Microsoft

דוח ההגנה הדיגיטלית של Microsoft לשנת 2022

תיאור של נוף האיומים המתפתח והעצמת ההגנה הדיגיטלית.

תוכן

הנתונים, התובנות והאירועים בדוח זה הם מיולי 2021 עד יוני 2022 (שנת הכספים 2022 של Microsoft), אלא אם כן צוין אחרת.

כדי לקבל את החוויה הטובה ביותר של צפייה וניווט בדוח זה, אנו ממליצים להשתמש ב-Adobe Reader, הזמין להורדה בחינם מאתר האינטרנט של Adobe.

הקדמה מאת Tom Burt

Corporate סגן נשיא, אבטחה ואמון הלקוחות

"טריליוני האותות שאנו מנתחים מהמערכת האקולוגית העולמית שלנו של מוצרים ושירותים חושפים את האכזריות, ההיקף וקנה המידה של איומים דיגיטליים ברחבי העולם "

תמונת מצב של הסביבה שלנו...

ההיקף וקנה המידה של נוף האיומים

כמות מתקפות הסיסמאות עלתה לכ-921 התקפות בכל שנייה – עלייה של 74% בשנה אחת בלבד.

פירוק פשעי סייבר

נכון להיום, Microsoft הסירה יותר מ-10,000 תחומים המשמשים פושעי סייבר ו-600 המשמשים גורמים מדינתיים.

טיפול בפגיעויות

93% מההתקשרויות שלנו לתגובה לאירועים של תוכנות כופר חשפו בקרות לא מספיקות על הרשאת גישה ועל תנועה רוחבית.

ב- 23 בפברואר 2022 נכנס עולם אבטחת הסייבר לעידן חדש, עידן המלחמה ההיברידית. באותו יום, שעות לפני שיגור טילים ומעבר טנקים מעבר לגבולות, גורמים רוסיים פתחו במתקפת סייבר הרסנית ומסיבית כנגד מטרות אוקראיניות ממשלתיות, טכנולוגיות ובמגזר הפיננסי. ניתן לקרוא עוד על התקפות אלה ועל הלקחים שיש ללמוד מהן בפרק 'איומים ברמת המדינה' במהדורה שנתית שלישית זו של דוח ההגנה הדיגיטלית של Microsoft (MDDR). המפתח בין הלקחים הללו הוא שהענן מספק את האבטחה הפיזית והלוגית הטובה ביותר מפני מתקפות סייבר ומאפשר התקדמות במודיעין איומים והגנה על נקודות קצה שהוכיחו את ערכן באוקראינה.

כל סקירה של ההתפתחויות שחלו השנה באבטחת סייבר חייבת להתחיל שם, אך השנה הדוח מספק מבט מעמיק אל הרבה יותר מכך. בפרק הראשון של הדוח אנו מתמקדים בפעילויות של פושעי סייבר, ולאחר מכן באיומים ברמת המדינה בפרק השני. שתי הקבוצות הגבירו מאוד את התחכום של ההתקפות שלהן, דבר שהגדיל באופן דרמטי את ההשפעה של פעולותיהן. בעוד רוסיה עלתה לכותרות, גורמים איראנים הסלימו את התקפותיהם בעקבות חילופי השלטון הנשיאותי, תוך שהם מבצעים מתקפות הרסניות נגד ישראל ופעולות של תוכנות כופר ושל פריצה והדלפה המכוונות לתשתיות חיוניות בארצות הברית. סין גם הגבירה את מאמצי הריגול שלה בדרום מזרח אסיה ובמקומות אחרים בדרום הגלובלי, בניסיון לנטרל את השפעתה של ארה"ב ולגנוב נתונים ומידע קריטיים.

גם שחקנים זרים משתמשים בטכניקות יעילות ביותר כדי להשפיע מבחינה תעמולתית באזורים שונים ברחבי העולם, כפי שסוקר הפרק השלישי. לדוגמה, רוסיה עבדה קשה כדי לשכנע את אזרחיה, ואת אזרחיהן של מדינות רבות אחרות, שהפלישה שלה לאוקראינה הייתה מוצדקת – תוך שהיא זורעת תעמולה המכפישה את חיסוני הקורונה במערב ובמקביל מקדמת את יעילותם בבית. בנוסף, שחקנים מתמקדים יותר ויותר במכשירי אינטרנט של הדברים (IoT) או במכשירי בקרה של טכנולוגיה תפעולית (OT) כנקודות כניסה לרשתות ותשתיות חיוניות אשר נדונות בפרק הרביעי. לבסוף, בפרק האחרון, אנו מספקים את התובנות והלקחים שלמדנו מהשנה האחרונה בהגנה מפני התקפות שכוונו כלפי Microsoft וכלפי לקוחותינו, תוך סקירת ההתפתחויות שחלו השנה בעמידות הסייבר.

כל פרק מספק את הלקחים העיקריים שנלמדו ותובנות המבוססות על נקודת המבט הייחודית של Microsoft. טריליוני האותות שאנו מנתחים מהמערכת האקולוגית העולמית שלנו של מוצרים ושירותים חושפים את האכזריות, ההיקף וקנה המידה של האיומים הדיגיטליים ברחבי העולם. Microsoft נוקטת פעולה כדי להגן על הלקוחות שלנו ועל המערכת האקולוגית הדיגיטלית מפני איומים אלה, וניתן לקרוא על הטכנולוגיה שלנו שמזהה וחוסמת מיליארדי ניסיונות דיוג, גניבות זהות ואיומים אחרים על הלקוחות שלנו.

הקדמה מאת Tom Burt

המשך

אנו משתמשים גם באמצעים משפטיים וטכניים כדי לתפוס ולסגור תשתיות המשמשות פושעי סייבר וגורמים ממדינות שונות וליידע לקוחות כאשר הם מאוימים או מותקפים על ידי גורם כזה. אנו פועלים לפיתוח תכונות ושירותים יעילים יותר ויותר המשתמשים בטכנולוגיית בינה מלאכותית/למידת מכונה (AI/ML) כדי לזהות ולחסום איומי סייבר, ומומחי אבטחה מגינים מפני פריצות סייבר ומזהים אותן במהירות וביעילות רבה יותר.

והכי חשוב אולי, בכל ה- MDDR אנו מציעים את העצות הטובות ביותר שלנו לגבי הצעדים שאנשים פרטיים, חברות וארגונים יכולים לנקוט כדי להגן מפני איומים דיגיטליים מתגברים אלה. אימוץ נוהלי היגיינת סייבר טובים הוא ההגנה הטובה ביותר ויכול להפחית משמעותית את הסיכון למתקפות סייבר.

מצב פשעי הסייבר

פושעי סייבר ממשיכים לפעול כמפעלים רווחיים מתוחכמים. התוקפים מסתגלים ומוצאים דרכים חדשות ליישם את הטכניקות שלהם, דבר שמגדיל את המורכבות של האופן והמקום שבו הם מארחים תשתית תפעול קמפיין. במקביל, פושעי סייבר הופכים חסכניים יותר. כדי להפחית את התקורה שלהם ולהגביר מראית עין של לגיטימיות, התוקפים מעמידים בסכנה רשתות ומכשירים עסקיים כדי לארח קמפיינים של דיוג, תוכנות זדוניות או אפילו להשתמש בכוח ה-computing שלהם לכריית מטבעות קריפטוגרפיים.

מידע נוסף בעמוד p6

"ההופעה של פריסת נשק סייבר במלחמה ההיברידית באוקראינה היא תחילתו של עידן חדש של עימות".

איומים ברמת המדינה

גורמים שונים במדינות משגרים מתקפות סייבר מתוחכמות יותר ויותר שנועדו להתחמק מזיהוי ולקדם את סדרי העדיפויות האסטרטגיים שלהם. הופעתה של פריסת נשק סייבר במלחמה ההיברידית באוקראינה היא שחר של עידן חדש של עימות. רוסיה גם תמכה במלחמתה באמצעות מבצעי השפעה על מידע, והשתמשה בתעמולה כדי להשפיע על דעות ברוסיה, באוקראינה ובעולם. מחוץ לאוקראינה, גורמים מדינתיים הגבירו את פעילותם והחלו להשתמש בפיתוחים חדשים באוטומציה, בתשתיות ענן ובטכנולוגיות גישה מרחוק כדי לתקוף סט מטרות רחב יותר. שרשראות אספקה ארגוניות של IT המאפשרות גישה ליעדים אולטימטיביים הותקפו לעתים קרובות. היגיינת אבטחת הסייבר הפכה קריטית עוד יותר כאשר גורמים ניצלו במהירות פגיעויות שלא תוקנו, השתמשו בטכניקות מתוחכמות ובטכניקות brute force כדי לגנוב אישורים, והסתירו את פעילותם על ידי שימוש בתוכנות קוד פתוח או בתוכנות לגיטימיות. בנוסף, איראן מצטרפת לרוסיה בשימוש בנשקי סייבר הרסניים, כולל תוכנות כופר, כמרכיב עיקרי בתקיפות שלה.

התפתחויות אלה מחייבות אימוץ דחוף של מסגרת גלובלית עקבית הנותנת עדיפות לזכויות אדם ומגינה על אנשים מפני התנהגות מדינתית חסרת אחריות ברשת. כל המדינות חייבות לעבוד יחד כדי ליישם נורמות וכללים להתנהגות מדינתית אחראית.

מידע נוסף בעמוד 30

מכשירים ותשתיות

מגפת הקורונה, בשילוב עם אימוץ מהיר של מכשירים הפונים לאינטרנט מכל הסוגים כמרכיב בהאצת הטרנספורמציה הדיגיטלית, הגדילו מאוד את שטח התקיפה של העולם הדיגיטלי. כתוצאה מכך, פושעי סייבר ומדינות מנצלים זאת במהירות. בעוד שאבטחת החומרה והתוכנה של ה-IT התחזקה בשנים האחרונות, האבטחה של אבטחת מכשירי IoT ומכשירי OT לא עמדה בקצב. גורמי איום מנצלים מכשירים אלה כדי ליצור גישה לרשתות ולאפשר תנועה רוחבית, לבסס דריסת רגל בשרשרת אספקה או לשבש את פעילות ה-OT של ארגון היעד.

מידע נוסף בעמוד 56

הקדמה מאת Tom Burt

המשך

מבצעי השפעה בסייבר

מדינות משתמשות יותר ויותר במבצעי השפעה מתוחכמים כדי להפיץ תעמולה ולהשפיע על דעת הקהל הן מקומית והן בזירה הבינלאומית. הקמפיינים האלה שוחקים את האמון, מגבירים את הקיטוב ומאיימים על תהליכים דמוקרטיים. גורמים מניפולטיביים מיומנים ומתקדמים בעלי יכולת התמדה משתמשים במדיה המסורתית בשילוב עם האינטרנט והמדיה החברתית כדי להגדיל במידה ניכרת את ההיקף, קנה המידה והיעילות של הקמפיינים שלהם, ואת ההשפעה הנרחבת שיש להם במערכת האקולוגית העולמית של המידע.
בשנה האחרונה ראינו את הפעולות הללו בשימוש כחלק מהמלחמה ההיברידית של רוסיה באוקראינה, אך גם ראינו את רוסיה ומדינות אחרות, כולל סין ואיראן, פורסות יותר ויותר פעולות תעמולה המופעלות על ידי המדיה החברתית כדי להרחיב את השפעתן העולמית במגוון נושאים.

מידע נוסף בעמוד 71

עמידות סייבר

אבטחה היא גורם עיקרי שמאפשר הצלחה טכנולוגית. ניתן להגיע לחדשנות ופרודוקטיביות משופרת רק על ידי הטמעת אמצעי אבטחה שהופכים ארגונים לעמידים ככל האפשר מפני התקפות מודרניות. המגפה אתגרה אותנו ב-Microsoft לשנות את נוהלי האבטחה והטכנולוגיות שלנו כדי להגן על העובדים שלנו בכל מקום שבו הם עובדים. בשנה האחרונה המשיכו גורמי האיום לנצל את הפגיעויות שנחשפו במהלך המגפה והמעבר לסביבת עבודה היברידית. מאז, האתגר העיקרי שלנו הוא ניהול השכיחות והמורכבות של שיטות תקיפה שונות ושל פעילות מדינתית מוגברת. בפרק זה אנו מפרטים את האתגרים שעמדו בפנינו, ואת ההגנות שגייסנו בתגובה עם יותר מ- 15,000 השותפים שלנו.

מידע נוסף בעמוד 86

נקודת המבט הייחודית שלנו

37 מיליארד
איומי דואר אלקטרוני נחסמו

34.7 מיליארד
איומי זהות שנחסמו

2.5 מיליארד
אותות של נקודות קצה מנותחים מדי יום

43 טריליון
אותות מסונתזים מדי יום, תוך שימוש בניתוח נתונים מתוחכם ובאלגוריתמים של בינה מלאכותית (AI) כדי להבין איומים דיגיטליים ופעילות סייבר פלילית ולהגן מפניהם.

מעל 8,500
מהנדסים, חוקרים, מדעני נתונים, מומחי אבטחת סייבר, ציידי איומים, אנליסטים גיאופוליטיים, חוקרים ומגיבים בקו הראשון ב-77 מדינות.

מעל 15,000
שותפים במערכת האבטחה האקולוגית שלנו המגבירים את עמידות הסייבר עבור לקוחותינו.

1 ביולי 2021 עד 30 ביוני 2022

הקדמה מאת Tom Burt

המשך

אנו מאמינים של- Microsoft – באופן עצמאי ובאמצעות שותפויות הדוקות עם אחרים בתעשייה הפרטית, בממשלה ובחברה האזרחית – יש אחריות להגן על המערכות הדיגיטליות העומדות בבסיס המרקם החברתי של החברה שלנו ולקדם סביבות מחשוב בטוחות ומאובטחות עבור כל אדם, בכל מקום שבו הוא נמצא. אחריות זו היא הסיבה שאנו מפרסמים את ה-MDDR בכל שנה מאז 2020. הדוח הוא שיאם של כמות הנתונים העצומה והמחקר המקיף של Microsoft. הוא משתף את התובנות הייחודיות שלנו על האופן שבו נוף האיומים הדיגיטליים מתפתח ועל הפעולות החיוניות שניתן לנקוט כיום כדי לשפר את האבטחה של המערכת האקולוגית.

אנו מקווים להחדיר תחושת דחיפות, כדי שהקוראים ינקטו פעולה מיידית על סמך הנתונים והתובנות שאנו מציגים הן כאן והן בפרסומי אבטחת הסייבר הרבים שלנו לאורך השנה. כאשר אנו שוקלים את חומרת האיום על הנוף הדיגיטלי – ותרגומו לעולם הפיזי – חשוב לזכור שלכולנו יש את הכוח לנקוט פעולה כדי להגן על עצמנו, על הארגונים ועל החברות שלנו מפני איומים דיגיטליים.

תודה שהחלטת להקדיש זמן ולקרוא את דוח ההגנה הדיגיטלית של Microsoft השנה. אנו מקווים שתגלה שהוא מספק תובנות והמלצות חשובות שיעזרו לנו להגן באופן קולקטיבי על המערכת האקולוגית הדיגיטלית.

Tom Burt
סגן נשיא,
אבטחה ואמון הלקוחות

מטרתנו בדוח זה היא כפולה:

1. להאיר את נוף האיומים הדיגיטליים המתפתח עבור הלקוחות, השותפים ובעלי העניין שלנו המתפרשים על פני המערכת האקולוגית הרחבה יותר, ולשפוך אור הן על מתקפות סייבר חדשות והן על מגמות מתפתחות באיומים מתמשכים מבחינה היסטורית.
2. כדי להעצים את כוחם של הלקוחות והשותפים שלנו לשפר את עמידות הסייבר שלהם ולהגיב לאיומים אלה.

מצב פשעי הסייבר

ככל שהגנות הסייבר משתפרות ויותר ארגונים נוקטים גישה פרואקטיבית למניעה, התוקפים מתאימים את הטכניקות שלהם.

סקירה כללית של

מצב פשעי הסייבר

ככל שהגנות הסייבר משתפרות ויותר ארגונים נוקטים גישה פרואקטיבית למניעה, התוקפים מתאימים את הטכניקות שלהם.

פושעי סייבר ממשיכים לפעול כמפעלים רווחיים מתוחכמים. התוקפים מסתגלים ומוצאים דרכים חדשות ליישם את הטכניקות שלהם, דבר שמגדיל את המורכבות של האופן והמקום שבו הם מארחים תשתית תפעול קמפיין. במקביל, פושעי סייבר הופכים חסכניים יותר. כדי להפחית את התקורה שלהם ולהגביר מראית עין של לגיטימיות, התוקפים מעמידים בסכנה רשתות ומכשירים עסקיים כדי לארח קמפיינים של דיוג, תוכנות זדוניות או אפילו להשתמש בכוח ה-computing שלהם לכריית מטבעות קריפטוגרפיים.

פשעי הסייבר נמצאים במגמת עלייה ככל שהתיעוש של כלכלת פשעי הסייבר גורם לירידת חסם המיומנות לכניסה על ידי כך שמתאפשרת גישה רבה יותר לכלים ולתשתיות.

מידע נוסף בעמוד 18

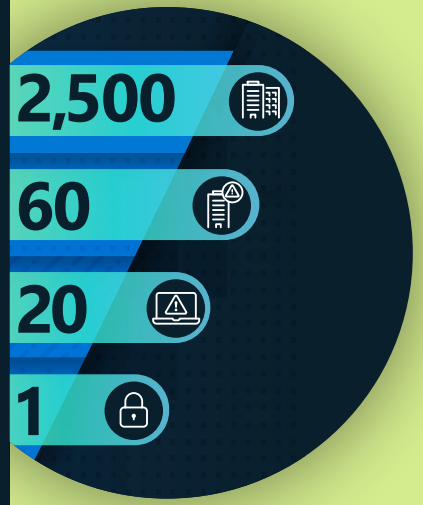
האיום של תוכנות כופר וסחיטה הופך נועז יותר עם התקפות המכוונות נגד ממשלות, עסקים ותשתיות חיוניות.

מידע נוסף בעמוד 9

תוקפים מאיימים יותר ויותר לחשוף נתונים רגישים כדי לעודד תשלומי כופר.

מידע נוסף בעמוד 10

תוכנות כופר המופעלות על ידי בני אדם הן הנפוצות ביותר, כאשר שליש מהמטרות נפגעות בהצלחה על ידי פושעים המשתמשים בהתקפות אלה ו- 5% מהן נפדות.

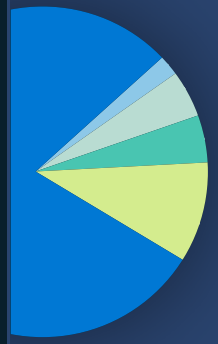


מידע נוסף בעמוד9

ההגנה היעילה ביותר מפני תוכנות כופר כוללת אימות רב-גורמי, תיקוני אבטחה תכופים ועקרונות 'אפס אמון' בארכיטקטורת הרשת.

מידע נוסף בעמוד 13

מזימות דיוג אישורים המכוונות ללא הבחנה לכל תיבות הדואר הנכנס נמצאות במגמת עלייה, ופגיעה בדואר אלקטרוני עסקי, כולל הונאת חשבוניות, מהווה סיכון משמעותי לפשעי סייבר עבור ארגונים.



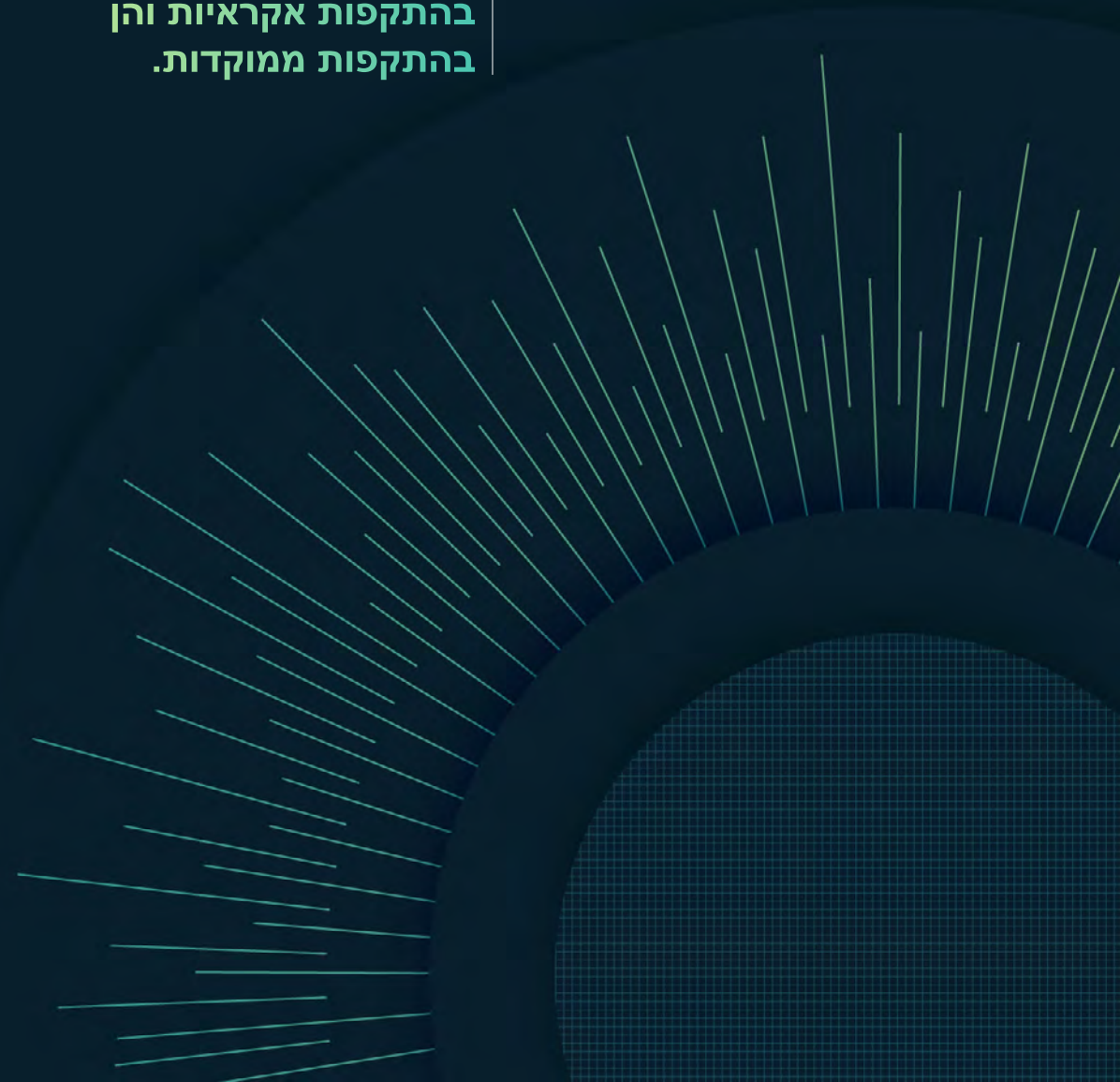
מידע נוסף בעמוד 21

כדי לשבש את התשתיות הזדוניות של פושעי סייבר ושל גורמים מדינתיים, Microsoft מסתמכת על גישות משפטיות חדשניות ועל השותפויות הציבוריות והפרטיות שלנו.

מידע נוסף בעמוד 25

מבוא

פשיעת הסייבר ממשיכה לעלות, עם עלייה הן בהתקפות אקראיות והן בהתקפות ממוקדות.



ככל שהגנות הסייבר משתפרות ויותר ממשלות ועסקים נוקטים גישה פרואקטיבית למניעה, אנו רואים תוקפים המשתמשים בשתי אסטרטגיות כדי להשיג את הגישה הנדרשת לביצוע פשעי סייבר. גישה אחת היא קמפיין עם יעדים רחבים שמסתמך על נפח. השנייה משתמשת במעקב ובמיקוד סלקטיבי יותר כדי להגדיל את שיעור התשואה. גם כאשר יצירת הכנסות אינה המטרה – למשל פעילות מדינתית למטרות גיאופוליטיות – נעשה שימוש הן בהתקפות אקראיות והן בהתקפות ממוקדות. בשנה האחרונה, פושעי סייבר המשיכו להסתמך על הנדסה חברתית ועל ניצול נושאים אקטואליים כדי למקסם את הצלחת הקמפיינים. לדוגמה, בעוד שפיתויי דיוג הקשורים לקורונה שימשו בתדירות נמוכה יותר, ראינו עלייה במספר הפיתויים המבקשים תרומות לתמיכה באזרחי אוקראינה.

התוקפים מסתגלים ומוצאים דרכים חדשות ליישם את הטכניקות שלהם, דבר שמגדיל את המורכבות של האופן והמקום שבו הם מארחים תשתית תפעול קמפיין. ראינו פושעי סייבר שהופכים לחסכניים יותר ותוקפים שכבר לא משלמים על טכנולוגיה. כדי להפחית את התקורה שלהם ולהגביר מראית עין של לגיטימיות, חלק מהתוקפים יותר ויותר מנסים להעמיד בסכנה עסקים כדי לארח קמפיינים של דיוג, תוכנות זדוניות או אפילו להשתמש בכוח המחשוב שלהם לכריית מטבעות קריפטוגרפיים.

בפרק זה נבחן גם את העלייה בהאקטיביזם, הפרעה הנגרמת על ידי אזרחים פרטיים המבצעים מתקפות סייבר לקידום מטרות חברתיות או פוליטיות. אלפי אנשים ברחבי העולם, מומחים ומתחילים כאחד, התגייסו מאז פברואר 2022 כדי לבצע מתקפות כגון השבתת אתרים והדלפת נתונים גנובים כחלק ממלחמת רוסיה-אוקראינה. מוקדם מדי לחזות אם מגמה זו תימשך גם לאחר תום מעשי האיבה הפעילים.

ארגונים חייבים לבחון ולחזק באופן קבוע את בקרות הגישה וליישם אסטרטגיות אבטחה כדי להתגונן מפני מתקפות סייבר. עם זאת, זה לא כל מה שביכולתם לעשות. אנו מסבירים כיצד היחידה לפשעים דיגיטליים (DCU) שלנו השתמשה במקרים אזרחיים כדי לתפוס תשתיות זדוניות המשמשות פושעי סייבר וגורמים מדינתיים. עלינו להילחם באיום זה יחד באמצעות שותפויות ציבוריות ופרטיות כאחד. אנו מקווים שבאמצעות שיתוף מה שלמדנו במהלך 10 השנים האחרונות, נעזור לאחרים להבין ולשקול את הצעדים הפרואקטיביים שהם יכולים לנקוט כדי להגן על עצמם ועל המערכת האקולוגית הרחבה יותר מפני האיום ההולך וגובר של פשעי סייבר.

איימי הוגן-ברני
מנכ"לית, היחידה לפשעים דיגיטליים

תוכנות כופר וסחיטה: איום ברמה הלאומית

מתקפות של תוכנות כופר מהוות סכנה מוגברת לכל האנשים מכיוון שתשתיות חיוניות, עסקים בכל הגדלים וממשלות מדינתיות ומקומיות מהווים מטרה עבור פושעים הממנפים מערכת אקולוגית הולכת וגדלה של פושעי סייבר.

במהלך השנתיים האחרונות, אירועים בעלי פרופיל גבוה של תוכנות כופר – כגון אלה שבהם היו מעורבים תשתיות חיוניות, שירותי בריאות וספקי שירותי IT – משכו תשומת לב ציבורית רבה. ככל שמתקפות כופר הפכו נועזות יותר בהיקפן, ההשפעות שלהן הפכו נרחבות יותר. להלן דוגמאות להתקפות שראינו כבר בשנת 2022:

- בחודש פברואר, התקפה על שתי חברות השפיעה על מערכות עיבוד התשלומים של מאות תחנות דלק בצפון גרמניה.[1]
- בחודש מרץ, מתקפה נגד שירות הדואר של יוון שיבשה באופן זמני את מסירת הדואר והשפיעה על עיבוד עסקאות פיננסיות.[2]
- בסוף חודש מאי, מתקפת כופר נגד גופי ממשל בקוסטה ריקה גרמה למצב חירום לאומי לאחר שבתי חולים הושבתו וגביית מכסים ומיסים שובשה.[3]
- בנוסף, בחודש מאי, מתקפה גרמה לעיכובים וביטולים בטיסות של אחת מחברות התעופה הגדולות בהודו, והותירה מאות נוסעים תקועים.[4]

הצלחתן של מתקפות אלה והיקף השפעותיהן בעולם האמיתי הם תוצאה של תיעוש כלכלת פשעי הסייבר, המאפשר גישה לכלים ולתשתיות והרחבת יכולות פושעי הסייבר על ידי הורדת חסם המיומנות שלהם לכניסה.

בשנים האחרונות, תוכנות כופר עברו ממודל שבו "כנופיה" אחת מפתחת ומפיצה מטען של תוכנת כופר למודל של תוכנת כופר כשירות (RaaS). מודל RaaS מאפשר לקבוצה אחת לנהל את הפיתוח של מטען תוכנת הכופר ולספק שירותים לתשלום וסחיטה באמצעות הדלפת נתונים לפושעי סייבר אחרים – אלה שלמעשה מפעילים את מתקפות הכופר – המכונים "שותפים" תמורת נתח מהרווחים. זכיינות זו של כלכלת פשעי הסייבר הרחיבה את מאגר התוקפים. תיעוש הכלים של פושעי הסייבר הקל על התוקפים לבצע חדירות, לחלץ נתונים ולפרוס תוכנות כופר.

תוכנת כופר המופעלת על ידי בני אדם[5] – מונח שטבעו חוקרי Microsoft כדי לתאר איומים המונעים על ידי בני אדם שמקבלים החלטות בכל שלב של ההתקפות בהתבסס על מה שהם מגלים ברשת היעד שלהם ומגדירים את האיום מהתקפות של תוכנות כופר על סחורות – ממשיכה להיות איום משמעותי על ארגונים.

המודל מבוסס על נתוני 'Microsoft Defender עבור נקודות קצה' (EDR) (ינואר-יוני 2022).

תוכנות כופר וסחיטה: איום ברמה הלאומית

המשך

מתקפות של תוכנות כופר הפכו לבעלות השפעה רבה עוד יותר מכיוון שאימוץ אסטרטגיית מונטיזציה של סחיטה כפולה הפך לנוהג סטנדרטי. פעולה הכרוכה בחילוץ נתונים ממכשירים שנפרצו, הצפנת הנתונים במכשירים ולאחר מכן פרסום הנתונים הגנובים בפומבי או איום לפרסמם כדי ללחוץ על הקורבנות לשלם כופר.

על אף שרוב תוקפי תוכנות הכופר פורסים באופן אופורטוניסטי תוכנות כופר בכל רשת שהם מקבלים גישה אליה, חלקם רוכשים גישה מפושעי סייבר אחרים, וממנפים קשרים בין מתווכי גישה למפעילי תוכנות כופר.

ההיקף הייחודי של מודיעין האותות שלנו נאסף ממקורות מרובים – זהות, דואר אלקטרוני, נקודות קצה וענן – ומספק תובנות לגבי כלכלת תוכנות הכופר הצומחת, בצרוף מערכת שותפים הכוללת כלים המיועדים לתוקפים בעלי יכולת טכנית נמוכה יותר.

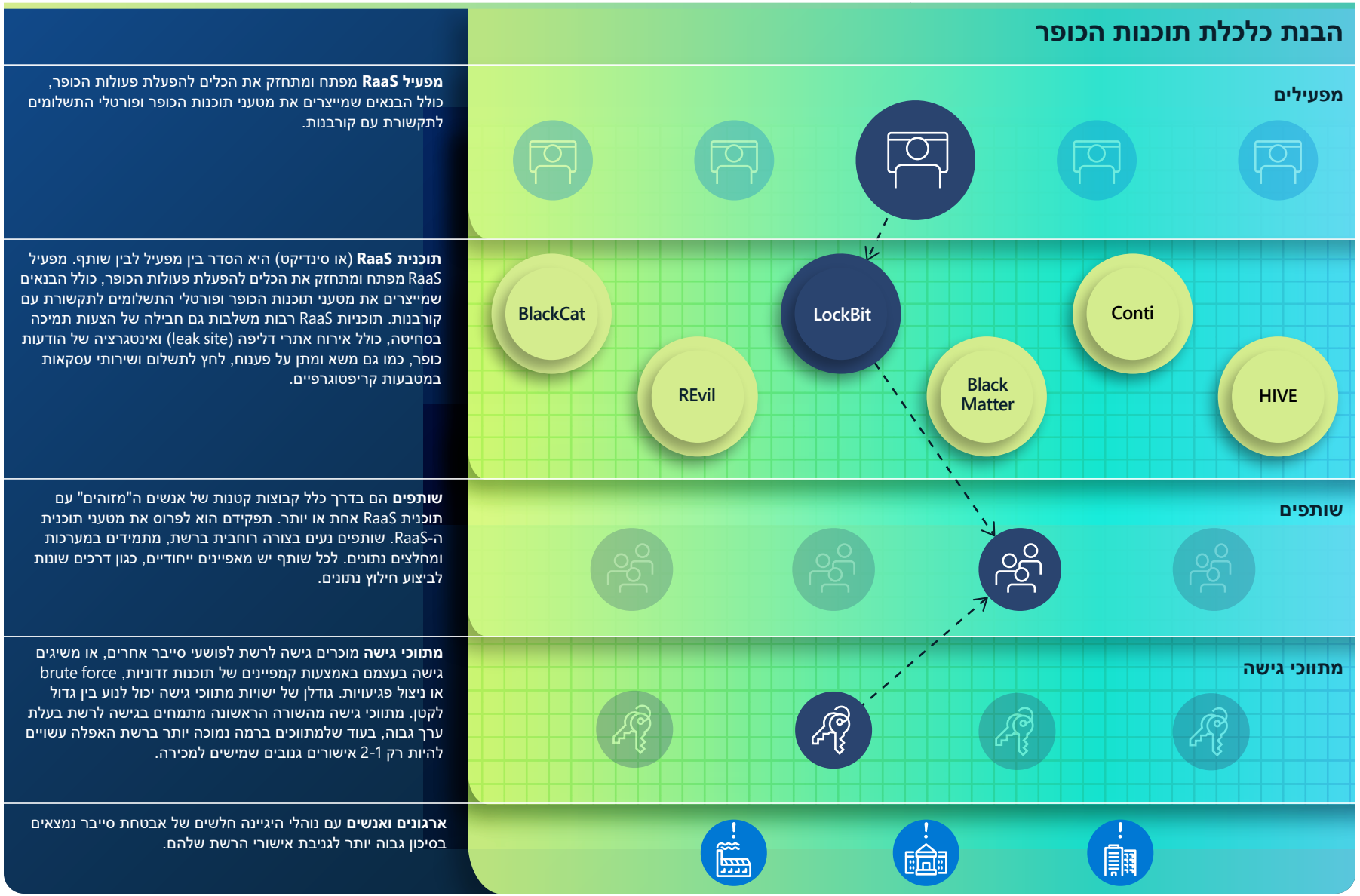
הרחבת הקשרים בין פושעי סייבר מתמחים הגבירה את הקצב, התחכום וההצלחה של מתקפות כופר. זה הניע את האבולוציה של המערכת האקולוגית של פושעי הסייבר לשחקנים המחוברים ביניהם עם טכניקות, מטרות ומערכי כישורים שונים שתומכים זה בזה בגישה ראשונית ליעדים, לשירותי תשלום ולכלים או לאתרים של פענוח או פרסום.

מפעילי תוכנות כופר יכולים כעת לרכוש גישה לארגונים או לרשתות ממשלתיות באופן מקוון או לקבל אישורים וגישה באמצעות יחסים בינאישיים עם מתווכים שמטרתם העיקרית היא אך ורק להפיק רווחים מהגישה שהם השיגו.

לאחר מכן, המפעילים משתמשים בגישה שנרכשה כדי לפרוס מטען של תוכנת כופר שנקנה דרך שווקים או פורומים ברשת האפלה. במקרים רבים, המשא ומתן עם הקורבנות מתנהל על ידי צוות RaaS, ולא על ידי המפעילים עצמם. עסקאות פליליות אלה הן חלקות והסיכוי שהמשתתפים ייעצרו ויועמדו לדין קטן בשל האנונימיות של הרשת האפלה והקושי לאכוף חוקים באופן על-לאומי.

מאמץ בר-קיימא ומוצלח נגד איום זה יחייב אסטרטגיה ממשלתית שלמה שתבוצע בשותפות הדוקה עם המגזר הפרטי.

פעילות האיומים הדיגיטליים נמצאת בשיא של כל הזמנים ורמת התחכום עולה מדי יום.



בניגוד לאופן שבו תוכנות כופר מוצגות לעתים בתקשורת, נדיר שגרסת תוכנות כופר אחת תנוהל על ידי "כנופיית כופר" אחת מקצה לקצה. במקום זאת, ישנן ישויות נפרדות שבונות תוכנות זדוניות, משיגות גישה לקורבנות, פורסות תוכנות כופר ומנהלות משא ומתן על סחיטה. התיעוש של המערכת האקולוגית הפלילית הוביל אל:

- מתווכי גישה שפורצים פנימה ומוסרים גישה (גישה כשירות).
- מפתחי תוכנות זדוניות שמוכרים כלים.
- מפעילים פליליים ושותפים המבצעים פריצות.
- ספקי שירותי הצפנה וסחיטה שמשתלטים על מונטיזציה משותפים (RaaS).

כל הקמפיינים של תוכנות כופר המופעלות על ידי בני אדם חולקים יחסי תלות משותפים בחולשות אבטחה. באופן ספציפי, תוקפים בדרך כלל מנצלים את היגיינת הסייבר הירודה של הארגון, הכוללת לעתים קרובות תיקונים בתדירות נמוכה וכשל ביישום אימות רב-גורמי (MFA).

