้ด้วยตนเอง สุดยอดพลังของเราในฐานะมนุษย์คือความสามารถของเราในการทำงานร่วมกันและความร่วมมือ สิ่งนี้มีความสำคัญเป็นพิเศษในขณะนี้ เพราะทุกคน—รัฐบาลทั่วโลก อุตสาหกรรม สถาบันการศึกษา และโดยเฉพาะอย่างยิ่งองค์กรข่าว สังคม และสื่อ—ทำงานร่วมกันเพื่อพัฒนาสังคมให้ดีขึ้นและมีสุขภาพดี

ลิงค์ไปยังข้อมูลเพิ่มเติม

- แอปพลิเคชันสำหรับปัญญาประดิษฐ์ในภารกิจไซเบอร์ของกระทรวงกลาโหม | Microsoft On the Issues
- ปัญญาประดิษฐ์และความปลอดภัยทางไซเบอร์: ความท้าทายที่เพิ่มขึ้นและทิศทางที่มีแนวโน้ม การรับฟังเกี่ยวกับการประยุกต์ใช้ปัญญาประดิษฐ์เพื่อปฏิบัติการในไซเบอร์สเปซต่อหน้าคณะอนุกรรมการด้านความปลอดภัยทางไซเบอร์ของคณะกรรมการบริการด้านอาวุธวุฒิสภา รัฐสภา ชุดที่ 117 (3 พฤษภาคม 2022 คำให้การของ Eric Horvitz)

การเสริมสร้างปัจจัยมนุษย์ด้วยทักษะ

การจัดการกับปัจจัยมนุษย์เป็นองค์ประกอบสำคัญของกลยุทธ์ทักษะความปลอดภัยทางไซเบอร์ จากการศึกษาการรักษาความปลอดภัยของระบบไอทีของ Kaspersky Human Factor[12] 46 เปอร์เซ็นต์ของเหตุการณ์ด้านความปลอดภัยทางไซเบอร์เกี่ยวข้องกับพนักงานที่ขาดความระมัดระวังหรือในเครื่องแบบที่อำนวยความสะดวกในการโจมตีโดยไม่ได้ตั้งใจ

ทีมการศึกษาและการรับรู้ของ Microsoft ในองค์กร Digital Security and Resilience มีหน้าที่รับผิดชอบในการป้องกันปัจจัยมนุษย์ในการรักษาความปลอดภัยทางไซเบอร์โดยให้อำนาจแก่พนักงานในการรักษาความปลอดภัยให้กับระบบและข้อมูลของเราเองและของลูกค้า เป้าหมายของเราคือ:

- ลดความเสี่ยงของ Microsoft และลูกค้าของเราด้วยการสร้างชุดทักษะการรักษาความปลอดภัยหลักทั่วทั้งองค์กรแบบรวมศูนย์กับพนักงานทั้งหมด
- เสริมสร้างความรู้ด้านความปลอดภัยของพนักงานผ่านแนวทางการเสริมแรงแบบหลายขั้นตอนเพื่อสนับสนุนผลลัพธ์พฤติกรรมที่ต้องการ
- ส่งเสริมการเปลี่ยนแปลงวัฒนธรรมโดยทำให้ความคิดด้านความปลอดภัยเป็นส่วนสำคัญของวัฒนธรรมของ Microsoft ผ่านการฝึกอบรมและกิจกรรมด้านความปลอดภัยที่จำเป็นประจำปี
- ส่งเสริมทรัพยากรบนเว็บแบบรวมศูนย์แบบครบวงจรสำหรับแนวทางปฏิบัติที่ดีที่สุด ข้อมูลนโยบายบริษัท และการรายงานเหตุการณ์สำหรับทุกสิ่งที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

โปรแกรมทักษะการรักษาความปลอดภัยทางไซเบอร์แบบรวมศูนย์ที่ตรงเป้าหมายเข้าถึงพนักงาน Microsoft ทุกคนอย่างน้อยปีละครั้ง ข้อเสนอการฝึกอบรมได้รับการปรับให้เหมาะสมเพื่อสนับสนุนความคิดริเริ่มด้านความปลอดภัยทางไซเบอร์ในปัจจุบันและส่งมอบผลลัพธ์พฤติกรรมที่วัดได้ สภาบริหารความเสี่ยงด้านข้อมูล (IRMC) ของ Microsoft มีบทบาทสำคัญในการระบุผลลัพธ์การเปลี่ยนแปลงพฤติกรรมความปลอดภัยในโลกไซเบอร์ที่สำคัญซึ่งจะได้รับการจัดการโดยการฝึกอบรม

ด้วยโปรแกรมทักษะความปลอดภัยทางไซเบอร์ทั้งหมดของเรา เราจะวัดประสิทธิภาพ ประสิทธิผล และผลลัพธ์ของโซลูชันหากเป็นไปได้ ตัวอย่างเช่น ข้อเสนอทักษะภัยคุกคามจากวงในของเรามีการปฏิบัติตามการฝึกอบรม 95 เปอร์เซ็นต์ ความพึงพอใจของผู้เรียนที่ยอดเยี่ยม และส่งผลให้ผู้จัดการเพิ่มขึ้นอย่างมากในการรายงานกรณีภัยคุกคามจากวงในที่เป็นไปได้ผ่านเครื่องมือ Report It Now ของบริษัท โปรแกรมประกอบด้วย:

พื้นฐานด้านความปลอดภัย: การฝึกอบรมการตระหนักรู้ด้านความปลอดภัยในโลกไซเบอร์แบบรวมศูนย์และการปฏิบัติตามกฎระเบียบ ซึ่งระบุหลักปฏิบัติด้านความปลอดภัยและความเป็นส่วนตัว ชุดการฝึกอบรมที่ได้รับการคาดหวังสูงนี้ใช้โมเดลความบันเทิงเพื่อทำให้การเรียนรู้เกี่ยวกับความปลอดภัยในโลกไซเบอร์มีส่วนร่วมและน่าสนใจ

การพัฒนา: การฝึกอบรมทางเทคนิคที่จำเป็นของ Microsoft สำหรับวิศวกรที่สร้างและดูแลโซลูชันสายงานธุรกิจ การฝึกอบรมที่ได้รับเชิญเท่านั้นนี้จะกล่าวถึงแนวทางปฏิบัติที่ดีที่สุดด้านสุขอนามัยความปลอดภัยในโลกไซเบอร์ในเวลาที่เหมาะสมและมีความสำคัญ และใช้รูปแบบการจัดส่งแบบไฮบริดสดที่ปรับให้เหมาะกับความต้องการของผู้ชม

โปรแกรมเฉพาะ: โปรแกรมการฝึกอบรมที่ตรงเป้าหมายสนับสนุนความคิดริเริ่มด้านความปลอดภัยทางไซเบอร์เฉพาะ เช่น Shadow IT, Insider Threat และ Microsoft Federal ข้อเสนอเหล่านี้ผสานรวมเข้ากับกลยุทธ์การมีส่วนร่วมโดยรวมอย่างแนบแน่นสำหรับโครงการริเริ่มด้านความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องผ่านการสนับสนุนของผู้บริหารและการรายงานดัชนีชี้วัดเพื่อป้องกันไม่ให้แนวทางการฝึกอบรม "ทำเครื่องหมายในกล่อง"

MSProtect: ทรัพยากรบนเว็บแบบรวมศูนย์ของ Microsoft ให้แนวทางปฏิบัติที่ดีที่สุด ข้อมูลนโยบายบริษัท และการรายงานเหตุการณ์สำหรับทุกสิ่งที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ทรัพยากรตามความต้องการนี้เป็นเป้าหมายสำหรับพนักงานนอกเหนือจากข้อเสนอการฝึกอบรมอย่างเป็นทางการ

> ทักษะการรักษาความปลอดภัยจะต้องไม่ถูกมองว่าเป็นกิจกรรมการทำเครื่องหมายในกล่อง แต่ให้เน้นที่การเปลี่ยนแปลงพฤติกรรมเพื่อให้ติดตามผลได้ทั่วทั้งพฤติกรรมเป้าหมายที่ระบุ และสร้างระบบการรับฟังเพื่อกำหนดผลกระทบของข้อเสนอ

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. ให้การฝึกอบรมด้านความปลอดภัยและทรัพยากรแก่พนักงานในเวลาและที่ที่พวกเขาต้องการ
2. พัฒนากลยุทธ์ทักษะแบบรวมศูนย์ที่แจ้งโดยผู้มีส่วนได้ส่วนเสียจากทั่วทั้งองค์กร
3. ตรวจสอบให้แน่ใจว่ามีการติดตามและวิเคราะห์ผลกระทบของการฝึกอบรมในด้านประสิทธิภาพ (ปริมาณ) ประสิทธิผล (คุณภาพ) และผลลัพธ์ (ผลกระทบทางธุรกิจ)