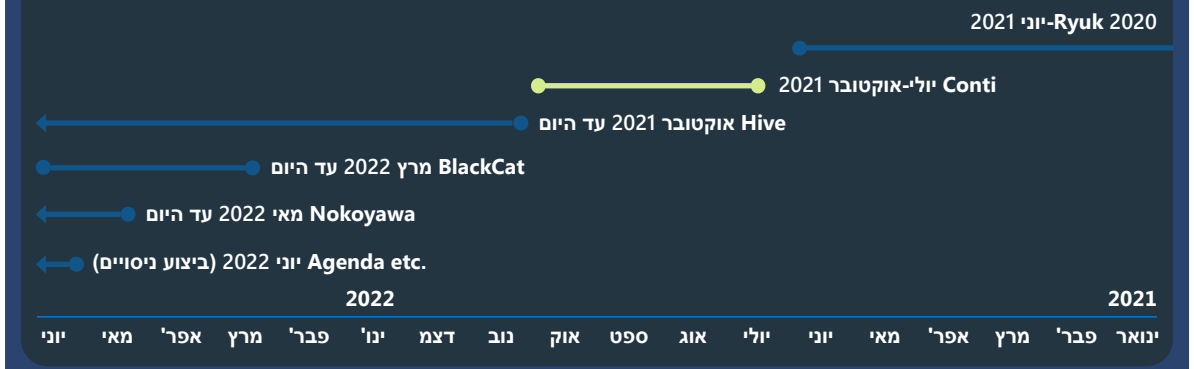
סיפור לקוח: הפירוק של Conti

Conti, אחת הגרסאות המובילות של תוכנות כופר בשנתיים האחרונות, החלה להשבית את פעילותה באמצע שנת 2022, כאשר מרכז מודיעין האיומים של Microsoft (MSTIC) הבחין בירידה משמעותית בפעילותה בסוף מרץ ובתחילת אפריל. הבחנו בפריסות האחרונות של תוכנות הכופר של Conti באמצע חודש אפריל. עם זאת, בדומה לסגירת פעולות אחרות של תוכנות כופר, לפירוק של Conti לא הייתה השפעה משמעותית על פריסות תוכנות הכופר, מאחר ש-MSTIC הבחין שהשותפים של Conti מתמקדים בפריסת מטעני כופר אחרים, בכללם BlackBasta, Lockbit 2.0, LockbitBlack ו-HIVE. הבחנה זו עולה בקנה אחד עם נתונים משנים קודמות ומעידה על כך שכאשר כנופיות תוכנות כופר עוברות למצב לא מקוון, הן צצות שוב חודשים לאחר מכן או מפיצות מחדש את היכולות הטכניות והמשאבים שלהן לקבוצות חדשות.

צוותי מודיעין האיום שלנו ב-Microsoft עוקבים אחר גורמי האיום של תוכנות הכופר כקבוצות בודדות (המסומנות כ- DEVs) בהתבסס על הכלים הספציפיים שלהם, במקום לעקוב אחריהם על בסיס התוכנה הזדונית שבה הם משתמשים. משמעות הדבר היא שכאשר השותפים של Conti התפזרו, יכולנו להמשיך לעקוב אחר ה-DEVs האלה באמצעות השימוש שלהם בכלים אחרים או בערכות RaaS. לדוגמה:

- DEV-0230, המזוהה עם Trickbot, היה משתמש פורה של Conti. בסוף אפריל, MSTIC הבחינה בו משתמש ב-QuantumLocker.
- DEV-0237 עבר מערכת הכופר של Conti ל-HIVE ול-Nokoyawa, כולל שימוש ב-HIVE במתקפה נגד גופי ממשל בקוסטה ריקה ב-31 במאי.
- DEV-0506, משתמש פורה נוסף בערכת תוכנות הכופר של Conti, נצפה משתמש ב-BlackBasta.

דוגמה לשותף (DEV-0237) שעובר במהירות בין תוכניות RaaS



לאחר שתוכנת RaaS כמו Conti נסגרת, שותף תוכנת הכופר עובר לתוכנת כופר אחרת (Hive) כמעט מיד.

RaaS מפתח את המערכת האקולוגית של תוכנות כופר ומעכב ייחוס

מכיוון שתוכנות כופר המופעלות על ידי בני אדם מונעות על ידי מפעילים בודדים, דפוסי התקיפה משתנים בהתאם ליעד ומתחלפים לאורך כל משך המתקפה. בעבר, ראינו קשר הדוק בין וקטור הכניסה הראשוני, הכלים ובחירות המטען של תוכנות הכופר בכל קמפיין של זן תוכנת כופר אחד. זה הפך את הייחוס לקל יותר. מודל השותפים של RaaS, לעומת זאת, מנתק את מערכת היחסים הזו. כתוצאה מכך, Microsoft עוקבת אחר שותפים לתוכנות כופר שפורסים מטענים בהתקפות ספציפיות, במקום לעקוב אחר מפתחי מטעני תוכנות הכופר כמפעילים.

במילים אחרות, אנחנו כבר לא מניחים שמפתח ה-HIVE הוא המפעיל מאחורי מתקפת כופר ה-HIVE; סביר יותר שהוא יהיה שותף.

תעשיית אבטחת הסייבר התקשתה ללכוד כראוי את התיחום הזה בין מפתחים למפעילים. התעשייה עדיין מדווחת לעתים קרובות על אירוע תוכנת כופר לפי שם המטען שלה, דבר שיוצר את הרושם המוטעה שישות אחת או כנופיית תוכנות כופר אחת, עומדת מאחורי כל ההתקפות שמשתמשות באותו מטען של תוכנות כופר מסוים, וכל האירועים הקשורים אליו חולקים טכניקות ותשתיות משותפות. כדי לתמוך במגיני רשת, חשוב לקבל מידע נוסף על השלבים שקדמו להתקפות של שותפים שונים – כגון חילוץ נתונים ומנגנוני התמדה נוספים – ועל הזדמנויות הזיהוי וההגנה שעשויות להתקיים.

כדי להצליח בפעולות שלהם, תוקפים זקוקים לאישורים יותר מאשר לתוכנות זדוניות. ההדבקה המוצלחת של ארגון שלם באמצעות תוכנות כופר המופעלות על ידי בני אדם מסתמכת על גישה לחשבון בעל הרשאות גבוהות.

זרקור על מתקפות כופר המופעלות על ידי בני אדם

במהלך השנה האחרונה, מומחי תוכנות הכופר של Microsoft ערכו חקירות מעמיקות של יותר מ-100 אירועי תוכנות כופר שהופעלו על-ידי בני אדם כדי לעקוב אחר הטכניקות של התוקפים ולהבין כיצד להגן טוב יותר על הלקוחות שלנו.

חשוב לציין שהניתוח שאנו משתפים כאן אפשרי רק עבור מכשירים שנקלטו בארגון ומנוהלים בו. מכשירים שלא נקלטו בארגון ואינם מנוהלים בו מייצגים את החלק הכי פחות מאובטח של נכסי החומרה של הארגון.

הטכניקות הנפוצות ביותר בשלב תוכנות הכופר:

75%

משתמשות בכלי ניהול.

75%

משתמשות בחשבון משתמש שנרכש, נפרץ ושופר כדי להפיץ מטענים זדוניים באמצעות פרוטוקול SMB.

99%

מנסות לחבל במוצרי אבטחה וגיבוי שהתגלו באמצעות כלים שנבנו על ידי מערכת ההפעלה.

ההתקפה הטיפוסית המופעלת על ידי בני אדם

ניתן לסווג מתקפות כופר המופעלות על ידי בני אדם לשלב קדם תוכנת הכופר ולשלב פריסת תוכנת הכופר. במהלך שלב קדם תוכנת הכופר, התוקפים מתכוננים לחדור לרשת על ידי למידה על הטיפולוגיה ועל תשתית האבטחה של הארגון.

החקירות שלנו מצאו שרוב הגורמים שעומדים מאחורי מתקפות כופר המופעלות על ידי בני אדם מנצלים חולשות אבטחה דומות וחולקים דפוסי תקיפה וטכניקות משותפים.

אסטרטגיית אבטחה עמידה

לחימה בהתקפות מסוג זה ומניעתן מחייבות שינוי בהלך הרוח של הארגון כדי להתמקד בהגנה המקיפה הנדרשת כדי להאט ולעצור תוקפים לפני שהם יכולים לעבור משלב קדם תוכנת הכופר לשלב פריסת תוכנות הכופר.

ארגונים חייבים ליישם ברשתות שלהם שיטות עבודה מומלצות לאבטחה באופן עקבי ואגרסיבי, במטרה לצמצם סוגים של התקפות. בשל קבלת ההחלטות האנושית, מתקפות כופר אלה יכולות ליצור התראות מוצרי אבטחה מרובות ושונות לכאורה, אשר יכולות בקלות ללכת לאיבוד או לא להיענות בתגובה בזמן. עייפות התראות היא אמיתית, ומרכזי תפעול האבטחה (SOCs) יכולים להקל על חייהם על-ידי התבוננות במגמות בהתראות שלהם או קיבוץ התראות לאירועים כדי שיוכלו לראות את התמונה הגדולה. לאחר מכן, SOCs יכולים לצמצם התראות באמצעות יכולות הקשחה כגון כללי צמצום שטח התקיפה. הקשחה מול איומים נפוצים לא רק שיכולה להפחית את נפח ההתראות, אלא גם לעצור תוקפים רבים לפני שהם מקבלים גישה לרשתות.

ארגונים חייבים לשמור באופן רצוף על סטנדרטים גבוהים של מערך האבטחה והיגיינת הרשת כדי להגן על עצמם מפני התקפות כופר המופעלות על ידי בני אדם.

תובנות מעשיות

המניעים של תוקפי תוכנות כופר הם לרוב רווחים קלים, ולכן אם מוסיפים מחסומים בפניהם באמצעות הקשחת האבטחה, זהו המפתח לשיבוש כלכלת פושעי הסייבר.

1. יצירת היגיינה של אישורי כניסה. כדי להצליח בפעולות שלהם, תוקפים זקוקים לאישורים יותר מאשר לתוכנות זדוניות. ההדבקה המוצלחת של ארגון שלם בתוכנת כופר המופעלת על-ידי בני אדם מסתמכת על גישה לחשבון בעל הרשאות גבוהות כגון חשבון מנהל תחום, או על יכולות לערוך מדיניות קבוצתית.
2. ביקורת חשיפה של אישורים.
3. תעדוף פריסה של עדכוני Active Directory.
4. תעדוף הקשחת הענן.
5. צמצום משטח התקיפה.
6. הקשחת נכסים הפונים לאינטרנט והבנת ההיקף שלכם.
7. הפחתת עייפות התראות SOC על-ידי הקשחת הרשת כדי להפחית את הנפח ולשמר את רוחב הפס עבור אירועים בעדיפות גבוהה.

קישורים למידע נוסף

- RaaS: הבנת כלכלת החלטורה של פשעי סייבר וכיצד להגן על עצמך | הבלוג של Microsoft Security
- מתקפות כופר המופעלות על ידי בני אדם: אסון הניתן למניעה | הבלוג של Microsoft Security

תובנות לגבי תוכנות כופר מהמגיבים בקו הראשון

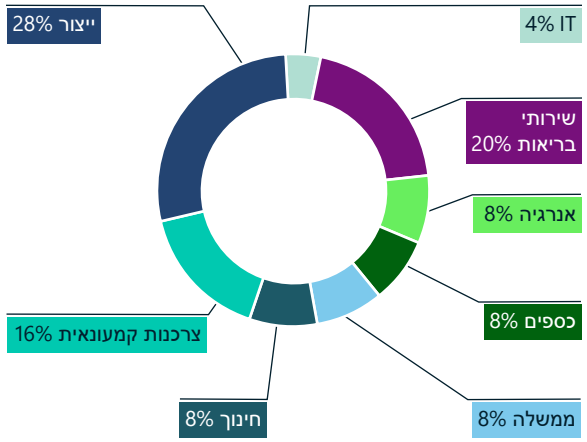
ארגונים ברחבי העולם חוו צמיחה מתמדת במתקפות כופר המופעלות על ידי בני אדם החל משנת 2019. עם זאת, למבצעי אכיפת החוק ולאירועים גיאופוליטיים בשנה האחרונה הייתה השפעה משמעותית על ארגוני פושעי הסייבר.

קו שירותי האבטחה של Microsoft תומך בלקוחות במהלך מתקפת הסייבר כולה, החל מחקירה וכלה בפעילויות הכלה ושחזור מוצלחות. שירותי התגובה והשחזור מוצעים באמצעות שני צוותים משולבים ברמה גבוהה, כאשר האחד מתמקד בחקירה וביסודות השחזור והשני בבלימה ובשחזור. חלק זה מציג סיכום של ממצאים המבוססים על התקשרויות כופר בשנה האחרונה.

93%

מהחקירות של Microsoft במהלך התקשרויות לשחזור מתוכנות כופר חשפו בקרות הרשאות גישה ובקרות תנועה רוחבית בלתי מספיקות.

התקשרויות של אירועי תוכנות כופר ושחזור לפי תעשייה

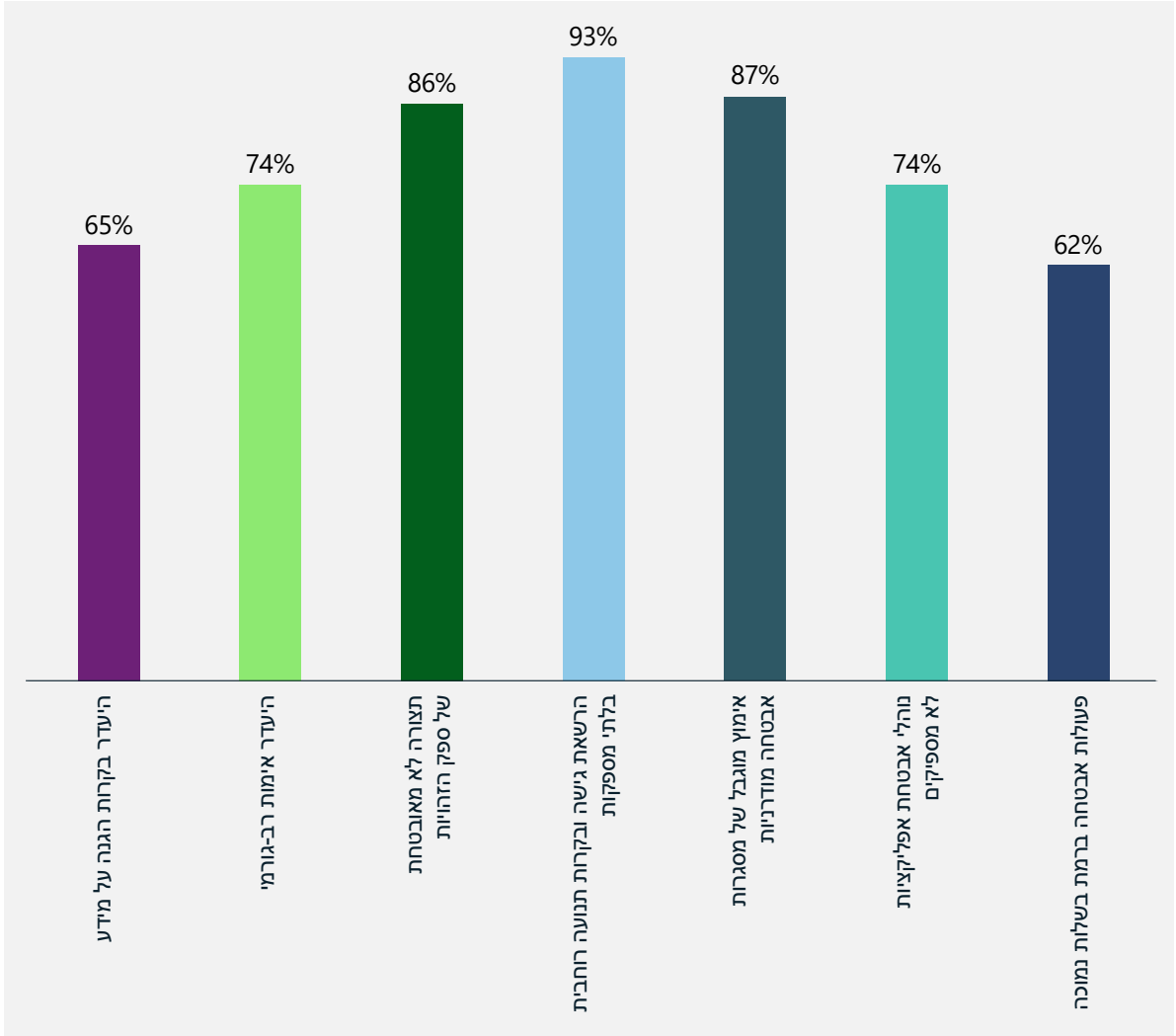


כאשר קבוצות קטנות ואיומים חדשים צצים, צוותי הגנה חייבים להיות מודעים לאיומי תוכנות כופר מתפתחים תוך הגנה מפני משפחות תוכנות זדוניות של תוכנות כופר שלא היו ידועות קודם לכן. גישת הפיתוח המהיר המשמשת קבוצות פשע הובילה ליצירת תוכנות כופר חכמות הארוזות בערכות קלות לשימוש. זה מאפשר גמישות רבה יותר בשיגור התקפות נרחבות על מספר רב יותר של מטרות.

הדפים הבאים מספקים מבט מעמיק יותר על הגורמים התורמים הנפוצים ביותר להגנה חלשה מפני תוכנות כופר, המקובצים לשלוש קטגוריות של ממצאים:

1. בקרת זהויות חלשה
2. פעולות אבטחה לא יעילות
3. הגנה מוגבלת על נתונים

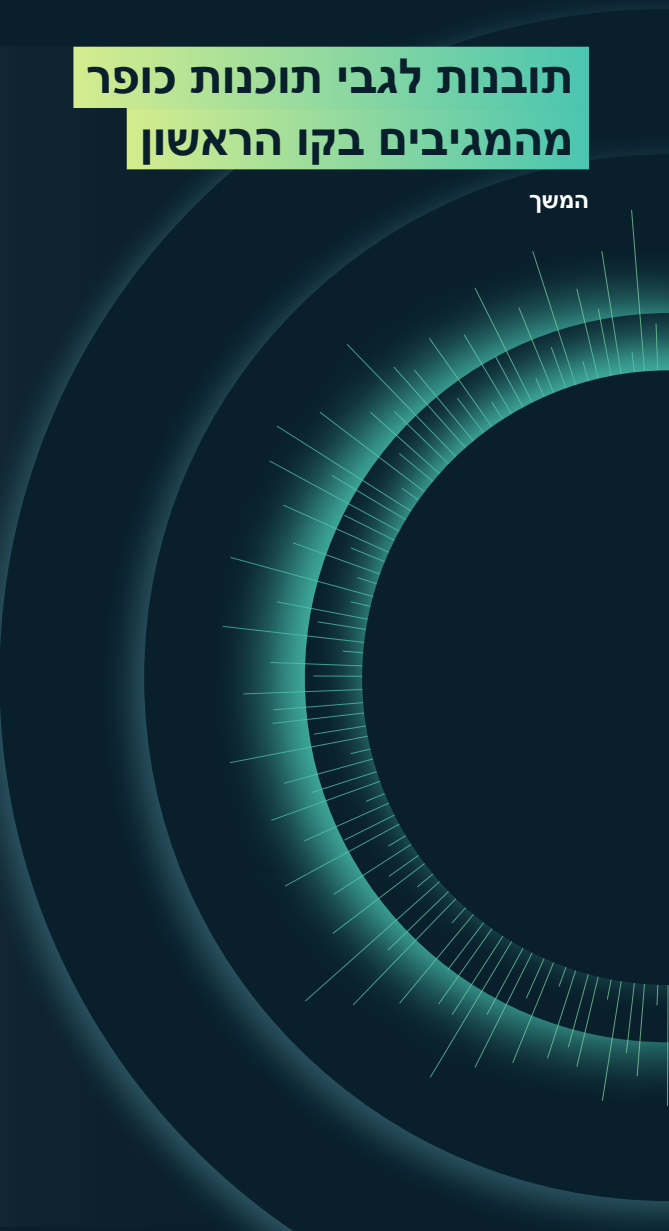
סיכום הממצאים הנפוצים ביותר בהתקשרויות תגובה לתוכנות כופר



הממצא הנפוץ ביותר בקרב התקשרויות תגובה לאירועי תוכנות כופר היה בקרות הרשאות גישה ובקרות תנועה רוחבית בלתי מספיקות.

תובנות לגבי תוכנות כופר מהמגיבים בקו הראשון

המשך



שלושת הגורמים התורמים העיקריים שנראו בהתקשרויות התגובה שלנו באתר:

① בקרת זהויות חלשה:
מתקפות גניבת אישורים הן עדיין אחד הגורמים התורמים המובילים

② תהליכי פעולות אבטחה
לא יעילים לא רק מהווים חלון הזדמנויות עבור התוקפים, אלא גם משפיעים באופן משמעותי על זמן ההתאוששות

③ בסופו של דבר זה מסתכם בנתונים – ארגונים מתקשים ליישם אסטרטגיה יעילה להגנה על נתונים התואמת את הצרכים העסקיים שלהם

① בקרת זהויות חלשה

תוכנות כופר המופעלות על ידי בני אדם ממשיכות להתפתח ולהשתמש בשיטות גניבת אישורים ותנועה רוחבית הקשורות באופן מסורתי להתקפות ממוקדות. מתקפות מוצלחות הן לעתים קרובות תוצאה של קמפיינים ארוכי טווח הכוללים פגיעה במערכות זהות, כגון Active Directory (AD), המאפשרות למפעילים אנושיים לגנוב אישורים, לגשת למערכות ולהמשיך להישאר ברשת.

אבטחה עם Active Directory (AD) ועם Azure AD

88%

מהלקוחות שנפגעו לא השתמשו בשיטות העבודה המומלצות לאבטחה של AD ו-Azure AD. זה הפך לווקטור תקיפה נפוץ כאשר תוקפים מנצלים תצורות שגויות ומערכי אבטחה חלשים יותר במערכות זהויות קריטיות כדי לקבל גישה והשפעה רחבות יותר לעסקים.

גישה ושימוש בהרשאות מינימליות בתחנות עבודה של גישה מורשית (PAW)

אף אחד מהארגונים המושפעים לא יישם את ההפרדה הנכונה בין אישורי ניהול ועקרונות הרשאת גישה מינימלית באמצעות תחנות עבודה ייעודיות במהלך ניהול הזהות הקריטית והנכסים בעלי הערך הגבוה שלהם, כגון מערכות קנייניות ואפליקציות קריטיות לפעילות העסקית.

אבטחת חשבון מורשה

88%

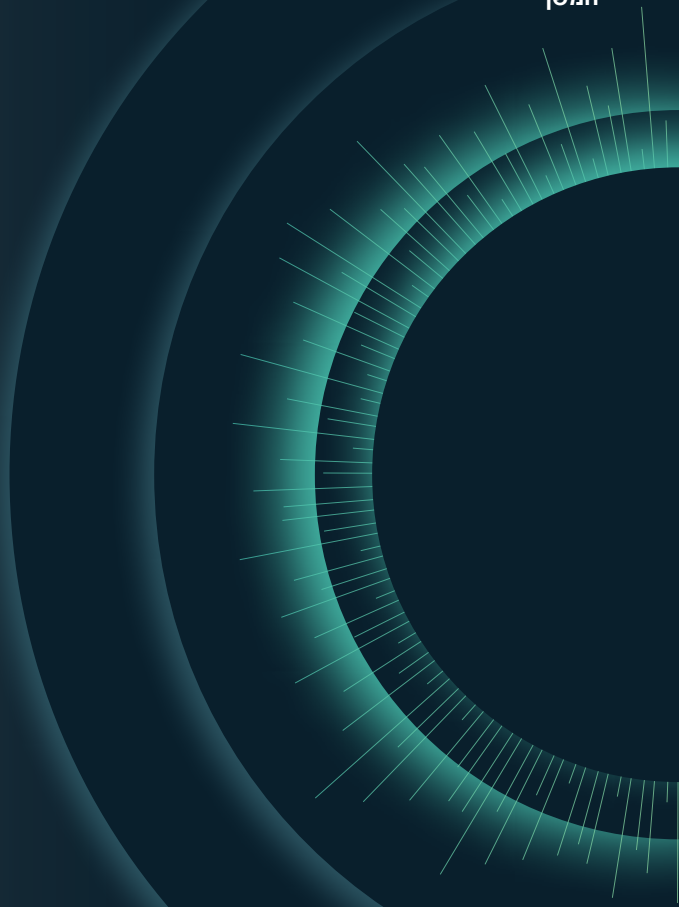
מבין ההתקשרויות, MFA לא יושם עבור חשבונות רגישים ובעלי הרשאות גבוהות, דבר שהותיר פער אבטחה לתוקפים לפרוץ לאישורים ולבצע התקפות נוספות באמצעות אישורים לגיטימיים.

84%

מנהלי מערכת ב-84 אחוז מהארגונים לא השתמשו באמצעי בקרת הרשאת זהויות כגון גישה 'בדיוק בזמן' כדי למנוע שימוש זדוני נוסף באישורים מורשים שנפרצו.

תובנות לגבי תוכנות כופר מהמגיבים בקו הראשון

המשך



② פעולות אבטחה לא יעילות

הנתונים שלנו מראים שלארגונים שסבלו ממתקפות כופר יש פערים משמעותיים בפעולות האבטחה, בכלים ובניהול מחזור החיים של נכסי טכנולוגיית המידע שלהם. בהתבסס על הנתונים הזמינים, הפערים הבאים נצפו ביותר:

תיקון:

68%

מהארגונים שנפרצו לא יישמו תהליך יעיל של ניהול פגיעויות ותיקונים, ותלות גבוהה בתהליכים ידניים לעומת תיקונים אוטומטיים הובילה לפרצות קריטיות. ייצור ותשתיות חיוניות ממשיכים להתקשות בתחזוקה ובתיקון של מערכות טכנולוגיה תפעולית מדור קודם (OT).

היעדר כלי פעולות אבטחה:

רוב הארגונים דיווחו על היעדר נראות אבטחה מקצה לקצה עקב היעדר כלי אבטחה או הגדרה שגויה שלהם, דבר שהוביל לירידה ביעילות הזיהוי והתגובה.

60%

מהארגונים דיווחו כי לא נעשה שימוש בכלי EDR[6], טכנולוגיה בסיסית לזיהוי ותגובה.

60%

לא השקיעו בטכנולוגיית אבטחת מידע וניהול אירועים (SIEM) המובילה לניטור ממגורות, יכולת מוגבלת לזהות איומים מקצה לקצה ופעולות אבטחה לא יעילות. אוטומציה נותרה פער מרכזי בכלים ובתהליכים של SOC, דבר שמאלץ את צוות ה-SOC להשקיע אינספור שעות בהבנת טלמטריה של אבטחה.

84%

מהארגונים המושפעים לא אפשרו אינטגרציה של הסביבות מרובות העננים שלהם בכלי פעולות האבטחה שלהם.

תהליכי תגובה והתאוששות:

76%

היעדר תוכנית תגובה יעילה היה תחום קריטי שנצפה ב-76 אחוז מהארגונים שנפגעו, דבר שמונע מוכנות ארגונית נכונה למשבר ומשפיע לרעה על זמן התגובה וההתאוששות.

③ הגנה מוגבלת על נתונים

לארגונים רבים שנפרצו לא היו תהליכים מתאימים להגנה על נתונים, עובדה שהובילה לפגיעה קשה בזמני ההתאוששות וביכולת לחזור לפעילות העסקית. הפערים הנפוצים ביותר שבהם נתקלנו כוללים:

גיבוי בלתי משתנה:

44%

מהארגונים לא היו ברשותם גיבויים בלתי משתנים עבור המערכות שנפגעו. הנתונים גם מראים שלמנהלי מערכת לא היו גיבויים ותוכניות שחזור עבור נכסים קריטיים כגון AD.

מניעת אובדן נתונים:

תוקפים בדרך כלל מוצאים את דרכם לפריצת מערכות באמצעות ניצול פגיעויות בארגון, חילוץ נתונים קריטיים לסחיטה, גניבת קניין רוחני או מונטיזציה.

92%

מהארגונים שנפגעו לא יישמו בקרות יעילות למניעת אובדן נתונים כדי לצמצם סיכונים אלה, דבר שהוביל לאובדן נתונים קריטיים.

תוכנות כופר ירדו באזורים מסוימים ועלו באחרים

השנה ראינו ירידה במספר הכולל של מקרי תוכנות כופר שדווחו לצוותי התגובה שלנו בצפון אמריקה ובאירופה בהשוואה לשנה הקודמת. במקביל, מספר המקרים שדווחו באמריקה הלטינית עלה.

בעוד שסביר להניח שפעילויות אכיפת החוק האטו את תדירות ההתקפות בשנת 2022, גורמי איום עשויים בהחלט לפתח אסטרטגיות חדשות כדי להימנע מלהיתפס בעתיד.

פי 2

מתקפות תוכנות כופר פחתו באזורים מסוימים, אך דרישות הכופר יותר מהכפילו את עצמן.

פרשנות אחת לתצפית זו היא שפושעי סייבר מתרחקים מתחומים הנתפסים כבעלי סיכון גבוה יותר לעורר חקירה של רשויות אכיפת החוק לטובת מטרות קלות יותר. מכיוון ש-Microsoft לא ראתה שיפור משמעותי באבטחת הרשתות הארגוניות ברחבי העולם כדי להסביר את הירידה בשיחות תמיכה הקשורות לתוכנות כופר, אנו מאמינים שהסיבה הסבירה ביותר היא שילוב של פעילות אכיפת החוק בשנים 2021 ו-2022 שהגדילה את עלות הפעילות הפלילית, יחד עם כמה אירועים גיאופוליטיים שאירעו ב-2022.

אחד ממבצעי ה-RaaS הנפוצים ביותר שייך לארגון פשע דובר רוסית המכונה REvil (הידוע גם בשם Sodinokibi) הפעיל מאז 2019. באוקטובר 2021, השרתים של REvil נותקו מהרשת כחלק ממבצע אכיפת החוק הבינלאומי GoldDust.[7] בינואר 2022 עצרה רוסיה 14 חברי REvil לכאורה ופשטה על 25 אתרים הקשורים אליהם.[8] זו הייתה הפעם הראשונה שרוסיה פעלה נגד מפעילי תוכנות כופר על אדמתה.

בעוד שסביר להניח שפעילויות אכיפת החוק האטו את תדירות ההתקפות בשנת 2022, גורמי איום עשויים בהחלט לפתח אסטרטגיות חדשות כדי להימנע מלהיתפס בעתיד. יתר על כן, נראה כי המתיחות בין רוסיה לארצות הברית סביב פלישת רוסיה לאוקראינה שמה קץ לשיתוף הפעולה המתהווה של רוסיה במאבק העולמי נגד תוכנות כופר. לאחר תקופה קצרה של חוסר ודאות בעקבות מעצרי REvil, ארצות הברית ורוסיה הפסיקו את שיתוף הפעולה במרדף אחר גורמי כופר, דבר שמשמעותו שפושעי סייבר עשויים לראות את רוסיה שוב כמקלט בטוח.

במבט קדימה, אנו צופים שקצב הפעילות של תוכנות כופר יהיה תלוי בתוצאה של כמה שאלות מפתח:

1. האם ממשלות יפעלו כדי למנוע מפושעי תוכנות כופר לפעול בגבולותיהן, או ישאפו להפריע לגורמים הפועלים ממדינות זרות?
2. האם קבוצות של תוכנות כופר ישנו את הטקטיקה כדי להסיר את הצורך בתוכנות כופר וישתמשו בהתקפות בסגנון סחיטה?
3. האם ארגונים יוכלו להפוך את פעולות ה-IT שלהם למודרניות ולשנות אותן מהר יותר מכפי שפושעים יכולים לנצל פגיעויות?
4. האם ההתקדמות במעקב אחר תשלומי כופר וההתחקות אחריהם תאלץ את מקבלי הכופר לשנות טקטיקות ומשא ומתן?

תובנות מעשיות

1. יש להתמקד באסטרטגיות אבטחה הוליסטיות, מכיוון שכל משפחות תוכנות הכופר מנצלות את אותן חולשות אבטחה כדי לפגוע ברשת.
2. יש לעדכן ולשמור על יסודות האבטחה כדי להגביר את רמת ההגנה הבסיסית המעמיקה של ההגנה ולהפוך את פעולות האבטחה למודרניות. המעבר לענן מאפשר זיהוי איומים במהירות רבה יותר ולהגיב מהר יותר.

קישורים למידע נוסף

- הגנה על הארגון מפני תוכנות כופר | Microsoft Security
- 7 דרכים להקשחת הסביבה מפני פריצה | הבלוג של Microsoft Security
- שיפור הגנות מבוססות בינה מלאכותית כדי לשבש תוכנות כופר המופעלות על ידי בני אדם | Microsoft 365 Defender
- Security Insider: גילוי התובנות והעדכונים האחרונים בנושא אבטחת סייבר | Microsoft Security

פשעי סייבר כשירות

פשעי סייבר כשירות (CaaS) הם איום הולך ומתפתח על לקוחות ברחבי העולם. יחידת הפשעים הדיגיטליים של Microsoft (DCU) הבחינה בצמיחה מתמשכת של המערכת האקולוגית של CaaS עם מספר גדל והולך של שירותים מקוונים המאפשרים פשעי סייבר שונים, כולל BEC ותוכנות כופר המופעלות על ידי בני אדם. דיוג ממשיך להיות שיטת תקיפה מועדפת מכיוון שפושעי סייבר יכולים להפיק ערך משמעותי מגניבה ומכירה מוצלחות של גישה לחשבונות גנובים.

בתגובה לשוק ה-CaaS המתרחב, DCU שיפרה את מערכות ההאזנה שלה כדי לאתר ולזהות הצעות CaaS בכל המערכת האקולוגית של האינטרנט, הרשת העמוקה, פורומים בדוקים,[9] אתרים ייעודיים, פורומים מקוונים לדיונים ופלטפורמות העברת הודעות.

פושעי סייבר משתפים כעת פעולה בין אזורי זמן ושפות שונות כדי לספק תוצאות ספציפיות. לדוגמה, אתר CaaS אחד המנוהל על ידי אדם באסיה מתחזק פעילות באירופה, ויוצר חשבונות זדוניים באפריקה. האופי מרובה תחומי השיפוט של פעולות אלה מציב אתגרים מורכבים בתחום החוק והאכיפה. בתגובה, DCU ממקדת את מאמציה בהשבתת תשתית פלילית זדונית המשמשת לסיוע בביצוע התקפות CaaS ומשתפת פעולה עם רשויות אכיפת החוק ברחבי העולם כדי למצות את הדין עם פושעים.

פושעי סייבר משתמשים יותר ויותר בניתוחי נתונים כדי למקסם את התפוצה, ההיקף והרווח. בדומה לעסקים לגיטימיים, אתרי CaaS חייבים לוודא את תקפותם של מוצרים ושירותים כדי לשמור על מוניטין מבוסס. לדוגמה, אתרי CaaS הופכים באופן שגרתי את הגישה לחשבונות שנפרצו לאוטומטית כדי לוודא את תקפותם של אישורים שנפרצו. פושעי סייבר יפסיקו למכור חשבונות ספציפיים כאשר סיסמאות מתאפסות או כאשר פגיעויות מתוקנות. יותר ויותר, זיהינו אתרי CaaS המספקים לקונים אימות לפי דרישה כתהליך בקרת איכות. כתוצאה מכך, הקונים יכולים להרגיש בטוחים שאתר ה-CaaS מוכר חשבונות וסיסמאות פעילים תוך הפחתת העלויות הפוטנציאליות לסוחר ה-CaaS אם האישורים הגנובים יתוקנו לפני מכירתם.

DCU גם הבחינה באתרי CaaS המציעים לקונים את האפשרות לרכוש חשבונות שנפרצו ממיקומים גיאוגרפיים ספציפיים, ספקי שירותים מקוונים ייעודיים, ואנשים פרטיים, מקצועות ותעשיות המהווים יעד באופן ספציפי. חשבונות שהוזמנו לעתים קרובות מתמקדים באנשי מקצוע או במחלקות שמעבדות חשבוניות, כגון סמנכ"לי כספים או "חשבונות חייבים". באופן דומה, תעשיות המשתתפות בקבלנות ציבורית מהוות לעתים קרובות מטרה בשל כמות המידע הזמינה באמצעות תהליך המכרז הציבורי.

חקירות ה-DCU בנוגע ל-CaaS העלו מספר מגמות מרכזיות:

מספר השירותים ותחכומם הולך וגדל.

דוגמה אחת היא האבולוציה של מעטפות אינטרנט המורכבות בדרך כלל משרתי אינטרנט פרוצים המשמשים לאוטומציה של התקפות דיוג. DCU הבחינה במשווקי CaaS שמפשטים את ההעלאה של ערכות דיוג או תוכנות זדוניות באמצעות דאשבורדים מיוחדים באינטרנט. מוכרי CaaS מנסים לעתים קרובות למכור לאחר מכן שירותים נוספים לגורם האיום דרך הדאשבורד, כגון שירותי הודעות ספאם ורשימות מיוחדות של נמעני דואר זבל המבוססות על תכונות מוגדרות, כולל מיקום גיאוגרפי או מקצוע. במקרים מסוימים, ראינו מעטפת אינטרנט אחת שנעשה בה שימוש בקמפיינים מרובים של תקיפות, עובדה המרמזת על כך שגורמי איום עשויים לשמור על גישה מתמשכת לשרת שנפרץ. ראינו גם עלייה בשירותי האנונימיזציה הזמינים כחלק מהמערכת האקולוגית של ה-CaaS, כמו גם בהצעות לחשבונות רשתות וירטואליות פרטיות (VPN) ושרתים וירטואליים פרטיים (VPS). ברוב המקרים, ה-VPN/VPS שהוצעו נרכשו תחילה באמצעות כרטיסי אשראי גנובים. אתרי CaaS הציעו גם מספר גדול יותר של פרוטוקולי שולחן עבודה מרוחק (RDP), מעטפת מאובטחת (SSH) ו-cPanels לשימוש כפלטפורמה לתיאום מתקפות פשעי סייבר. סוחרי CaaS מגדירים את ה-RDP, SSH ו-cPanels עם כלים וקובצי script מתאימים כדי לסייע בביצוע סוגים שונים של מתקפות סייבר.