ลิงค์ไปยังข้อมูลเพิ่มเติม

- Microsoft เปิดตัวความคิดริเริ่มทักษะขั้นต่อไปหลังจากช่วยเหลือผู้คนกว่า 30 ล้านคน

ข้อมูลเชิงลึกจากโปรแกรมกำจัดแรนซัมแวร์ของเรา

Microsoft ได้ใช้การเดินทาง[13] Zero Trust ของตนเอง ในช่วงห้าปีที่ผ่านมาเพื่อให้มั่นใจถึงตัวตน และอุปกรณ์ได้รับการจัดการอย่างดีและมีประสิทธิภาพ ในขณะที่ความเสี่ยงของแรนซัมแวร์เพิ่มมากขึ้น เราได้พัฒนามุมมองเชิงลึกเพื่อสนับสนุนแนวทางของเราในการปกป้องตนเองและลูกค้าของเรา

หลังจากการประเมินภายในในเชิงลึก เราได้สร้างโปรแกรมกำจัดแรนซัมแวร์เพื่อแก้ไขช่องว่างในการควบคุมและความครอบคลุม มีส่วนร่วมในการปรับปรุงคุณสมบัติสำหรับบริการต่างๆ เช่น Defender for Endpoint, Azure และ M365 และพัฒนา playbooks สำหรับ SOC และทีมวิศวกรรมของเราเกี่ยวกับวิธีการ เพื่อกู้คืนในกรณีที่มีการโจมตีของแรนซัมแวร์

ขั้นตอนแรกคือการทำความเข้าใจขอบเขตของการป้องกันของเราจากการโจมตีของแรนซัมแวร์ที่มุ่งเป้าไปที่ Microsoft มีความพยายามอย่างดีอยู่แล้วในการปรับใช้ Defender for Endpoint และเพื่อให้แน่ใจว่าอุปกรณ์ทั้งหมดได้รับการจัดการและเป็นไปตามนโยบาย Zero Trust ของเรา แต่เราจำเป็นต้องหาวิธีทำความเข้าใจทุกแง่มุมของคำถามที่ใหญ่กว่าว่าเราจะสามารถกู้คืนจากการโจมตีได้อย่างมีประสิทธิภาพหรือไม่ เพื่อให้ได้รับข้อมูลเชิงลึก เราได้ประเมิน NIST 8374: การจัดการความเสี่ยงแรนซัมแวร์: โปรไฟล์ Cybersecurity Framework (CSF)[14] ซึ่งสอดคล้องกับนโยบายองค์กรโดยรวมของเราเทียบกับรายการควบคุมที่เราทราบ การวิเคราะห์นี้ระบุช่องว่างในความครอบคลุมอย่างรวดเร็ว

ต่อไป เราจัดลำดับความสำคัญของช่องว่างระหว่างฟังก์ชันระบุ ตรวจหา ป้องกัน ตอบสนอง และกู้คืนของ CSF เราพบความสอดคล้องเชิงกลยุทธ์กับ Zero Trust และโปรแกรมอื่นๆ และยังค้นพบช่องว่างที่ไม่มีกระแสงานที่มีอยู่ หลังจากประเมินปริมาณงานและความพยายามที่จำเป็นในการแก้ไขช่องว่างเหล่านี้แล้ว เราได้แยกออกเป็นสองเสาหลัก:

- **ปกป้ององค์กร (PtE):** กำหนดรายการงานที่เราต้องทำในฐานะองค์กรเพื่อป้องกันตนเองและสามารถกู้คืนจากการโจมตีได้ หากสำเร็จ
- **ปกป้องลูกค้า (PtC):** สร้างความสามารถในข้อเสนอของเราเพื่อปกป้องลูกค้าและธุรกิจของเรา

การฝังการค้นพบไว้ในองค์กรของเราเอง

เพื่อแก้ไขความเสี่ยงสูงสุดและปกป้องบริการที่สำคัญของเราจากการโจมตีของแรนซัมแวร์ เราวางแผนที่จะเน้นการลงทุนในช่วง 6 ถึง 12 เดือนข้างหน้าเพื่อบรรลุสถานการณ์ห้าประการด้านล่างซึ่งเป็นส่วนหนึ่งของโปรแกรมแรนซัมแวร์โดยเฉพาะ เมื่อเราประสบความสำเร็จในแต่ละสถานการณ์ เราจะค่อยๆ ขยายขอบเขตของโปรแกรมให้เข้าถึงทุกส่วนขององค์กร

สถานการณ์ที่ 1: สมาชิกในทีมรักษาความปลอดภัยเข้าใจถึงความเสี่ยงโดยรวมที่เกี่ยวข้องกับการโจมตีแรนซัมแวร์ และมีกระบวนการที่จัดตั้งขึ้นเพื่อให้ผู้บริหารตระหนักถึงช่องว่างในการควบคุมและสถานะความเสี่ยง

สถานการณ์ที่ 2: สมาชิกในทีมรักษาความปลอดภัยสามารถเข้าถึง playbooks ที่ออกแบบมาเพื่อช่วยให้พวกเขาและทีมอื่นๆ ภายใน Microsoft ตอบสนองและกู้คืนบริการที่สำคัญจากการโจมตีของแรนซัมแวร์

สถานการณ์ที่ 3: สมาชิกในทีม Enterprise Resilience มีมาตรฐานในการสำรองข้อมูลระบบที่สำคัญ เพลย์บุ๊คมีอยู่ และมีการสำรองและกู้คืนข้อมูลเป็นประจำเพื่อให้แน่ใจว่าข้อมูลสามารถกู้คืนได้ในกรณีที่มีการโจมตีแรนซัมแวร์

สถานการณ์ที่ 4: เจ้าของบริการเข้าใจและนำนโยบายและการควบคุมด้านความปลอดภัยและการปฏิบัติงานที่จำเป็นไปใช้เพื่อปกป้องบริการ ข้อมูลลูกค้า อุปกรณ์ปลายทาง และสินทรัพย์เครือข่ายจากการโจมตีของแรนซัมแวร์ โดยมุ่งเน้นเป็นพิเศษในบริการที่จัดลำดับความสำคัญเป็นบริการที่สำคัญของ Microsoft

สถานการณ์ที่ 5: พนักงานทุกคนสามารถเข้าถึงทรัพยากรด้านการศึกษาและการฝึกอบรมที่อธิบายวิธีรับรู้การโจมตีของแรนซัมแวร์และวิธีแจ้งทีมรักษาความปลอดภัยและเริ่มการตอบสนอง

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

1. จัดทำเอกสารและตรวจสอบกิจกรรมการกู้คืนและการแก้ไขแบบครบวงจรที่เกี่ยวข้องกับการโจมตีของแรนซัมแวร์กับบริการที่สำคัญ
2. ให้ผู้มีส่วนได้ส่วนเสียมีส่วนร่วมในการอัปเดตคู่มือของ Enterprise Crisis Management เพื่อรวมกิจกรรมเฉพาะของแรนซัมแวร์และกระบวนการตัดสินใจและคำแนะนำเพื่อพิจารณาว่า/เมื่อใดควรจ่ายเงินสำหรับแรนซัมแวร์
3. ปรับปรุงการตรวจจับและความคุ้มครองโดยเปิดใช้งานความสามารถที่มีอยู่ในผลิตภัณฑ์รักษาความปลอดภัยที่ใช้งานของคุณ (เช่น Defender for Endpoint Attack Surface Reduction Rules)
4. ทำงานร่วมกับทีมมาตรฐานความปลอดภัยเพื่อกำหนดพื้นฐานสำหรับการป้องกันการโจมตีจากแรนซัมแวร์ และให้การฝึกอบรมและจัดทำเอกสารแก่ทีมวิศวกรรมเกี่ยวกับวิธีป้องกันการโจมตีจากแรนซัมแวร์
5. นำระบบอัตโนมัติมาใช้เพื่อทำให้การปรับใช้นโยบายความปลอดภัยและการดำเนินงานง่ายขึ้นในทีม DevOps และตรวจสอบให้แน่ใจว่าหากระบบไม่เป็นไปตามข้อกำหนด ระบบจะตั้งค่าสถานะและแก้ไขอย่างรวดเร็ว

ลิงค์ไปยังข้อมูลเพิ่มเติม

- การแบ่งปันวิธีที่ Microsoft ป้องกันแรนซัมแวร์ | Microsoft Inside Track

ดำเนินการในขณะนี้เกี่ยวกับผลกระทบด้านความปลอดภัยควอนตัม

แรงกดดันอยู่ที่การจัดการภัยคุกคามการประมวลผลควอนตัมที่ก่อให้เกิดการเข้ารหัสในปัจจุบันและทุกอย่างที่ป้องกัน บันทึกข้อตกลงที่ออกเมื่อเร็วๆ นี้ว่าด้วยการปรับปรุงความปลอดภัยทางไซเบอร์ของกระทรวงกลาโหมและระบบชุมชนข่าวกรอง[15] สร้างขึ้นจากคำสั่งผู้บริหารสหรัฐฯ 10428[16] สำหรับการปรับปรุงความปลอดภัยทางไซเบอร์ของประเทศ เน้นความปลอดภัยของซอฟต์แวร์ซัพพลายเชนว่ามีความสำคัญอย่างยิ่งต่อการจัดการกับการโจมตีของรัฐชาติในอนาคต