שירותי יצירת תחומים הומוגליפים דורשים יותר ויותר תשלום במטבעות קריפטוגרפיים.

תחומים הומוגליפים מתחזים לשמות תחומים לגיטימיים על ידי שימוש בתווים זהים או כמעט זהים במראם לתו אחר. המטרה היא להטעות את הצופה כדי שיחשוב שתחום ההומוגליף הוא התחום האמיתי. תחומים אלה הם איום בכל מקום ומהווים שער לכמות משמעותית של פשעי סייבר. אתרי CaaS מוכרים כיום שמות תחומים הומוגליפים מותאמים אישית, המאפשרים לקונים לבקש שמות חברה ותחום ספציפיים כדי להתחזות אליהם. לאחר קבלת התשלום, סוחרי CaaS משתמשים בכלי מחולל הומוגליפים כדי לבחור את שם התחום ולאחר מכן לרשום את ההומוגליף הזדוני. התשלום עבור שירות זה הוא כמעט אך ורק במטבעות קריפטוגרפיים.

2,750,000

רישומי אתרים נחסמו בהצלחה על ידי DCU השנה כדי להקדים גורמים פליליים שתכננו להשתמש בהם לביצוע פשעי סייבר גלובליים.

פשעי סייבר כשירות

המשך

מוכרי CaaS מציעים לקנייה יותר ויותר אישורים שנפרצו.

אישורים שנפרצו מאפשרים גישה לא מורשית לחשבונות משתמשים, כולל שירות העברת הודעות דואר אלקטרוני, משאבי שיתוף קבצים ארגוניים ו-OneDrive for Business. אם אישורי מנהל מערכת נפרצים, משתמשים לא מורשים עלולים לקבל גישה לקבצים סודיים, למשאבי Azure ולחשבונות משתמשים של החברה. במקרים רבים, חקירות DCU זיהו שימוש לא מורשה באותו אישור בשרתים מרובים כאמצעי לאימות אישורים באופן אוטומטי. דפוס זה מצביע על כך שהמשתמש שנפרץ עלול להיות קורבן להתקפות דיוג מרובות או שיש לו תוכנה זדונית במכשיר המאפשרת לרישום הקשות (keyloggers) של רשת botnet לאסוף אישורים.

שירותי ומוצרי CaaS עם תכונות משופרות צצים כדי למנוע זיהוי.

מוכר CaaS אחד מציע ערכות דיוג עם שכבות מוגדלות של מורכבות ותכונות אנונימיזציה שנועדו לעקוף מערכות זיהוי ומניעה תמורת סכום מינימלי של $6 דולר ליום. השירות מציע סדרה של הפניות שמבצעות בדיקות לפני שהן מאפשרות תעבורה לשכבה או לאתר הבא. באחת מהן מתבצעות יותר מ-90 בדיקות לזיהוי טביעת אצבע במכשיר, כולל האם מדובר במכונה וירטואלית, איסוף פרטים על הדפדפן והחומרה שבהם נעשה שימוש ועוד. אם כל הבדיקות עוברות, התעבורה נשלחת לדף נחיתה המשמש לדיוג.

שירותי פשעי סייבר מקצה לקצה מוכרים מנויים לשירותים מנוהלים.

בדרך כלל, כל שלב בביצוע פשע מקוון יכול לחשוף גורמי איום אם האבטחה התפעולית ירודה. הסיכון לחשיפה ולזיהוי גדל אם השירותים נרכשים מאתרי CaaS מרובים. DCU הבחינה במגמה מדאיגה ברשת האפלה לפיה יש עלייה בהיצע השירותים לאנונימיזציה של קוד תוכנה וגנריזציה של טקסט באתר כדי להפחית את החשיפה. ספקי שירותי מנויים לפשעי סייבר מקצה לקצה מנהלים את כל השירותים ומבטיחים תוצאות המפחיתות עוד יותר את סיכוני החשיפה ל-OCN המנוי. הסיכון המופחת הגביר את הפופולריות של שירותי מקצה לקצה אלה.

דיוג כשירות (PhaaS) הוא דוגמה אחת לשירות פשעי סייבר מקצה לקצה. PhaaS הוא אבולוציה של שירותים קודמים הידועים כשירותים בלתי ניתנים לגילוי באופן מלא (FUD) והוא מוצע על בסיס מינוי. תנאי PhaaS טיפוסיים כוללים שמירה על אתרי דיוג פעילים למשך חודש.

DCU זיהה גם סוחר CaaS המציע מניעת שירות מבוזרת (DDoS) במודל מינוי. מודל זה מוציא למיקור חוץ את היצירה והתחזוקה של רשת ה-botnet הדרושה לביצוע התקפות לסוחר ה-CaaS. כל לקוח מינוי DDoS מקבל שירות מוצפן לשיפור האבטחה התפעולית ושנה אחת של תמיכה 24/7.

שירות המנויים של DDoS מציע ארכיטקטורות ושיטות תקיפה שונות, כך שהרוכש פשוט בוחר משאב לתקיפה והמוכר מספק גישה למערך של מכשירים פרוצים ברשת ה-botnet שלו כדי לבצע את המתקפה. העלות עבור מינוי DDoS היא $500 דולר ארה"ב בלבד.

עבודתה של DCU לפיתוח כלים וטכניקות המזהים ומשבשים פושעי סייבר מסוג CaaS נמשכת. האבולוציה של שירותי CaaS מציבה אתגרים משמעותיים, במיוחד בשיבוש תשלומים במטבעות קריפטוגרפיים.

PhaaS, פושעי סייבר מציעים שירותים מרובים בתוך מינוי אחד. באופן כללי, רוכש צריך לבצע שלוש פעולות בלבד:

1. **לבחור תבנית/עיצוב של אתר דיוג מבין מאות האפשרויות המוצעות.**
2. **לספק כתובת דואר אלקטרוני כדי לקבל אישורים שהושגו מקורבנות דיוג.**
3. **לשלם לסוחר PhaaS במטבעות קריפטוגרפיים.**

לאחר השלמת שלבים אלה, סוחר ה-PhaaS יוצר שירותים עם שלוש או ארבע שכבות של משאבי ניתוב מחדש ואירוח כדי להתמקד במשתמשים ספציפיים. לאחר מכן הקמפיין מתחיל, ואישורי הקורבן נקצרים, מאומתים ונשלחים לכתובת הדואר האלקטרוני שסיפק הרוכש. תמורת פרמיה, סוחרי PhaaS רבים מציעים לארח אתרי דיוג בבלוקצ'יין הציבורי כך שכל דפדפן יוכל לגשת אליהם, וניתובים מחדש יכולים להפנות משתמשים למשאב בספר החשבונות המבוזר.

שימוש פלילי במטבעות קריפטוגרפיים

ככל שאימוץ מטבעות קריפטוגרפיים הופך למיינסטרים, פושעים משתמשים בהם יותר ויותר כדי להתחמק מאכיפת החוק ומאמצעים למניעת הלבנת הון (AML). זה מגביר את האתגר של רשויות אכיפת החוק לעקוב ולהתחקות אחר תשלומים במטבעות קריפטוגרפיים כדי להגיע אל פושעי סייבר.

ההוצאה העולמית על פתרונות בלוקצ'יין גדלה בכ-340 אחוז בארבע השנים האחרונות, בעוד שארנקי מטבעות קריפטוגרפיים חדשים צמחו בכ-270 אחוז. ישנם יותר מ-83 מיליון ארנקים ייחודיים ברחבי העולם, ושווי השוק הכולל של כל המטבעות הקריפטוגרפיים היה כ-1.1$ טריליון דולר נכון ל-28 ביולי 2022.[10]

מקור: PeckShield is) @PeckShieldAlert—Twitter.com a China-based blockchain security company).

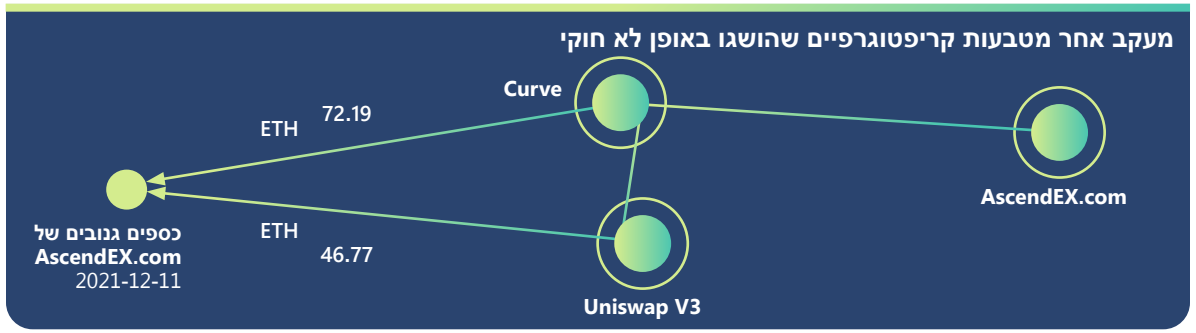
מעקב אחר תשלומי תוכנות כופר

תוכנות כופר הן אחד המקורות הגדולים ביותר של מטבעות קריפטוגרפיים שהושגו באופן לא חוקי. במאמץ לשבש תשתית טכנית זדונית המשמשת בהתקפות של תוכנות כופר – לדוגמה, השיבוש של Zloader באפריל 2022[11] – ה-DCU של Microsoft עוקב אחר ארנקים פליליים כדי לאפשר יכולות מעקב ושחזור של מטבעות קריפטוגרפיים.

חוקרי ה-DCU הבחינו בגורמי תוכנות כופר שמפתחים את טקטיקות התקשורת שלהם עם קורבנות כדי להסתיר את נתיב הכסף. במקור, פושעי סייבר כללו כתובות ביטקוין בהערות הכופר שלהם. עם זאת, זה הקל על מעקב אחר עסקאות תשלום בבלוקצ'יין, כך שגורמי תוכנות כופר הפסיקו לכלול כתובות ארנק ובמקום זאת צירפו כתובות דואר אלקטרוני או קישורים לאתרי צ'אט כדי להעביר כתובות תשלום כופר לקורבנות. חלק מהגורמים אף יצרו דפי אינטרנט וכניסות ייחודיים לכל קורבן כדי למנוע מחוקרי אבטחה ורשויות אכיפת החוק להשיג את כתובות הארנק של הפושעים על ידי התחזות לקורבנות. למרות מאמציהם של פושעים להסתיר את עקבותיהם, עדיין ניתן לשחזר חלק מתשלומי הכופר על ידי עבודה עם רשויות אכיפת החוק וחברות ניתוח קריפטו שיכולות לעקוב אחר התנועה בבלוקצ'יין.

מגמה: הלבנה של הכנסות לא חוקיות באמצעות DEX

סוגיה מרכזית עבור פושעי סייבר היא המרת מטבעות קריפטוגרפיים למטבע פיאט. לפושעי סייבר יש כמה אפיקים פוטנציאליים להמרה, שכל אחד מהם טומן בחובו מידה שונה של סיכון. שיטה אחת המשמשת להפחתת הסיכון היא הלבנת ההכנסות באמצעות בורסה מבוזרת (DEX) לפני פדיון באמצעות אופציות זמינות למזומנים, כגון בורסות ריכוזיות (CEX), בורסות עמית לעמית (P2P) ובורסות מעבר לדלפק (OTC). בורסות DEX הן מיקום הלבנת הון אטרקטיבי מכיוון שלעתים קרובות הם אינן עוקבות אחר אמצעי AML.



באמצעות כלי החקירה של מטבעות קריפטוגרפיים Chainalysis, יחידת הפשעים הדיגיטליים של Microsoft גילתה שההאקרים של AcendEX המירו את הכספים הגנובים שלהם בבורסת DEX קטנה יותר שנקראת Curve בנוסף ל-Uniswap. דיאגרמה זו ממחישה את נתיבי הלבנת ההון שהצוות חשף. כל עיגול מייצג אשכול ארנקים והמספרים על כל קו מייצגים את הכמות הכוללת של Ethereum שהועברה למטרות הלבנת הון.

בדצמבר 2021, האקרים תקפו את פלטפורמת המסחר העולמית במטבעות קריפטוגרפיים AscendEx וגנבו כ-$77.7 מיליון דולר במטבעות קריפטוגרפיים השייכים ללקוחותיה.[12] AscendEx שכרה חברות ניתוח בלוקצ'יין ויצרה קשר עם בורסות CEX אחרות כדי שהארנקים המקבלים כספים גנובים יוכלו להיכנס לרשימה השחורה. בנוסף, כתובות שאליהן נשלחו המטבעות סומנו ככאלה בסייר הבלוקצ'יין Etherscan ב-Ethereum.[13] כדי להימנע מהפעלת ההתרעה והכניסה לרשימה השחורה, ההאקרים שלחו $1.5 מיליון דולר ב-Ethereum ל-Uniswap, אחת מבורסות ה-DEX הגדולות בעולם, ב-18 בפברואר 2022.[14]

אימוץ אמצעי AML חזקים יותר על ידי בורסות DEX עלול לפגוע בחדות בפעילות הלבנת ההון בפלטפורמות שלהן ולאלץ פושעי סייבר להשתמש בשיטות ערפול אחרות כמו ערבוב מטבעות או בורסות ללא רישיון. כדוגמה, Uniswap הודיעה לאחרונה כי תתחיל להשתמש ברשימות שחורות כדי לחסום ארנקים הידועים כמעורבים בפעילויות לא חוקיות מלבצע עסקאות בבורסה.[15]

תובנות מעשיות

1. אם אתה קורבן של פשע סייבר ששילם לפושע באמצעות מטבעות קריפטוגרפיים, פנה לרשויות החוק המקומיות שאולי יוכלו לעזור להתחקות אחר כספים שאבדו ולהשיבם.
2. יש להכיר את אמצעי ה-ALM הקיימים בעת בחירת DEX.

קישורים למידע נוסף

- הגנה מבוססת חומרה מפני איומים אל מול חוטפי קריפטו מורכבים יותר ויותר | צוות המחקר של Microsoft 365 Defender

נוף איומי הדיוג המתפתח

מזימות דיוג אישורים נמצאות במגמת עלייה וממשיכות להוות איום משמעותי על משתמשים בכל מקום מכיוון שהן מתמקדות ללא הבחנה בכל תיבות הדואר הנכנס. מבין האיומים שהחוקרים שלנו עוקבים אחריהם ומגינים מפניהם, היקף מתקפות הדיוג הוא בסדר גודל גדול בהרבה מכל האיומים האחרים.

באמצעות נתונים מ-Defender עבור Office, אנו רואים דואר אלקטרוני זדוני ופעילות זהויות שנפרצו. Azure Active Directory Identity Protection מספק עדיין מידע נוסף באמצעות התרעות על אירועי זהויות שנפרצו. באמצעות Defender עבור אפליקציות ענן, אנו רואים אירועי גישה לנתוני זהויות שנפרצו, ו-Microsoft 365 Defender (M365D) מספק מתאם בין מוצרים. מדד התנועה הרוחבית מגיע מ-Defender עבור נקודת קצה (התרעות ואירועים על אופן פעולה של התקפה), Defender עבור Office (דואר אלקטרוני זדוני) ושוב M365D עבור מתאם בין מוצרים).

710 מיליון

הודעות דואר אלקטרוני של דיוג חסומות בשבוע.

שעה ו-12 דקות

הזמן החציוני שנדרש לתוקף כדי לגשת לנתונים הפרטיים שלך אם אתה נופל קורבן להודעת דואר אלקטרוני של דיוג.[16]

שעה ו-42 דקות

הזמן החציוני שבו תוקף מתחיל לנוע רוחבית בתוך הרשת הארגונית שלך ברגע שמכשיר נפרץ.[17]

אישורי Microsoft 365 נשארים אחד מסוגי החשבונות המבוקשים ביותר עבור תוקפים. לאחר שאישורי הכניסה נפרצים, התוקפים יכולים להיכנס למערכות מחשב הקשורות לארגונים כדי לבצע הדבקה בתוכנות זדוניות ובתוכנות כופר, לגנוב נתונים ומידע סודיים של החברה על-ידי גישה לקובצי SharePoint ולהמשיך את התפשטות הדיוג על-ידי שליחת הודעות דואר אלקטרוני זדוניות נוספות באמצעות Outlook, בין פעולות אחרות.

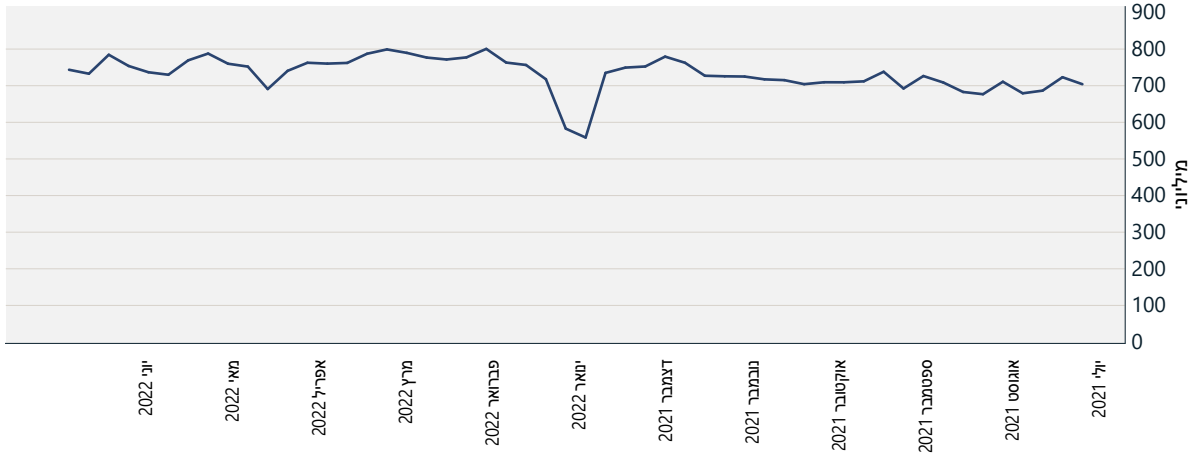
בנוסף לקמפיינים עם מטרות רחבות יותר, דיוג לאישורים, תרומות ומידע אישי, התוקפים מתמקדים בעסקים סלקטיביים לקבלת תשלומים גדולים יותר. מתקפות דיוג בדואר אלקטרוני נגד עסקים למטרות רווח כספי נקראות באופן קולקטיבי התקפות BEC. Microsoft מזהה מיליוני הודעות דואר אלקטרוני של BEC מדי חודש, כמות שהיא שווה ערך ל-0.6 אחוז מכל הודעות הדואר האלקטרוני של דיוג שנצפו. דוח של IC3[18] שפורסם במאי 2022 מצביע על מגמת עלייה בהפסדים שנחשפו עקב התקפות BEC.

הטכניקות המשמשות בהתקפות דיוג ממשיכות לעלות במורכבותן. כתגובה לשימוש באמצעי נגד, התוקפים מסתגלים ומוצאים דרכים חדשות ליישם את הטכניקות שלהם, דבר שמגדיל את המורכבות של האופן והמקום שבו הם מארחים תשתית תפעול קמפיין. משמעות הדבר היא שארגונים חייבים באופן קבוע להעריך מחדש את האסטרטגיה שלהם ליישום פתרונות אבטחה לחסימת הודעות דואר אלקטרוני זדוניות ולחיזוק בקרת הגישה עבור חשבונות משתמשים בודדים.

531,000

בנוסף לכתובות ה-URL שנחסמו על-ידי Defender for Office, יחידת הפשעים הדיגיטליים שלנו הנחתה הסרה של 531,000 כתובות URL ייחודיות של דיוג שהתארחו מחוץ ל-Microsoft.

הודעות דואר אלקטרוני של דיוג שזוהו



מספר זיהויי הדיוג בשבוע ממשיך לעלות. הירידה בדצמבר-ינואר היא ירידה עונתית צפויה, שדווחה גם בדוח של השנה שעברה.
מקור: אותות הגנה של Exchange Online.

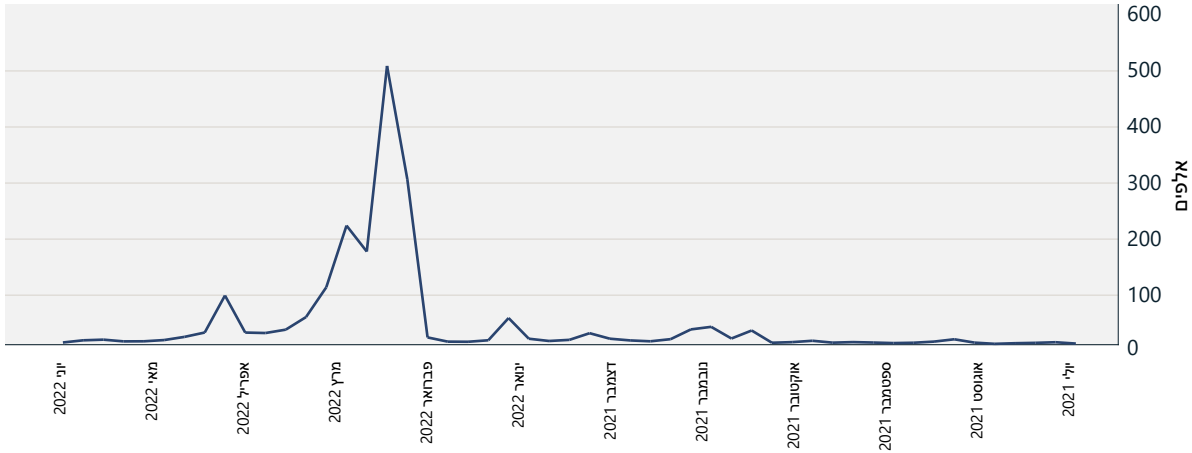
נוף איומי הדיוג המתפתח

המשך

אנו ממשיכים להבחין בעלייה מתמדת משנה לשנה בהודעות דואר אלקטרוני של דיוג. המעבר לעבודה מרחוק בשנים 2020 ו-2021 הביא לעלייה משמעותית בהתקפות דיוג שמטרתן לנצל את סביבת העבודה המשתנה. מפעילי דיוג ממהרים לאמץ תבניות דואר אלקטרוני חדשות באמצעות פיתיונות המותאמים לאירועים מרכזיים בעולם כגון מגפת הקורונה ונושאים הקשורים לכלי שיתוף פעולה ופרודוקטיביות כגון Google Drive או שיתוף קבצים ב- OneDrive. בזמן שנושאים הקשורים למגפת הקורונה פחתו, המלחמה באוקראינה הפכה לפיתוי חדש החל מתחילת מרץ 2022. החוקרים שלנו הבחינו בעלייה מדהימה בכמות הודעות דואר אלקטרוני המתחזות לארגונים לגיטימיים המבקשים תרומות של מטבעות קריפטוגרפיים בביטקוין וב-Ethereum, לכאורה כדי לתמוך באזרחים אוקראינים.

ימים ספורים בלבד לאחר תחילת המלחמה באוקראינה בסוף פברואר 2022, מספר הודעות הדואר האלקטרוני של דיוג שזוהו המכילות כתובות Ethereum שנתקלנו בהן בקרב לקוחות ארגוניים גדל באופן דרמטי. המספר הכולל שנתקלנו בו הגיע לשיאו בשבוע הראשון של מרץ, כאשר חצי מיליון הודעות דואר אלקטרוני של דיוג הכילו כתובת ארנק של Ethereum. לפני תחילת המלחמה, מספר כתובות הארנק של Ethereum בהודעות דואר אלקטרוני אחרות שזוהו כדיוג היה קטן משמעותית, ועמד בממוצע על כמה אלפי הודעות דואר אלקטרוני ביום.

הודעות דואר אלקטרוני של דיוג עם כתובות ארנק של Ethereum



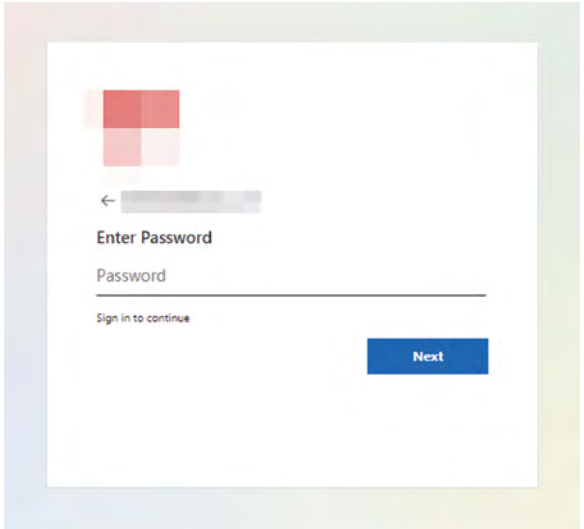
סך כל הודעות הדואר האלקטרוני שזוהו כדיוג המכילות כתובות ארנק של Ethereum עלה בתחילת העימות בין אוקראינה לרוסיה והצטמצם בהדרגה לאחר הדחיפה הראשונית.

יותר מתמיד, דיוגים מסתמכים על תשתית לגיטימית כדי לפעול, דבר שמניע עלייה בקמפיינים של דיוג שמטרתם לפגוע בהיבטים שונים של תפעול כדי שלא יצטרכו לרכוש, לארח או להפעיל בעצמם. לדוגמה, הודעות דואר אלקטרוני זדוניות עשויות להגיע מחשבונות שולח שנפרצו. התוקפים נהנים משימוש בכתובות דואר אלקטרוני אלה, שלהן ציון מוניטין גבוה יותר והן נתפסות כאמינות יותר מחשבונות ותחומים חדשים שנוצרו. בכמה קמפיינים מתקדמים יותר של דיוג, ראינו תוקפים שמעדיפים לשלוח ולזייף מתחומים שבהם DMARC[19] מוגדר באופן שגוי עם מדיניות "ללא פעולה", דבר שפותח פתח לזיוף דואר אלקטרוני.

פעולות דיוג גדולות נוטות להשתמש בשירותי ענן ובמכונות וירטואליות בענן (VMs) כדי לתפעל התקפות בקנה מידה גדול. תוקפים יכולים להפוך לאוטומטי באופן מלא את תהליך הפריסה והמסירה של הודעות דואר אלקטרוני ממכונות וירטואליות (VMs) באמצעות ממסרי דואר אלקטרוני SMTP או תשתית דואר אלקטרוני בענן כדי ליהנות משיעורי המסירה הגבוהים ומהמוניטין החיובי של שירותים לגיטימיים אלה. אם דואר אלקטרוני זדוני מורשה להישלח דרך שירותי ענן אלה, המגינים חייבים להסתמך על יכולות סינון דואר אלקטרוני חזקות כדי לחסום הודעות דואר אלקטרוני מלהיכנס לסביבה שלהם.

חשבונות Microsoft נשארים יעד מוביל עבור מפעילי דיוג, כפי שמעידים דפי הנחיתה הרבים של דיוג שמתחזים לדף הכניסה של Microsoft 365. לדוגמה, דיוגים מנסים להתאים את חוויית הכניסה של Microsoft בערכות הדיוג שלהם על-ידי יצירת כתובת URL ייחודית המותאמת אישית לנמען. כתובת URL זו מכוונת אל דף אינטרנט זדוני שפותח כדי לקצור אישורים, אך פרמטר בכתובת ה-URL יכיל את כתובת הדואר האלקטרוני של הנמען הספציפי. לאחר שהיעד ינווט אל הדף, ערכת הדיוג תאכלס מראש את נתוני הכניסה של המשתמש ואת סמל החברה המותאם אישית לנמען הדואר האלקטרוני, ותשקף את המראה של דף הכניסה המותאם אישית של Microsoft 365 של החברה הממוקדת.

דף דיוג המתחזה לכניסה של Microsoft עם תוכן דינמי

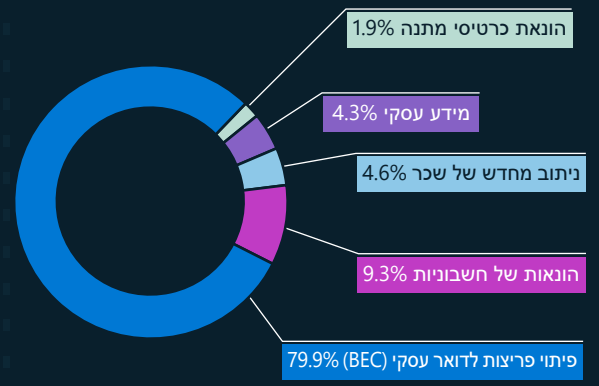


זרקור על פריצה לדואר אלקטרוני עסקי

פושעי סייבר מפתחים תוכניות וטכניקות מורכבות יותר ויותר כדי להביס את הגדרות האבטחה ולהתמקד באנשים, עסקים וארגונים. בתגובה, אנו משקיעים משאבים משמעותיים כדי לשפר עוד יותר את תוכנית האכיפה של BEC.

BEC היא פשע הסייבר הפיננסי היקר ביותר, עם הפסדים מתואמים של $2.4 מיליארד דולר בשנת 2021, המייצגים יותר מ-59 אחוז מחמשת הפסדי פשעי האינטרנט המובילים בעולם.[20] כדי להבין את היקף הבעיה ואת הדרך הטובה ביותר להגן על משתמשים מפני BEC, חוקרי אבטחה של Microsoft עקבו אחר הנושאים הנפוצים ביותר המשמשים בהתקפות.

נושאים של BEC (ינואר-יוני 2022)



נושאים של BEC לפי אחוז התרחשות

מגמות BEC

כנקודת כניסה, תוקפי BEC בדרך כלל מנסים להתחיל שיחה עם קורבנות פוטנציאליים כדי ליצור קרבה. התוקף המתחזה לעמית או מכר עסקי, מוביל בהדרגה את השיחה לכיוון של העברה כספית. הדואר האלקטרוני המהווה מבוא, שאנו עוקבים אחריו כפיתוי BEC, מייצג קרוב ל-80 אחוז מהודעות הדואר האלקטרוני מסוג BEC שזוהו. מגמות אחרות שזוהו על-ידי חוקרי האבטחה של Microsoft בשנה האחרונה כוללות:

- הטכניקות הנפוצות ביותר שהיו בשימוש בהתקפות BEC שנצפו בשנת 2022 היו זיוף[21] והתחזות.[22]
- תת-הסוג BEC שגרם את הנזק הכספי הרב ביותר לקורבנות היה הונאת חשבוניות (בהתבסס על נפח וסכומי הדולרים שהתוקפים דרשו שנראו בחקירות קמפיין ה-BEC שלנו).
- גניבת מידע עסקי, כגון דוחות חשבונות זכאים ואנשי קשר של לקוחות, מאפשרת לתוקפים ליצור הונאות חשבוניות משכנעות.
- רוב הבקשות לניתוב מחדש של שכר נשלחו משירותי דואר אלקטרוני חינמיים ורק לעתים רחוקות מחשבונות שנפרצו. נפח הדואר האלקטרוני ממקורות אלה זינק סביב הראשון והחמישה עשר בכל חודש, תאריכי תשלום השכר הנפוצים ביותר.
- למרות היותן אפיק ידוע להונאות, הונאות כרטיסי מתנה היוו רק 1.9 אחוז מהתקפות ה-BEC שזוהו.

תובנות מעשיות

הגנה מפני דיוג

כדי לצמצם את החשיפה של הארגון לדיוג, אנו מעודדים מנהלי IT ליישם את המדיניות והתכונות הבאות:

1. יש לדרוש שימוש ב-MFA בכל החשבונות כדי להגביל גישה לא מורשית.
2. יש להפוך תכונות גישה מותנית לזמינות עבור חשבונות בעלי הרשאות גבוהות כדי לחסום גישה ממדינות, אזורים וכתובות IP שאינם מייצרים בדרך כלל תעבורה בארגון.
3. יש לשקול להשתמש במפתחות אבטחה פיזיים עבור מנהלים, עובדים המעורבים בפעילויות תשלום או רכישה וחשבונות מורשים אחרים.
4. יש לאכוף את השימוש בדפדפנים התומכים בשירותים כגון Microsoft SmartScreen כדי לנתח כתובות URL לאיתור התנהגויות חשודות ולחסימת הגישה לאתרי אינטרנט זדוניים ידועים.[23]
5. יש להשתמש בפתרון אבטחה מבוסס למידת מכונה שמבודד דיוג בהסתברות גבוהה ומנטרל כתובות URL וקבצים מצורפים בארגז חול לפני שהדואר האלקטרוני מגיע לתיבת הדואר הנכנס, כגון Microsoft Defender for Office 365.[24]
6. יש לאפשר תכונות הגנה מפני התחזות וזיוף ברחבי הארגון.
7. קביעת תצורה של מדיניות הפעולה עבור DomainKeys Identified Mail (DKIM) ו-Domain-based Message Authentication Reporting & Conformance (DMARC) כדי למנוע מסירה של הודעות דואר אלקטרוני שאינן מאומתות שעלולות לזייף שולחים בעלי מוניטין.
8. דייר ומשתמש ביקורת שנוצרו מאפשרים כללים ומסירים חריגות המבוססות על תחום רחב ו-IP. כללים אלה מקבלים לעתים קרובות עדיפות ויכולים לאפשר הודעות דואר אלקטרוני זדוניות ידועות באמצעות סינון דואר אלקטרוני.
9. להפעיל באופן קבוע סימולטורים של דיוג כדי לאמוד את הסיכון הפוטנציאלי ברחבי הארגון שלך וכדי לזהות ולהדריך משתמשים פגיעים.

קישורים למידע נוסף

- מגניבת קובצי Cookie ועד BEC: התוקפים משתמשים באתרי דיוג של AiTM כנקודת כניסה להונאות פיננסיות נוספות | צוות המחקר של Microsoft 365 Defender, מרכז המודיעין לגבי איומים של Microsoft (MSTIC)

הונאת הומוגליף

BEC ודיוג הן טקטיקות נפוצות של הנדסה חברתית. הנדסה חברתית משחקת תפקיד משמעותי בפשע, בכך שהיא משכנעת את היעד לקיים אינטראקציה עם הפושע על ידי רכישת אמון.

במסחר פיזי, סימנים מסחריים משמשים להשגת אמון במקורו של המוצר או השירות, ומוצרים מזויפים הם שימוש לרעה בסימן המסחרי. באופן דומה, פושעי סייבר מתחזים לאיש קשר המוכר ליעד במהלך מתקפת דיוג, ומשתמשים בהומוגליפים כדי להטעות קורבנות פוטנציאליים.

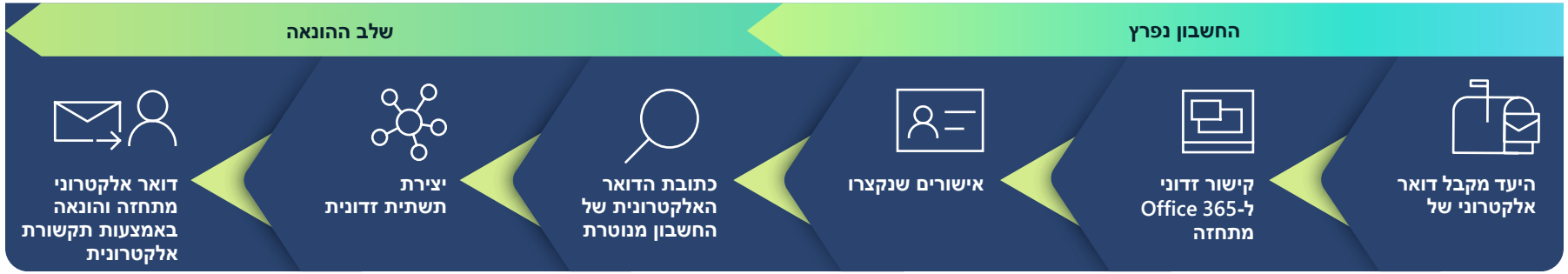
הומוגליף הוא שם תחום המשמש לתקשורת דואר אלקטרוני ב-BEC, שבו תו מוחלף על ידי תו זהה או כמעט זהה במראהו, כדי להטעות את היעד.

טכניקות הומוגליפים המשמשות בניסיונות BEC

ל-BEC יש בדרך כלל שני שלבים, הראשון שבהם כרוך בפריצה של אישורים. סוגים אלה של דליפות אישורים יכולים להיות תוצאה של התקפות דיוג או הפרות נתונים גדולות. לאחר מכן האישורים נמכרים או נסחרים ברשת האפלה.

השלב השני הוא שלב ההונאה, שבו התוקפים משתמשים באישורים שנפרצו כדי לעסוק בהנדסה חברתית מתוחכמת באמצעות תחומי דואר אלקטרוני הומוגליפים.

התקדמות התקפת BEC



טכניקה	% מהתחומים המציגים טכניקת הומוגליף
החלפת l ב- I	25%
החלפת i ב- l	12%
החלפת q ב- g	7%
החלפת rn ב- m	6%
החלפת cam. ב- com.	6%
החלפת 0 ב- o	5%
החלפת ll ב- l	3%
החלפת ii ב- i	2%
החלפת vv ב- w	2%
החלפת l ב- ll	2%
החלפת e ב- a	2%
החלפת nn ב- m	1%
החלפת ll ב- I, החלפת l ב- i	1%
החלפת o ב- u	1%

ניתוח של יותר מ-1,700 תחומים הומוגליפים בין ינואר ליולי 2022 העלה. שבעוד שנעשה שימוש ב-170 טכניקות הומוגליפים, 75% מהתחומים השתמשו ב-14 טכניקות בלבד.

הומוגליף בפעולה

תחום הומוגליף שנראה זהה לתחום דואר שהקורבן מזהה רשום אצל ספק דואר עם שם משתמש זהה. דואר אלקטרוני חטוף נשלח לאחר מכן מהתחום החטוף עם הוראות תשלום חדשות.

באמצעות מינוף מודיעין קוד פתוח וגישה לשרשורי דואר אלקטרוני, הפושע מזהה אנשים שאחראים על הפקת חשבוניות וביצוע תשלומים. לאחר מכן הוא יכול ליצור התחזות של כתובת דואר אלקטרוני של האדם ששולח חשבוניות. התחזות זו מורכבת משם משתמש זהה ותחום דואר המהווה הומוגליף של השולח המקורי.

התוקף מעתיק שרשרת דואר אלקטרוני המכילה חשבונית לגיטימית, ולאחר מכן משנה את החשבונית כך שתכיל את פרטי הבנק שלו. חשבונית חדשה זו, ששונתה, נשלחת לאחר מכן שוב ליעד מהתחזות של דואר אלקטרוני הומוגליף. מכיוון שההקשר הגיוני והדואר האלקטרוני נראה אמיתי, לעתים קרובות היעד פועל על פי ההוראות המזויפות.

תובנות מעשיות

1. לאכוף את השימוש בדפדפנים התומכים בשירותים כגון Safe Links ו-SmartScreen כדי לנתח כתובות URL לאיתור התנהגויות חשודות ולחסום את הגישה לאתרי אינטרנט זדוניים ידועים.[25]
2. להשתמש בפתרון אבטחה מבוסס למידת מכונה שמבודד דיוג בהסתברות גבוהה ומנטרל כתובות URL וקבצים מצורפים בארגז חול לפני שהדואר האלקטרוני מגיע לתיבת הדואר הנכנס.

קישורים למידע נוסף

- המרכז לתלונות על פשעי אינטרנט (IC3) | פריצה לדואר אלקטרוני עסקי: הונאת ה- 43$ מיליארד
- תובנה של מודיעין מזויף – Office 365 | Microsoft Docs
- תובנה של התחזות – Office 365 | Microsoft Docs

ציר הזמן של שיבושים ברשת הבוטים מהימים הראשונים של שיתוף הפעולה של Microsoft

במשך יותר מעשור, DCU פעלה כדי לעצור באופן יזום פשעי סייבר שתוצאתם הייתה 26 תוכנות זדוניות ושיבושים ברמת המדינה. ככל שצוות ה-DCU משתמש בטקטיקות ובכלים מתקדמים יותר כדי להשבית את הפעולות הלא חוקיות הללו, אנו רואים שגם פושעי הסייבר מפתחים את הגישות שלהם בניסיון להישאר צעד אחד קדימה. להלן ציר זמן המציג מדגם של רשתות ה-botnet ששובשו על-ידי DCU והאסטרטגיות ש-Microsoft אימצה כדי להשבית אותן.

2008

Conficker botnet

תיאור: תולעת מחשב המתפשטת במהירות ומכוונת למערכת ההפעלה Windows, מדביקה מיליוני מחשבים ומכשירים ברשת משותפת; יצרה הפסקות רשת ברחבי העולם.

שיתוף פעולה: הקמת קבוצת העבודה Conficker Working Group), הקונסורציום הראשון מסוגו. Microsoft שיתפה פעולה עם 16 ארגונים ברחבי העולם כדי להביס את הבוט.

תגובת Microsoft: הקבוצה שיתפה פעולה בתחומי שיפוט בינלאומיים רבים והצליחה להפיל את Conficker.

2009

Waledac botnet

תיאור: רשת בוטים מורכבת של דואר זבל עם תחומים בארה"ב שאספה כתובות דואר אלקטרוני והפיצה דואר זבל שהדביק עד 90,000 מחשבים ברחבי העולם.[26]

שיתוף פעולה: יצירת קונסורציום נוסף, המרכז להגנה מפני תוכנות זדוניות של Microsoft (MMPC) עם דגש על שיתוף פעולה הדוק עם אנשי אקדמיה.[27]

תגובת Microsoft: Microsoft השתמשה בגישת שיבוש מדורגת של C2 והפתיעה גורמים זדוניים על ידי השתלטות על תחומים שבסיסם בארה"ב ללא הודעה מוקדמת.[28] Microsoft העניקה בעלות זמנית על כמעט 280 תחומים המשמשים את השרתים של Waledac.

2011

היחידה לפשעי מחשב של Microsoft הוקמה

שיתוף פעולה: נועד לסכל פשעי סייבר המשפיעים על המערכת האקולוגית של Microsoft באמצעות אינטגרציה הדוקה בין צוותים של חוקרים, עורכי דין ומהנדסים.

גישת Microsoft: המטרה היא להבין טוב יותר את ההיבטים הטכניים של תוכנות זדוניות שונות ולספק תובנות אלה לצוות המשפטי של Microsoft כדי לפתח אסטרטגיית שיבוש יעילה.

2013

Rustock botnet

תיאור: בוט דואר זבל סוס טרויאני בדלת האחורית המשתמש בספקי אינטרנט כשרתי C2 עיקריים; שנועד למכור תרופות.

שיתוף פעולה: Microsoft יצרה שותפות עם חברת התרופות Pfizer Pharmaceuticals כדי להבין את התרופות שנמכרו על ידי Rustock ועבדה בשיתוף פעולה הדוק עם גורמי אכיפת החוק בהולנד.[29]

תגובת Microsoft: חברת Microsoft עבדה עם מרשלים בארה"ב ועם רשויות אכיפת החוק בהולנד כדי להוריד את שרתי ה-C2 במדינה זו. רשמה וחסמה את כל האלגוריתמים העתידיים ליצירת דומיין (DGAs).

Sirefef/Zero Access botnet

תיאור: botnet של פרסום שנועד להפנות אנשים לאתרים מסוכנים שיתקינו תוכנות זדוניות או יגנבו מידע אישי; הדביק יותר משני מיליון מחשבים ועלה למפרסמים יותר מ-2.7$ מיליון דולר בחודש; בעיקר בארה"ב ובמערב אירופה.

שיתוף פעולה: עבד בשיתוף פעולה הדוק עם ה-FBI ועם מרכז פשעי האינטרנט של ה-Europol כדי להפיל את תשתית ה'עמית לעמית'.

תגובת Microsoft:הצטרפה לרשת Zero Access, החליפה את שרתי C2 ששימשו למטרות פליליות ותפסה בהצלחה תחומי שרתי הורדה.

2019

Trickbot botnet

תיאור: רשת בוטים מתוחכמת עם תשתית מפוצלת ברחבי העולם שהתמקדה בתעשיית השירותים הפיננסיים; מכשירי IoT שנפרצו.

שיתוף פעולה: Microsoft שיתפה פעולה עם המרכז לשיתוף וניתוח מידע של שירותים פיננסיים (FS-ISAC) כדי להפיל את Trickbot.[30]

תגובת Microsoft: DCU בנתה מערכת לזיהוי ומעקב אחר תשתית בוטים ויצרה הודעות עבור ספקי אינטרנט פעילים, תוך התחשבות בחוקים ספציפיים במדינות שונות.

2022

המשך ההתמקדות בשיבוש

תיאור: Microsoft שיבשה את התשתית של שבעה גורמי איום בשנה האחרונה, ומנעה מהם להפיץ תוכנות זדוניות נוספות, לשלוט במחשבים של הקורבנות ולסמן קורבנות נוספים כיעדים.

שיתוף פעולה: בשותפות עם ספקי שירותי אינטרנט, ממשלות, רשויות אכיפת החוק והתעשייה הפרטית, Microsoft שיתפה מידע כדי לתקן יותר מ-17 מיליון קורבנות של תוכנות זדוניות ברחבי העולם.

מבט קדימה

DCU ממשיכה לחדש ומתכננת להשתמש בניסיון שלה בשיבושי רשת botnet כדי לנהל פעולות מתואמות מעבר לתוכנות זדוניות. ההצלחה המתמשכת שלנו דורשת הנדסה יצירתית, שיתוף מידע, תיאוריות משפטיות חדשניות ושותפויות ציבוריות ופרטיות.

ניצול לרעה של התשתית על ידי פושעי סייבר

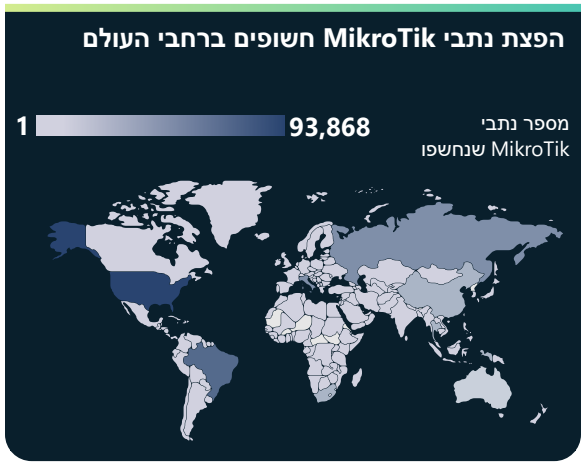
שערי אינטרנט כתשתית שליטה ובקרה פלילית

מכשירי IoT הופכים למטרה פופולרית יותר ויותר עבור פושעי סייבר המשתמשים ברשתות בוטים נרחבות. כאשר נתבים אינם מתוקנים ונשארים חשופים ישירות לאינטרנט, גורמי האיום יכולים לנצל אותם לרעה כדי לקבל גישה לרשתות, לבצע התקפות זדוניות ואפילו לתמוך בפעולותיהם.

צוות Microsoft Defender for IoT עורך מחקר לגבי סוגים שונים של ציוד, מפקדי מערכת בקרה תעשייתית מדור קודם ועד לחיישני IoT חדשניים. הצוות חוקר תוכנות זדוניות ספציפיות ל-IoT ו-OT כדי לתרום לרשימה המשותפת של מדדי הפריצה.

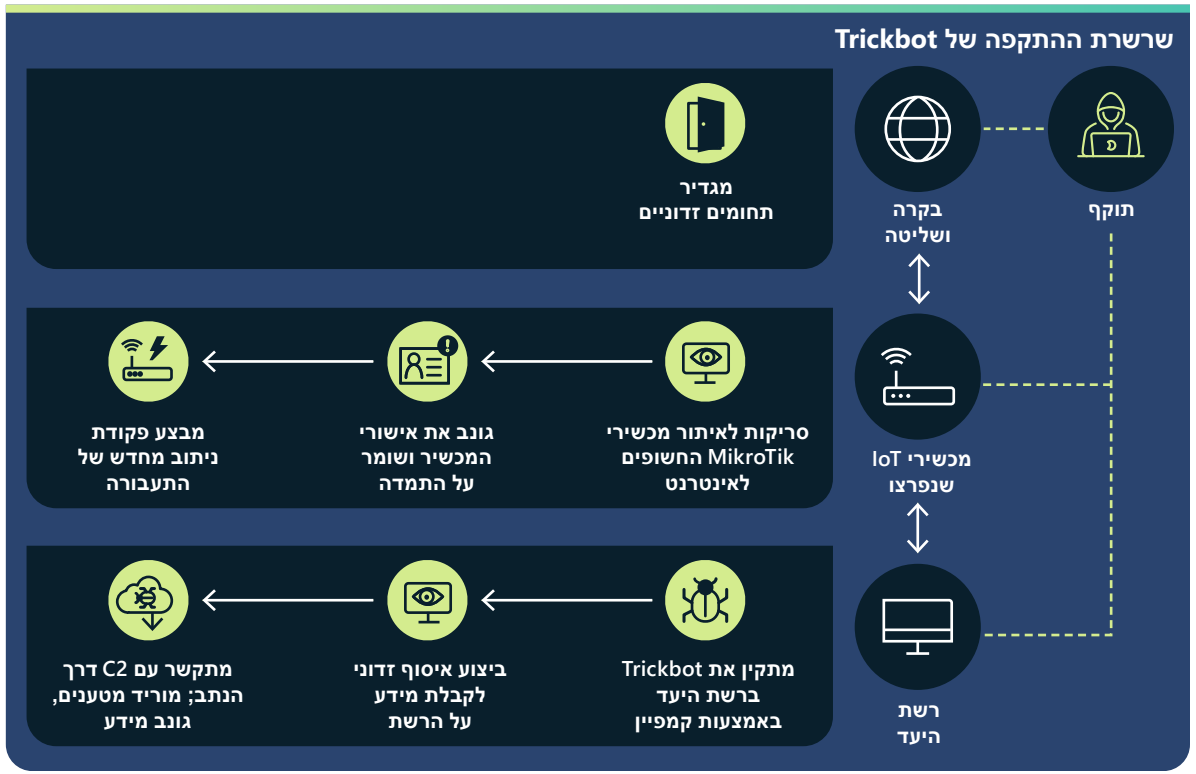
נתבים הם וקטורים פגיעים במיוחד לתקיפה מכיוון שהם נמצאים בכל מקום בבתים ובארגונים המחוברים לאינטרנט. עקבנו אחר הפעילות של נתבי MikroTik, נתב פופולרי ברחבי העולם הן בבתי מגורים והן במגזר המסחרי, וזיהינו כיצד הם מנוצלים לשליטה ובקרה (C2), להתקפות מערכת שמות תחומים (DNS) ולחטיפת כריית קריפטו.

באופן ספציפי יותר, זיהינו כיצד מפעילי Trickbot משתמשים בנתבי MikroTik שנפרצו ומגדירים אותם מחדש כך שיפעלו כחלק מתשתית ה-C2 שלהם. הפופולריות של מכשירים אלה מעצימה את חומרת השימוש לרעה בהם על ידי Trickbot, והחומרה והתוכנה הייחודיות שלהם מאפשרות לגורמי איום להתחמק מאמצעי אבטחה מסורתיים, להרחיב את התשתית שלהם ולפרוץ ליותר מכשירים ורשתות.



נתבים חשופים נמצאים בסיכון לניצול פגיעויות פוטנציאליות.

על ידי מעקב וניתוח תעבורה המכילה פקודות מעטפת מאובטחת (SSH), ראינו תוקפים המשתמשים בנתבי MikroTik כדי לתקשר עם תשתית Trickbot לאחר השגת אישורים לגיטימיים למכשירים. ניתן להשיג אישורים אלה באמצעות התקפות brute force, המנצלות פגיעויות ידועות עם תיקונים הזמינים באופן מיידי ומשתמשות בסיסמאות ברירת מחדל. לאחר שהושגה גישה למכשיר, התוקף יוצר פקודה ייחודית שמנתבת מחדש את התעבורה בין שתי יציאות בנתב, ויוצרת את קו התקשורת בין מכשירים המושפעים על ידי Trickbot לבין ה-C2.



שרשרת ההתקפה של Trickbot חושפת את השימוש במכשירי IoT של MikroTik כשרתי proxy עבור C2.

צברנו את הידע שלנו על השיטות השונות לתקיפת מכשירי MikroTik, מעבר ל-Trickbot בלבד, כמו גם נקודות תורפה וחשיפות נפוצות וידועות (CVEs) לכלי קוד פתוח עבור מכשירי MikroTik, שיכול לחלץ את הממצאים הפורנזיים הקשורים להתקפות על מכשירים אלה.[31]

מכשירים הפועלים כשרתי Proxy הפוכים עבור תוכנות זדוניות C2 אינם ייחודיים רק לנתבי Trickbot ו-MikroTik. בשיתוף פעולה עם צוות Microsoft RiskIQ, איתרנו את ה-C2 המעורב, ובאמצעות בחינת אישורי SSL, זיהינו מכשירי Ubiquiti ו-LigoWave שהושפעו גם הם.[32] זוהי אינדיקציה חזקה לכך שמכשירי IoT הופכים לרכיבים פעילים בהתקפות מתואמות ברמת המדינה ויעד פופולרי לפושעי סייבר המשתמשים ברשתות בוטים נרחבות.

פושעי קריפטו משתמשים לרעה במכשירי IoT

מכשירי שער הם יעד בעל ערך שהולך וגדל עבור גורמי איום מכיוון שמספר הפגיעויות הידועות גדל בעקביות משנה לשנה. הם משמשים לכריית קריפטו ולסוגים אחרים של פעילות זדונית.

ככל שמטבעות קריפטוגרפיים הפכו פופולריים יותר, אנשים וארגונים רבים השקיעו כוח חישובי ומשאבי רשת ממכשירים כגון נתבים כדי לכרות מטבעות בשרשרת בלוקים (בלוקצ'יין). עם זאת, כריית מטבעות קריפטוגרפיים היא תהליך הגוזל זמן ומשאבים עם סבירות נמוכה להצלחה. כדי להגדיל את הסבירות לכריית מטבע, הכורים מתקבצים יחד ברשתות מבוזרות ושיתופיות, ומקבלים קודי hash ביחס לאחוז המטבע שהם הצליחו לכרות באמצעות המשאבים המחוברים שלהם.

בשנה האחרונה, Microsoft הבחינה במספר גדל והולך של התקפות המנצלות לרעה נתבים כדי לנתב מחדש את מאמצי כריית המטבעות הקריפטוגרפיים. פושעי סייבר פורצים לנתבים המחוברים למאגרי כרייה ומנתבים מחדש את תעבורת הכרייה לכתובות ה-IP המשויכות אליהם באמצעות התקפות הרעלת DNS, דבר שמשנה את הגדרות ה-DNS של מכשירים המהווים יעד. נתבים מושפעים רושמים כתובת IP שגויה לשם תחום נתון, ושולחים את משאבי הכרייה שלהם – או קודי Hash – למאגרים המשמשים את גורמי האיום. מאגרים אלה עשויים לכרות מטבעות אנונימיים הקשורים לפעילות פלילית או להשתמש בקודי Hash לגיטימיים שנוצרו על ידי כורים כדי להשיג אחוז מהמטבע שהם כרו, וכך לקצור את הפירות.

במצב שבו יותר ממחצית מהפגיעויות הידועות שנמצאו בשנת 2021 היו ללא תיקון, עדכון ואבטחת נתבים ברשתות ארגוניות ופרטיות עדיין מהווים אתגר משמעותי עבור בעלי מכשירים ומנהלי מערכת.

פריצה למכשירים לכריית קריפטו לא חוקית.

הרעלת DNS של מכשירי שער פוגעת בפעילויות כרייה לגיטימיות ומנתבת מחדש משאבים לפעילויות כרייה פליליות.

מכונות וירטואליות כתשתית פלילית

המעבר הנרחב לענן כולל פושעי סייבר שמנצלים נכסים פרטיים של קורבנות תמימים שהושגו באמצעות דיוג או על ידי גנבי אישורים מפיצי תוכנות זדוניות. פושעי סייבר רבים בוחרים להקים את התשתיות הזדוניות שלהם על מכונות וירטואליות מבוססות ענן (VMs), גורמים מכילים ומיקרו-שירותים.

ברגע שלפושע הסייבר יש גישה, רצף של אירועים יכול להתרחש כדי להקים תשתית – כגון סדרת מכונות וירטואליות באמצעות scripting ותהליכים אוטומטיים. תהליכים אוטומטיים אלה המבוססים על קבצי Script משמשים להפעלת פעילות זדונית, כולל התקפות דואר זבל אלקטרוני בקנה מידה גדול, התקפות דיוג ודפי אינטרנט המארחים תוכן זדוני. היא יכולה אפילו לכלול הקמת סביבה וירטואלית בקנה מידה גדול המבצעת כריית מטבעות קריפטוגרפיים, וגורמת לקורבן חשבון של מאות אלפי דולרים בסוף החודש.

פושעי סייבר מבינים שלפעילות הזדונית שלהם יש אורך חיים מוגבל לפני שהיא מזוהה ומושבתת. כתוצאה מכך, הם התרחבו וכעת הם פועלים באופן יזום עם תוכניות מגירה בראש סדר עדיפויותיהם. הם נצפו מכינים חשבונות שנפרצו מבעוד מועד ומנטרים את סביבתם. ברגע שחשבון (שהוגדר באמצעות מאות אלפי מכונות וירטואליות) מזוהה, הם עוברים לחשבון הבא – שכבר הוכן על-ידי קובצי Script להפעלה מיידית – והפעילות הזדונית שלהם ממשיכה עם מעט מאוד או ללא הפרעה.

בדומה לתשתית ענן, ניתן להשתמש בתשתית מקומית בהתקפות עם סביבות מקומיות וירטואליות שאינן ידועות למשתמש המקומי. לצורך כך על נקודת הגישה הראשונית להישאר פתוחה ונגישה. גם נכסים פרטיים מקומיים נוצלו לרעה על ידי פושעי סייבר לפתיחת שרשרת תשתיות ענן מתמשכת, שהוקמה כדי לטשטש את מקורן למניעת זיהוי יצירת תשתית חשודה.

תובנות מעשיות

1. להטמיע היגיינת סייבר טובה ולספק הדרכות אבטחת סייבר לעובדים עם הנחיה למניעת הנדסה חברתית.
2. לבצע בדיקות חריגה אוטומטיות של פעילות משתמשים באופן קבוע באמצעות זיהוי בקנה מידה גדול כדי לסייע בהפחתת סוגים אלה של התקפות.
3. לעדכן ולאבטח נתבים ברשתות ארגוניות ופרטיות.

האם ההאקטיביזם לא מתכוון להיעלם?

בעוד האקטיביזם אינו תופעה חדשה, המלחמה באוקראינה הובילה לגל של האקרים מתנדבים, כולל כאלה שהונחו על ידי ממשלות לפרוס כלי סייבר כדי לפגוע במוניטין או בנכסים של יריבים פוליטיים, ארגונים ואפילו מדינות.

בפברואר 2022, ממשלת אוקראינה קראה לאזרחים פרטיים ברחבי העולם לבצע מתקפות סייבר על רוסיה כחלק מ-"צבא ה-IT" שלה המונה 300,000 פעילים.[33] במקביל, קבוצות האקטיביסטיות מבוססות כמו Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans ו-RaidForum2 החלו לבצע מתקפות לתמיכה באוקראינה. קבוצות אחרות, כולל כמה מכנופיית תוכנות הכופר Conti, צידדו ברוסיה.[34]

בחודשים שלאחר מכן, פעילותה של Anonymous הייתה גלויה מאוד. האקרים הפועלים בשמה של הקבוצה – או בשם אחד משותפיה – השביתו זמנית אלפי אתרים רוסיים ובלארוסיים, הדליפו מאות ג'יגה-בייטים של נתונים גנובים, פרצו לערוצי טלוויזיה רוסיים כדי להציג תוכן פרו-אוקראיני, ואף הציעו לשלם בביטקוין לטנקים רוסיים שנכנעו.

עלייתם של האקרים אזרחיים

פלטפורמות המדיה החברתית אפשרו התארגנות מהירה וגיוס של אלפי אזרחים המתיימרים להיות האקרים, שקיבלו הנחיות לביצוע מתקפות הניתנות להפעלה בקלות כגון מתקפות DDoS. המארגנים מינפו את Twitter, Telegram ופורומים פרטיים כדי לגייס האקרים, לארגן פעולות ולהפיץ מדריכי הוראות לפריצה.

עם זאת, סביר להניח שלרוב ההאקרים האלה יש כישורים מוגבלים, אפילו עם הדרכה. זה מצביע על שני תרחישים פוטנציאליים עתידיים: האחד שבו מאות או אלפי אנשים עם יכולות טכניות בסיסיות ישתמשו בתבניות תקיפה כדי לנהל התקפות האקטיביסטיות מתואמות או אינדיבידואליות עתידיות נגד יעדים, או תרחיש עתידי שני שבו סוף מעשי האיבה באוקראינה יגרום להם להשאיר את ההאקטיביזם שלהם מאחור, לפחות עד שהנושא הפוליטי או החברתי הבא יעורר אותם לפעולה.

פוליטיזציה של האקרים

הסיכון הגדול יותר הנשקף מהתגייסות פוליטית זו הוא פריסתם של האקרים בעלי ידע טכני שעלולים להמשיך לבצע מתקפות סייבר נגד מטרות ממשלתיות זרות כדי לתמוך בסדרי העדיפויות הלאומיים שלהם, מיוזמתם האישית או לבקשת ממשלתם.

איראן, סין ורוסיה כבר משתמשות בהאקטיביזם כקו הזנה לגיוס לקבוצות הפריצה המדינתיות שלהן. לדוגמה, באפריל 2022, קבוצת הפריצה הפרו-רוסית Killnet הפעילה מתקפות DDoS נגד מסילות רכבת צ'כיות, שדות תעופה אזוריים ושרת השירות הציבורי של צ'כיה, אף על פי שצ'כיה אינה מעורבת ישירות במלחמה.[35] בה בעת, ממשלות מסוימות עשויות להשתמש בהאקטיביזם ככיסוי לריגול סייבר מסורתי או לפעולות חבלה – למשל, פעילות איראנית נגד ישראל.

בסביבה של מתקפות DDoS מוגברות הקשורות להאקטיביזם, תעשיית הטכנולוגיה מאותגרת לפענח במהירות את ההבדל בין זרימת תעבורה רגילה ולא רגילה לאתר. Microsoft ושותפיה פיתחו אוסף של כלים המבחינים בין תעבורת DDoS זדונית ועוקבים אחריה בחזרה למקורה. בנוסף, פלטפורמת Azure של Microsoft יכולה לזהות מחשבים בפלטפורמה שמייצרים רמות גבוהות במיוחד של תעבורה יוצאת ולהשבית אותם.

הופעתה של ה-protestware

protestware הופיעה כתוצאה ישירה מתגובות רגשיות למלחמה בין רוסיה לאוקראינה. כמה מפתחי תוכנות קוד פתוח השתמשו בפופולריות של התוכנה שלהם כאמצעי להבעת עמדה או לנקיטת פעולה נגד מצב גיאופוליטי מתגלגל. זה כלל קובצי טקסט לא מזיקים שנפתחו בשולחן עבודה או בדפדפן כדי להפיץ מסרים של שלום, אך כלל גם התקפות ממוקדות המבוססות על מיקום גיאוגרפי של כתובת IP ופעולות הרסניות כמו מחיקת כונן קשיח. עם התפתחותם של אירועים גלובליים אחרים, אנו צפויים לראות שוב את ה-protestware בעתיד. מכיוון שבדרך כלל מדובר במקרים שבהם מתחזקי קוד פתוח מכובדים מחליטים להצהיר הצהרות אישיות תוך שימוש ברכיבי הקוד הפתוח שלהם, אין כיום הגנה כדי למנוע משינויים מסוג זה להתרחש בחבילות קובצי המקור והמשתמשים צריכים לשמור על ערנות לפגיעה פוטנציאלית.

> פלטפורמות המדיה החברתית אפשרו התארגנות מהירה וגיוס של אלפי אזרחים המתיימרים להיות האקרים, שקיבלו הנחיות לביצוע מתקפות הניתנות להפעלה בקלות כגון מתקפות DDoS.

תובנות מעשיות

1. תעשיית הטכנולוגיה חייבת להתאחד כדי לתכנן תגובה מקיפה לאיום החדש הזה.
2. לחברות טכנולוגיה מובילות, כולל Microsoft, יש כלים לזיהוי תעבורה זדונית הקשורה להתקפות DDoS ולהשבתת המחשבים האחראיים.
3. משתמשי קוד פתוח צריכים להשגיח יותר בעתות של סכסוכים גיאופוליטיים.

הערות סיום

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. זיהוי נקודות קצה ותגובה. 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. Vetted Forum (פורום בדוק) הוא פורום דיונים מקוון הדורש מחבר קיים לערוב להוספת חבר חדש.
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. מקור נתונים: Defender for Office (דואר אלקטרוני זדוני/פעילות זהויות שנפרצו), Azure Active Directory Identity Protection (אירועי/התראות זהויות שנפרצו), Defender עבור אפליקציות בענן (אירועי גישה לנתוני זהויות שנפרצו) ו-M365D (מתאם בין מוצרים).
17. מקור נתונים: Defender עבור נקודת קצה (התראות/אירועים על אופן פעולה של התקפה), Defender for Office (דואר אלקטרוני זדוני) ו-M365D (מתאם בין מוצרים).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. אימות הודעות המבוסס על תחום, דיווח והתאמה: פרוטוקול אימות, מדיניות ודיווח של דואר אלקטרוני שנועד להעניק לבעלי תחומי דואר אלקטרוני את היכולת להגן על התחום שלהם מפני שימוש לא מורשה.
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 בפברואר 2010).
27. ראה באודן, מארק. תולעת: מלחמת העולם הדיגיטלית הראשונה. Grove/Atlantic, Inc.,. 27 בספטמבר 2011.
28. באופן ספציפי, כלל מס' 65 בכללים הפדרליים של סדר הדין האזרחי מאפשר לצד לבקש סעד כזה אם: 1) הצד יסבול נזק מיידי ובלתי הפיך אם הסעד לא יינתן, ו-2) הצד מנסה לספק לצד השני הודעה במועד. יתרה מכך, החוק מחייב להחיל מבחן איזון, כזה המאזן בין זכותו של הנאשם ליידוע לבין מידת הפגיעה בציבור.
29. Microsoft Corporation v. John Does 1-11 ,et. al. ,No. 2:11cv222 ,W.D. Wa. (9 בפברואר 2011).
30. Microsoft Corp. v. Does ,(AJT/IDD) No. 1:20-cv-01171 ,2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. 12 באוגוסט 2021).
31. https://github.com/microsoft/routeros-scanner
32. RiskIQ: מכשירי Ubiquiti נפרצו ומשמשים כתוכנות זדוניות C2 שרתי Proxy הפוכים | מהדורת קהילת 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

איומים ברמת המדינה

גורמים מדינתיים משגרים מתקפות סייבר מתוחכמות יותר ויותר שנועדו להתחמק מזיהוי ולקדם את סדרי העדיפויות האסטרטגיים שלהם.

סקירה כללית של

איומים ברמת המדינה

גורמים מדינתיים משגרים מתקפות סייבר מתוחכמות יותר ויותר שנועדו להתחמק מזיהוי ולקדם את סדרי העדיפויות האסטרטגיים שלהם. הופעתה של פריסת נשק סייבר במלחמה ההיברידית באוקראינה היא שחר של עידן חדש של עימות.

רוסיה גם תמכה במלחמתה באמצעות מבצעי השפעה על מידע, והשתמשה בתעמולה כדי להשפיע על דעות ברוסיה, באוקראינה ובעולם. הקונפליקט ההיברידי הראשון הזה בקנה מידה מלא לימד לקחים חשובים אחרים. ראשית, ניתן להגן בצורה הטובה ביותר על האבטחה של פעולות ונתונים דיגיטליים – הן במרחב הסייבר והן במרחב הפיזי – על ידי מעבר לענן. ההתקפות הרוסיות הראשוניות התמקדו בשירותים מקומיים באמצעות תוכנות זדוניות שמבצעות מחיקה, והתמקדו במרכזי Datacenter פיזיים באמצעות אחד הטילים הראשונים ששוגרו.

אוקראינה הגיבה על ידי העברה מהירה של עומסי עבודה ונתונים לעננים בקנה מידה גדול מאוד המתארחים במרכזי Datacenter מחוץ לאוקראינה. שנית, ההתקדמות במודיעין איומי סייבר והגנה על נקודות קצה המופעלות על ידי הנתונים ושירותי AI ו-ML מתקדמים בענן סייעו לאוקראינה להתגונן מפני מתקפות סייבר רוסיות.

במקומות אחרים, גורמים מדינתיים הגבירו את פעילותם והחלו להשתמש בפיתוחים חדשים באוטומציה, בתשתיות ענן ובטכנולוגיות גישה מרחוק כדי לתקוף אוסף מטרות רחב יותר. שרשראות אספקה ארגוניות של IT המאפשרות גישה ליעדים אולטימטיביים הותקפו לעתים קרובות. היגיינת אבטחת הסייבר הפכה קריטית עוד יותר כאשר גורמים ניצלו במהירות פגיעויות שלא תוקנו, השתמשו בטכניקות מתוחכמות ובטכניקות brute force כדי לגנוב אישורים, והסתירו את פעילותם על ידי שימוש בתוכנות קוד פתוח או בתוכנות לגיטימיות. בנוסף, איראן מצטרפת לרוסיה בשימוש בנשקי סייבר הרסניים, כולל תוכנות כופר, כמרכיב עיקרי בתקיפות שלה.

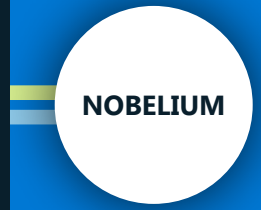
התפתחויות אלה מחייבות אימוץ דחוף של מסגרת גלובלית עקבית הנותנת עדיפות לזכויות אדם ומגינה על אנשים מפני התנהגות מדינתית חסרת אחריות ברשת. כל המדינות חייבות לעבוד יחד כדי ליישם נורמות וכללים מוסכמים להתנהגות מדינתית אחראית.

הגנה על אוקראינה: לקחים ראשונים ממלחמת הסייבר - Microsoft On the Issues

מיקוד מוגבר של תשתיות חיוניות, במיוחד במגזר ה-IT, השירותים הפיננסיים, מערכות התחבורה ותשתיות התקשורת.

מידע נוסף בעמוד 35

שרשרת אספקת IT משמשת כשער לגישה ליעדים.



מידע נוסף בעמוד 36

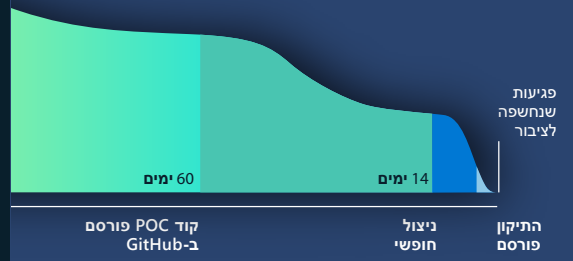
סין מרחיבה את המיקוד הגלובלי במיוחד למדינות קטנות יותר בדרום מזרח אסיה, כדי להשיג מודיעין ויתרון תחרותי.

מידע נוסף בעמוד 44

איראן הפכה אגרסיבית יותר ויותר בעקבות חילופי השלטון, הרחיבה את מתקפות הכופר מעבר ליריבות האזוריות לקורבנות בארה"ב ובאיחוד האירופי, ושמה לה למטרה תשתיות חיוניות אמריקאיות בעלות פרופיל גבוה.

מידע נוסף בעמוד 46

זיהוי וניצול מהיר של פגיעויות שלא תוקנו הפך לטקטיקה מרכזית. פריסה מהירה של עדכוני אבטחה היא המפתח להגנה.



מידע נוסף בעמוד 39

צפון קוריאה התמקדה חברות בתחום הביטחון, התעופה והחלל, מטבעות קריפטוגרפיים, כלי תקשורת, עריקים וארגוני סיוע, כדי להשיג את מטרות המשטר: לבנות הגנה, לחזק את הכלכלה ולהבטיח יציבות פנימית.

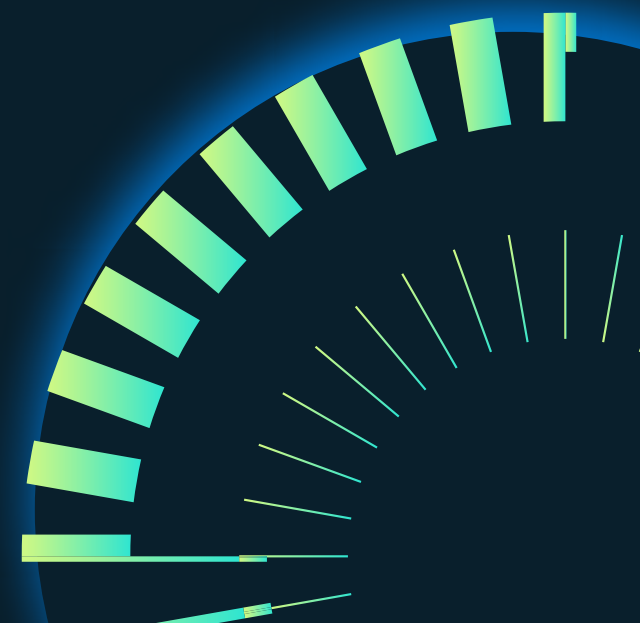
מידע נוסף בעמוד 49

שכירי חרב בתחום הסייבר מאיימים על יציבות מרחב הסייבר כאשר תעשייה הולכת וגדלה זו של חברות פרטיות מפתחת ומוכרת כלים, טכניקות ושירותים מתקדמים כדי לאפשר ללקוחותיהם (לעתים קרובות ממשלות) לפרוץ לרשתות ולמכשירים.

מידע נוסף בעמוד 52

מבוא

בעקבות מתקפות בעלות פרופיל גבוה בשנים 2020 ו-2021, גורמי איום מדינתיים השקיעו משאבים משמעותיים בהסתגלות להגנות אבטחה חדשות שיושמו על ידי ארגונים כדי להתגונן מפני איומים מתוחכמים.



בדומה לארגונים גדולים, יריבים החלו להשתמש בפיתוחים חדשים באוטומציה, בתשתיות ענן ובטכנולוגיות גישה מרחוק כדי להרחיב את ההתקפות שלהם נגד סט מטרות רחב יותר. התאמות טקטיות אלה הובילו לגישות חדשות ולהתקפות בקנה מידה גדול נגד שרשראות אספקה ארגוניות. היגיינת אבטחת IT הפכה לחשובה אף יותר כאשר גורמים פיתחו דרכים חדשות לנצל במהירות פגיעויות שלא תוקנו, הרחיבו טכניקות לפגיעה ברשתות ארגוניות וטשטשו את פעילותם באמצעות תוכנת קוד פתוח או תוכנה לגיטימית. טכניקות תקיפה חדשות סיפקו וקטורים חדשים וקשים יותר לזיהוי להשגת גישה לרשת של היעד. לבסוף, ככל שההתקפות הפיזיות המלחמתיות הסלימו, ראינו את מתקפות הסייבר ממלאות תפקיד בולט יותר בפעילות הצבאית.

העימות באוקראינה סיפק דוגמה נוקבת למדי לאופן שבו מתקפות סייבר מתפתחות כדי להשפיע על העולם במקביל לעימות צבאי בשטח. מערכות חשמל, מערכות טלקומוניקציה, מדיה ותשתיות חיוניות אחרות הפכו כולן למטרות הן של התקפות פיזיות והן של מתקפות סייבר. ניסיונות פריצה לרשת שנחשבו בדרך כלל כחלק ממבצעי ריגול וחילוץ מידע התמקדו במלחמה ההיברידית בהתקפות תוכנות זדוניות הרסניות שמבצעות מחיקה נגד מערכות תשתיות חיוניות. חיבור האבטחה של מערכות אלה לענן הביא לגילוי מוקדם ולשיבוש של התקפות בעלות פוטנציאל הרסני.[1]

בפעם הראשונה באירוע סייבר גדול, זיהויים התנהגותיים הממנפים למידת מכונה השתמשו בדפוסי תקיפה ידועים כדי לזהות ולעצור בהצלחה התקפות נוספות ללא ידע מוקדם על התוכנות הזדוניות שבבסיסן – אפילו לפני שבני האדם היו מודעים לאיומים. אישרנו גם את הערך של שיתוף מודיעין איומים בזמן אמת עם מגיני מערכות אלה, שמספק להם מידע חיוני לחיזוי ולהגנה מפני התקפות פעילות.