คอมพิวเตอร์ควอนตัมคืออะไร

คอมพิวเตอร์ควอนตัมเป็นเครื่องจักรที่ใช้คุณสมบัติของฟิสิกส์ควอนตัมเพื่อเก็บข้อมูลและทำการคำนวณ สิ่งนี้สามารถเป็นประโยชน์อย่างยิ่งสำหรับงานบางอย่างซึ่งสามารถทำงานได้ดีกว่าแม้แต่ซูเปอร์คอมพิวเตอร์ที่ดีที่สุดของเรา การประมวลผลแบบควอนตัมกำลังเปิดขอบเขตใหม่สำหรับการเข้ารหัสและการประมวลผลข้อมูล การศึกษาคาดการณ์ว่าการประมวลผลควอนตัมจะกลายเป็นอุตสาหกรรมควอนตัมมูลค่าหลายพันล้านดอลลาร์ (USD) อย่างเร็วที่สุดในปี 2030[17] อันที่จริง การประมวลผลควอนตัมและการสื่อสารควอนตัมพร้อมที่จะสร้าง ความเปลี่ยนแปลง ในอุตสาหกรรมต่างๆ มากมาย ตั้งแต่การดูแลสุขภาพและพลังงาน ไปจนถึงการเงินและความปลอดภัย

การประมวลผลควอนตัมเป็นภัยคุกคามต่อการเข้ารหัสในปัจจุบันและทุกสิ่งที่ปกป้อง

ภัยคุกคามต่อการเข้ารหัสในปัจจุบัน

ด้วยอัลกอริทึมของ Shor ในปี 1994 และคอมพิวเตอร์ควอนตัมในระดับอุตสาหกรรมที่มีคิวบิตเชิงกายภาพมากกว่าสองสามล้านชุด อัลกอริทึมการเข้ารหัสคีย์สาธารณะที่ใช้กันอย่างแพร่หลายในปัจจุบันทั้งหมดอาจเสียหายได้อย่างมีประสิทธิภาพ สิ่งสำคัญคือต้องพิจารณา ประเมิน และสร้างมาตรฐานระบบเข้ารหัสลับที่ “ปลอดภัยด้วยควอนตัม” ที่มีประสิทธิภาพ คล่องตัว และปลอดภัยจากการโจมตีด้วยควอนตัมของฝ่ายตรงข้าม การโยกย้ายซอฟต์แวร์ไปยัง “การเข้ารหัสภายหลังควอนตัม” ซึ่งก็คืออัลกอริธึมและโปรโตคอลแบบคลาสสิกที่มีอยู่ซึ่งแข็งแกร่งต่อการโจมตีด้วยควอนตัม จะใช้เวลาหลายปี—หากไม่ใช่หนึ่งทศวรรษหรือมากกว่านั้น—กว่าจะบรรลุผลสำเร็จ[18]

ซึ่งหมายความว่าแรงกดดันอยู่ที่การจัดการภัยคุกคามที่ก่อให้เกิดการเข้ารหัสในปัจจุบันและทุกอย่างที่ป้องกัน ผู้ไม่หวังดีสามารถบันทึกข้อมูลที่เข้ารหัสได้ในขณะนี้และใช้ประโยชน์ในภายหลังเมื่อมีคอมพิวเตอร์ควอนตัม การรอให้การประมวลผลควอนตัมมาถึงก่อนที่จะจัดการกับนัยของการเข้ารหัสจะสายเกินไป

เนื่องจากมีการใช้การเข้ารหัสทั่วทั้งระบบนิเวศไซเบอร์ ซึ่งหมายความว่าบริการรักษาความปลอดภัยที่ใช้การเข้ารหัสของเราอาจถูกบุกรุกได้ ตัวอย่างเช่น บริการนี้รวมถึงบริการสำหรับการสื่อสาร (TLS, IPSec) การส่งข้อความ (อีเมล การประชุมทางเว็บ) การจัดการข้อมูลประจำตัวและการเข้าถึง การเรียกดูเว็บ การลงนามรหัส ธุรกรรมการชำระเงิน และบริการอื่นๆ ที่ขึ้นอยู่กับการเข้ารหัสเพื่อป้องกัน

เมื่อคอมพิวเตอร์ควอนตัมกลายเป็นจริง ส่วนประกอบซอฟต์แวร์ของบุคคลที่สามที่มีการใช้งานอัลกอริทึมการเข้ารหัสและความสามารถก็ต้องการการตรวจสอบเพิ่มเติมเช่นกัน สิ่งนี้กำหนดให้ทุกองค์กรในห่วงโซ่คุณค่าต้องทำส่วนของตนเพื่อให้แน่ใจว่าห่วงโซ่มีความปลอดภัย องค์กรอุตสาหกรรมและรัฐบาลกำลังเพิ่มความพยายามในการกำหนดข้อกำหนดด้านความปลอดภัยของห่วงโซ่อุปทานของซอฟต์แวร์ และในบางกรณี การแนะนำข้อบังคับใหม่สำหรับการรักษาความปลอดภัยของห่วงโซ่อุปทาน บันทึกข้อตกลงความมั่นคงแห่งชาติ NSM-8[19] กำหนดข้อกำหนดและลำดับเวลาสำหรับการนำการเข้ารหัสหลังควอนตัมไปใช้ในระบบความมั่นคงแห่งชาติ (NSS) โดยเรียกร้องให้มีการกำหนดเวลาภายใน 180 วันสำหรับ "การวางแผนการปรับปรุงให้ทันสมัย การใช้การเข้ารหัสที่ไม่รองรับ โปรโตคอลเฉพาะของภารกิจที่ได้รับอนุมัติ โปรโตคอลการต้านทานควอนตัม และการวางแผนสำหรับการใช้การเข้ารหัสที่ต้านทานควอนตัมหากจำเป็น"

การกำหนดมาตรฐานเป็นกิจกรรมที่ต้องใช้เวลานานในการเปลี่ยนไปใช้การเข้ารหัสที่ปลอดภัยด้วยควอนตัม หน่วยงานมาตรฐานที่ทำงานบนมาตรฐานโดยใช้การเข้ารหัสคีย์สาธารณะจะต้องเริ่มทำการทดลองและปรับให้เข้ากับอัลกอริทึมหลังควอนตัมทันที

อัลกอริธึมการเข้ารหัสหลังควอนตัม (PQC) ใหม่ ซึ่งเป็นอัลกอริทึมแบบคลาสสิกที่คิดว่าแข็งแกร่งต่อการโจมตีด้วยควอนตัม กำลังอยู่ระหว่างการตรวจสอบผ่านโครงการมาตรฐานหลังควอนตัมของ NIST[20] งานนี้จะมีอิทธิพลต่อความพยายามระดับโลกภายในหน่วยงานมาตรฐาน แม้ว่าจะมีความทับซ้อนกับการเลือกอัลกอริทึมของรัฐบาลสหรัฐฯ แต่การเลือกหน่วยงาน/หน่วยงานกำกับดูแลในระดับประเทศที่แตกต่างกันสำหรับอัลกอริทึมที่สอดคล้องกันอาจก่อให้เกิดความท้าทายในระดับสากล การกระจายตัวนี้จะทำให้วิศวกรรมผลิตภัณฑ์และบริการซับซ้อนขึ้น

อัลกอริธึมการเข้ารหัสหลังควอนตัมใหม่อยู่ระหว่างการตรวจสอบผ่านโปรแกรมมาตรฐานการเข้ารหัสหลังควอนตัมของ NIST งานนี้จะมีอิทธิพลต่อความพยายามระดับโลกภายในหน่วยงานมาตรฐาน

ข้อมูลเชิงลึกที่ใช้ปฏิบัติได้จริง

นอกเหนือจาก SAFECode และสมาชิกที่เป็นพันธมิตรแล้ว อุตสาหกรรมควรดำเนินกิจกรรมระยะสั้นในทันทีเพื่อเตรียมพร้อมสำหรับการเปลี่ยนแปลง PQC[21] ซึ่งเหล่านี้รวมถึง:

1. ใช้รายการผลิตภัณฑ์/รหัสของคุณที่ใช้การเข้ารหัส
2. ใช้กลยุทธ์ความคล่องตัวของการเข้ารหัสทั่วทั้งองค์กรของคุณ ซึ่งรวมถึงการลดจำนวนโค้ดที่จำเป็นเมื่อมีการเปลี่ยนแปลงการเข้ารหัส
3. นำร่องการใช้อัลกอริทึมที่ปลอดภัยด้วยควอนตัมของผู้สมัครในผลิตภัณฑ์หรือบริการของคุณที่ใช้การเข้ารหัส
4. เตรียมพร้อมที่จะใช้อัลกอริธึมคีย์สาธารณะที่แตกต่างกันสำหรับการเข้ารหัส การแลกเปลี่ยนคีย์ และลายเซ็น
5. ทดสอบแอปพลิเคชันของคุณเพื่อดูผลกระทบของขนาดคีย์ การเข้ารหัส และลายเซ็นที่ใหญ่มาก

ลิงค์ไปยังข้อมูลเพิ่มเติม

- Microsoft ได้สาธิตฟิสิกส์พื้นฐานที่จำเป็นสำหรับการสร้าง qubit | Microsoft Research

การผสานรวมธุรกิจ ความปลอดภัย และ IT เพื่อความยืดหยุ่นที่มากขึ้น

ความยืดหยุ่นทางไซเบอร์ที่แข็งแกร่งนั้นขึ้นอยู่กับผู้นำทางธุรกิจที่ทำงานร่วมกับทีมรักษาความปลอดภัยเพื่อใช้การรักษาความปลอดภัยจากประสบการณ์ของ Microsoft ความเป็นผู้นำด้านความปลอดภัยถือเป็นวินัยที่ท้าทายซึ่งต้องการการสนับสนุนจากผู้นำองค์กรเพื่อปกป้ององค์กรอย่างมีประสิทธิภาพสูงสุด

ผู้นำด้านความปลอดภัยจะรับมือกับความท้าทายแบบไดนามิกที่ครอบคลุมหัวข้อต่างๆ ที่เกี่ยวข้องกับความเสี่ยง เทคโนโลยี เศรษฐศาสตร์ กระบวนการขององค์กร โมเดลธุรกิจ การเปลี่ยนแปลงวัฒนธรรม ผลประโยชน์ทางภูมิรัฐศาสตร์ การจารกรรม และการปฏิบัติตามมาตรการคว่ำบาตรระหว่างประเทศ แต่ละข้อมีความแตกต่างที่ต้องทำความเข้าใจและจัดการอย่างใกล้ชิด

ผู้นำด้านความปลอดภัยยังได้รับมอบหมายให้ขัดขวางทั้งผู้โจมตีมนุษย์ที่ชาญฉลาด ได้รับทุนสนับสนุนอย่างดี และมีแรงจูงใจสูง ตลอดจนอาชญากรไซเบอร์ที่มีทักษะต่ำแต่มีประสิทธิภาพ ทีมของพวกเขาต้องปกป้องพื้นที่ทางเทคนิคที่ซับซ้อนซึ่งมักสร้างขึ้นทีละน้อยเป็นเวลากว่า 30 ปีหรือมากกว่านั้น เมื่อความปลอดภัยมีความสำคัญต่ำหรือไม่มีเลย การตัดสินใจเมื่อหลายปีก่อนอาจก่อให้เกิดความเสี่ยงในวันนี้ จนกว่าเราจะชำระหนี้ทางเทคนิคและแก้ไขช่องว่างในการรักษาความปลอดภัย

ผู้นำองค์กรและผู้กำหนดนโยบายสามารถมีผลกระทบเชิงบวกอย่างมีนัยสำคัญต่อการรักษาความปลอดภัยโดยการสนับสนุนผู้นำด้านการรักษาความปลอดภัยอย่างแข็งขันและช่วยสร้างสะพานเชื่อมระหว่างการรักษาความปลอดภัยแบบรวมและส่วนอื่นๆ ขององค์กร เมื่อ Microsoft ทำงานร่วมกับลูกค้าที่มีความสอดคล้องกัน เราจะเห็นพวกเขาสร้างองค์กรที่ยืดหยุ่นมากขึ้น และยังปรับปรุงความสามารถในการปรับตัวและสร้างสรรค์สิ่งใหม่ๆ

ผู้นำในองค์กรสามารถสนับสนุนผู้นำด้านการรักษาความปลอดภัยโดยมุ่งเน้นไปที่สามส่วนหลัก:

1. สร้างความปลอดภัยด้วยการออกแบบ

บางครั้งการรักษาความปลอดภัยถูกมองว่าเป็นอุปสรรคหรือความคิดภายหลังในกระบวนการทางธุรกิจ มักจะถูกพิจารณาในการตัดสินใจก็ต่อเมื่อสายเกินไปที่จะหลีกเลี่ยงความเสี่ยงหรือแก้ไขอย่างถูกวิธีและง่ายดาย

ผู้นำองค์กรและผู้กำหนดนโยบายควรตรวจสอบให้แน่ใจว่า:

รวมการรักษาความปลอดภัยในช่วงต้นของความคิดริเริ่มใหม่ ความคิดริเริ่มด้านดิจิทัลใหม่และการนำระบบคลาวด์มาใช้ควรให้ความสำคัญกับความปลอดภัยเพื่อให้แน่ใจว่าความเสี่ยงขององค์กรจะไม่เพิ่มขึ้นตามแอปพลิเคชันใหม่หรือความสามารถด้านดิจิทัลแต่ละรายการ เมื่อรวมการรักษาความปลอดภัยที่เชื่อถือได้แล้ว คุณสามารถใช้กระบวนการเหล่านั้นเพื่อปรับปรุงระบบเดิมให้ทันสมัยเพื่อรับทั้งความปลอดภัยและประโยชน์ด้านประสิทธิภาพในเวลาเดียวกัน

ปรับการบำรุงรักษาเชิงป้องกันให้เป็นมาตรฐานเพื่อความปลอดภัย ตรวจสอบให้แน่ใจว่าการบำรุงรักษาความปลอดภัยขั้นพื้นฐาน เช่น การใช้การอัปเดตความปลอดภัยและแพตช์และการกำหนดค่าที่ปลอดภัย มีการจัดสรรการสนับสนุนองค์กรอย่างเต็มรูปแบบ (รวมถึงงบประมาณ การหยุดทำงานตามกำหนดเวลา ข้อกำหนดการได้มาสำหรับการสนับสนุนผลิตภัณฑ์ของผู้ขาย)

น่าเสียดายที่หลายองค์กรชะลอ เลื่อนเวลา หรือใช้แนวทางปฏิบัติทั่วไปเหล่านี้เพียงบางส่วนเท่านั้น สิ่งนี้เปิดโอกาสให้ผู้โจมตีสามารถใช้ประโยชน์ได้อย่างกว้างขวาง ความจำเป็นในการปรับมาตรฐานความปลอดภัยให้อยู่ใน US NIST 800-40[22]

2. มีส่วนร่วมกับการรักษาความปลอดภัย

ผู้นำองค์กรควรมีส่วนร่วมอย่างแข็งขันและสนับสนุนกระบวนการรักษาความปลอดภัยที่สำคัญเพื่อให้แน่ใจว่ามีการจัดลำดับความสำคัญของทรัพยากรและเตรียมพร้อมสำหรับภัยพิบัติด้านความปลอดภัย ซึ่งรวมถึงการมีส่วนร่วมใน:

ระบุสินทรัพย์ทางธุรกิจที่สำคัญ ผู้นำและทีมด้านความปลอดภัยจำเป็นต้องรู้ว่าสินทรัพย์ใดมีความสำคัญต่อธุรกิจ เพื่อมุ่งเน้นทรัพยากรด้านความปลอดภัยไปยังสิ่งที่สำคัญที่สุด ซึ่งมักจะเป็นการฝึกปฏิบัติใหม่ที่รวมถึงการถามและตอบคำถามใหม่ๆ ที่ยังไม่ได้รับการกล่าวถึงก่อนหน้านี้

ความต่อเนื่องทางธุรกิจด้านความปลอดภัยทางไซเบอร์และการฝึกปฏิบัติการกู้คืนความเสียหาย การโจมตีทางไซเบอร์อาจกลายเป็นเหตุการณ์สำคัญที่ขัดขวางหรือหยุดการดำเนินธุรกิจส่วนใหญ่หรือทั้งหมด การดูแลทีมงานทั่วทั้งองค์กรให้เตรียมพร้อมรับมือกับสถานการณ์เหล่านี้ จะช่วยลดเวลาในการฟื้นฟูการดำเนินธุรกิจ จำกัดความเสียหายต่อองค์กร และช่วยรักษาความไว้วางใจและความเชื่อมั่นของลูกค้า ประชาชน และองค์ประกอบ สิ่งนี้ควรรวมเข้ากับความต่อเนื่องทางธุรกิจที่มีอยู่และกระบวนการกู้คืนระบบ