גורמי איום מדינתיים ברחבי העולם ממשיכים להרחיב את פעילותם בדרכים חדשות וישנות. סין, צפון קוריאה, איראן ורוסיה ביצעו כולן התקפות על לקוחות של Microsoft. שרשרת האספקה של שירותי IT הפכה למטרה נפוצה כאשר גורמים העבירו את המיקוד לשירותי תמסורת (upstream) שיכולים להוות נקודות גישה לארגונים מרובים. אנו מצפים שהגורמים ימשיכו לנצל קשרים מהימנים בשרשראות האספקה הארגוניות, דבר המדגיש את חשיבות האכיפה המקיפה של כללי האימות, ביצוע התיקונים בהתמדה וקביעת תצורת החשבונות לתשתית גישה מרחוק, וביקורות תכופות של קשרי שותפים כדי לאמת אותנטיות.

גורמים מדינתיים, בדומה למפעילי תוכנות כופר ולמפעילים פליליים, הגיבו לחשיפה המוגברת על ידי מעבר להתמקדות במערכות ארגוניות שאינן מוגדרות כהלכה או לא מתוקנות (תשתיות VPN/VPS, שרתים מקומיים, תוכנות צד שלישי) כדי לבצע התקפות 'living-off-the-land'. רבים מהם הגבירו את השימוש בתוכנות זדוניות שנרכשו ובכלי צוות אדום בקוד פתוח כדי לטשטש את הפעילות הזדונית שלהם.

כתוצאה מכך, שמירה על בסיס חזק של היגיינת אבטחת IT באמצעות תיקונים מתועדפים, הפעלת תכונות למניעת חבלה, שימוש בכלי ניהול שטח התקיפה כמו RiskIQ כדי לקבל מבט מבחוץ על שטח התקיפה והפעלת אימות רב-גורמי ברחבי הארגון כולו, הפכו ליסודות בסיסיים להגנה יזומה מפני גורמים מתוחכמים רבים.

גם שחקנים מדינתיים הגבירו את השימוש בתוכנות כופר כטקטיקה בהתקפות שלהם, ולעתים קרובות השתמשו בתוכנות כופר זדוניות שנוצרו על ידי אותה מערכת אקולוגית פלילית בהתקפות שלהם. ראינו גורמים שבסיסם הן באיראן והן בצפון קוריאה, ממנפים כלי תוכנות כופר שנרכשו כדי לפגוע במערכות שסומנו כמטרה הכוללות לעתים קרובות תשתיות חיוניות, במסגרת יריבויות אזוריות. לבסוף, ראינו את האיום הגובר של שכירי חרב בסייבר המפתחים ומוכרים כלים, טכניקות ושירותים להרחבת נקודות התורפה המנוצלות לרעה נגד פתרונות של ספקים חיצוניים. התחכום והזריזות של התקפות מצד גורמים מדינתיים ימשיכו להתפתח מדי שנה. ארגונים חייבים להגיב על ידי קבלת מידע על השינויים בגורמים אלה ובמקביל לפתח הגנות.

ג'ון למברט
סמנכ"ל החברה ומהנדס בכיר, מרכז המודיעין לגבי איומים של Microsoft

רקע על נתונים ברמת המדינה

איומים ברמת המדינה מוגדרים כפעילות איומי סייבר שמקורה במדינה מסוימת מתוך הכוונה לקדם לכאורה את האינטרסים הלאומיים. גורמים מדינתיים מציגים כמה מהאיומים המתקדמים והמתמשכים ביותר שלקוחותינו מתמודדים איתם, כולל גניבת קניין רוחני, ריגול, מעקבים, גניבת אישורים, התקפות הרסניות ועוד.

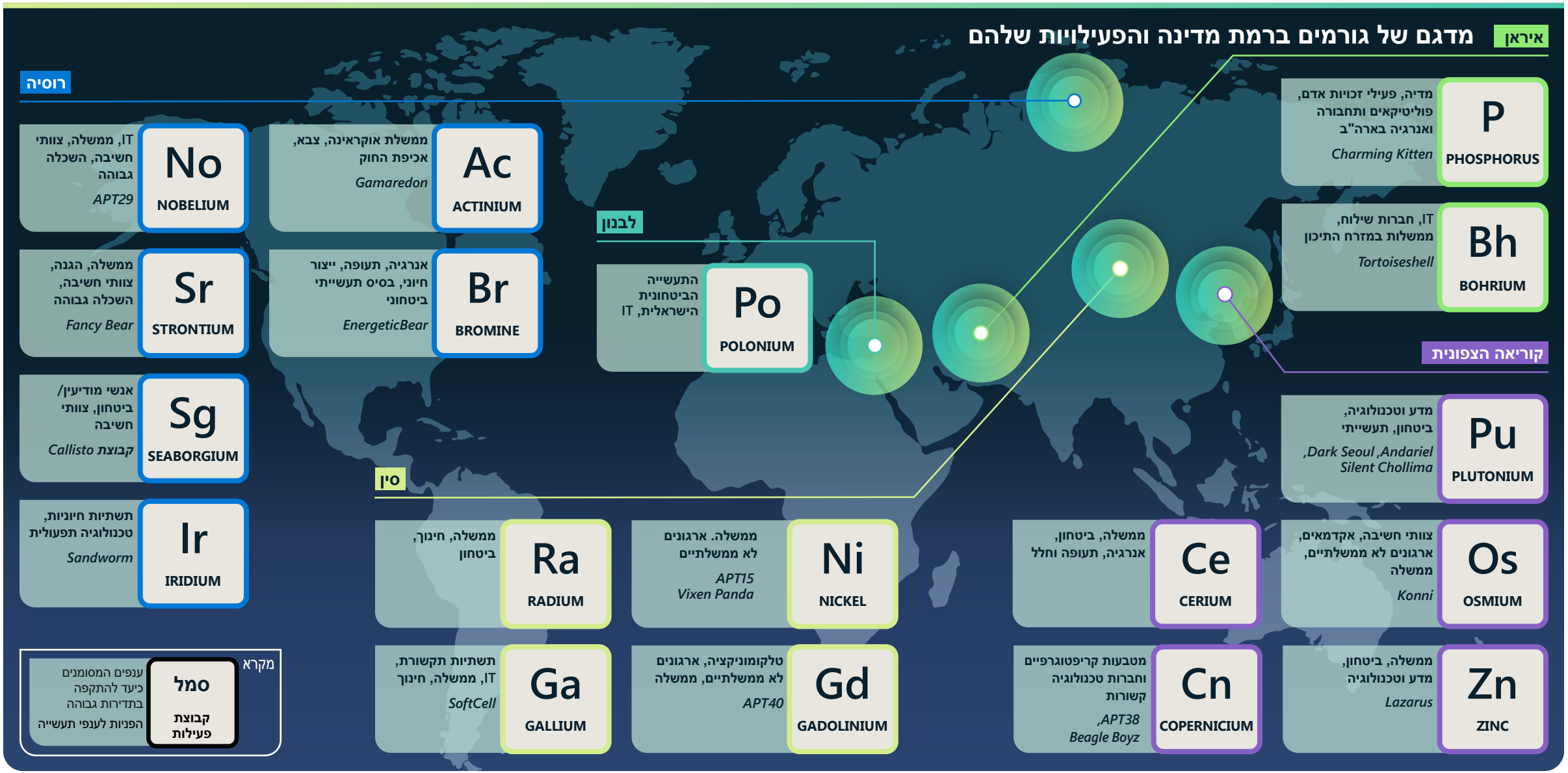
אנו משקיעים משאבים רבים בגילוי, הבנה והתמודדות עם איומים אלה. כאשר ארגון או בעלים יחיד של חשבון מותקף או נפרץ על-ידי פעילויות של מדינה שנצפו, Microsoft מספקת התראה בצורה של הודעת מצב מדינתי (NSN) ישירות ללקוח, כולל המידע הדרוש לו כדי לחקור את הפעילות. נכון ליוני 2022, סיפקנו יותר מ-67,000 התראות NSN מאז שהתחלנו ב-2018.

נתוני התראות NSN של Microsoft מוצגים בפרק זה כדי לספק תצוגה של פעילות מדידה. רמת הפעילות המדינתית המוצגת בתרשימים מבוססת על מספר התראות ה-NSN ש-Microsoft הנפיקה ללקוחות בתגובה לזיהוי של גורמים מדינתיים המתמקדים בחשבון אחד לפחות בארגון הלקוח או פורצים אליו.

ארבעת המדינות העיקריות שאת קבוצות האיומים שלהן אנו כוללים בדוח זה הן רוסיה, סין, איראן וצפון קוריאה. אלה מייצגות את מדינות המוצא של הגורמים הנפוצים ביותר שנצפו ששמו להם כמטרה את לקוחות Microsoft בשנה האחרונה. הדוח כולל גם את ההבחנות שלנו לגבי קבוצות איומים מלבנון ושכירי חרב בסייבר, או גורמים התקפיים מהמגזר הפרטי הניתנים להשכרה.

Microsoft מזהה קבוצות מדינתיות לפי שמות של יסודות כימיים (כגון NOBELIUM), שרק חלקם מוצגים בדף הבא. אנו משתמשים בכינויי ####-DEV כשם זמני שניתן לאשכול לא ידוע, חדש בשטח או מתפתח של פעילות איומים, גושה המאפשרת לנו לעקוב אחריו כערכת מידע ייחודית עד שנגיע לרמה גבוהה של ביטחון לגבי מקורו או זהותו של הגורם העומד מאחורי הפעילות.

ברגע שהוא עומד בקריטריונים, DEV מומר לגורם בעל שם או מתמזג עם גורמים קיימים. לאורך פרק זה, אנו מצטטים דוגמאות של קבוצות מדינתיות וקבוצות DEV כדי לספק מבט מעמיק יותר על יעדי התקיפה, הטכניקות וניתוח המניעים. על אף שרבות מקבוצות אלו משתמשות באותם כלים כמו פושעי סייבר, הן מציגות איומים ייחודיים בצורה של תוכנות זדוניות מותאמות, היכולת לגלות ולנצל פגיעויות מסוג "אפס ימים" וחסינות משפטית.


מדגם של גורמים ברמת מדינה והפעילויות שלהם
איראן
רוסיה
לבנון
סין
קוריאה הצפונית
P PHOSPHORUS
מדיה, פעילי זכויות אדם, פוליטיקאים ותחבורה ואנרגיה בארה"ב
Charming Kitten
Bh BOHRIUM
IT, חברות שילוח, ממשלות במזרח התיכון
Tortoiseshell
Pu PLUTONIUM
מדע וטכנולוגיה, ביטחון, תעשייתי
Andariel, Dark Seoul, Silent Chollima
Os OSMIUM
צוותי חשיבה, אקדמאים, ארגונים לא ממשלתיים, ממשלה
Konni
Zn ZINC
ממשלה, ביטחון, מדע וטכנולוגיה
Lazarus
Ce CERIUM
ממשלה, ביטחון, אנרגיה, תעופה וחלל
Cn COPERNICIUM
מטבעות קריפטוגרפיים וחברות טכנולוגיה קשורות
APT38, Beagle Boyz
Ni NICKEL
ממשלה. ארגונים לא ממשלתיים
APT15
Vixen Panda
Gd GADOLINIUM
טלקומוניקציה, ארגונים לא ממשלתיים, ממשלה
APT40
Ra RADIUM
ממשלה, חינוך, ביטחון
Ga GALLIUM
תשתיות תקשורת, IT, ממשלה, חינוך
SoftCell
Po POLONIUM
התעשייה הביטחונית הישראלית, IT
Ac ACTINIUM
ממשלת אוקראינה, צבא, אכיפת החוק
Gamaredon
Br BROMINE
אנרגיה, תעופה, ייצור חיוני, בסיס תעשייתי ביטחוני
EnergeticBear
No NOBELIUM
IT, ממשלה, צוותי חשיבה, השכלה גבוהה
APT29
Sr STRONTIUM
ממשלה, הגנה, צוותי חשיבה, השכלה גבוהה
Fancy Bear
Sg SEABORGIUM
אנשי מודיעין/ ביטחון, צוותי חשיבה
קבוצת Callisto
Ir IRIDIUM
תשתיות חיוניות, טכנולוגיה תפעולית
Sandworm
מקרא
סמל קבוצת פעילות
ענפים המסומנים כיעד להתקפה בתדירות גבוהה הפניות לענפי תעשייה

נוף האיומים המתפתח

המשימה של Microsoft לעקוב אחר פעילות הגורמים המדינתיים ולהודיע ללקוחות כאשר אנו רואים שהם מהווים יעד או נפרצים נעוצה במשימתנו להגן על לקוחותינו מפני התקפות.

הודעה זו היא חלק חיוני ממחויבותנו ליידע את הלקוחות אם התקפות שנצפו נמנעות בהצלחה על-ידי הגנות מוצרי האבטחה שלנו, או אם ההתקפות יעילות עקב חולשות אבטחה לא ידועות. מעקב אחר הודעות לאורך זמן עוזר ל-Microsoft לזהות מגמות איומים מתפתחות לפי גורמים ולמקד את הגנות המוצר בצמצום יזום של איומים על לקוחות בשירותי הענן שלנו.

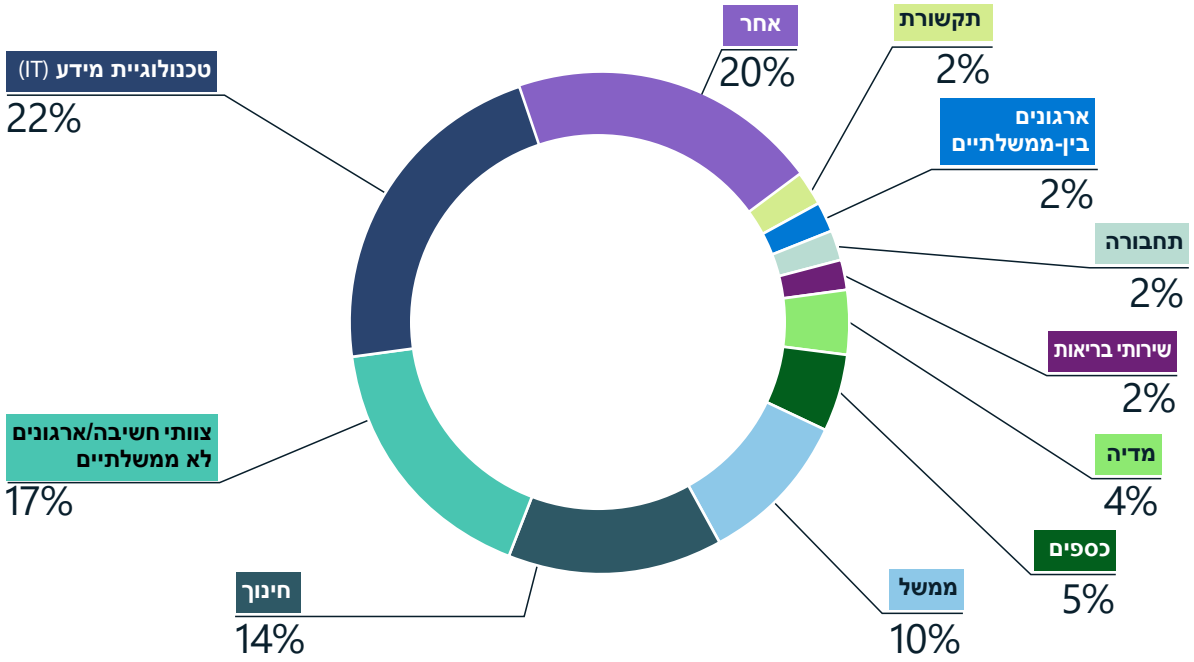
מעקב זה גם מאפשר לנו לשתף נתונים ותובנות לגבי מה שאנו רואים. האנליסטים העוקבים אחר גורמים אלה ואחר התקפותיהם מסתמכים על שילוב של אינדיקטורים טכניים ומומחיות גיאופוליטית כדי להבין את המניעים של הגורמים, ומשלבים הקשר טכני וגלובלי לקבלת תובנות חדשות. אצירת נתונים זו מספקת מבט ייחודי על סדרי העדיפויות של גורמי סייבר ברמת המדינה ועל האופן שבו המניעים שלהם עשויים לשקף את סדרי העדיפויות הפוליטיים, הצבאיים והכלכליים של המדינות המעסיקות אותם.

ההתפתחויות הפוליטיות בשנה האחרונה עיצבו את סדרי העדיפויות ואת העמידות לסכנות של קבוצות איומים בחסות מדינות ברחבי העולם. ככל שהיחסים הגיאופוליטיים נשברו ואלמנטים ניציים השיגו שליטה רבה יותר במדינות מסוימות, גורמי הסייבר הפכו חצופים ואגרסיביים יותר. לדוגמה:

- רוסיה תקפה ללא רחם את ממשלת אוקראינה ואת התשתיות החיוניות של המדינה כדי להשלים את הפעולה הצבאית שלה בשטח.[2]
- איראן חיפשה באגרסיביות דרך לחדור לתשתיות חיוניות של ארה"ב, כגון רשויות הנמלים.
- קוריאה הצפונית המשיכה בקמפיין של גניבת מטבעות קריפטוגרפיים מחברות פיננסיות וטכנולוגיות.
- סין הרחיבה את פעילות ריגול הסייבר הגלובלית שלה.

אף על פי שגורמים מדינתיים יכולים להיות מתוחכמים מבחינה טכנית ולהשתמש במגוון רחב של טקטיקות, לעתים קרובות ניתן לצמצם את ההתקפות שלהם באמצעות היגיינת סייבר טובה. רבים מגורמים אלה מסתמכים על אמצעים פשוטים יחסית, כגון מתקפות ממוקדות (spear-phishing) בהודעות דואר אלקטרוני, להעברת תוכנות זדוניות מתוחכמות במקום להשקיע בפיתוח נקודות תורפה בהתאמה אישית או להשתמש בהנדסה חברתית ממוקדת כדי להשיג את מטרותיהם.

מגזרי תעשייה המהווים מטרה עבור גורמים מדינתיים



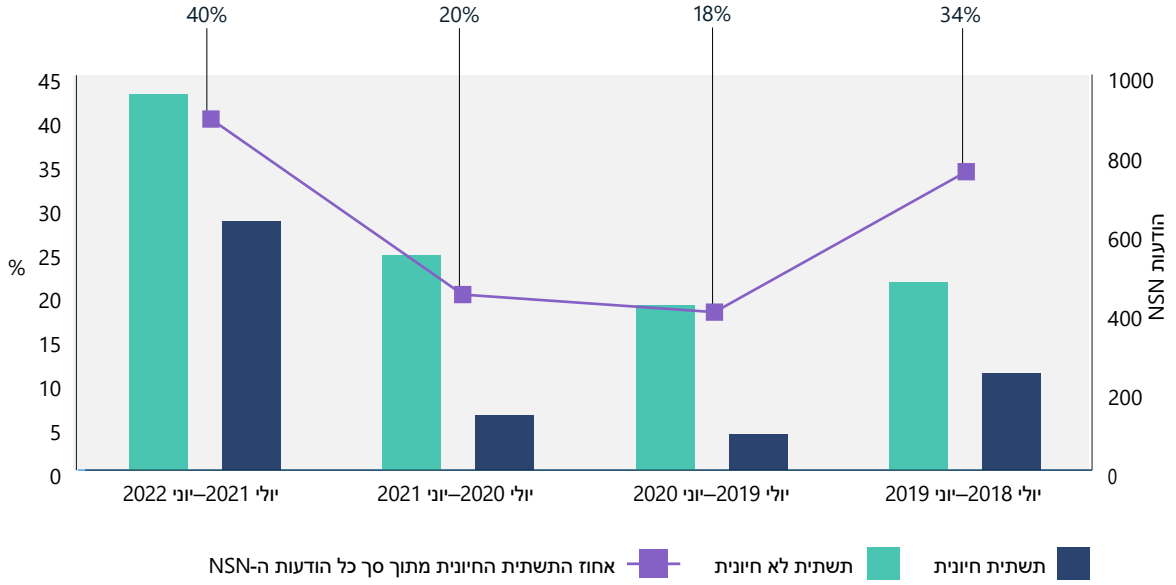
קבוצות מדינתיות התמקדו במגוון מגזרים. גורמים מדינתיים רוסיים ואיראניים התמקדו בתעשיית ה-IT כאמצעי גישה ללקוחות חברות ה-IT. צוותי חשיבה, ארגונים לא ממשלתיים (NGOs), אוניברסיטאות וגופי ממשל המשיכו להוות מטרות נפוצות אחרות עבור גורמים מדינתיים.

לגורמים מדינתיים יש מגוון מטרות שיכולות לגרום להתמקדות בקבוצות ספציפיות של ארגונים או אנשים. בשנה האחרונה, התקפות שרשראות האספקה גברו, עם דגש מיוחד על חברות IT. על ידי פגיעה בספקי שירותי IT, גורמי איום מסוגלים לעתים קרובות להגיע ליעד המקורי שלהם באמצעות מערכת יחסים מבוססת אמון עם החברה המנהלת מערכות מחוברות, או אפילו לבצע התקפות בקנה מידה גדול בהרבה על ידי פגיעה במאות לקוחות במורד הזרם בהתקפה אחת. אחרי מגזר ה-IT, הגופים שהותקפו בתדירות הגבוהה ביותר היו צוותי חשיבה, אקדמאים הקשורים לאוניברסיטאות ופקידי ממשל. אלה הן "מטרות רכות" רצויות לריגול לצורך איסוף מודיעין בנושאים גיאופוליטיים.

נוף האיומים המתפתח

המשך

מגמות בתשתיות החיוניות

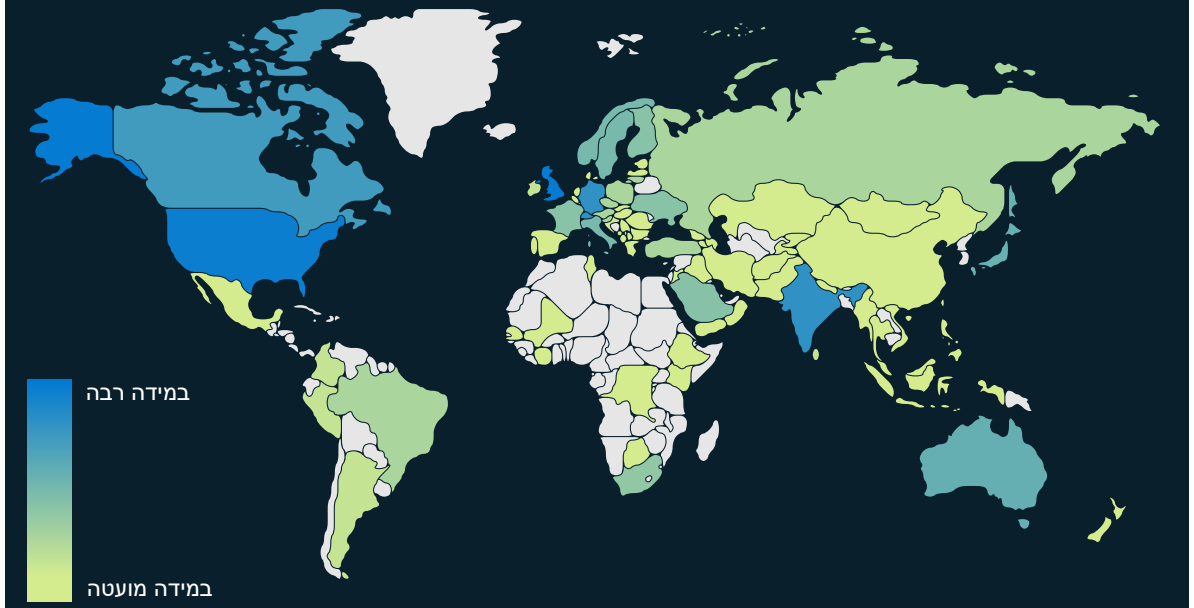


ההתמקדות של קבוצות מדינתיות בתשתיות חיוניות[3] גברה בשנה האחרונה, כאשר הגורמים התמקדו בחברות במגזר ה-IT, בשירותים פיננסיים, במערכות התחבורה ובתשתיות התקשורת.

"לפני הפלישה לאוקראינה, ממשלות חשבו שנתונים צריכים להישאר בתוך מדינה כדי להיות מאובטחים. לאחר הפלישה, העברת נתונים לענן ומעבר אל מחוץ לגבולות טריטוריאליים הם כעת חלק מתכנון עמידות ומנהל תקין".

כריסטין פלין גודווין,
יועצת משפטית עמיתה, אבטחת לקוחות ואמון

המיקוד הגיאוגרפי של גורמים מדינתיים



מיקוד הסייבר של קבוצות מדינתיות התפשט ברחבי העולם בשנה האחרונה, עם דגש מיוחד על ארגונים בארה"ב ובבריטניה. ארגונים בישראל, באיחוד האמירויות הערביות, בקנדה, בגרמניה, בהודו, בשוויץ וביפן היו גם הם בין המותקפים ביותר, על פי נתוני ה-NSN שלנו.

תובנות מעשיות

1. יש לזהות את יעדי הנתונים הפוטנציאליים בעלי הערך הגבוה, הטכנולוגיות בסיכון, המידע והפעולות העסקיות שעשויים להתאים לסדרי העדיפויות האסטרטגיים של קבוצות מדינתיות ולהגן עליהם.
2. יש לאפשר הגנות ענן כדי לספק זיהוי וצמצום של איומים ידועים וחדשים על הרשת שלך בקנה מידה גדול.

שרשרת אספקת ה-IT כשער למערכת האקולוגית הדיגיטלית

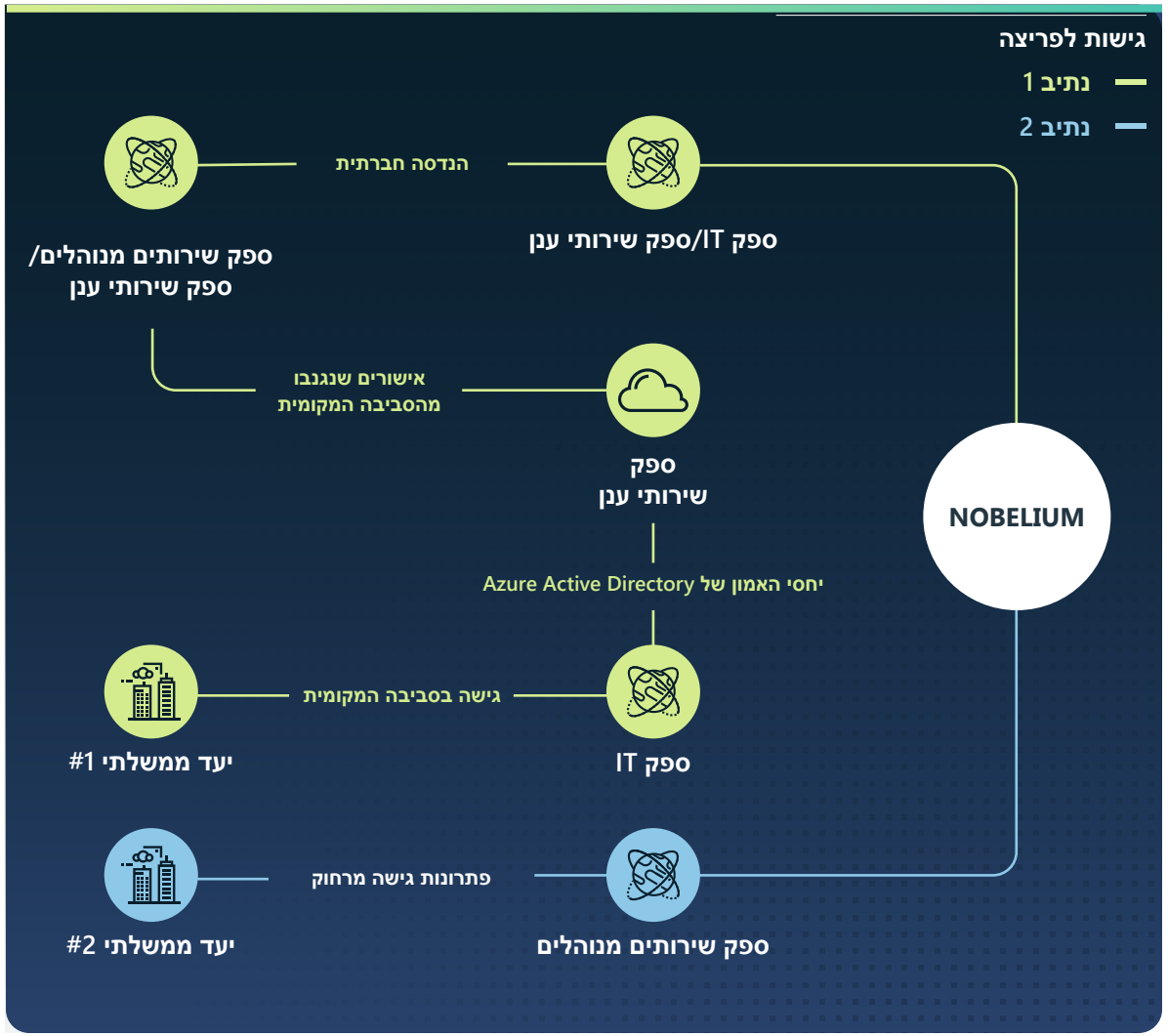
התמקדות של מדינות בספקי שירותי IT עשויה לאפשר לגורמי האיום לנצל ארגונים אחרים המעניינים אותם על-ידי ניצול האמון והגישה המוענקים לספקי שרשרת אספקה אלה. בשנה האחרונה, קבוצות איומי סייבר מדינתיות התמקדו בספקי שירותי IT כדי לתקוף מטרות צד שלישי ולקבל גישה ללקוחות במורד הזרם במגזרי הממשלה, המדיניות והתשתיות החיוניות.

ספקי שירותי IT הם יעדי ביניים אטרקטיביים מכיוון שהם משרתים מאות לקוחות ישירים ואלפי לקוחות עקיפים שמעניינים את שירותי המודיעין הזרים. אם הן מנוצלות לרעה, הנהלים העסקיים השגרתיים והרשאות הניהול המוקצות שמהם נהנות חברות אלה, עלולים לאפשר לגורמים זדוניים לגשת לרשתות הלקוח של ספקי שירותי IT ולהשתמש בהן מבלי להפעיל התראות באופן מיידי.

בשנה האחרונה, NOBELIUM ניסתה לפרוץ ולמנף חשבונות מורשים בפתרונות ענן ובספקי שירותים מנוהלים אחרים כדי לנסות להשיג גישה ממוקדת במורד הזרם ללקוחות ממשלתיים ולקוחות מדיניות בעיקר בארה"ב ובאירופה.

NOBELIUM הדגימה כיצד גישה של "פריצה לאחד לצורך פריצה לרבים" יכולה להיות מכוונת נגד מי שנתפס כיריב גיאופוליטי. בשנה האחרונה, גורם האיום עסק בפריצות צד שלישי ופריצות ישירות לארגונים רגישים שבסיסם במדינות החברות בארגון האמנה הצפון אטלנטית (נאט"ו), שממשלת רוסיה תופסת כאיום קיומי. בין יולי 2021 לתחילת יוני 2022, 48 אחוז מההודעות ללקוחות Microsoft על פעילות איומים רוסית נגד לקוחות שירותים מקוונים הגיעו לחברות ממגזר ה-IT שבסיסן במדינות החברות בנאט"ו, ככל הנראה כנקודות גישה מתווכות. בסך הכול, 90 אחוז מההודעות על פעילות האיומים הרוסית באותה תקופה הגיעו ללקוחות שבסיסם במדינות החברות בנאט"ו, בעיקר במגזרי ה-IT, צוותי החשיבה והארגונים הלא ממשלתיים (NGOs) ובמגזרים ממשלתיים, דבר המרמז על אסטרטגיה של חיפוש אחר מספר אמצעים לגישה ראשונית ליעדים אלה.

> חל מעבר מניצול שרשרת אספקת התוכנה לניצול שרשרת האספקה של שירותי IT, תוך התמקדות בפתרונות ענן ובספקי שירותים מנוהלים כדי להגיע ללקוחות במורד הזרם.



תרשים זה מתאר את הגישה הרב-וקטורית של NOBELIUM לפריצה ליעדים האולטימטיביים שלה ואת הנזק המשני שגרמה לקורבנות אחרים בדרך. בנוסף לפעולות המוצגות לעיל, NOBELIUM שיגרה התקפות תרסיס סיסמאות (password spray) והתקפות דיוג נגד הגופים המעורבים, ואף כוונה לחשבון האישי של לפחות עובד ממשלתי אחד כנתיב פוטנציאלי נוסף לפריצה.

שרשרת אספקת ה-IT כשער למערכת האקולוגית הדיגיטלית

המשך

במהלך השנה, מרכז המודיעין לגבי איומים של Microsoft (MSTIC) זיהה מספר גדל והולך של גורמים מדינתיים איראניים וגורמים הקשורים לאיראן הפורצים לחברות IT. במקרים רבים, גורמים זוהו גונבים אישורי כניסה כדי להשיג גישה ללקוחות במורד הזרם לצורך מגוון מטרות, החל מאיסוף מודיעין ועד התקפות נקמה הרסניות.

- בחודשים יולי ואוגוסט 2021, DEV-0228 פרצה לספקית תוכנה עסקית ישראלית כדי לפגוע מאוחר יותר בלקוחות במורד הזרם בתחומי הביטחון, האנרגיה והמשפט בישראל.[4]
- מאוגוסט עד ספטמבר 2021, Microsoft זיהתה זינוק במספר הגורמים המדינתיים האיראניים ששמו להם למטרה חברות IT שבסיסן בהודו. היעדרן של סוגיות גיאופוליטיות בוערות שהיו יכולות להניע שינוי כזה מצביע על כך שהתמקדות זו נועדה להשגת גישה עקיפה לחברות בת וללקוחות מחוץ להודו.
- בינואר 2022, DEV-0198, קבוצה שאנו מעריכים כי היא מזוהה עם ממשלת איראן, פרצה לספקית פתרונות ענן ישראלית. Microsoft מעריכה שסביר להניח שהגורם השתמש באישורים שנפרצו מהספק כדי לבצע אימות לצורך כניסה לחברת לוגיסטיקה ישראלית. MSTIC הבחינה שאותו גורם ניסה לבצע מתקפת סייבר הרסנית נגד חברת הלוגיסטיקה מאוחר יותר באותו חודש.
- באפריל 2022, POLONIUM, קבוצה שבסיסה בלבנון שאנו מעריכים ששיתפה פעולה עם קבוצות מדינתיות איראניות בטכניקות שרשרת אספקת IT, פרצה לחברת IT ישראלית נוספת כדי להשיג גישה לארגונים ביטחוניים ומשפטיים ישראליים.[5]

שנת הפעילות האחרונה ממחישה כי גורמי איום כמו NOBELIUM ו-DEV-0228 לומדים להכיר את נוף יחסי האמון של הארגון טוב יותר מאשר מכירים הארגונים עצמם. איום מוגבר זה מדגיש את הצורך של הארגונים להבין ולהקשיח את הגבולות ונקודות הכניסה של הנכסים הדיגיטליים שלהם. הוא גם מדגיש את החשיבות עבור ספקי שירותי IT לנטר בקפדנות את תקינות אבטחת הסייבר שלהם. לדוגמה, על ארגונים ליישם אימות רב-גורמי ומדיניות גישה מותנית שמקשים על גורמים זדוניים ללכוד חשבונות מורשים או להתפשט ברחבי הרשת.

ביצוע בדיקה וביקורת יסודיות של קשרי שותפים עוזרות לצמצם הרשאות מיותרות בין הארגון לספקים במעלה הזרם ומסירות באופן מיידי את הגישה מכל קשר שנראה לא מוכר. הגברת ההיכרות עם יומני הפעילות וסקירת הפעילות הזמינה מקלות על זיהוי חריגות שעלולות לגרור חקירה נוספת.

> מיקוד של מדינות בצדדים שלישיים מאפשר להם לנצל ארגונים רגישים על ידי ניצול האמון והגישה בשרשרת אספקה.

תובנות מעשיות

1. יש לבצע סקירה וביקורת על הקשרים עם ספקי שירות במעלה הזרם ובמורדו ועל הרשאות גישה מוקצות כדי לצמצם הרשאות מיותרות. יש להסיר גישה מקשרי שותפים שנראים לא מוכרים או שעדיין לא נבדקו.[6]
2. יש לאפשר רישום וסקירה של כל פעילות האימות עבור תשתית גישה מרחוק ורשתות וירטואליות פרטיות (VPN), תוך התמקדות בחשבונות המוגדרים עם אימות גורם יחיד, כדי לאשר את האותנטיות ולחקור פעילות חריגה.
3. יש להפעיל MFA עבור כל החשבונות (כולל חשבונות שירות) ולוודא ש-MFA נאכף עבור כל הקישוריות מרחוק.
4. יש להשתמש בפתרונות ללא סיסמה כדי לאבטח חשבונות.[7]

קישורים למידע נוסף

- NOBELIUM מתמקדת בהרשאות ניהול מוקצות להקלה על ביצוען של התקפות רחבות יותר | מרכז המודיעין לגבי איומים של Microsoft (MSTIC)
- ההתמקדות האיראנית במגזר ה-IT גוברת | מרכז המודיעין לגבי איומים של Microsoft (MSTIC), יחידת האבטחה הדיגיטלית של Microsoft
- חשיפת פעילותה ותשתיתה של POLONIUM המכוונות נגד ארגונים ישראליים | מרכז המודיעין לגבי איומים של Microsoft (MSTIC)

ניצול מהיר של פגיעות

ככל שארגונים מחזקים את מערך אבטחת הסייבר שלהם, גורמים מדינתיים מגיבים בנקיטת טקטיקות חדשות וייחודיות לשיגור התקפות ולהתחמקות מזיהוי. הזיהוי והניצול של פגיעויות שלא היו ידועות קודם לכן – הידועות כפגיעויות מסוג "אפס-ימים" – היא טקטיקה מרכזית במאמץ זה.