การตัดสินใจความเสี่ยงด้านความปลอดภัยทำได้ดีที่สุดโดยเจ้าของธุรกิจหรือภารกิจที่สามารถมองเห็นความเสี่ยงและโอกาสทั้งหมดได้อย่างเต็มที่



การผสานรวมธุรกิจ ความปลอดภัย และ IT เพื่อความยืดหยุ่นที่มากขึ้น

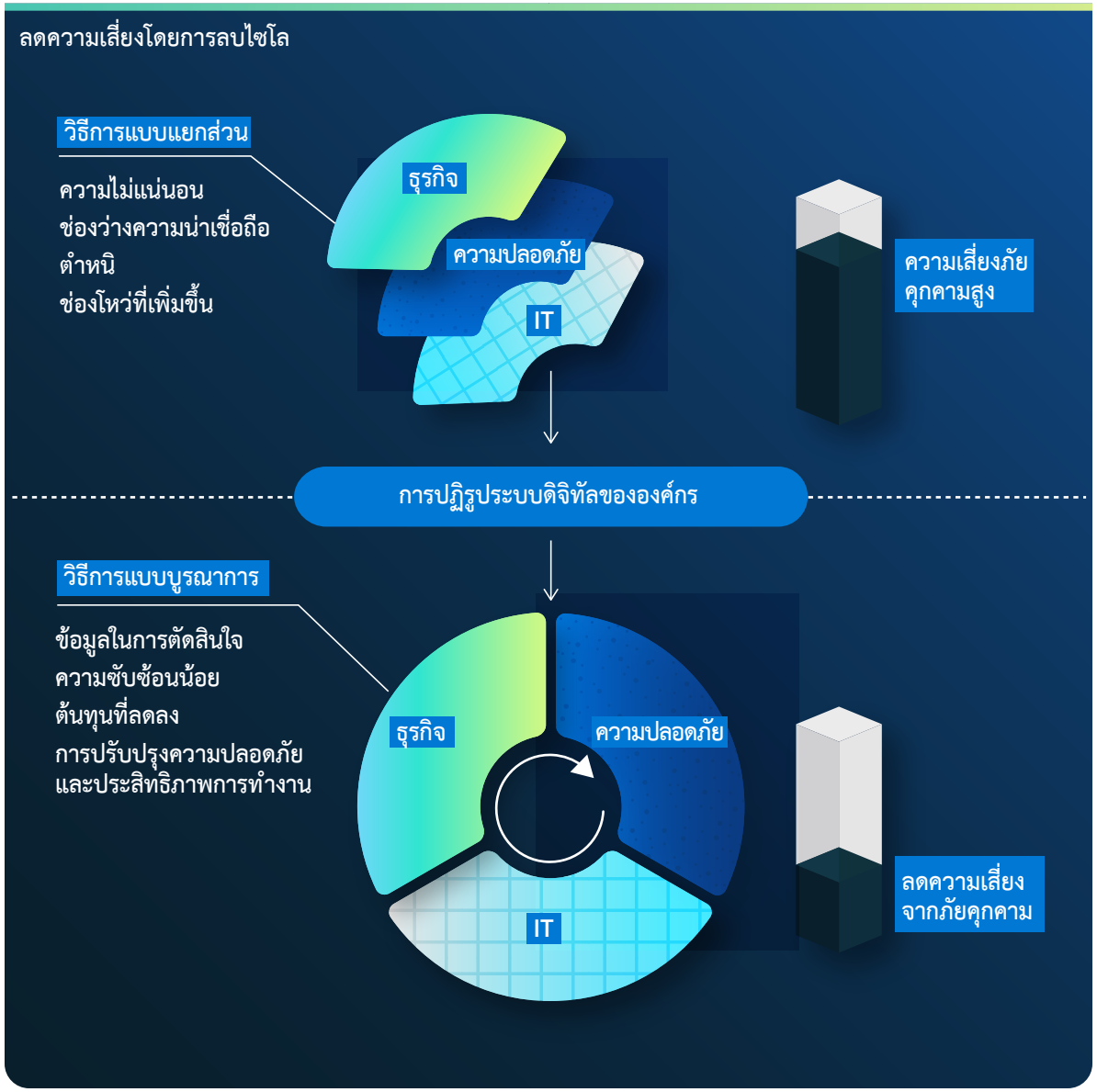
ต่อไป

3. การรักษาความปลอดภัยของตำแหน่งอย่างถูกต้อง

วิธีที่องค์กรจัดโครงสร้างความรับผิดชอบต่อความเสี่ยงด้านความปลอดภัยมักตั้งค่าไว้สำหรับการตัดสินใจความเสี่ยงด้านความปลอดภัยที่ไม่ดี การตัดสินใจเกี่ยวกับความเสี่ยงทำได้ดีที่สุดโดยเจ้าของธุรกิจหรือภารกิจที่มองเห็นความเสี่ยงและโอกาสทั้งหมดได้อย่างเต็มที่ แต่องค์กรต่างๆ มักจะ (โดยปริยายหรือโดยชัดแจ้ง) มอบหมายความรับผิดชอบต่อความเสี่ยงด้านความปลอดภัยให้กับผู้เชี่ยวชาญเฉพาะเรื่องในทีมรักษาความปลอดภัยแทน สิ่งนี้สร้างภาระที่ไม่ดีต่อสุขภาพให้กับทีมรักษาความปลอดภัย ในขณะเดียวกันก็กีดกันเจ้าของธุรกิจในการมองเห็นและควบคุมความเสี่ยงที่สำคัญต่อธุรกิจของพวกเขา องค์กรสามารถแก้ไขสิ่งนี้ได้โดย:

การเตรียมเจ้าของธุรกิจ: ให้ความรู้แก่เจ้าของธุรกิจเกี่ยวกับความเสี่ยงด้านความปลอดภัยโดยรวม และภัยคุกคามเหล่านี้สามารถและจะส่งผลกระทบต่อธุรกิจของพวกเขาอย่างไร การมีส่วนร่วมกับทีมรักษาความปลอดภัยโดยตรงในความพยายามนี้ยังเพิ่มความสัมพันธ์ในการทำงานร่วมกันกับความปลอดภัยและความคล่องตัวทางธุรกิจโดยรวม

การกำหนดความเสี่ยงด้านความปลอดภัยให้กับเจ้าของธุรกิจ: เมื่อเจ้าของธุรกิจได้รับข้อมูลมากพอที่จะเข้าใจและยอมรับความเสี่ยงด้านความปลอดภัย องค์กรควรเปลี่ยนความรับผิดชอบอย่างชัดเจนสำหรับความเสี่ยงด้านความปลอดภัยให้พวกเขา ในขณะที่ยังคงให้ทีมรักษาความปลอดภัยรับผิดชอบในการจัดการความเสี่ยงนั้น และมอบความรู้และคำแนะนำแก่เจ้าของธุรกิจ



"ความยืดหยุ่นทางไซเบอร์อยู่ในระดับที่เลื่อนจากความต่อเนื่องทางธุรกิจแบบคลาสสิกและการกู้คืนความเสียหายที่เริ่มต้นด้วยการสำรองข้อมูลที่ดี ความก้าวหน้าไปสู่ความสามารถในการกู้คืนสำหรับกระบวนการ เทคโนโลยี และการพึ่งพา (รวมถึงบุคคลและบุคคลที่สาม) และก้าวไปสู่บริการการรักษาด้วยตนเองตลอดเวลา ความยืดหยุ่นสำหรับบทบาทที่สำคัญ และความล้มเหลวสำหรับบุคคลที่สามที่สำคัญ องค์กรที่มีความยืดหยุ่นมากที่สุดส่งเสริมการผสานรวมระหว่างฝ่ายไอที ผู้จัดการธุรกิจ และผู้เชี่ยวชาญด้านความปลอดภัย ความยืดหยุ่นที่ยอดเยี่ยมรวมถึงการออกแบบเพื่อความยืดหยุ่นตั้งแต่เริ่มต้น มีการจัดการการเปลี่ยนแปลงที่ปลอดภัย และการแยกข้อผิดพลาดแบบละเอียด ความยืดหยุ่นทางไซเบอร์เป็นเพียงสถานการณ์หนึ่งในโปรแกรมการวางแผนที่ดีสำหรับทุกอันตราย เมื่อความเสี่ยงทางไซเบอร์เพิ่มขึ้นและการแยกระหว่างความปลอดภัยทางไซเบอร์และความยืดหยุ่นมีความสำคัญมากขึ้น การเชื่อมต่อของ Chief Information Security Officer (CISO) กับโปรแกรมความยืดหยุ่นขององค์กรก็แข็งแกร่งขึ้น ทุกปี CISO จำนวนมากขึ้นมีความเป็นเจ้าของเพื่อความยืดหยุ่นทั่วทั้งบริษัท"

Lisa Reshaur
ผู้จัดการทั่วไป ฝ่ายบริหารความเสี่ยง Microsoft

ลิงค์ไปยังข้อมูลเพิ่มเติม

- จากความยืดหยุ่นสู่ความอุตสาหะด้านดิจิทัล: วิธีที่องค์กรต่างๆ ใช้เทคโนโลยีดิจิทัลเพื่อเปลี่ยนมุมในเวลาที่ไม่เคยเกิดขึ้นมาก่อน | บล็อก Microsoft อย่างเป็นทางการ
- ทีมไอทีและทีมรักษาความปลอดภัยสามารถทำงานร่วมกันเพื่อปรับปรุงความปลอดภัยปลายทางได้อย่างไร | Microsoft Security

เส้นโค้งความยืดหยุ่นทางไซเบอร์

ปัจจัยแห่งความสำเร็จของความยืดหยุ่นที่ทุกองค์กรควรนำมาใช้

ดังที่เราได้เห็น การโจมตีทางไซเบอร์จำนวนมากประสบความสำเร็จเพียงเพราะไม่ได้ปฏิบัติตามสุขอนามัยความปลอดภัยขั้นพื้นฐาน มาตรฐานขั้นต่ำที่ทุกองค์กรควรนำมาใช้คือ:

- **เปิดใช้งานการรับรองความถูกต้องโดยใช้หลายปัจจัย (MFA):** เพื่อป้องกันรหัสผ่านของผู้ใช้ที่ถูกบุกรุกและช่วยเพิ่มความยืดหยุ่นให้กับข้อมูลประจำตัว
- **ใช้หลักการ Zero Trust:** รากฐานที่สำคัญของแผนความยืดหยุ่นที่จำกัดผลกระทบต่อองค์กร หลักการเหล่านี้คือ:
  - ตรวจสอบอย่างชัดเจน—ตรวจสอบให้แน่ใจว่าผู้ใช้และอุปกรณ์อยู่ในสถานะที่ดีก่อนที่จะอนุญาตให้เข้าถึงทรัพยากร
  - ใช้การเข้าถึงที่มีสิทธิพิเศษน้อยที่สุด—อนุญาตเฉพาะสิทธิ์ที่จำเป็นสำหรับการเข้าถึงทรัพยากรเท่านั้นและจะไม่อนุญาตอีกต่อไป
  - สมมติว่ามีการละเมิด—สมมติว่าการป้องกันระบบถูกละเมิด และระบบอาจถูกบุกรุก ซึ่งหมายถึงการตรวจสอบสภาพแวดล้อมอย่างต่อเนื่องเพื่อหาการโจมตีที่อาจเกิดขึ้น
- **ใช้การตรวจจับและการตอบสนองเพิ่มเติมในการป้องกันมัลแวร์:** ใช้ซอฟต์แวร์เพื่อตรวจจับและบล็อกการโจมตีโดยอัตโนมัติ และให้ข้อมูลเชิงลึกเกี่ยวกับการดำเนินการด้านความปลอดภัย การตรวจสอบข้อมูลเชิงลึกจากระบบตรวจจับภัยคุกคามมีความสำคัญต่อการตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที
- **อัปเดตให้ทันสมัยอยู่เสมอ:** ระบบที่ไม่ได้แพตช์และล้าสมัยเป็นสาเหตุหลักที่หลายองค์กรตกเป็นเหยื่อของการโจมตี ตรวจสอบให้แน่ใจว่าระบบทั้งหมดได้รับการอัปเดตอยู่เสมอ รวมทั้งเฟิร์มแวร์ ระบบปฏิบัติการและแอปพลิเคชัน
- **ปกป้องข้อมูล:** การทราบข้อมูลสำคัญของคุณว่าข้อมูลนั้นอยู่ที่ใด และมีการนำระบบที่เหมาะสมไปใช้หรือไม่ มีความสำคัญต่อการดำเนินการป้องกันที่เหมาะสม

98%

การรักษาความปลอดภัยที่มั่นคงขั้นพื้นฐานยังคงป้องกันการโจมตีได้ถึง 98%



Key

- เปิดใช้งานการรับรองความถูกต้องโดยใช้หลายปัจจัย
- นำหลักการ Zero Trust มาใช้
- ใช้การป้องกันมัลแวร์ที่ทันสมัย
- อัปเดตให้ทันสมัยอยู่เสมอ
- ปกป้องข้อมูล

อ้างอิงท้ายเอกสาร

1. การตรวจจับและการตอบสนองอุปกรณ์ปลายทาง (EDR) เป็นแพลตฟอร์มความปลอดภัยปลายทางระดับองค์กรที่ออกแบบมาเพื่อช่วยให้เครือข่ายองค์กรป้องกัน ตรวจจับ ตรวจสอบ และตอบสนองต่อภัยคุกคามขั้นสูง ความสามารถในการตรวจจับปลายทางและการตอบสนองให้การตรวจจับการโจมตีขั้นสูงที่ใกล้เคียงกับเวลาจริงและสามารถดำเนินการได้ นักวิเคราะห์ด้านความปลอดภัยสามารถจัดลำดับความสำคัญของการแจ้งเตือนได้อย่างมีประสิทธิภาพ มองเห็นขอบเขตทั้งหมดของการละเมิด และดำเนินการตอบโต้เพื่อแก้ไขภัยคุกคาม
2. แพลตฟอร์มการป้องกันอุปกรณ์ปลายทาง (EPP) เป็นโซลูชันที่ติดตั้งบนอุปกรณ์ปลายทางเพื่อป้องกันมัลแวร์ตามไฟล์ เพื่อตรวจจับและบล็อกกิจกรรมที่เป็นอันตรายจากแอปพลิเคชันที่เชื่อถือได้และไม่น่าเชื่อถือ และเพื่อให้ความสามารถในการตรวจสอบและการแก้ไขที่จำเป็นในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยและการแจ้งเตือนแบบไดนามิก
3. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted
4. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match
5. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context
6. สมุดความปลอดภัยของ Windows: พาณิชย์
7. คุณลักษณะด้านความปลอดภัยใหม่สำหรับ Windows 11 จะช่วยป้องกันการทำงานแบบไฮบริด | บล็อก Microsoft Security
8. FIDO Alliance: มาตรฐานการรับรองความถูกต้องแบบเปิดที่ปลอดภัยกว่ารหัสผ่าน
9. https://interpret.ml/
10. OWASP สิบอันดับแรก | มูลนิธิ OWASP
11. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/
12. https://www.kaspersky.com/blog/the-human-factor-in-it-security/
13. https://aka.ms/ZTatMSFT
14. https://csrc.nist.gov/publications/detail/nistir/8374/final
15. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
16. คำสั่งผู้บริหาร 14028 การปรับปรุงความปลอดภัยทางไซเบอร์ของประเทศ
17. https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth
18. “หนทางอีกยาวไกลสู่การเปลี่ยนไปสู่การเข้ารหัสหลังควอนตัม” https://cacm.acm.org/magazines/2022/1/257440-the-long-road-ahead-to-transition-to-post-quantum-cryptography/fulltext
19. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
20. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
21. https://safecode.org/blog/preparing-for-post-quantum-cryptography-roadmap-initial-guidance/
22. https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

ทีมงาน ที่มีส่วนร่วม

ทีมงานที่มีส่วนร่วม

ข้อมูลและข้อมูลเชิงลึกในรายงานนี้จัดทำโดยกลุ่มผู้เชี่ยวชาญที่มุ่งเน้นการรักษาความปลอดภัยที่หลากหลาย ซึ่งทำงานใน Microsoft Teams ต่างๆ มากมาย โดยรวมแล้ว เป้าหมายของพวกเขาคือการปกป้อง Microsoft ลูกค้าของ Microsoft และโลกทั้งใบจากการคุกคามของการโจมตีทางไซเบอร์ เรามีความภูมิใจที่จะแบ่งปันข้อมูลเชิงลึกเหล่านี้ด้วยความโปร่งใส โดยมีเป้าหมายร่วมกันคือการทำให้โลกเป็นสถานที่ที่ปลอดภัยสำหรับทุกคน

AI สำหรับห้องปฏิบัติการวิจัยที่ดี: การใช้ประโยชน์จากพลังของข้อมูลและ AI เพื่อจัดการกับความท้าทายต่างๆ ของโลก ห้องปฏิบัติการทำงานร่วมกับองค์กรภายนอก Microsoft โดยใช้ AI เพื่อปรับปรุงการดำรงชีวิตและสภาพแวดล้อม ประเด็นสำคัญ ได้แก่ ความปลอดภัยทางออนไลน์ (ข้อมูลบิดเบือน ความปลอดภัยในโลกไซเบอร์ ความปลอดภัยของเด็ก) การตอบสนองต่อภัยพิบัติ ความยั่งยืน และ AI for Health