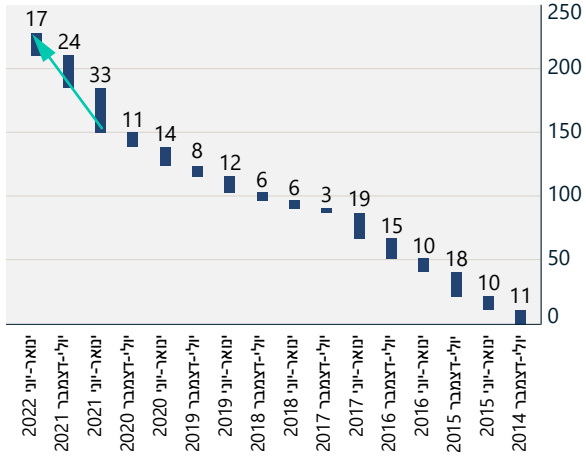
פגיעויות מסוג "אפס-ימים" הן אמצעי יעיל במיוחד לניצול ראשוני, ולאחר שנחשפו לציבור, הפגיעויות יכולות במהרה להיות בשימוש חוזר על ידי מדינות וגורמים פליליים אחרים. מספר הפגיעויות מסוג "אפס ימים" שנחשפו לציבור בשנה האחרונה משתווה למספר הפגיעויות מהשנה הקודמת, שהיה הגבוה ביותר שנרשם.

ככל שגורמי איומי סייבר – הן מדינתיים והן פליליים – הופכים מיומנים יותר במינוף פגיעויות אלה, ראינו צמצום בזמן שבין ההכרזה על פגיעות לבין ההתמסחרות של פגיעות זו. לכן חיוני שארגונים יתקנו נקודות תורפה באופן מיידי. באופן דומה, חיוני שארגונים או אנשים שמגלים פגיעויות חדשות יחשפו אותן או ידווחו עליהן באופן אחראי לספקים המושפעים בהקדם האפשרי, בהתאם לנהלי חשיפה מתואמת של פגיעויות.

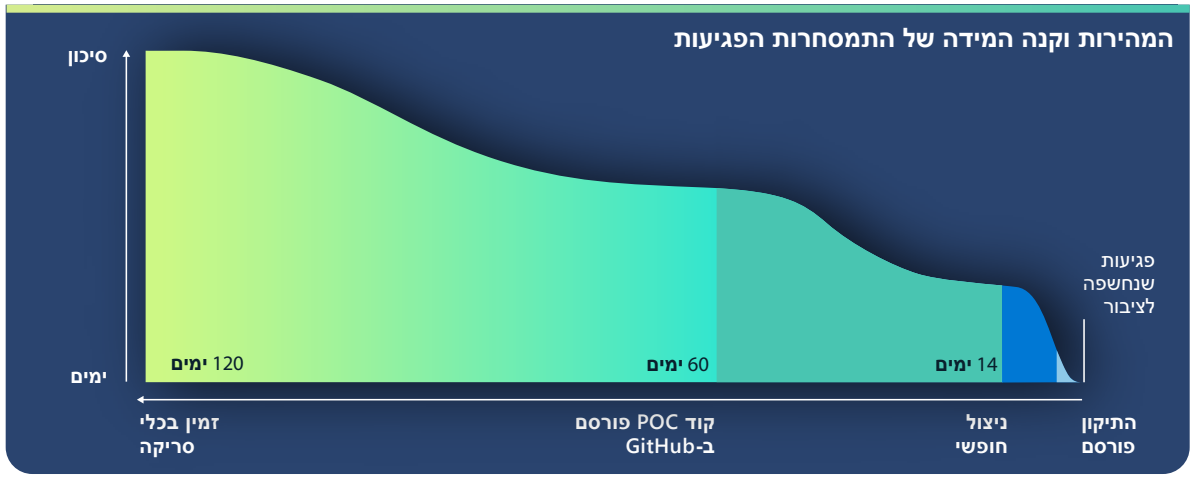
כך ניתן לוודא כי פגיעויות מזוהות, ותיקונים מפותחים בזמן כדי להגן על הלקוחות מפני איומים שלא היו ידועים בעבר.

ארגונים רבים מניחים שפחות סביר שהם יהיו קורבן להתקפות נקודות תורפה מסוג יום-אפס אם ניהול פגיעויות הוא חלק בלתי נפרד מאבטחת הרשת שלהם. עם זאת, ההתמסחרות של נקודות התורפה גורמת להן להגיע בקצב הרבה יותר מהיר. נקודות תורפה מסוג יום אפס מתגלות לעתים קרובות על ידי גורמים אחרים ונעשה בהן שימוש חוזר באופן נרחב בפרק זמן קצר, כך שמערכות לא מתוקנות נמצאות בסיכון. אף על פי שקשה לזהות נקודות תורפה מסוג יום אפס, לעתים קרובות קל יותר לזהות פעולות של שחקנים לאחר ניצולן, ואם הן מגיעות מתוכנות מתוקנות לחלוטין, הן יכולות לשמש כסימן אזהרה לפריצה.

תיקונים שפורסמו עבור פגיעויות של יום אפס



מספר נקודות התורפה של יום-אפס שנחשפו לציבור מתוך רשימת נקודות התורפה והחשיפות הנפוצות (CVEs).



בממוצע, נדרשים רק 14 יום לנקודת תורפה להפוך להיות זמינה בחוץ לאחר שפגיעות נחשפת לציבור. תצוגה זו מספקת ניתוח של לוחות הזמנים של ניצול פגיעויות יום-אפס, יחד עם מספר המערכות הפגיעות לנקודת התורפה הנתונה והפעילות באינטרנט מרגע החשיפה הראשונה לציבור.

> בעוד שהתקפות נקודות תורפה של יום-אפס נוטות בתחילה להתמקד בקבוצה מוגבלת של ארגונים, הן מאומצות במהרה למערכת האקולוגית הגדולה יותר של גורם האיום. כך מתחיל מרוץ של שחקני האיום לנצל את הפגיעות בצורה רחבה ככל האפשר לפני שהיעדים הפוטנציאליים שלהם מתקינים תיקונים.

בעוד שאנו רואים גורמים מדינתיים רבים המפתחים נקודות תורפה מפגיעויות לא ידועות, גורמי איום מדינתיים המבוססים בסין מיומנים במיוחד בגילוי ופיתוח של נקודות תורפה של יום-אפס. תקנת דיווח הפגיעויות של סין נכנסה לתוקף בספטמבר 2021, והפכה למקרה הראשון בעולם שבו ממשלה מחייבת דיווח על פגיעויות לרשות ממשלתית לבדיקה לפני שהפגיעות משותפת עם בעל המוצר או השירות. תקנה חדשה זו עשויה לאפשר לגורמים בממשלת סין לאגור נקודות תורפה מדווחות לקראת הפיכתן לכלי נשק. השימוש המוגבר ביום-אפס בשנה האחרונה מצד גורמים שבסיסם בסין משקף ככל הנראה את השנה המלאה הראשונה של הדרישה לגילוי הפגיעויות של סין עבור קהילת הביטחון הסינית והינו צעד משמעותי בשימוש בנקודות תורפה של יום-אפס כעדיפות ממלכתית. הפגיעויות המתוארות להלן פותחו ונפרסו לראשונה על ידי גורמים מדינתיים שבסיסם בסין במסגרת התקפות, לפני שהתגלו והתפשטו בקרב גורמים אחרים במערכת האקולוגית הגדולה יותר של האיומים.

ניצול מהיר של פגיעות

המשך

אפילו לארגונים שאינם מהווים מטרה לגורמי איום מדינתיים יש פרק זמן מוגבל לתיקון פגיעויות יום-אפס במערכות מושפעות לפני שהפגיעויות מנוצלות על ידי המערכת האקולוגית הרחבה יותר של הגורם.

דוגמאות אלה של פגיעויות שזוהו לאחרונה מראות שלרשות הארגונים עומדים 60 יום בממוצע מרגע תיקון הפגיעות והפיכת קוד הוכחת ההיתכנות (POC) לזמין באינטרנט, אשר לעתים קרובות נאסף על-ידי גורמים אחרים לשימוש חוזר. באופן דומה, לרשות הארגונים עומדים 120 יום בממוצע לפני שפגיעות הופכת זמינה בכלי סריקה וניצול אוטומטיים של פגיעויות כגון Metasploit – שלעתים קרובות גורמים לשימוש בנקודת התורפה בקנה מידה עצום. עובדות אלה מדגישות שגם לארגונים שאינם מהווים מטרה לגורמי איום מדינתיים יש פרק זמן מוגבל לתיקון פגיעויות יום-אפס במערכות מושפעות לפני שהפגיעויות מנוצלות על ידי המערכת האקולוגית הרחבה יותר של הגורם.

CVE-2021-35211 SolarWinds Serv-U

ביולי 2021, SolarWinds פרסמה עלון ייעוץ בנושא אבטחה עבור CVE-2021-35211, והעניקה ל-Microsoft קרדיט על ההודעה.[8] באותו זמן, גילינו את גורם האיום התואם למדינה DEV-0322 מנצל באופן פעיל את הפגיעות SolarWinds Serv-U. צוות RiskIQ שלנו הבחין ב-12,646 כתובות IP המארחות גרסאות מחוברות לאינטרנט של המכשירים שהושפעו בין ה-15 ביוני ל-9 ביולי.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

בספטמבר 2021, החוקרים שלנו הבחינו בגורמים הקשורים לסין שמנצלים את Zoho ManageEngine במספר ישויות שבסיסן בארה"ב. הפגיעות דווחה לציבור ב-6 בספטמבר תחת השם Zoho CVE-2021-40539 ManageEngine ADSelfService Plus, שבו ארגונים משתמשים בדרך כלל כדי לטפל באיפוס סיסמאות.[9]

DEV-0322 ניצל את הפגיעות מאוחר יותר בספטמבר, והשתמש בה כווקטור ראשוני להשגת דריסת רגל ברשתות ולביצוע פעולות נוספות כולל פרסום שמות משתמש וסיסמאות, התקנת קבצים בינאריים מותאמים אישית ושחרור תוכנות זדוניות כדי לשמור על התמדה. בזמן הגילוי, RiskIQ הבחין ב-4,011 מקרים של מערכות אלה פעילות ובאינטרנט.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

בסוף אוקטובר 2021, הבחנו ב-DEV-0322 ממנף פגיעות (CVE-2021-44077) במוצר נוסף של Zoho ManageEngine, ServiceDesk Plus – תוכנת צוות תמיכה של IT עם ניהול נכסים. DEV-0322 השתמש בפגיעות זו כדי להתמקד בישויות במגזרי שירותי הבריאות, טכנולוגיית המידע, ההשכלה הגבוהה והייצור החיוני ולפרוץ אליהן. ב-2 בדצמבר, הבולשת הפדרלית (FBI) והסוכנות לאבטחת סייבר ותשתיות (CISA) פרסמו אזהרה משותפת לציבור על גורמי איום מדינתיים הממנפים את הפגיעות. בזמן הגילוי, RiskIQ הבחין ב-7,956 מקרים של מערכות אלה פעילות ובאינטרנט.

CVE-2021-42321 Microsoft Exchange

נקודת תורפה יום-אפס לפגיעות של Exchange CVE-2021-42321 נחשפה במהלך גביע Tianfu, פסגת אבטחת סייבר בינלאומית ותחרות פריצה שהתקיימה ב-16 וב-17 באוקטובר 2021 בצ'נגדו שבסין. חוקרי אבטחה ב-Microsoft הבחינו בנקודת התורפה לפגיעות ה-Exchange באה לידי שימוש בחוץ ב-21 באוקטובר, שלושה ימים בלבד לאחר חשיפת הפגיעות. בזמן הגילוי, RiskIQ הבחין ב-61,559 מקרים של מערכות אלה פעילות ובאינטרנט. המשכנו לעקוב אחר פעילות הניצול אל תוך נובמבר 2021.

CVE-2022-26134 Confluence

סביר להניח שלגורם הקשור לסין היה את קוד נקודת התורפה יום-אפס לפגיעות ה-Confluence (CVE-2022-26134) ארבעה ימים לפני שהפגיעות נחשפה לציבור ב-2 ביוני, וככל הנראה מינף אותה נגד ישות שבסיסה בארה"ב. בזמן הגילוי, RiskIQ הבחין ב-53,621 מקרים של מערכות פגיעות של Confluence באינטרנט.

פגיעויות נאספות ומנוצלות בקנה מידה עצום, ובטווחי זמן קצרים יותר ויותר.

תובנות מעשיות

1. יש לתעדף תיקון של פגיעויות יום-אפס ברגע שהן מתפרסמות; אין לחכות לפריסת מחזור ניהול התיקונים.
2. יש לתעד את כל נכסי החומרה והתוכנה הארגוניים ולערוך רשימת מלאי שלהם כדי לקבוע סיכון ולקבוע במהירות מתי לפעול לפי תיקונים.

טקטיקות הסייבר של גורמים מדינתיים רוסיים בזמן המלחמה מאיימות על אוקראינה ומעבר לה

השנה ראינו גורמים מדינתיים רוסיים משגרים פעולות סייבר כהשלמה לפעולה צבאית במהלך הפלישה הרוסית לאוקראינה, לעתים קרובות תוך שימוש באותן טקטיקות וטכניקות שהופעלו נגד מטרות מחוץ לאוקראינה. חיוני שארגונים ברחבי העולם ינקטו צעדים כדי להקשיח את אבטחת הסייבר מפני איומים דיגיטליים הנובעים מגורמי איום המזוהים עם רוסיה.

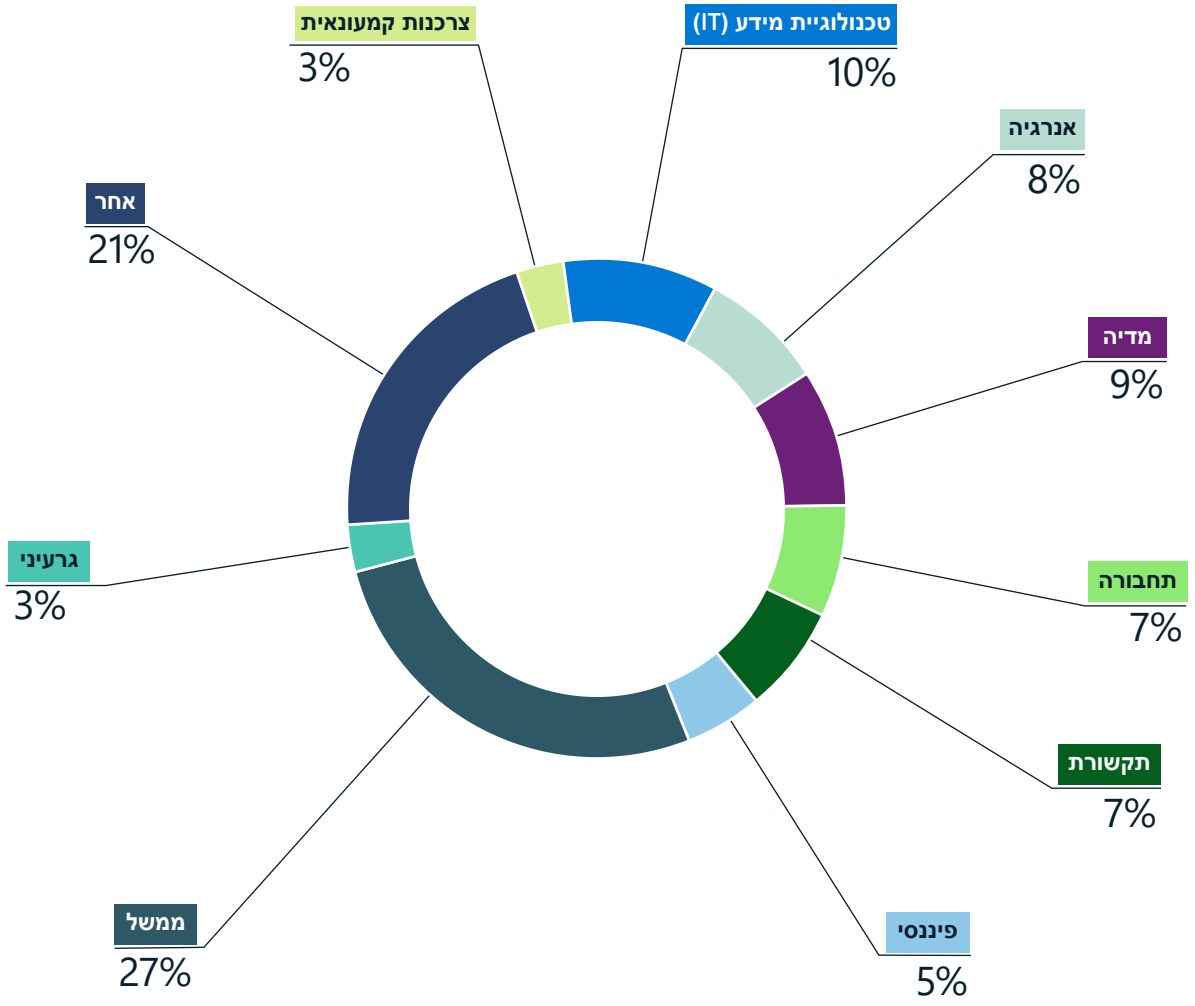
המצב בשטח ממשיך להשתנות ככל שהעימות הצבאי נמשך, ואוקראינה ובעלות בריתה צריכות להיות מוכנות להגן על עצמן אם מפעילי סייבר מדינתיים רוסיים יגבירו את התדירות או העוצמה של הפריצות בהתאם למטרות הצבאיות. במהלך ארבעת החודשים הראשונים של המלחמה, Microsoft הבחינה בגורמי איום הקשורים לצבא הרוסי משגרים גלים מרובים של מתקפות סייבר הרסניות נגד קרוב ל-50 גופים וארגונים אוקראינים שונים ופריצות ממוקדות ריגול נגד רבים אחרים. מבלי להכליל פעולות נגד לקוחות שירותים מקוונים, 64 אחוז מפעילות האיומים הרוסית נגד מטרות ידועות כוונה אל ארגונים שבסיסם באוקראינה בין סוף פברואר ליוני.

בכל פעולה, גורמי האיום הרוסיים השתמשו ברבות מהטקטיקות, הטכניקות והנהלים (TTPs) שראינו בשימוש לפני הפלישה נגד מטרות בתוך אוקראינה ומחוצה לה. גורמים אלה התכוונו להשמיד נתונים ולהוציא את גופי הממשל האוקראינים מאיזון בתקופה הראשונה של העימות. מאז הם שאפו להכשיל את העברת הסיוע הצבאי וההומניטרי לאוקראינה, לשבש את גישת הציבור לשירותים ולמדיה ולגנוב מידע בעל ערך מודיעיני או כלכלי ארוך טווח יותר עבור רוסיה.

התמקדות בתחבורה מאיימת על אזור בעל חשיבות קריטית לאזרחים אוקראינים המנסים לשרוד את העימות. על פי סקר שנערך בחסות UNICEF במאי, משיבים באזורים עירוניים שנפגעו מהעימות היו מודאגים ביותר לגבי התחבורה והדלק, השיבושים באספקה, הביטחון והגישה המוגבלת למזון, השירותים הרפואיים והשירותים הפיננסיים.[10] ביוני אמר מתאם המשברים של האו"ם באוקראינה כי לפחות 15.7 מיליון אנשים באוקראינה זקוקים בדחיפות לסיוע הומניטרי, והמספר יגדל ככל שהמלחמה תימשך.[11]

מחוץ לאוקראינה, Microsoft זיהתה מאמצי חדירה לרשת הרוסית נגד 128 ארגונים ב-42 מדינות בין סוף פברואר ליוני. ארצות הברית הייתה יעד מספר אחת של רוסיה. פולין, שדרכה עובר חלק גדול מהסיוע הצבאי וההומניטרי הבינלאומי לאוקראינה, הייתה גם היא מטרה משמעותית בתקופה זו. גורמי איום המזוהים עם המדינה הרוסית רדפו אחר ארגונים במדינות הבלטיות ורשתות מחשבים בדנמרק, נורבגיה, פינלנד ושוודיה באפריל וגם במאי.

מגזרי התעשייה שסומנו כיעדים במידה הרבה ביותר באוקראינה מאז הפלישה



ארגונים ממשלתיים פדרליים, מדינתיים ומקומיים באוקראינה המשיכו להוות יעדים מועדפים עבור קבוצות איום המזוהות עם המדינה הרוסית והקשורות אליה לאורך כל העימות. ההתמקדות בארגוני מגזרי התחבורה, האנרגיה, הפיננסים והמדיה מדגישה את הסיכון שפעולות סייבר אלה מציגות לשירותים שעליהם מסתמכים אזרחי אוקראינה.

טקטיקות הסייבר של גורמים מדינתיים רוסיים בזמן המלחמה מאיימות על אוקראינה ומעבר לה

המשך

ראינו עלייה בפעילות דומה המכוונת נגד משרדי החוץ של מדינות נאט"ו.

קבוצות האיום של המדינה הרוסית המשיכו להתעניין בפריצה לתשתיות חיוניות הן בתוך אוקראינה והן מחוצה לה בשנה האחרונה. IRIDIUM פרסה את התוכנה הזדונית Industroyer2 במאמץ כושל להשאיר מיליוני אנשים באוקראינה ללא חשמל. מחוץ לאוקראינה, BROMINE ביצעה פריצות נגד ארגונים המעורבים בייצור, ומערכות בקרה תעשייתיות בתחילת 2022.

גורמים מדינתיים רוסיים וגורמים הקשורים אליה כיוונו השנה פעולות סייבר נגד אוקראינה, בעלות בריתה ויעדים אחרים בעלי ערך מודיעיני באמצעות רבים מה-TTPs הבאים:

דיוג מסוג Spear phishing עם קבצים מצורפים או קישורים זדוניים

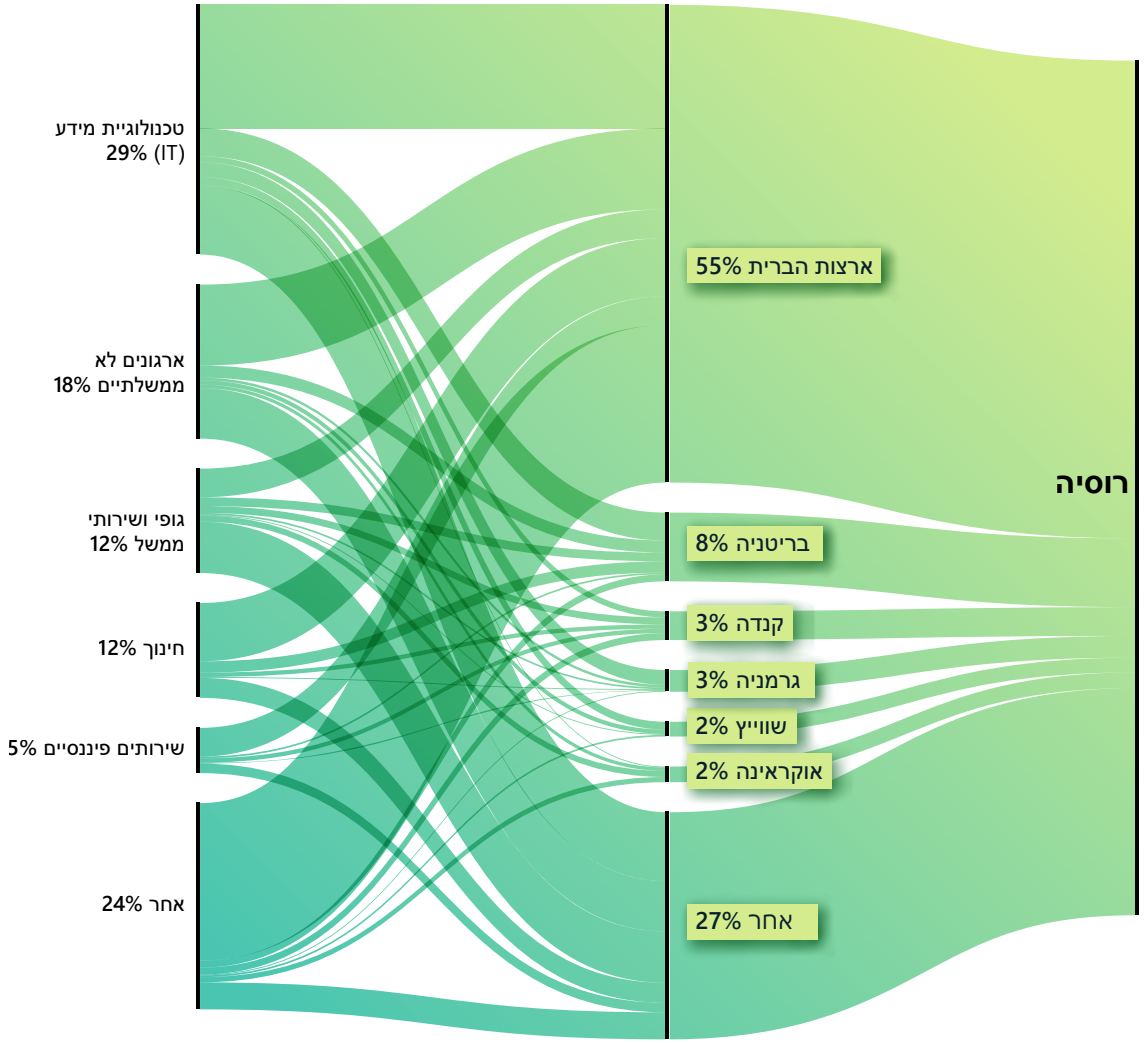
קבוצות מדינתיות רוסיות וקבוצות הקשורות לרוסיה כמו ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM ו-IRIDIUM השתמשו כולן בקמפיינים של דיוג כדי לקבל גישה ראשונית לחשבונות ורשתות רצויים בארגונים בתוך אוקראינה ומחוצה לה. קמפיינים רבים השתמשו בחשבונות פרוצים או מזויפים בארגונים ממוקדים או באותה תעשייה ובנושאים משכנעים כדי לפתות קורבנות. NOBELIUM השתמשה בחשבונות דיפלומטיים שנפרצו כדי לשלוח דואר דיוג במסווה של תקשורת דיפלומטית לעובדי משרד החוץ ברחבי העולם. STRONTIUM יצרה חשבונות מזויפים המבוססים על שמות זמינים לציבור של בעלי חשבונות בצוותי חשיבה בארצות הברית ושלחה הודעות דיוג כדי להשיג גישה לחשבונות באותם צוותי חשיבה. SEABORGIUM ביצע דיוג באמצעות פיתיונות הקשורים לדיווח על העימות באוקראינה כדי להשיג גישה ראשונית לחשבונות בצוותי חשיבה ליחסים בינלאומיים במדינות הנורדיות.

ניצול שרשרת האספקה של שירותי IT כדי להשפיע על לקוחות במורד הזרם

בסוף 2021, גורמים מדינתיים רוסיים פרצו לספקי שירותי IT והשתמשו בגישה כדי שיהיה להם קל יותר להשחית אתרים ולפרוס תוכנות זדוניות הרסניות של Whispergate על ידי DEV-0586 בינואר.[12] DEV-0586 גם פרצה לרשת של חברת IT שבנתה מערכות ניהול משאבים עבור משרד ההגנה האוקראיני וארגונים אחרים במגזרי התקשורת והתחבורה, עובדה המצביעה על כך שהקבוצה בחנה אפשרויות תקיפה דרך צד שלישי גם במגזרים אלה.

ברחבי העולם, אך במיוחד בארצות הברית ובמערב אירופה, NOBELIUM התמקדה בספקי שירותי IT כדי להשיג גישה לרשתות ממשלתיות ורשתות רגישות אחרות במהלך 2021-2022 (ראה דיון בפגיעויות בשרשראות האספקה מוקדם יותר בפרק זה).

רוסיה: המדינות ומגזרי התעשייה המובילים המסומנים כיעד



למרות ההתמקדות המוגברת בארגונים שבסיסם באוקראינה מאז תחילת 2022, ארגונים שבסיסם בצפון אמריקה ובמערב אירופה המשיכו להיות לקוחות השירות המקוון המובילים שהגורמים הרוסיים סימנו כיעד. הקמפיין של NOBELIUM נגד מגזר ה-IT הפך אותו למגזר המוביל שסומן כיעד בשנה האחרונה.

טקטיקות הסייבר של גורמים מדינתיים רוסיים בזמן המלחמה מאיימות על אוקראינה ומעבר לה

המשך

ניצול אפליקציות הפונות לציבור כדי להשיג גישה ראשונית לרשתות

לפחות מאז סוף 2021, STRONTIUM עבדה כדי לפתח ולשכלל את היכולות שלה לניצול שירותים הפונים לציבור, כגון שרתי Microsoft Exchange, כדי לגנוב מידע. STRONTIUM ניצלה שרתי Exchange שלא תוקנו כדי לגשת לחשבונות ממשלתיים אוקראיניים, כמו גם לארגונים צבאיים ולארגונים הקשורים לתעשייה הביטחונית בארצות הברית, לבנון, פרו ורומניה, ולגופי ממשל אחרים שבסיסם בארמניה, בוסניה, קוסובו ומלזיה. DEV-0586, המזוהה גם היא עם הצבא הרוסי, ניצלה פגיעויות בשרתי Confluence כדי להשיג גישה ראשונית לארגונים ממשלתיים ולארגונים במגזר ה-IT באוקראינה ובמדינות אחרות במזרח אירופה.

המדינה הרוסית וגורמי איום הקשורים אליה משתמשים ברבים מאותם טקטיקות, טכניקות ונהלים (TTPs) כדי לפרוץ לארגונים המעניינים אותם בעתות מלחמה ושלום.

שימוש בחשבונות ופרוטוקולים ניהוליים ובכלי עזר מקוריים לגילוי רשת ולתנועה רוחבית

לאחר שהשיגו גישה ראשונית לרשת, Microsoft הבחינה בגורמים מדינתיים רוסיים הממנפים חשבונות לגיטימיים וכלי תוכנה שמשמשים לביצוע משימות תחזוקה בסיסיות כדי לחמוק מזיהוי למשך זמן רב ככל האפשר. הם הסתמכו על זהויות שנפרצו עם יכולות ניהוליות ופרוטוקולי ניהול תקפים, כלים ושיטות כדי לנוע באופן רוחבי בתוך רשתות מבלי למשוך מיד את תשומת ליבם של ניטורים אוטומטיים ומגיני רשת.

היגיינת סייבר בסיסית ושימוש בכלי זיהוי ותגובה בנקודות קצה יכולים לסייע בצמצום ההשפעה השלילית של פעולות מסוג זה בעתות שלום, כמו גם בעתות מלחמה.

אופיו הבלתי צפוי של העימות המתמשך דורש כי ארגונים ברחבי העולם ינקטו צעדים להקשחת אבטחת הסייבר מפני איומים דיגיטליים הנובעים מגורמי איום מדינתיים רוסיים וגורמי איום המזוהים עם המדינה הרוסית.

תובנות מעשיות

1. יש לצמצם את גניבת האישורים ואת השימוש לרעה בחשבונות על-ידי הגנה על זהויות המשתמשים באמצעות יישום כלים להגנה על זהויות MFA ואכיפת הרשאת גישה מינימלית לאבטחת החשבונות והמערכות הרגישים והמורשים ביותר.
2. יש להחיל עדכונים כדי לוודא שכל המערכות יקבלו את רמת ההגנה הגבוהה ביותר בהקדם האפשרי ויישארו מעודכנות.
3. יש לפרוס פתרונות נגד תוכנות זדוניות, פתרונות לזיהוי נקודות קצה ופתרונות להגנה על זהויות ברחבי הארגון. שילוב של פתרונות אבטחה להגנה בכל רמה עם כוח אדם מיומן ומוכשר, יכול להעצים את הארגון לזיהוי, איתור ומניעה של חדירות המשפיעות על העסק.
4. יש לאפשר חקירות ושחזור במקרה של זיהוי איום על סביבתך או קבלת הודעה על כך על-ידי גיבוי מערכות קריטיות והפעלת רישום. מומלץ מאוד להקים תוכנית תגובה לתקריות.

קישורים למידע נוסף

- הגנה על אוקראינה: לקחים ראשונים ממלחמת הסייבר | Microsoft On the Issues
- המלחמה ההיברידית באוקראינה | Microsoft On the Issues
- פעילות איומי סייבר באוקראינה: ניתוח ומשאבים | מרכז אבטחה ותגובה של Microsoft (MSRC)
- שיבוש מתקפות סייבר המכוונות לאוקראינה | Microsoft On the Issues
- מתקפות תוכנות זדוניות המכוונות לממשלת אוקראינה | Microsoft On the Issues
- MagicWeb: הטריק של NOBELIUM לאחר פריצה כדי לבצע אימות ככל אדם | מרכז המודיעין לגבי איומים של Microsoft (MSTIC), צוות הזיהוי והתגובה (DART), צוות המחקר של Microsoft 365 Defender

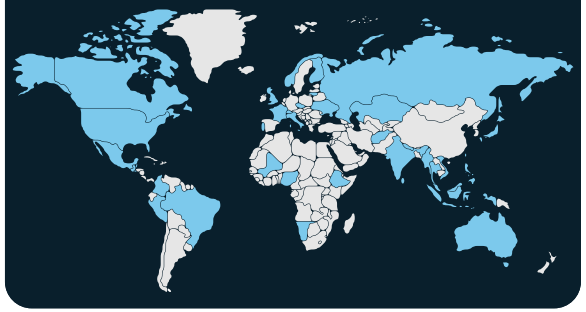
סין מרחיבה את המיקוד הגלובלי להשגת יתרון תחרותי

באקלים הגיאופוליטי המורכב של ימינו, גורמי איום מדינתיים סיניים וגורמי איום המזוהים עם המדינה הסינית המבצעים פעולות סייבר שואפים לעתים קרובות לקדם את המטרות האסטרטגיות של המדינה בתחום הצבא, הכלכלה ויחסי החוץ כחלק ממטרתה של סין להשיג יתרון תחרותי. בשנה האחרונה, Microsoft הבחינה בפעילות איומים סינית נרחבת המכוונת למדינות ברחבי העולם.

מאז אמצע 2021, סין מתמרנת כדי להבטיח יציבות כלכלית ופיננסית על רקע הזינוק החמור ביותר של מגפת הקורונה מזה שנתיים.[13] סין המשיכה ללהטט בעמדתה ביחס לאירועים גיאופוליטיים, כגון המאבק לאזן את שותפותה "הבלתי מוגבלת" עם רוסיה,[14] עם שמירת מעמדה על בימת העולם.[15] בנוסף, עמדתה של סין נגד ארצות הברית ובעלות בריתה בנוגע לטייוואן[16] וים סין הדרומי המשיכה למתוח את יחסי החוץ עם מדינות רבות.[17]

קבוצות איום סיניות מדינתיות וקבוצות איום המזוהות עם המדינה הסינית הגבירו את התמקדותן במדינות קטנות יותר ברחבי העולם עם דגש על דרום מזרח אסיה כדי להשיג יתרון תחרותי בכל החזיתות.

מדינות המותקפות על ידי קבוצות מדינתיות סיניות וקבוצות המזוהות עם המדינה הסינית

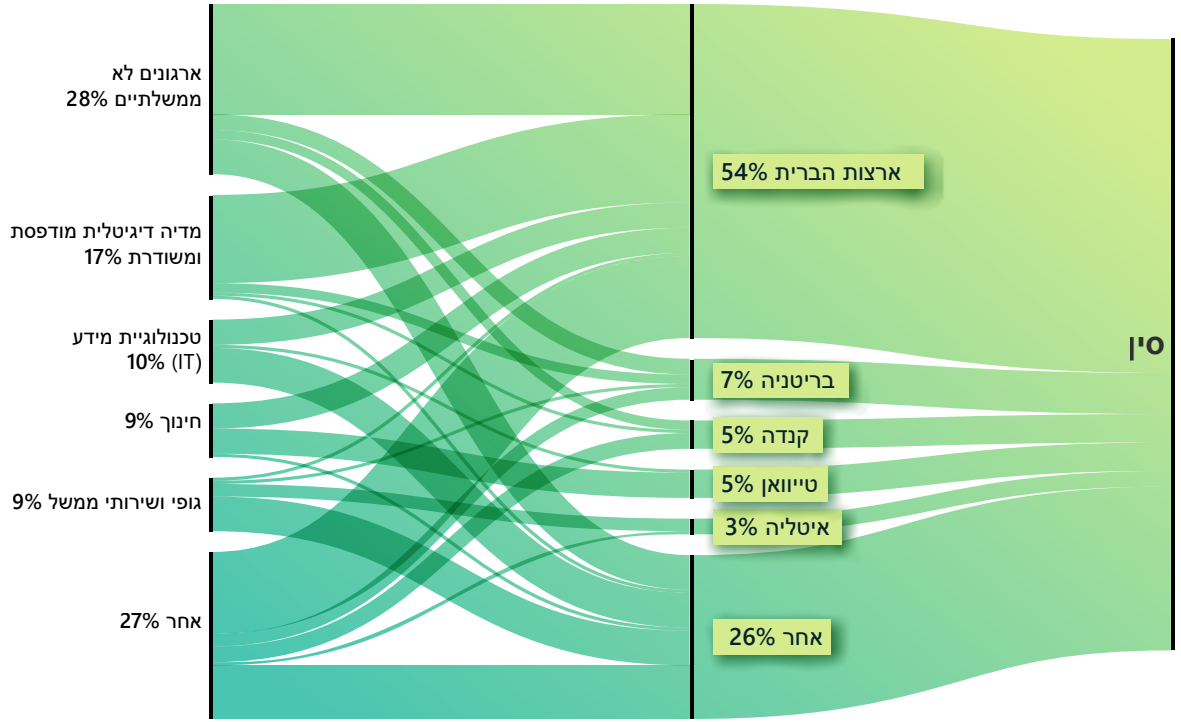


סין גם המשיכה להרחיב את השפעתה הכלכלית ברחבי העולם באמצעות יוזמת החגורה והדרך (BRI) שהוקמה בעבר, בניסיון לעורר לחיים מסגרת השקעות מקיפה עם האיחוד האירופי,[18] ולנהל משא ומתן על הסכם סחר אזורי חדש עם 15 מדינות באזור אסיה והאוקיינוס השקט המכונה "השותפות הכלכלית האזורית המקיפה".[19] להערכתה של Microsoft, סין תמשיך להשתמש באיסוף סייבר ככלי לסיוע בקידום יעדיה האסטרטגיים בתחום הפוליטיקה, הצבא והכלכלה בשל פעולות הסייבר שנצפו והיקף הגופים המותקפים.