Azure Edge & Platform การรักษาความปลอดภัยขององค์กร & OS: รับผิดชอบระบบปฏิบัติการหลักและความปลอดภัยของแพลตฟอร์มใน Windows, Azure และผลิตภัณฑ์อื่นๆ ของ Microsoft ทีมสร้างโซลูชันการรักษาความปลอดภัยและฮาร์ดแวร์ระดับแนวหน้าของอุตสาหกรรมลงในแพลตฟอร์มของ Microsoft เพื่อลดช่องโหว่ การระบุตัวตน และมัลแวร์ที่ประนีประนอมจากชิปไปยังระบบคลาวด์ ผู้สร้างแพลตฟอร์มหลักที่ปลอดภัยของ Microsoft บนพีซี Edge และเซิร์ฟเวอร์ ตัวประมวลผลความปลอดภัยของ Microsoft Pluton และอีกมากมาย

Azure network, Core: ทีมเครือข่ายระบบคลาวด์มุ่งเน้นไปที่ Microsoft WAN, เครือข่ายศูนย์ข้อมูล และซอฟต์แวร์กำหนดโครงสร้างพื้นฐานเครือข่ายของ Azure รวมถึงแพลตฟอร์ม DDoS, แพลตฟอร์มขอบเครือข่าย และผลิตภัณฑ์รักษาความปลอดภัยเครือข่าย เช่น Azure WAF, Azure Firewall และมาตรฐานการป้องกัน DDoS ของ Azure

ทีมงานวิจัยด้านความมั่นคงปลอดภัยบนระบบคลาวด์: ด้วยการรักษาความปลอดภัยบนคลาวด์ของ Microsoft สร้างคุณลักษณะและผลิตภัณฑ์ด้านความปลอดภัยที่เป็นนวัตกรรมใหม่ และดำเนินการวิจัย ทีมนี้จะปกป้องและให้อำนาจแก่ลูกค้าของ Microsoft ในการเปลี่ยนแปลงองค์กรของพวกเขาอย่างปลอดภัย

ความปลอดภัยและความไว้วางใจของลูกค้า (CST): ทีมที่ขับเคลื่อนการปรับปรุงความปลอดภัยของลูกค้าอย่างต่อเนื่องในผลิตภัณฑ์และบริการออนไลน์ของ Microsoft CST ทำให้แน่ใจว่ามีการปฏิบัติตามข้อกำหนด ปรับปรุงความปลอดภัยและให้ความโปร่งใสเพื่อปกป้องลูกค้าและส่งเสริมความไว้วางใจ Microsoft ในระดับโลก โดยทำงานร่วมกับทีมวิศวกรรมและการรักษาความปลอดภัยทั่วทั้งบริษัท

ความสำเร็จของลูกค้า: ทีมรักษาความปลอดภัยในความสำเร็จของลูกค้าทำงานโดยตรงกับลูกค้าเพื่อแบ่งปันแนวทางปฏิบัติที่ดีที่สุด บทเรียนที่ได้รับ และคำแนะนำเพื่อเร่งการเปลี่ยนแปลงด้านความปลอดภัยและความทันสมัย ทีมนี้รวบรวมและจัดระเบียบแนวทางปฏิบัติที่ดีที่สุดและบทเรียนที่ได้รับจากการเดินทางของ Microsoft—รวมถึงลูกค้าของเรา—ในกลยุทธ์การอ้างอิง สถาปัตยกรรมอ้างอิง แผนอ้างอิง และอื่นๆ

ศูนย์ปฏิบัติการป้องกันการโจมตีทางไซเบอร์ (CDOC): สิ่งอำนวยความสะดวกด้านความปลอดภัยและการป้องกันทางไซเบอร์ของ Microsoft เป็นศูนย์กลางที่รวบรวมผู้เชี่ยวชาญด้านความปลอดภัยจากทั่วทั้งบริษัทมาไว้ด้วยกัน เพื่อปกป้องโครงสร้างพื้นฐานขององค์กรและโครงสร้างพื้นฐานในระบบคลาวด์ที่ลูกค้าสามารถเข้าถึงได้ ผู้รับมือเหตุการณ์จะนั่งเคียงข้างนักวิทยาศาสตร์ข้อมูลและวิศวกรด้านความปลอดภัยจากทั่วทั้งกลุ่มบริการ ผลิตภัณฑ์ และอุปกรณ์ของ Microsoft เพื่อช่วยปกป้อง ตรวจจับ และตอบสนองต่อภัยคุกคามตลอด 24 ชั่วโมงทุกวัน

ความคิดริเริ่มประชาธิปไตย: ทีมงานของ Microsoft ที่ทำงานเพื่อรักษา ปกป้อง และพัฒนาพื้นฐานของประชาธิปไตยโดยการส่งเสริมระบบนิเวศข้อมูลที่สมบูรณ์ ปกป้องกระบวนการประชาธิปไตยที่เปิดกว้างและปลอดภัย และสนับสนุนความรับผิดชอบต่อพลเมืองขององค์กร

หน่วยอาชญากรรมดิจิทัล (DCU): ทีมทนายความ ผู้ตรวจสอบ นักวิทยาศาสตร์ข้อมูล วิศวกร นักวิเคราะห์ และผู้เชี่ยวชาญด้านธุรกิจที่อุทิศตนเพื่อต่อสู้กับอาชญากรรมทางไซเบอร์ในระดับโลกโดยใช้เทคโนโลยี นิติเวช การดำเนินการทางแพ่ง การส่งต่ออาชญากร และความร่วมมือทั้งภาครัฐและเอกชน

การทูตดิจิทัล: ทีมงานระดับนานาชาติของอดีตนักการทูต ผู้กำหนดนโยบาย และผู้เชี่ยวชาญด้านกฎหมายที่ทำงานเพื่อพัฒนาพื้นที่ไซเบอร์ที่สงบ มั่นคง และปลอดภัยในการเผชิญกับความขัดแย้งของรัฐชาติที่เพิ่มขึ้น

ความปลอดภัยและความยืดหยุ่นทางดิจิทัล (DSR): องค์กรที่อุทิศตนเพื่อให้ Microsoft สามารถสร้างอุปกรณ์และบริการที่น่าเชื่อถือที่สุด ในขณะเดียวกันก็รักษาบริษัทของเราให้ปลอดภัย และได้รับการปกป้องทั้งข้อมูลของบริษัทและข้อมูลลูกค้า

หน่วยรักษาความปลอดภัยแบบดิจิทัล (DSU): ทีมทนายความและนักวิเคราะห์ด้านความปลอดภัยในโลกไซเบอร์ที่ให้ความเชี่ยวชาญด้านกฎหมาย ภูมิรัฐศาสตร์ และทางเทคนิคเพื่อปกป้อง Microsoft และลูกค้าของบริษัท DSU สร้างความไว้วางใจในการป้องกันความปลอดภัยระดับองค์กรของ Microsoft จากศัตรูทางไซเบอร์ขั้นสูงทั่วโลก

ศูนย์กลางการวิเคราะห์ภัยคุกคามทางดิจิทัล (DTAC): ทีมผู้เชี่ยวชาญที่วิเคราะห์และรายงานเกี่ยวกับภัยคุกคามของรัฐชาติ รวมถึงการโจมตีทางไซเบอร์และการปฏิบัติการที่มีอิทธิพล ทีมงานรวมข้อมูลและข้อมูลภัยคุกคามทางไซเบอร์เข้ากับการวิเคราะห์ทางภูมิรัฐศาสตร์เพื่อให้ข้อมูลเชิงลึกแก่ลูกค้าของเราและ Microsoft เพื่อแจ้งให้ทราบถึงการตอบสนองและการป้องกันที่มีประสิทธิภาพ

องค์กรและการรักษาความปลอดภัย: ทีมงานมุ่งเน้นไปที่การจัดหาแพลตฟอร์มที่ทันสมัย ปลอดภัย และจัดการได้บนระบบคลาวด์และบนอุปกรณ์ปลายทางอัจฉริยะ

Enterprise Mobility: ทีมที่ช่วยส่งมอบสถานที่ทำงานที่ทันสมัยและการจัดการที่ทันสมัยเพื่อรักษาข้อมูลให้ปลอดภัย ทั้งในระบบคลาวด์และในสถานที่ Endpoint Manager รวมถึงบริการและเครื่องมือที่ Microsoft และลูกค้าใช้เพื่อจัดการและตรวจสอบอุปกรณ์พกพา คอมพิวเตอร์เดสก์ท็อป เครื่องเสมือน อุปกรณ์ฝังตัว และเซิร์ฟเวอร์