מיקוד סייבר עשוי לקדם אינטרסים כלכליים וצבאיים.

Microsoft הבחינה בהתמקדות נרחבת במדינות קטנות יותר ברחבי העולם על ידי קבוצות איום מדינתיות סיניות וקבוצות איום המזוהות עם המדינה הסינית, עובדה המרמזת על כך שסין ככל הנראה משתמשת בריגול סייבר כמרכיב בהשפעתה העולמית בתחומי הכלכלה והצבא.

סין: המדינות ומגזרי התעשייה המובילים המסומנים כיעד



מגזרי צוותי החשיבה/הארגונים הלא ממשלתיים, המדיה, ה-IT, הממשל והחינוך היו בין המגזרים המובילים שסומנו כיעד עבור קבוצות איום המבוססות בסין, ככל הנראה לצורך איסוף וסיור מודיעיני מתמשך.

טווח המטרות כלל, בין היתר, מדינות באפריקה, האיים הקריביים, המזרח התיכון, אוקיאניה ודרום אסיה, עם דגש מיוחד על מדינות אותן שבדרום מזרח אסיה ובאיי האוקיינוס השקט.

בהתאם לאסטרטגיית יוזמת החגורה והדרך (BRI) של סין, קבוצות איום שבסיסן בסין התמקדו בישויות באפגניסטן, קזחסטן, מאוריציוס, נמיביה וטריניד וטובגו.[20] לדוגמה, טרינידד וטובגו הייתה המדינה הקריבית הראשונה שתמכה באסטרטגיית יוזמת החגורה והדרך של סין בשנת 2018, וסין רואה בה שותפה חשובה באזור. NICKEL מבצעת פעולות רשת מתמשכות המכוונת נגד טרינידד וטובגו מאז 2021. לדוגמה, במרץ 2022, NICKEL ביצעה פעילויות סיור נגד סוכנות ממשלתית, ככל הנראה למטרות איסוף מודיעין.

סין מרחיבה את המיקוד הגלובלי להשגת יתרון תחרותי

המשך

בינתיים, Microsoft ראתה קבוצות איום מדינתיות סיניות וקבוצות איום המזוהות עם המדינה הסינית ממקדות את פעולות הרשת שלהן נגד ישויות בדרום מזרח אסיה ומתרחבות למדינות איי האוקיינוס השקט כאשר סין שינתה את סדרי העדיפויות הצבאיים והכלכליים שלה כדי להתמודד עם אתגרי העניין המחודש של ארצות הברית באזור. בינואר 2022, Microsoft ראתה את RADIUM מתמקדת בחברת אנרגיה ובסוכנות ממשלתית הקשורה לאנרגיה בווייטנאם, ובסוכנות ממשלתית אינדונזית. פעילותה של RADIUM תאמה ככל הנראה ליעדיה האסטרטגיים של סין בים סין הדרומי.[21] בסוף פברואר ובתחילת מרץ, GALLIUM פרצה ליותר מ-100 חשבונות הקשורים לארגון בין-ממשלתי בולט (IGO) באזור דרום מזרח אסיה. עיתוי התמקדותה של GALLIUM ב-IGO באזור תאם להודעה על פגישה מתוכננת בין ארצות הברית למנהיגי האזור. על חברי GALLIUM הוטלה ככל הנראה המשימה לעקוב אחר התקשורת ולאסוף מודיעין לפני האירוע.

בעקבות הרחבת השפעתה של סין במדינות איי האוקיינוס השקט, החלה פעילותן של קבוצות האיום הסיניות. באפריל, חתמו סין ואיי שלמה על הסכם ביטחוני שנועד "לקדם שלום וביטחון". פוטנציאלית, ההסכם מאפשר לסין לפרוס משטרה חמושה וכוחות צבאיים באיי שלמה.[22] במאי, אירחה סין את פגישת שרי החוץ השנייה של סין ומדינות האוקיינוס השקט (PICs) בפיג'י והציעה לקדם "שותפות אסטרטגית מקיפה" לקידום אינטרסים פוליטיים, תרבותיים, חברתיים, ביטחוניים והנוגעים לשינויי אקלים וגם למאבק במגפה.[23] בערך באותו זמן במאי, Microsoft זיהתה את התוכנה הזדונית של GADOLINIUM במערכות ממשלתיות של איי שלמה. גם RADIUM הריצה קוד זדוני על מערכות של חברת תקשורת בפפואה גינאה החדשה. אנו מעריכים כי פעילויות אלה ככל הנראה נועדו למטרות איסוף מודיעין כדי לתמוך באסטרטגיה האזורית הכוללת של סין.

Microsoft משבשת את פעולותיה של NICKEL, אך קבוצת האיומים מפגינה את התמדתה.

בדצמבר 2021, היחידה לפשעי מחשב של Microsoft (DCU) הגישה כתבי טענות לבית המשפט המחוזי בארה"ב במחוז המזרחי של וירג'יניה בדרישה לקבל סמכות כדי להשתלט על 42 תחומי שליטה ובקרה (C2) שהיו בשליטת NICKEL. תחומי C2 אלה שימשו לפעולות נגד ממשלות, ישויות דיפלומטיות וארגונים לא ממשלתיים ברחבי מרכז ודרום אמריקה, הקריביים, אירופה וצפון אמריקה מאז ספטמבר 2019.[24] באמצעות פעולות אלה, NICKEL השיגה גישה ארוכת טווח למספר ישויות וחילצה בעקביות נתונים ממספר קורבנות מאז סוף 2019.

ככל שסין תמשיך לכונן יחסים כלכליים דו-צדדיים עם מדינות נוספות – לעתים קרובות במסגרת הסכמים הקשורים ליוזמת החגורה והדרך (BRI) – השפעתה הגלובלית של סין תמשיך לגדול. אנו מעריכים כי גורמי איום מדינתיים סיניים וגורמי איום המזוהים עם המדינה הסינית יסמנו כיעדים את המגזרים הממשלתיים, הדיפלומטיים והלא ממשלתיים שלהם להשגת תובנות חדשות, ככל הנראה במטרה לבצע ריגול כלכלי או למטרות איסוף מודיעין מסורתי. מאז השיבוש שביצעה Microsoft, NICKEL התמקדה בכמה גופי ממשל, ככל הנראה בניסיון להחזיר לעצמה גישה שאבדה. בין סוף מרץ למאי 2022, NICKEL פרצה מחדש לפחות לחמש גופי ממשל ברחבי העולם. עובדה זו מצביעה על כך שלקבוצה היו נקודות כניסה נוספות לישויות אלה או שהיא החזירה לעצמה את הגישה דרך תחומי C2 חדשים. התמדתה של NICKEL לפרוץ שוב ושוב לאותם גופי ממשל ברחבי העולם מצביעה על חשיבות המשימה ברמה גבוהה.

> סין אסרטיבית יותר בעמדתה לגבי מדיניות החוץ. אנו מעריכים כי ריגול כלכלי ואיסוף מודיעין מבוססי סייבר צפויים להימשך.

תובנות מעשיות

1. יש לשפר את הגנת הסייבר לצמצום איומי הסייבר באופן יזום. התמדתם של שחקני האיום הסיניים מחייבת ארגונים לזהות, להגן, לאתר ולהגיב לפריצות אפשריות בזמן.
2. גורמי איום מנצלים לרעה משימות מתוזמנות[25] כשיטה נפוצה של התמדה והתחמקות מהגנה, יש לוודא שהסביבה משתמשת בהנחיות אבטחה נוספות כדי להגן מפני טכניקה נפוצה זו.[26]
3. אנו ממשיכים לראות את השימוש במעטפות אינטרנט כווקטור ראשוני לרשתות המהוות יעד.[27] על ארגונים להקשיח את המערכות שלהם מפני התקפות מעטפות אינטרנט שיכולות לספק לתוקפים גישה להפעלת פקודות מרחוק.[28]

קישורים למידע נוסף

- NICKEL מסמנת כיעד ארגונים ממשלתיים ברחבי אמריקה הלטינית ואירופה | מרכז המודיעין לגבי איומים של Microsoft (MSTIC), יחידת האבטחה הדיגיטלית של Microsoft (DSU)
- הגנה על אנשים מפני מתקפות הסייבר האחרונות | Microsoft On the Issues

איראן הופכת אגרסיבית יותר ויותר בעקבות חילופי השלטון

Microsoft הבחינה בקבוצות מדינתיות איראניות וגורמים המזוהים עמן מגבירים אתקצב מתקפות הסייבר נגד ישראל ומגדילים את היקפן, מרחיבים את מתקפות הכופר מעבר ליריבים אזוריים לקורבנות בארה"ב ובאיחוד האירופי, ומכוונים לתשתיות חיוניות אמריקאיות בעלות פרופיל גבוה לפחות לצורך מיקום מקדים למתקפות סייבר הרסניות פוטנציאליות.

תוקפנות הסייבר הגוברת של הגורמים המדינתיים האיראנים באה בעקבות חילופי השלטון הנשיאותי שלה. בקיץ 2021 החליף הנשיא הרדיקלי אבראהים ראיסי את הנשיא המתון חסן רוחאני. בניגוד חריף לראיסי, בן חסותו של המנהיג העליון ובעל ברית קרוב של משמרות המהפכה האסלאמית (IRGC), נטייתו של הנשיא לשעבר רוחאני לדיפלומטיה העמידה אותו לעתים קרובות בסתירה עם המנהיג העליון והמנהיגים הבכירים של משמרות המהפכה.[29] נראה כי עמדותיו הניציות של ממשל ראיסי הגבירו את נכונותם של גורמים איראניים לפעול ביתר שאת נגד ישראל והמערב, ובמיוחד נגד ארצות-הברית, על אף חידוש המעורבות הדיפלומטית להחייאת הסכם הגרעין עם איראן.

עלייה בקצב ובהיקף מתקפות הסייבר האיראניות נגד ישראל

שבועות ספורים לאחר שראיסי השלים את הקמת צוות מדיניות החוץ שלו,[30] גורמים מדינתיים איראניים חידשו את מתקפות הסייבר ההרסניות נגד ישראל בקצב מהיר יותר מאשר בשנה הקודמת. מתקפות הכופר והפריצה והתקפות הפריצה והדליפה הללו נערכו אחת לכמה שבועות החל מספטמבר והיו מעורבים בהן לפחות שלושה גורמים המזוהים עם איראן, דבר המרמז על כך שייתכן כי ההתקפות היו חלק ממסע נקמה כלל-ארצי נגד ישראל. לפחות במקרה אחד, Microsoft העריכה כי מתקפת כופר נגד ארגון ישראלי בסוף 2021 נועדה להסתיר מתקפת מחיקת נתונים שהתרחשה מתחת לפני השטח. ניתוח התוכנות הזדונית של Microsoft קבע כי תוכנת הכופר שנמסרה לקורבן תוכנתה להפעיל תוכנה זדונית שמבצעת מחיקה לאחר הצפנה.

עד שנת 2022, מתקפות הסייבר האיראניות הסלימו בבחירת המטרות ובסוג התקיפות. בפברואר, DEV-0198 ניסתה לבצע התקפה הרסנית נגד תשתית חיונית ישראלית. Microsoft גם מעריכה כי גורם המזוהה עם איראן היה אחראי ככל הנראה למתקפת סייבר מתוחכמת שהפעילה אזעקות חירום של ירי טילים בישראל בחודש יוני, ככל הנראה באמצעות שימוש בתוכנה שמתאימה שמע ברשתות IP.

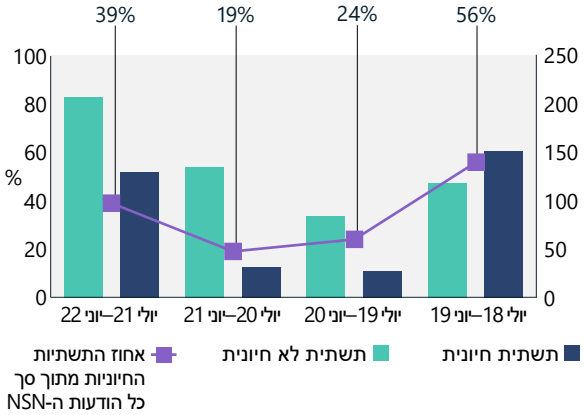
האיום האיראני על תשתיות חיוניות בארה"ב ובישראל גדל לאורך כל השנה

גורמים מדינתיים איראניים שלהערכת Microsoft מזוהים עם משמרות המהפכה האסלאמית (PHOSPHORUS ו-DEV-0198) התמקדו בתשתיות חיוניות אמריקאיות וישראליות בעלות פרופיל גבוה מסוף 2021 ועד אמצע 2022. זאת, ככל הנראה, כדי לספק לטהראן אפשרויות לנקום באותם מגזרים שבכירי משמרות המהפכה האשימו את ארצות הברית וישראל בשיבושם באיראן.[31] אנו מעריכים כי פעילות זו קשורה להתבטאויותיו בסוף אוקטובר 2021, של גנרל משמרות המהפכה, ע'ולאם-רזא ג'לאלי, ראש ארגון ההגנה הפסיבית של איראן, שהדהד האשמות של אישים אחרים בעלי השפעה במשטר, לפיהן ארצות-הברית וישראל ביצעו מתקפות סייבר על נמלים, מסילות רכבת ותחנות תדלוק באיראן.[32] ג'לאלי השמיע את ההאשמה הזו בפעם השנייה בהערות שהוכנו מראש במהלך נאום מבוים של תפילת יום השישי על פודיום עם תמונה של טיל שפוגע במילים "ארה"ב", דבר המרמז על כך שבכירים ממנו החזיקו באותה דעה.[33]

PHOSPHORUS החלה בסריקה נרחבת של ארגונים בארה"ב באוקטובר 2021 בחיפוש אחר פגיעויות Fortinet ו-ProxyShell שלא תוקנו. לאחר שנפרצו, מערכות לא מתוקנות אלה שימשו לביצוע מתקפות כופר, במספר מקרים נגד תשתיות חיוניות בארצות הברית ובמדינות מערביות אחרות. אלה היו המקרים המאושרים הראשונים של מתקפות כופר המזוהות עם המדינה האיראנית מחוץ למזרח התיכון. בעקבות מתקפת הסייבר נגד תחנות התדלוק של איראן בסוף אוקטובר, Microsoft הבחינה בעלייה חדה במתקפות כופר איראניות נגד חברות אמריקאיות, דבר המרמז על קשר אפשרי.

במקביל, PHOSPHORUS עברה להתמקדות מכוונת, לעתים קרובות באמצעות דיוג ממוקד (spear phishing), של חברות תשתיות חיוניות אמריקאיות בעלות פרופיל גבוה, כולל נמלים ושדות תעופה מרכזיים, מערכות תחבורה ציבורית, חברות שירותים ציבוריים וחברות נפט וגז. מיקוד זה, שנערך לעתים קרובות באמצעות דיוג ממוקד (spear phishing), נמשך עד אמצע 2022. היעדים תאמו באופן ישיר למגזרים שארצות הברית וישראל תקפו באיראן לטענת טהראן, וככל הנראה סיפקו לאיראן אפשרויות לפעולות גמול. הפריצה למטרות כמעט זהות מספקת הזדמנות להרתעת התקפות עתידיות מסוג זה, תוך ניסיון להימנע מהסלמה על ידי איתות על סיבת ההתקפות מבלי להודות באשמה.

התעוררות מחודשת של התמקדות איראנית בתשתיות



ההתמקדות האיראנית בתשתיות חיוניות עלתה לרמה הגבוהה ביותר שנראתה מאז סוף 2018 ועד תחילת 2019. השתמשנו בהוראת המדיניות הנשיאותית (PPD-21) של ארה"ב כדי לקבוע אם חברה מתאימה לקריטריונים של תשתיות חיוניות. (יולי 2021–יוני 2022).

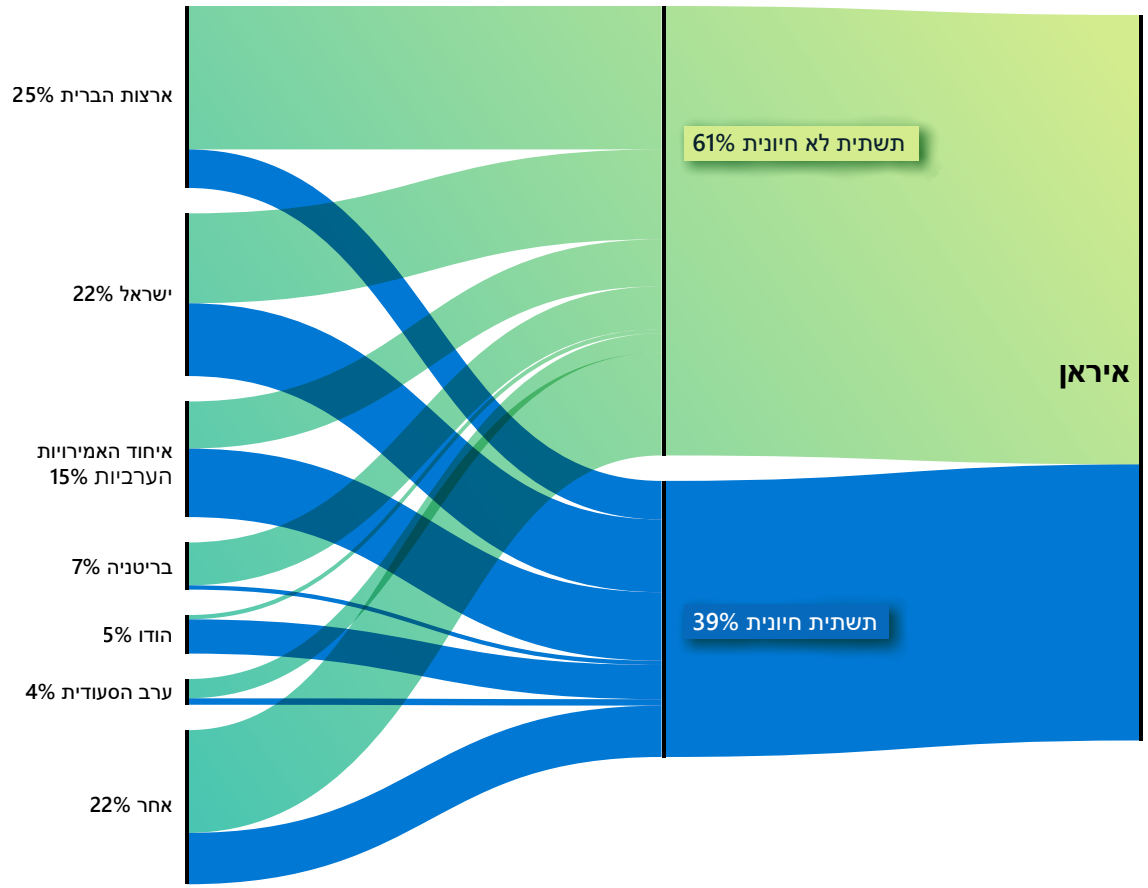
איראן הופכת אגרסיבית יותר ויותר בעקבות חילופי השלטון

המשך

בישראל, DEV-0198 התמקדה ברכבת ישראל, בחברות לוגיסטיקה, בספקי תוכנה של חברות לוגיסטיקה ובחברות דלק בדגש על תחנות דלק. בתחילת 2022 ביצעה הקבוצה מתקפה משבשת על הרשת של חברת לוגיסטיקה ישראלית גדולה, שאילצה את החברה להשבית את המחשבים שלה וחלק מפעילותה כדי לבלום את המתקפה. במקרה אחר, ראינו את הקבוצה מנסה לגשת לרשת של ספק תחבורה ישראלי גדול באמצעות אישורים גנובים או משומשים. בתוך כך, גורם איראני אחר, DEV-0343 – שהתמקדותו בחברות ביטחון, תחבורה ימית וצילומי לוויין מרמזת על קשרים למשמרות המהפכה (IRGC) – פרץ לחשבונות של גורמים ישראליים הקשורים לתחבורה ולנמלים במהלך תחילת 2021.

קבוצות איומים איראניות צפויות להמשיך להוות איום על חברות התחבורה והאנרגיה של ארה"ב וישראל, במיוחד כאשר המאמצים הדיפלומטיים להחיות את הסכם הגרעין האיראני דועכים וושינגטון, תל אביב וטהראן מחפשות אמצעים חלופיים לכפיית ויתורים ולמינופם.

איראן מסמנת תשתיות חיוניות כיעד לפי מדינה



ההתמקדות האיראנית בתשתיות חיוניות התרחשה באופן הבולט ביותר נגד ארגונים ישראליים, אמירתיים ואמריקאיים.

גורמים איראניים צפויים להמשיך להוות איום על חברות התחבורה והאנרגיה של ארה"ב וישראל בשנה הקרובה.

קבוצות איראניות הרחיבו את מתקפות הכופר מעבר ליריבים אזוריים והן מתמקדות ביעדי תשתיות חיוניות בעלי פרופיל גבוה בארה"ב ובישראל.

תובנות מעשיות

1. יש לשפר את היגיינת הסייבר הכוללת של הארגון על-ידי הפעלת פתרונות ללא סיסמה כגון אימות רב-גורמי (MFA) ואכיפת השימוש בהם עבור כל קישוריות מרחוק כדי לצמצם את פוטנציאל קיומם של אישורים שנפרצו.
2. יש להעריך את האותנטיות של כל תעבורת הדואר האלקטרוני הנכנס כדי לוודא שכתובת השולח חוקית.
3. יש לבצע תיקונים מוקדם ולעתים קרובות.[34]
4. יש לסקור ולבדוק כל אחד מקשרי השותפים עם ספקי השירות כדי לצמצם הרשאות בלתי הכרחיות בין הארגון לספקים במעלה הזרם. Microsoft ממליצה להסיר גישה באופן מיידי מכל קשרי השותפים שאינם נראים מוכרים או שטרם נבדקו.[35]

קישורים למידע נוסף

- ההתמקדות האיראנית במגזר ה-IT גוברת | מרכז המודיעין לגבי איומים של Microsoft (MSTIC), יחידת האבטחה הדיגיטלית של Microsoft (DSU)
- DEV-0343 הקשורה לאיראן מתמקדת במגזר הבטחוני, GIS והימי | מרכז המודיעין לגבי איומים של Microsoft (MSTIC), יחידת האבטחה הדיגיטלית של Microsoft (DSU)

קבוצה שבסיסה בלבנון עם קשרים לאיראן המתמקדת בישראל

Microsoft מנטרת פעילויות של איומי סייבר ללא קשר לפלטפורמה, לקורבן המהווה יעד או לאזור הגיאוגרפי. אנו שומרים על נראות וציד איומים פעיל ברחבי העולם כדי לכתוב זיהויים טובים יותר עבור לקוחותינו.

על אף שאיומים מכיוון רוסיה, סין, איראן וצפון קוריאה מייצגים את רוב פעילות הגורמים המדינתיים הנצפית, אנו גם עוקבים אחר איומים מכיוון מדינות החברות בנאט"ו ומדינות דמוקרטיות ומתקשרים לגביהם. בשנה שעברה הצגנו פעילות של גורם שבסיסו בטורקיה (SILICON) וגורם שבסיסו בווייטנאם (BISMUTH). השנה, נרחיב על פרטיה של קבוצה שבסיסה בלבנון שחשפנו בעבר באופן פומבי.[36]

Microsoft חשפה קבוצה שבסיסה בלבנון שלא תועדה בעבר, שאנו מעריכים במידת ביטחון בינונית שהיא פעלה בתיאום עם גורמים המזוהים עם משרד המודיעין והביטחון של איראן (MOIS). שיתוף פעולה או הנחייה מסוג זה מצד טהראן עולים בקנה אחד עם גילויים מסוף 2020, שלפיהם ממשלת איראן משתמשת בצדדים שלישיים לביצוע פעולות סייבר, ככל הנראה כדי לשפר את יכולת ההכחשה הסבירה של איראן.

בפעילות שנצפתה, POLONIUM שמה לה למטרה או פרצה לשני תריסר ארגונים שבסיסם בישראל ולארגון בין ממשלתי (IGO) אחד עם פעילות בלבנון בין פברואר למאי 2022, לפני ש-Microsoft שיבשה את הפעילות וחשפה אותה לציבור. קרוב למחצית מהארגונים הישראליים היו חלק מהתעשייה הביטחונית הישראלית או שהיו להם קשרים עם חברות ביטחוניות ישראליות, עובדה המעידה על כך שלקבוצה יש אינטרסים דומים לאלה של איראן בנוגע לאיסוף מודיעין על ישראל ו/או ישירות נגדה.[37]

הקשרים המוערכים של POLONIUM לקבוצות המשויכות למשרד המודיעין והביטחון של איראן (MOIS) מבוססים על חפיפה בין קורבנות ועל אחידות הכלים והטכניקות שהובחנו.

- חפיפה בין קורבנות: קבוצה מדינתית איראנית הקשורה למשרד המודיעין והביטחון (MOIS) של איראן, ש-Microsoft עוקבת אחריה כ-MERCURY, פרצה בעבר למספר קורבנות של POLONIUM, עובדה המעידה על convergence של דרישות המשימה או על "מסירה" אפשרית של קורבנות בין קבוצות.
- כלים וטכניקות נפוצים: בדומה ל-POLONIUM, מרכז המודיעין לגבי איומים (MSTIC) הבחין ב-DEV-0588 (הידועה גם בשם CopyKittens) משתמשת ב-AirVPN בדרך כלל לפעולות וב-DEV-0133 (הידועה גם בשם Lyceum[38]) משתמשת ב-OneDrive עבור C2 וחילוץ. בדומה לגורמים המדינתיים האיראניים, POLONIUM השתמשה בספק שירותי ענן כדי לפרוץ לחברת תעופה ולמשרד עורכי דין ישראליים.[39]

POLONIUM פרסה סדרה של שתלים מותאמים אישית באמצעות שירותי ענן עבור C2 וחילוץ נתונים – במיוחד OneDrive ו-DropBox. POLONIUM יצרה לעתים קרובות אפליקציות OneDrive ייחודיות עבור יעדים, ככל הנראה כדי להתחמק מזיהוי.

נכון ליוני 2022, Microsoft השעתה מעל 20 אפליקציות OneDrive שנוצרו על-ידי POLONIUM, הודיעה על כך לארגונים המושפעים ופרסה סדרה של עדכוני בינת אבטחה כדי לבודד כלים שפותחו על-ידי POLONIUM.

Microsoft זיהתה והשביתה בהצלחה את השימוש לרעה של POLONIUM ב-OneDrive כ-C2.

תובנות מעשיות

1. יש לעדכן את כלי האנטי-וירוס[40] ולוודא שהגנת הענן[41] מופעלת כדי לזהות את האינדיקטורים הקשורים.
2. עבור לקוחות עם קשרי ספק שירות, יש להקפיד לסקור ולבקר את כל קשרי השותפים כדי לצמצם הרשאות שאינן הכרחיות בין הארגון לספקים במעלה הזרם.[42] יש להסיר באופן מיידי את הגישה מכל קשרי השותפים שאינם נראים מוכרים או שלא נבדקו.

קישורים למידע נוסף

- חשיפת פעילותה ותשתיתה של POLONIUM המתמקדת בארגונים ישראליים | מרכז המודיעין לגבי איומים של Microsoft (MSTIC). יחידת האבטחה הדיגיטלית של Microsoft (DSU)
- MERCURY ממנפת את פגיעויות Log4j 2 במערכות לא מתוקנות לצורך התמקדות בארגונים ישראליים | מרכז המודיעין לגבי איומים של Microsoft (MSTIC), צוות המחקר של Microsoft 365 Defender, מודיעין האיומים של Microsoft Defender

יכולות הסייבר של צפון קוריאה משמשות להשגת שלושת המטרות העיקריות של המשטר

סדרי העדיפויות של צפון קוריאה בתחום הסייבר בשנה האחרונה שיקפו את סדרי העדיפויות הגלובליים המוצהרים של הממשלה. קים ג'ונג-און הדגיש במספר נאומים מרכזיים את שלושת סדרי העדיפויות של בניית יכולת ההגנה, חיזוק הכלכלה הנאבקת של המדינה והבטחת היציבות הפנימית.[43] הפעולות שננקטו על ידי הגורמים המדינתיים של צפון קוריאה מראות בבירור כי הסייבר מנוצל להשגת שלושת מטרות אלו.

גורמים מדינתיים צפון קוריאניים השתמשו במגוון טקטיקות כדי לנסות לחדור לחברות תעופה וחלל ברחבי העולם.

קבוצות האיומים המדינתיות בצפון קוריאה, בעיקר CERIUM ו-ZINC, השתמשו במגוון טקטיקות כדי לנסות לחדור לרשתות של חברות בתחום הביטחון, התעופה והחלל ברחבי העולם. כשצפון קוריאה החלה את תקופת ניסויי הטילים האגרסיבית ביותר שלה אי פעם במחצית הראשונה של 2022, היא השתמשה בריגול סייבר כדי לסייע לחוקרים צפון קוריאנים להשיג יתרון בפיתוח מערכות הגנה מקומיות ואמצעי נגד להתקדמויות שהשיגו יריביה.

ראינו את COPERNICIUM מתמקדת במגוון חברות הקשורות למטבעות קריפטוגרפיים ברחבי העולם, לעתים קרובות בהצלחה, כדי לעזור לתמוך בכלכלה הנאבקת של צפון קוריאה. בעוד שאיננו יכולים לאשר אם הקבוצה הצליחה לחלץ כסף לאחר פריצה, ראינו את COPERNICIUM מדביקה עשרות מכונות על ידי שליחת מסמכים זדוניים המתחזים להצעות מחברות קריפטו אחרות.

לבסוף, קבוצה ש-Microsoft עוקבת אחריה כ-DEV-0215 פעלה כדי לשמור על יציבות ונאמנות בצפון קוריאה על ידי התמקדות בארגוני חדשות המדווחים על נושאים צפון קוריאניים. לכלי תקשורת אלה יש מקורות הן בצפון קוריאה והן בתוך קהילות של עריקים, שפיונגיאנג רואה בהם איום קיומי. בנוסף, הקבוצה פעלה כדי להשיג גישה לרשתות של קבוצות נוצריות דוברות קוריאנית, שנוטות לדבר בגלוי נגד צפון קוריאה ולעבוד באופן פעיל עם עריקים צפון קוריאנים.

התמקדות בחברות בתחום הביטחון, התעופה והחלל

גורמים מדינתיים צפון קוריאניים בראשות CERIUM ו-ZINC משקיעים מאמצים רבים בפיתוח טקטיקות שמטרתן לחדור לחברות בתחום הביטחון, התעופה והחלל. CERIUM בדקה שוב ושוב רשתות וירטואליות פרטיות (VPN) דרום קוריאניות על ידי הורדת לקוחות וחיפוש חולשות. היא גם הורידה אפליקציות נפוצות המשמשות לקוחות צבאיים וממשלתיים בדרום קוריאה, ככל הנראה בחיפוש אחר פגיעויות. הקבוצה עקבה מקרוב אחר אירועים אקטואליים וכתבה מסמכי פיתוי חדשים שהשתמשו בנושאים בעלי פרופיל גבוה כפיתיון כדי לעודד יעדים ללחוץ על קובצי ההפעלה והקישורים של התוכנות הזדוניות שלהם.

הן ZINC והן CERIUM השתמשו במדיה החברתית ובהנדסה חברתית בקמפיינים. ZINC הייתה מיומנת במיוחד ביצירת פרופילים מזויפים ב-LinkedIn ובאתרי מדיה חברתית מקצועיים אחרים, שבהם מפעיליה התחזו למגייסים עבור חברות גדולות בתחום הביטחון, התעופה והחלל. באמצעות פרופילים אלה, הם שלחו קישורים או קבצים מצורפים זדוניים לקורבנות פוטנציאליים על ידי שימוש בהודעות ישירות במדיה החברתית או בדואר אלקטרוני.

בנוסף לעובדי חברות, CERIUM תקפה באופן נרחב גם אנשים בצבא דרום קוריאה, והפגינה עניין מיוחד הן באקדמיות צבאיות דרום קוריאניות והן באנשי צבא העובדים באקדמיה.

התמקדות במטבעות קריפטוגרפיים לצורך איזון הפסדים

מאז הטלת סנקציות האו"ם ב-2016, כלכלת צפון קוריאה המשיכה להתכווץ, ולכך נוספו אסונות טבע כגון שיטפונות[44] ובצורת,[45] כמו גם סגר כמעט מוחלט של גבולות לייבוא מאז תחילת מגפת הקורונה בתחילת 2020.[46] על אף שצפון קוריאה פתחה את גבולותיה לסחר עם סין לזמן קצר בתחילת 2022, הם נסגרו במהרה שוב.[47] באמצע מאי, דיווחה צפון קוריאה על מקרה הקורונה המקומי הראשון.[48] מאז היא יישמה אסטרטגיית "אפס קורונה" בסגנון סין של סגרים המוניים כדי להילחם בנגיף שהשפיע לרעה על הכלכלה השברירית ממילא של צפון קוריאה.

הקבוצה המדינתית הצפון קוריאנית COPERNICIUM ניסתה לקזז חלק מההכנסות האבודות על ידי גניבת כסף – בדרך כלל בצורה של מטבעות קריפטוגרפיים – מכל חברה שהיה ביכולתה לחדור לרשתות שלה. ראינו עשרות מכונות שנפרצו השייכות לחברות הקשורות למטבעות קריפטוגרפיים בארצות הברית, בקנדה, באירופה וברחבי אסיה. COPERNICIUM אפילו פרצה למכונות השייכות לחברות הקשורות למטבעות קריפטוגרפיים בתוך בעלת הברית החזקה ביותר של צפון קוריאה, סין, הן בסין היבשתית והן בהונג קונג. הקבוצה הסתמכה רבות על המדיה החברתית לצורך האיסוף הזדוני המוקדם שלה וגישות ליעדים. גורמים היו בונים פרופילים שמתחזים למפתחים או לבכירים בחברות הקשורות למטבעות קריפטוגרפיים. לאחר מכן הם היו יוצרים קשרים עם גורמים בתעשייה, ושולחים קישורים או קבצים זדוניים לאחר שהם בנו קרבה.

יכולות הסייבר של צפון קוריאה משמשות להשגת שלושת המטרות העיקריות של המשטר

המשך

קבוצה הקשורה ל-PLUTONIUM מפתחת ופורסת תוכנות כופר

קבוצה של גורמים שמקורם בצפון קוריאה ש-Microsoft עוקבת אחריהם כ-DEV-0530 החלה לפתח ולהשתמש בתוכנות כופר בהתקפות ביוני 2021. קבוצה זו, שכינתה את עצמה H0lyGh0st, השתמשה במטען כופר עם אותו שם עבור הקמפיינים שלה והצליחה לפרוץ לעסקים קטנים במספר מדינות כבר בספטמבר 2021.

Microsoft העריכה כי היו ל-DEV-0530 קשרים עם קבוצה אחרת שבסיסה בצפון קוריאה שמתבצע אחריה מעקב כ- PLUTONIUM (הידועה גם בשם DarkSeoul או Andariel). בעוד שהשימוש בתוכנת הכופר H0lyGh0st בקמפיינים הוא ייחודי ל-DEV-0530, מרכז המודיעין לגבי איומים של Microsoft (MSTIC) הבחין בתקשורת בין שתי הקבוצות, כמו גם בכך ש-DEV-0530 השתמשה בכלים שנוצרו באופן בלעדי על ידי PLUTONIUM.