ทีมงานที่มีส่วนร่วม

ต่อไป

การบริหารความเสี่ยงองค์กร: ทีมที่ทำงานร่วมกันในหน่วยธุรกิจเพื่อจัดลำดับความสำคัญของการหารือเกี่ยวกับความเสี่ยงกับผู้นำระดับสูงของ Microsoft ERM เชื่อมต่อทีมความเสี่ยงด้านปฏิบัติการหลายทีม จัดการเฟรมเวิร์กความเสี่ยงระดับองค์กรของ Microsoft และอำนวยความสะดวกในการประเมินความปลอดภัยภายในของบริษัทโดยใช้กรอบงานความปลอดภัยด้านไซเบอร์ของ NIST

นโยบายด้านความปลอดภัยทางไซเบอร์ทั่วโลก: ทีมงานที่ทำงานร่วมกับรัฐบาล องค์กรพัฒนาเอกชน และพันธมิตรในอุตสาหกรรม เพื่อส่งเสริมนโยบายสาธารณะด้านความปลอดภัยทางไซเบอร์ที่ส่งเสริมให้ลูกค้าสามารถเสริมความปลอดภัยและความยืดหยุ่นในการปรับใช้เทคโนโลยีของ Microsoft

ความปลอดภัยของข้อมูลประจำตัวและการเข้าถึงเครือข่าย (IDNA): ทีมงานที่ทำงานเพื่อปกป้องลูกค้า Microsoft ทั้งหมดจากการเข้าถึงและการฉ้อโกงโดยไม่ได้รับอนุญาต IDNA Security เป็นทีมที่ประกอบด้วยวิศวกร ผู้จัดการผลิตภัณฑ์ นักวิทยาศาสตร์ข้อมูล และผู้ตรวจสอบความปลอดภัย

M365 Security: องค์กรที่พัฒนาโซลูชันด้านความปลอดภัย ได้แก่ Microsoft Defender for Endpoint (MDE), Microsoft Defender for Identity (MDI) และอื่นๆ เพื่อรักษาความปลอดภัยแก่ลูกค้าองค์กร

AI, จริยธรรม และผลกระทบในด้านวิศวกรรมและการวิจัย (AETHER) ของ Microsoft: คณะกรรมการที่ปรึกษาของ Microsoft ที่มีพันธกิจในการสร้างความมั่นใจว่าเทคโนโลยีใหม่ๆ ได้รับการพัฒนาและนำเสนอในลักษณะที่มีความรับผิดชอบ

การค้นหาและการกระจายของ Microsoft Bing: ทีมงานที่อุทิศตนเพื่อให้บริการเสิร์ชเอ็นจิ้นทางอินเทอร์เน็ตระดับโลก ช่วยให้ผู้ใช้ทั่วโลกสามารถค้นหาผลการค้นหาและข้อมูลที่เชื่อถือได้อย่างรวดเร็ว รวมถึงการติดตามหัวข้อและเรื่องราวที่กำลังเป็นกระแสซึ่งมีความสำคัญต่อพวกเขา ในขณะที่ให้ผู้ใช้ควบคุมความเป็นส่วนตัวของตน

โซลูชันลูกค้าและคู่ค้าของ Microsoft: องค์กรเชิงพาณิชย์แบบครบวงจรของ Microsoft ที่รับผิดชอบบทบาทภาคสนาม เช่น ผู้เชี่ยวชาญด้านความปลอดภัยและการขายด้านเทคนิคและที่ปรึกษา

Microsoft Defender Experts: องค์กรระดับโลกที่ใหญ่ที่สุดของ Microsoft ที่ประกอบด้วยนักวิจัยด้านความปลอดภัยที่มุ่งเน้นไปที่ผลิตภัณฑ์ นักวิทยาศาสตร์ประยุกต์ และนักวิเคราะห์ข่าวกรองภัยคุกคาม Defender Experts นำเสนอความสามารถในการตรวจจับและการตอบสนองที่เป็นนวัตกรรมใหม่ในผลิตภัณฑ์รักษาความปลอดภัยของ Microsoft 365 และบริการที่มีการจัดการของ Microsoft Defender Experts

Microsoft Defender สำหรับ IoT: ทีมงานประกอบด้วยนักวิจัยผู้เชี่ยวชาญด้านโดเมนที่เชี่ยวชาญด้านวิศวกรรมย้อนกลับของมัลแวร์ IoT/OT โปรโตคอล และเฟิร์มแวร์ ทีมค้นหาภัยคุกคาม IoT/OT เพื่อเปิดเผยแนวโน้มและแคมเปญที่เป็นอันตราย

Microsoft Defender Threat Intelligence (RiskIQ): ทีมงานที่สร้างข่าวกรองทางยุทธวิธีผ่านการวิเคราะห์คอลเลกชันการวัดและส่งข้อมูลทางไกลภายนอกที่กว้างขวางของ Microsoft จัดทำแผนภูมิภูมิทัศน์ของภัยคุกคามในขณะที่วิวัฒนาการเพื่อค้นหาโครงสร้างพื้นฐานของภัยคุกคามที่ไม่รู้จักก่อนหน้านี้ และเพิ่มบริบทให้กับผู้คุกคามและแคมเปญ ทีมงานเผยแพร่งานวิจัยที่โดดเด่นและทันท่วงทีเป็นประจำเพื่อส่งมอบข่าวกรองทางยุทธวิธีที่สำคัญให้กับผู้ป้องกัน

ทีมพัฒนาธุรกิจด้านความมั่นคงปลอดภัย Microsoft: ทีมที่เป็นผู้นำกลยุทธ์การเติบโตด้านความปลอดภัยทางไซเบอร์ พันธมิตร และการลงทุนเชิงกลยุทธ์ของ Microsoft

ศูนย์ตอบกลับด้านความปลอดภัยของ Microsoft (MSRC): ทีมที่ทำงานร่วมกับนักวิจัยด้านความปลอดภัยที่ทำงานเพื่อปกป้องลูกค้าและระบบนิเวศคู่ค้าของ Microsoft ส่วนสำคัญของศูนย์ปฏิบัติการป้องกันการโจมตีไซเบอร์ของ Microsoft (CDOC) MSRC รวบรวมผู้เชี่ยวชาญด้านการตอบสนองด้านความมั่นคงปลอดภัยเพื่อตรวจสอบ และตอบสนองต่อภัยคุกคามในแบบเรียลไทม์

บริการการรักษาความปลอดภัยของ Microsoft สำหรับการตอบสนองต่อเหตุการณ์: ทีมผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ช่วยเหลือลูกค้าผ่านการโจมตีทางไซเบอร์ทั้งหมดตั้งแต่การสืบสวนไปจนถึงกิจกรรมที่เกี่ยวข้องกับการกักกันและการกู้คืนที่ประสบความสำเร็จ มีการนำเสนอบริการผ่านสองทีมที่มีการบูรณาการสูง ได้แก่ ทีมตรวจสอบและตอบสนอง (DART) โดยมุ่งเน้นที่การสืบสวนและรากฐานสำหรับการกู้คืน และ แนวทางปฏิบัติด้านความปลอดภัยในการกู้คืนการบุกรุก (CRSP) ซึ่งมุ่งเน้นไปที่ด้านการกักกันและการกู้คืน

ศูนย์ข่าวกรองภัยคุกคามของ Microsoft (MSTIC): ทีมงานมุ่งเน้นที่การระบุ ติดตาม และรวบรวมข้อมูลที่เกี่ยวข้องกับฝ่ายตรงข้ามที่มีความทันสมัยที่สุดที่ส่งผลกระทบกับลูกค้าของ Microsoft ซึ่งรวมถึงภัยคุกคามระดับชาติ มัลแวร์และฟิชชิ่ง

One Engineering System (1ES): ทีมที่มีพันธกิจในการส่งมอบเครื่องมือระดับโลกเพื่อช่วยให้นักพัฒนาของ Microsoft มีประสิทธิผลและปลอดภัยมากที่สุดเท่าที่จะเป็นไปได้ ทีมงานเป็นผู้นำกลยุทธ์หลักในการรักษาความปลอดภัยห่วงโซ่อุปทานซอฟต์แวร์แบบครบวงจรของ Microsoft

ศูนย์ปฏิบัติการข่าวกรองภัยคุกคาม (OpTIC): ทีมที่รับผิดชอบในการจัดการและเผยแพร่ข่าวกรองภัยคุกคามทางไซเบอร์ที่สนับสนุนภารกิจของศูนย์ปฏิบัติการป้องกันไซเบอร์ Microsoft (CDOC) เพื่อปกป้อง Microsoft และลูกค้าของเรา

Microsoft

ส่องสว่างแนวภัยคุกคามและเพิ่มพลัง ให้กับการป้องกันทางดิจิทัล

- เรียนรู้เพิ่มเติม: **https://microsoft.com/mddr**
- เจาะลึกลงกว่าเดิม: **https://blogs.microsoft.com/on-the-issues/**
- เชื่อมต่ออยู่เสมอ: **@msftissues and @msftsecurity**

© 2022 Microsoft. All rights reserved.