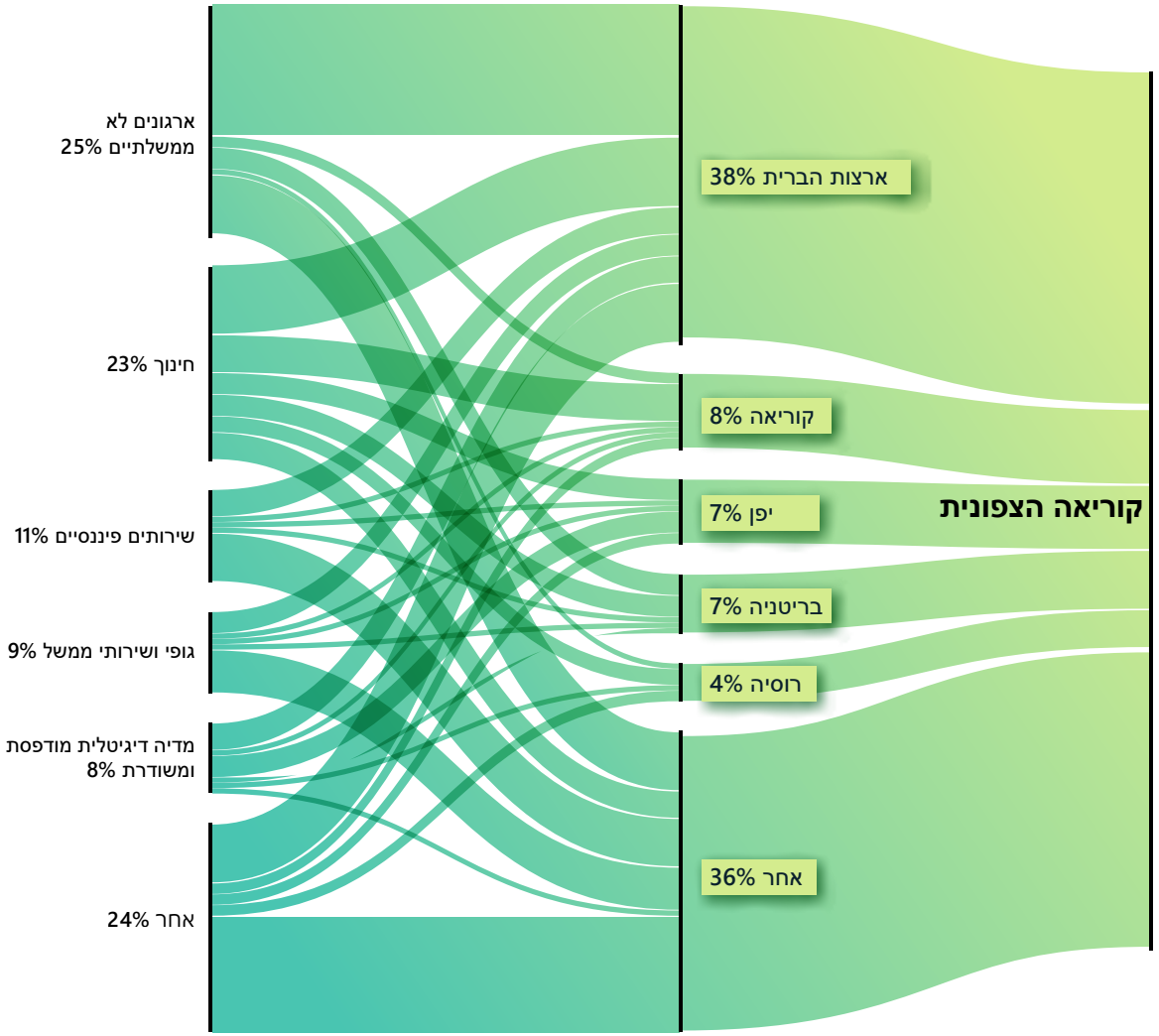
אין זה בטוח שהפעילות של DEV-0530 הייתה בחסות ממשלתית. על אף שהממשלה יכלה להזמין מתקפות כופר מאותה סיבה שהיא נותנת חסות לגניבות מחברות קריפטו, ייתכן גם שהגורמים העומדים מאחורי DEV-0530 פעלו באופן עצמאי כדי להרוויח כסף עבור עצמם. אם היו אלה האקרים צפון קוריאניים הפועלים באופן עצמאי, זה היה מסביר מדוע הפעילות לא הייתה נרחבת בהשוואה לפעולות גניבה בחסות ממשלתית נגד חברות קריפטו.

התמקדות בכלי תקשורת, בעריקים, בקבוצות דתיות ובארגוני סיוע צפון קוריאניים

בשנה האחרונה, המנהיג העליון קים ג'ונג-און התמקד יותר בביטחון הפנים ובנאמנות באופן פומבי מאשר בטילים ובנשק גרעיני. כביטוי לעיסוק זה בסוגיות פנים, לפחות שתי קבוצות מדינתיות צפון קוריאניות התמקדו בהיבטים שהמשטר היה רואה כאיומים פנימיים.

הראשון היה קבוצה ש-Microsoft עוקבת אחריה כ-DEV-0215, שמתמקדת בארגוני תקשורת שעוקבים מקרוב אחר החדשות הצפון קוריאניות. אחת הסיבות האפשריות להתמקדות זו היא שכלי התקשורת הללו משיגים את החדשות שלהם מעריקים צפון קוריאניים, מאזרחים סינים שעובדים בשיתוף פעולה הדוק עם צפון קוריאה, ואפילו מכמה אזרחים צפון קוריאניים הממוקמים בתוך המדינה, המשתמשים במגוון שיטות כדי לתקשר עם העולם החיצוני. ממשלת צפון קוריאה רואה בקבוצות אלה איום קיומי על הישרדותה, במיוחד באזרחים בתוך צפון קוריאה שנתפסים כבוגדים וכמרגלים. סביר להניח ש-DEV-0215 חתרה לזהות את המקורות של כלי התקשורת הללו כדי שתוכל לנטרל דליפות מידע פוטנציאליות.

צפון קוריאה: המדינות והמגזרים המובילים המסומנים כיעדים



צפון קוריאה רואה בארצות הברית, בדרום קוריאה וביפן את אויבותיה העיקריות. בעוד שרוסיה היא בעלת ברית ותיקה, גורמי האיום הצפון קוריאניים מתמקדים בצוותי חשיבה, אקדמאים ופקידים דיפלומטיים רוסיים כדי להשיג מודיעין על השקפות ונושאים גלובליים רוסיים.

יכולות הסייבר של צפון קוריאה משמשות להשגת שלושת המטרות העיקריות של המשטר

המשך

Microsoft גם ראתה עדות לכך ש-DEV-0215 שמה לה למטרה קהילות נוצריות דוברות קוריאנית. כנסיות קוריאניות נוצריות אוונגליסטיות נוטות להיות ביקורתיות כלפי ממשלות צפון ודרום קוריאה גם יחד המעדיפות מעורבות עם צפון קוריאה. כנסיות אלה עשויות להגיש סיוע לעריקים, וחלקן עוסקות בעבודה הומניטרית עם צפון קוריאה. צפון קוריאה רואה בהם איום משום שבעוד שזרם העריקים המגיעים מצפון קוריאה כמעט התייבש במהלך המגפה,[49] קבוצות נוצריות אלה ממלאות לעתים קרובות תפקיד קריטי בסיוע לעריקים להימלט. DEV-0215 יצרה מסמכים מזויפים על כנסים נוצריים לדוברי קוריאנית כפיתיונות כדי להתמקד בקבוצה ולגלות מי עוזר לארגן עריקות.

לבסוף, הקבוצה המדינתית OSMIUM גילתה עניין עקבי בארגוני סיוע בינלאומיים לאורך כל השנה, כולל ארגונים שסייעו לצפון קוריאה בעבר. בעוד שצפון קוריאה נמנעה בדרך כלל מהצעות לעזרה מחוץ למדינה, במיוחד מאז התפרצות מגפת הקורונה,[50] ייתכן שצפון קוריאה שוקלת לקבל הצעות עזרה, אך נזהרת מההשלכות הביטחוניות של מתן אפשרות לעובדי סיוע זרים להיכנס למדינה. ייתכן שצפון קוריאה חודרת לרשתות של ארגוני סיוע ברחבי העולם כדי להחליט אם לאפשר לסיוע כזה להיכנס לארצם.

תובנות מעשיות

1. הגורמים המדינתיים הצפון קוריאניים הם מיומנים, בלתי נלאים ויצירתיים, אך ארגונים יכולים להתגונן מפניהם.
2. את רוב ההתקפות המוצלחות ניתן לעצור באמצעות היגיינת סייבר בסיסית, כגון אימות דו-שלבי או אי פתיחת קבצים מצורפים מאנשים לא מוכרים בסביבה וירטואלית.

קישורים למידע נוסף

- גורם האיום הצפון קוריאני מתמקד בעסקים קטנים ובינוניים באמצעות תוכנת הכופר H0lyGh0st | מרכז המודיעין לגבי איומים של Microsoft (MSTIC), יחידת האבטחה הדיגיטלית של Microsoft (DSU)

בקרב מומחים לצפון קוריאה, יש כבר זמן רב ויכוח בשאלה האם ממשלת צפון קוריאה רצינית בהצהרותיה הפומביות או שהיא עושה הצגות בשביל הרושם. ההתאמה בין מתקפות הסייבר לסדרי העדיפויות המוצהרים של צפון קוריאה מאמתת את האמונה שצפון קוריאה מתכוונת למה שהיא אומרת כשהיא מדברת בפומבי על מטרותיה.

שכירי חרב בסייבר מאיימים על יציבות מרחב הסייבר

יש תעשייה הולכת וגדלה של חברות פרטיות שמפתחות ומוכרות כלים, טכניקות ושירותים שמאפשרים ללקוחות שלהן – לעתים קרובות ממשלות – לפרוץ לרשתות, מחשבים, טלפונים ומכשירים המחוברים לאינטרנט. גופים אלה, שהן נכס עבור גורמים מדינתיים, מסכנים לעתים קרובות מתנגדי משטר, מגיני זכויות אדם, עיתונאים, פעילי חברה אזרחית ואזרחים פרטיים אחרים. אנו מתייחסים אליהם כאל שכירי חרב בסייבר או גורמים התקפיים במגזר הפרטי.

עולם שבו חברות מהמגזר הפרטי יוצרות ומוכרות נשק סייבר מסוכן יותר לצרכנים, לעסקים בכל הגדלים ולממשלות. ניתן להשתמש בכלים פוגעניים אלה בדרכים שאינן עולות בקנה אחד עם הנורמות והערכים של מנהל תקין ודמוקרטיה. Microsoft מאמינה שההגנה על זכויות האדם היא חובה בסיסית, ואנו מתייחסים אליה ברצינות על-ידי צמצום "המעקב כשירות" ברחבי העולם.

Microsoft העריכה כי גורמים מדינתיים מסוימים במשטרים דמוקרטיים ואוטוריטריים מבצעים מיקור חוץ של הפיתוח או השימוש בטכנולוגיית "מעקב כשירות". כך הם נמנעים ממתן דין וחשבון ומפיקוח, כמו גם רוכשים יכולות שיהיה קשה לפתח באופן מקומי.

> נשקי סייבר אלה מספקים למדינות יכולות מעקב שהן לא היו יכולות לפתח בכוחות עצמן.

השוק שבו פועלים שכירי חרב בסייבר הוא אטום. עם זאת, אנו ממשיכים לראות את קבוצות אלה משתמשות בנקודות תורפה מסוג אפס-ימים ואפילו בנקודות תורפה מסוג אפס קליק שאינן דורשות אינטראקציה עם הקורבן כלל, ומאפשרות מעקב כשירות.

Microsoft הכריזה לאחרונה על גורם התקפי מהמגזר הפרטי האירופי שאנו מכנים KNOTWEED, PSOA שבסיסו באוסטריה בשם DSIRF. דיווחי חדשות רבים קישרו את החברה לפיתוח וניסיון המכירה של ערכת כלים של תוכנות זדוניות בשם Subzero.[51] הקורבנות כוללים משרדי עורכי דין, בנקים ויועצים אסטרטגיים במדינות כמו אוסטריה, בריטניה ופנמה.[52]

מכיוון שיכולות מעקב התקפיות אלה אינן עוד יכולות מסווגות ביותר שנוצרו על ידי סוכנויות ביטחון ומודיעין, אלא מוצרים מסחריים המוצעים כיום לחברות וליחידים, כל משטר רגולטורי לנשקי סייבר צריך להתקדם מעבר לפיקוח על הייצוא. ההשפעה של נשקי הסייבר הללו יכולה להיות הרסנית.

כאשר שכיר חרב בסייבר מנצל פגיעות במוצר או בשירות, הוא מסכן את כל המערכת האקולוגית של המחשוב. כאשר פגיעויות מזוהות באופן פומבי, חברות נמצאות במרוץ נגד הזמן כדי לשחרר הגנות לפני שיתרחשו מתקפות נרחבות (ראה את הדיון הקודם שלנו על ניצול פגיעויות לרעה). זהו מעגל מסוכן וקשה הן עבור ספקי התוכנה (אשר חייבים לפתח במהירות תיקונים) והן עבור צרכני המוצרים (אשר חייבים ליישם את התיקונים באופן מיידי).

כחברה מייסדת בהסכם הטכנולוגי לאבטחת סייבר (Cybersecurity Tech Accord)[53] – ברית מובילה המאגדת יותר מ-150 חברות טכנולוגיה – Microsoft התחייבה שלא לעסוק בפעולות התקפיות באינטרנט. אנו עומדים במחויבות זו ובמחויבויותינו בתחום זה בנושא זכויות האדם. עסקנו בשיבושים טכניים ובאתגרים משפטיים כדי להדגיש את ההשפעות השליליות הנגרמות על ידי השירותים הניתנים על ידי שכירי חרב בסייבר ונמשיך להגן על לקוחותינו כאשר נראה שימוש לרעה.

> שכירי חרב בסייבר יוצרים ומספקים יכולות "מעקב כשירות", מתוחכמות טכנולוגית וזמינות באופן נרחב, כוללות תוכנות זדוניות מתקדמות ומגוון טכניקות.

תובנות מעשיות עבור ממשלות

1. יש ליישם דרישות שקיפות ופיקוח למעקב כשירות, במיוחד בתחום הרכש, כולל החרמת גורמים פוגעניים אלה, כפי שעשתה ארה"ב עם משרד המסחר המפרט חברות ברשימת הישויות.
2. יש לקבוע הגבלות לאחר העסקה לעובדים לשעבר במגזר זה.
3. יש לשאוף ליישם את מחויבויות "הכר את הלקוח שלך" ולעודד חברות לקיים את התחייבויותיהן בתחום זכויות האדם.

קישורים למידע נוסף

- התרת קשרים עם KNOTWEED: גורם התקפי מהמגזר הפרטי האירופי המשתמש בנקודות תורפה מסוג 0 ימים | מרכז המודיעין לגבי איומים של Microsoft (MSTIC), מרכז התגובה לאבטחה של Microsoft (MSRC), RiskIQ (בינת איומים של Microsoft Defender)
- המשך המאבק בנשק סייבר במגזר הפרטי | Microsoft On the Issues

הפעלת נורמות אבטחת סייבר לשלום וביטחון במרחב הסייבר

אנו זקוקים באופן דחוף למסגרת גלובלית עקבית הנותנת עדיפות לזכויות אדם ומגינה על אנשים מפני התנהגות מדינתית חסרת אחריות ברשת. בשום מקום זה לא מודגם בצורה ברורה יותר מאשר במלחמה המתמשכת באוקראינה. בנוסף למאמץ אסטרטגי גלובלי, ממשלות יכולות לפעול כעת כדי שתהיה להן השפעה חיובית מיידית.

לפני חמש שנים, Microsoft קראה ליצירת "אמנת ג'נבה דיגיטלית" כדי לקדם תחומי אחריות והתחייבויות חוצי מגזרים להגנה על השלום והביטחון באינטרנט. מרחב הסייבר התגלה כתחום מובחן ונפיץ של עימות ותחרות בין מדינות, כאשר ההתקפות הופכות נפוצות יותר ויותר, גם בעתות שלום.

כיום, עדיין יש צורך ברור במסגרת כזו – עדות לכך היא מתקפות הסייבר הרוסיות נגד אוקראינה כחלק מהפלישה של רוסיה. מלחמה זו יצרה קו חזית חדש השונה באופן דרמטי מכל מה שהכרנו בעבר.

הבאת יציבות למרחב הסייבר תדרוש חיזוק ותכנון מחדש של מוסדות פיקוח גלובליים כדי להתאימם למטרה. מרחב הסייבר שונה מהותית מתחומים אחרים – הוא חסר גבולות, סינתטי ומתוחזק בעיקר על ידי התעשייה הפרטית. משמעות הדבר היא לבקש מתעשיית הטכנולוגיה לקחת אחריות גדולה יותר הן על אבטחת המוצרים והשירותים והן על המערכת האקולוגית הדיגיטלית הרחבה יותר. בעוד שאמנם חלה התקדמות ניכרת בכל החזיתות, האתגרים גדלו באופן דרמטי.

עלינו להכפיל את המאמצים הקולקטיביים להגנה על ביטחון מרחב הסייבר. איננו יכולים לקחת כמובנות מאליהן את הזכויות והחירויות שלמדנו לצפות להן באינטרנט. בזמן שאנו נאבקים להתמודד עם האתגרים, גורמים זדוניים מתכננים איך והיכן להכות בפעם הבאה באמצעות בינה מלאכותית (AI), ממנפים דיסאינפורמציה ומוצאים דרכים לערער את ה-metaverse המתהווה. מגיני זכויות האדם, תעשיית הטכנולוגיה וממשלות המכבדות זכויות חייבים לעבוד יחד למען חזון חיובי של עולם מקוון בטוח ומאובטח. הדרך לפנינו עוד ארוכה, אך יש דברים שממשלות יכולות לעשות כעת כדי לשפר באופן מיידי את המערכת האקולוגית של אבטחת הסייבר:

- לצטט נורמות, חוקים והשלכות בייחוסים. אחד השיפורים המשמעותיים בחמש השנים האחרונות היה המהירות והתיאום של ייחוסים ממשלתיים למתקפות סייבר. מעבר להזכרת השמות והשיימינג, הצהרות אלה צריכות להדגיש אילו חוקים או נורמות בינלאומיים הופרו ובאיזה אופן יוטלו ההשלכות כדי לסייע בחיזוק ההכרה בציפיות הבינלאומיות.
- יש להבהיר את פרשנות המשפט הבינלאומי באינטרנט. בעוד שממשלות מסכימות ביניהן שהמשפט הבינלאומי חל באינטרנט, עדיין נותרו שאלות לגבי האופן שבו הוא חל במקרים ספציפיים. עניין זה רלוונטי במיוחד לאחר הפלישה לאוקראינה. ממשלות יכולות לתרום רבות לקביעת ציפיות, הימנעות מאי-הבנות ובניית אמון על-ידי ציון האופן שבו הן מבינות את מחויבויותיהן על-פי המשפט הבינלאומי.
- יש להתייעץ עם בעלי עניין אחרים. בעוד שפורומים בינלאומיים ממשיכים לגלות את הדרכים הטובות ביותר להקל על הכללה חזקה של בעלי מניות מרובים, ממשלות יכולות לתמוך בדיאלוג מושכל על ידי התייעצות עם קהילות של בעלי מניות מרובים, במיוחד עם תעשיית הטכנולוגיה, כדי לוודא את קבלת יתרונות הדיאלוג מאנשים בעלי מומחיות חיונית.
- יש להקים גוף קבוע שיתמוך בהתנהגות אחראית של מדינות במרחב הסייבר. עבודתם של פורומים דיפלומטיים בינלאומיים לקידום התנהגות מדינתית אחראית באינטרנט מעולם לא הייתה חשובה יותר. יש צורך ברור במנגנון קבוע של האו"ם שיעסוק במרחב הסייבר כתחום של עימות.
- יש להגדיר נורמות חדשות לאיומים מתפתחים. איומי מרחב הסייבר מתפתחים ללא הרף לצד חידושים טכנולוגיים. בעוד שנורמות בינלאומיות צריכות להיות ניטרליות מבחינה טכנולוגית, יהיה צורך לעדכן אותן ולהפחיתן בהתבסס על שינויים בנוף האיומים והאופן שבו אנו משתמשים בטכנולוגיה. גם כיום אנו רואים ניצול לרעה של פערים במסגרת הבינלאומית הקיימת. מדינות צריכות להתחייב להגן במפורש על תהליכי הליבה העומדים בבסיס המערכת האקולוגית הדיגיטלית שאינם מוגנים כעת, כמו תהליך עדכון התוכנה. יתרה מכך, תחומים ספציפיים ראויים להגנות נוספות. לדוגמה, כפי שלמדנו על רקע המגפה, נורמות להגנה על שירותי הבריאות הן חיוניות.

גורמים והתקפות מדינתיים הולכים וגדלים בנפחם ובתחכומם, ויוצרים מצב בלתי אפשרי.

פעולה מיידית היא הכרחית – יש דברים שממשלות יכולות לעשות עכשיו כדי לשפר באופן מיידי את המערכת האקולוגית של אבטחת הסייבר, כולל יישום נורמות וכללים מוסכמים להתנהגות מדינתית במרחב הסייבר ועבודה עם הקהילה הרחבה יותר של בעלי עניין מרובים כדי לטפל בפערים המתעוררים.

יש לתכנן מחדש מוסדות רב-צדדיים כדי להתמודד עם האתגר הדחוף של מתקפות סייבר מדינתיות.

קישורים למידע נוסף

- רגע של חשבון נפש: הצורך בתגובה לאבטחת סייבר חזקה וגלובלית | Microsoft On the Issues
- מתקפות סייבר המכוונות נגד שירותי בריאות חייבות להיפסק | Microsoft On the Issues
- הפרק הבא של דיפלומטיית הסייבר באו"ם מבשר | Microsoft On the Issues

הערות סיום

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. תשתיות חיוניות בפרק זה מוגדרות על ידי הוראת המדיניות הנשיאותית 21 (PPD-21), ביטחון ועמידות של תשתיות חיוניות (פברואר 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

הערות סיום – המשך

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. בפרט, תיקון שרתי Exchange עבור פגיעויות ProxyShell (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, ו- CVE-2021-27065, CVE-2021-34473). כמו כן, יש להקפיד לתקן מכשירי Fortinet עבור פגיעויות FortiOS SSL VPN.
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. כפי שצוין בבלוג הטכני שלנו, זיהוי מטרות במדינה אינו אומר בהכרח שלקוח DSIRF מתגורר באותה מדינה, שכן התמקדות בינלאומית היא נפוצה.
53. דף הבית | Cybersecurity Tech Accord (cybertechaccord.org)

מכשירים ותשתיות

עם האצת הטרנספורמציה הדיגיטלית, אבטחת התשתית הדיגיטלית חשובה יותר מתמיד.

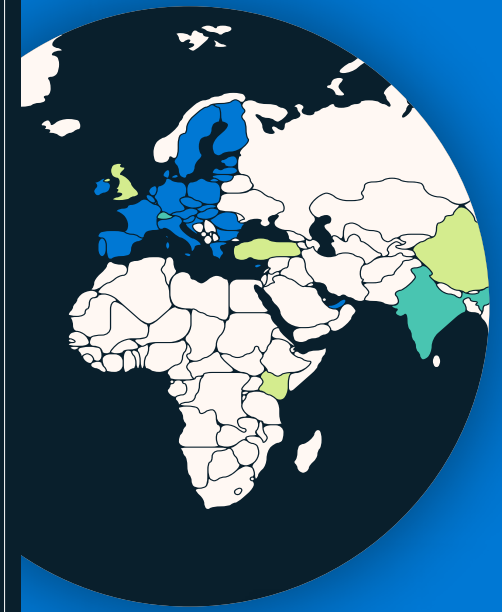
סקירה כללית על

מכשירים ותשתית

המגפה, בשילוב עם אימוץ מהיר של מכשירים הפונים לאינטרנט מכל הסוגים כמרכיב בהאצת הטרנספורמציה הדיגיטלית, הגדילו מאוד את שטח התקיפה של העולם הדיגיטלי.

פושעי סייבר ומדינות מנצלים זאת במהירות. בעוד שאבטחת החומרה והתוכנה של ה-IT התחזקה בשנים האחרונות, האבטחה של מכשירי האינטרנט של הדברים (IoT) ומכשירי טכנולוגיה תפעולית (OT) לא עמדה בקצב. גורמי איום מנצלים מכשירים אלה כדי ליצור גישה לרשתות ולאפשר תנועה רוחבית, לבסס דריסת רגל בשרשרת אספקה או לשבש את פעילות ה-OT של ארגון היעד.

ממשלות ברחבי העולם עוברות להגן על תשתיות חיוניות על ידי שיפור אבטחת IoT ו-OT.

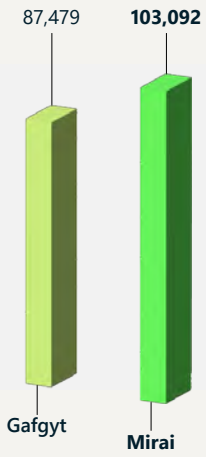


מידע נוסף בעמוד 59

יש צורך במדיניות אבטחה עקבית והניתנת לפעולה הדדית גלובלית כדי להבטיח אימוץ נרחב.

מידע נוסף בעמוד 59

תוכנות זדוניות כשירות עברו לפעולות בקנה מידה גדול נגד IoT ו-OT חשופים בתשתיות ושירותים, כמו גם ברשתות ארגוניות.



מידע נוסף בעמוד 63

מתקפות נגד מכשירי ניהול מרחוק נמצאות במגמת עלייה, עם יותר מ-100 מיליון מתקפות שנצפו במאי 2022 – עלייה של פי חמישה בשנה האחרונה.

מידע נוסף בעמוד 62

התוקפים מנצלים יותר ויותר פגיעויות בקושחת מכשירי IoT כדי לחדור לרשתות ארגוניות ולבצע התקפות הרסניות.

מידע נוסף בעמוד 65

32% מתמונות הקושחה שנותחו הכילו לפחות 10 פגיעויות קריטיות ידועות.

מידע נוסף בעמוד 66

מבוא

האצת הטרנספורמציה הדיגיטלית הגבירה את סיכון אבטחת הסייבר לתשתיות חיוניות ולמערכות סייבר-פיזיות.

בשנים האחרונות חל שינוי חסר תקדים בעולם הדיגיטלי. ארגונים מתפתחים כדי לרתום את ההתקדמות ביכולת המחשוב הן מהענן החכם והן מהקצה החכם. כתוצאה מהמגפה שאילצה גופים לבצע דיגיטציה כדי לשרוד והקצב שבו תעשיות ברחבי העולם מאמצות מכשירים הפונים לאינטרנט, משטח התקיפה של העולם הדיגיטלי גדל באופן אקספוננציאלי.

מעבר מהיר זה מתקדם מהר יותר מכפי יכולתה של קהילת האבטחה לעמוד בקצב. במהלך השנה האחרונה, ראינו איומים המנצלים מכשירים בכל חלקי הארגון, החל מציוד IT מסורתי ועד בקרי טכנולוגיה תפעולית (OT) או חיישני אינטרנט של הדברים (IoT) פשוטים. על אף שאבטחת ציוד ה-IT התחזקה בשנים האחרונות, אבטחת מכשירי IoT ו-OT לא עמדה בקצב. גורמי איום מנצלים מכשירים אלה כדי ליצור גישה לרשתות ולאפשר תנועה רוחבית או כדי לשבש את פעילות ה-OT של הארגון. ראינו התקפות על רשתות חשמל, התקפות כופר המשבשות את פעולות ה-OT, נתבי IoT הממונפים ליכולת התמדה מוגברת, והתקפות המתמקדות בפגיעויות קושחה.

בעוד שהשכיחות של פגיעויות IoT ו-OT מהווה אתגר עבור כל הארגונים, תשתיות חיוניות נמצאות בסיכון מוגבר מכיוון שגורמי איום למדו שהשבתת שירותים חיוניים היא מנוף רב עוצמה. מתקפת הכופר על חברת Colonial Pipeline ב-2021 המחישה כיצד פושעים יכולים לשבש שירות קריטי כדי להגדיל את הסבירות לתשלום כופר. ומתקפות הסייבר של רוסיה נגד אוקראינה מוכיחות כי מדינות מסוימות רואות במתקפות סייבר נגד תשתיות חיוניות אמצעי חבלה מקובל להשגת מטרותיהן הצבאיות.

עם זאת, יש תקווה באופק. קובעי מדיניות ומגיני רשת פועלים לשיפור אבטחת הסייבר של תשתיות חיוניות, כולל מכשירי IoT ו-OT שעליהם הן מסתמכות. קובעי המדיניות מאיצים את פיתוחם של חוקים ותקנות כדי לבנות את אמון הציבור באבטחת הסייבר של תשתיות ומכשירים חיוניים.

Microsoft משתפת פעולה עם ממשלות ברחבי העולם כדי לנצל הזדמנות זו כדי לשפר את אבטחת הסייבר, ואנו מקדמים בברכה מעורבות נוספת. עם זאת, אנו מודאגים מכך שלדרישות לא עקביות, מותאמות אישית או מורכבות עלולות להיות השפעות לא מכוונות, בכללן הפחתת האבטחה במקרים מסוימים על-ידי הסטת משאבי אבטחה הנמצאים במחסור לעבר תאימות להסמכות כפולות מרובות.

מנקודת מבט של תפעול אבטחה, למגיני הרשת יש גישות שונות לשיפור מערך אבטחת ה-IoT/OT בארגון שלהם. גישה אחת היא ליישם ניטור רציף של מכשירי IoT ו-OT. גישה נוספת היא "לקחת ולהעביר" (shift-left) – כלומר לדרוש וליישם שיטות עבודה טובות יותר לאבטחת סייבר עבור מכשירי ה-IoT וה-OT עצמם. גישה שלישית היא ליישם פתרון ניטור אבטחה המתפרס הן על רשתות IT והן על רשתות OT. לגישה הוליסטית זו יש יתרון משמעותי נוסף של תרומה לתהליכים ארגוניים קריטיים, כגון "שבירת ההפרדה" בין OT ל- IT, אשר בתורו מאפשר לארגון להגיע למערך אבטחה משופר תוך עמידה ביעדים העסקיים.

מיכל ברוורמן-בלומנסטיק
סגנית נשיא, סמנכ"לית טכנולוגיה, אבטחת ענן ובינה מלאכותית

ממשלות הפועלות לשיפור האבטחה והעמידות של תשתיות חיוניות

ממשלות ברחבי העולם מפתחות ומקדמות מדיניות לניהול סיכוני אבטחת סייבר לתשתיות חיוניות. רבות גם מחוקקות מדיניות לשיפור אבטחת מכשירי IoT ו-OT. הגל העולמי הגובר של יוזמות מדיניות יוצר הזדמנות נהדרת לשיפור אבטחת הסייבר, אך גם מציב אתגרים בפני בעלי עניין ברחבי המערכת האקולוגית.

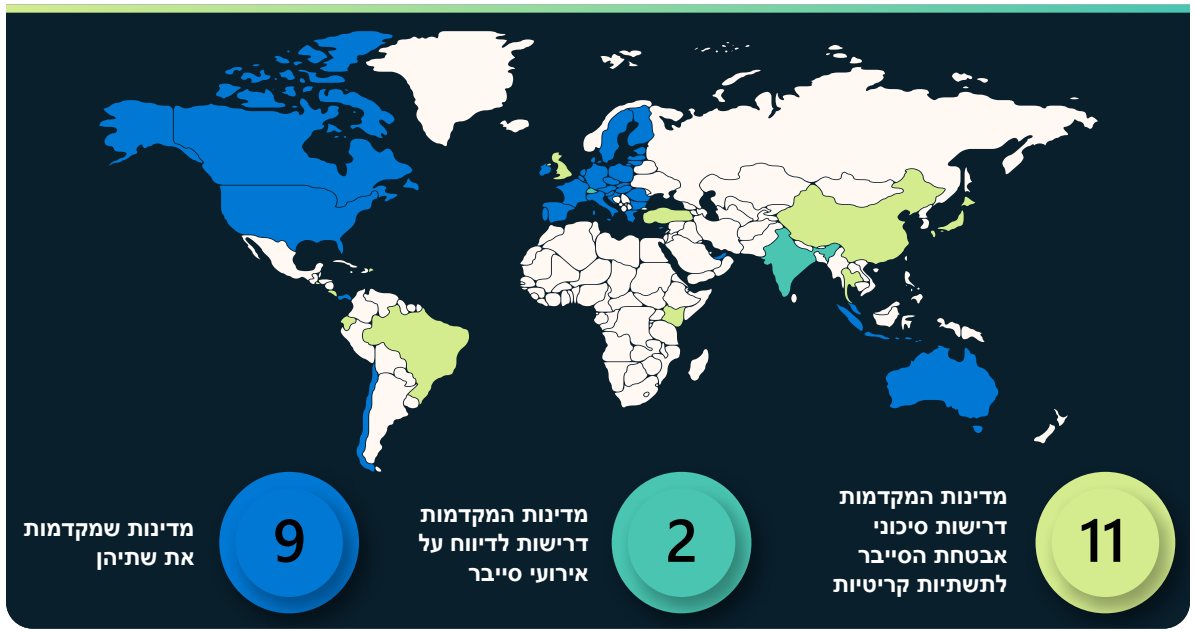
פיתוח חזון הוליסטי לניהול סיכוני סייבר בתשתיות חיוניות הוא הכרחי, אך מורכב, במיוחד לאור מידת החיבור ההדדי הקיים בין טכנולוגיות וספקים גלובליים, מגוון השימושים הטכנולוגיים והסיכונים הנלווים, והצורך להשקיע באסטרטגיות לטווח הקצר והארוך כאחד. מדיניות בהיקף יעיל המניעה למידה איטרטיבית ושיפורים, ותומכת ביכולת פעולה הדדית גלובלית חוצת מגזרים, יכולה לסייע בניהול המורכבות ולאפשר טרנספורמציה דיגיטלית בעלת מודעות אבטחה רבה יותר. עם זאת, גישה מקוטעת לחקיקה עלולה להוביל לדרישות רגולטוריות חופפות ולא עקביות. זה עלול להשפיע על המשאבים ובסופו של דבר לפגוע ביעדי האבטחה. לדוגמה, ארגונים יכולים להסיט משאבים מחדשנות ואבטחה לתרגילי תאימות פורמליסטיים.

Microsoft שואפת לשתף פעולה עם ממשלות ברחבי העולם לקידום מדיניות אבטחת סייבר יעילה של תשתיות חיוניות, להגברת הבנת האתגרים וההזדמנויות ולתמיכה במאמצים לשיפור רמת הסיכון הקולקטיבית.

התפתחויות במדיניות ניהול הסיכונים לאבטחת סייבר בתשתיות חיוניות

במהלך השנה האחרונה, תחומי שיפוט רבים, כולל אוסטרליה, צ'ילה, האיחוד האירופי (EU), יפן, סינגפור, בריטניה (UK) וארצות הברית, פיתחו, עדכנו או יישמו דרישות אבטחת סייבר חוצות מגזרים או במגזרים ספציפיים.[1] רבות מממשלות אלו – ואחרות כגון הודו[2] ושווייץ[3] – כבר פרסמו או מפתחות דרישות לדיווח על אירועי אבטחת סייבר עבור תשתיות חיוניות וספקי שירותים חיוניים.[4]

כמה התפתחויות מדיניות ראויות לציון התרחשו באוסטרליה, באיחוד האירופי, באינדונזיה ובארצות הברית במהלך השנה האחרונה. אוסטרליה חוקקה שני חוקים שיעזרו לה לנהל סיכוני אבטחת סייבר חוצי מגזרים לתשתיות חיוניות. החוקים, בין היתר, מגדירים מגזרי תשתיות חיוניות חדשים, מחייבים פיתוח תוכניות לניהול סיכונים, מחייבים דיווח על אירועי אבטחת סייבר ומסמיכים את הממשלה להתערב אם היא קובעת שמפעיל תשתית חיונית אינו מוכן או אינו מסוגל להגיב כראוי לאירוע.



האיחוד האירופי פעל לעדכון הדירקטיבה בנושא אבטחת מערכות מידע ורשת (NIS) שלו משנת 2016, המספקת מסגרת למדינות החברות באיחוד האירופי לוויסות שירותים ומוצרים טכנולוגיים הנחשבים קריטיים לכלכלותיהן ולתפקוד החברה. דירקטיבת NIS 2 המוצעת כוללת תיקונים שייצרו קטגוריה חדשה של תשתיות דיגיטליות קריטיות, יגדילו את הדרישות לדיווח על אירועי סייבר ויטילו דרישות נוספות לניהול סיכוני אבטחת סייבר. האיחוד האירופי גם פיתח עדכון מוצע לחוק החוסן התפעולי הדיגיטלי שלו (DORA), היוצר דרישות חדשות לטכנולוגיות תקשורת מידע המשמשות במגזר השירותים הפיננסיים.

במאי, פרסמה אינדונזיה תקנה נשיאותית להגנה על תשתיות מידע חיוניות ("IIV"), שתיכנס לתוקף במאי 2024 ותכסה בין היתר מגזרים כגון אנרגיה, תחבורה, פיננסים ובריאות. המטרה של אינדונזיה בתקנה זו היא להגן על המשכיות היישום של IIV, למנוע מתקפות סייבר ולהגביר את המוכנות לטיפול באירועי סייבר. ספקי IIV יהיו אחראים על ביצוע הגנה מאובטחת ואמינה, יישום ניהול סיכוני סייבר יעיל ודיווח על תוצאות סיכוני סייבר לגופי הממשל המתאימים. התקנה כוללת דרישה לדיווח על אירועי סייבר תוך 24 שעות.

ממשלות הפועלות לשיפור האבטחה והעמידות של תשתיות חיוניות

המשך

הקונגרס האמריקאי העביר חוק שהסמיך את הסוכנות לאבטחת סייבר ואבטחת תשתיות (CISA) להוציא תקנות שיחייבו מפעילי תשתיות חיוניות לדווח על אירועי סייבר, ומנהל אבטחת התחבורה האמריקאי (TSA) פרסם דרישות אבטחת סייבר חדשות ספציפיות למגזר בתחום התחבורה. בשנת 2021, TSA הוציאה שתי הנחיות אבטחה למפעילי צינורות נוזלים מסוכנים וגז טבעי בתגובה למתקפת הכופר על חברת Colonial Pipeline:

- ההנחיה הראשונה דרשה מהמפעילים למנות מתאם אבטחת סייבר, לדווח על אירועי סייבר תוך 12 שעות ולבצע הערכת פגיעות במערכות שלהם.
- ההנחיה השנייה, ש-TSA תיקנה ב-2022, חייבה אותם ליישם אמצעי הפחתה ספציפיים להגנה מפני מתקפות כופר ואיומים ידועים אחרים על מערכות IT ו-OT, לפתח וליישם תוכנית מגירה ותגובה לאבטחת סייבר תוך 30 יום, ולעבור סקירה שנתית של תכנון ארכיטקטורת אבטחת סייבר.

בהתבסס על תקנותיה בנוגע לצינורות, TSA הוציאה שתי הנחיות אבטחה נוספות בהמשך 2021 שקבעו דרישות אבטחת סייבר לרכבות משא, חברות רכבות נוסעים או מערכות תחבורה מסילתית. ההנחיות דרשו מהמפעילים הרלוונטיים למנות מתאם אבטחת סייבר, לדווח על אירועי אבטחת סייבר תוך 24 שעות, לפתח וליישם תוכנית תגובה לאירועי אבטחת סייבר ולהשלים הערכת פגיעות באבטחת סייבר. TSA הודיעה במקביל כי עדכנה גם את תוכניות אבטחת התעופה שלה כך שיחייבו את מפעילי שדות התעופה וחברות התעופה ליישם את שתי ההוראות הראשונות, להקצאת מתאם ולדיווח על אירועים תוך 24 שעות.

התפתחויות מדיניות באבטחת מכשירי IoT ו-OT

בעשרות מדינות, ממשלות פעילות בפיתוח דרישות לקידום אבטחת הסייבר של מוצרים ושירותים של טכנולוגיית המידע והתקשורת (ICT), כולל מכשירי IoT ו-OT. בהקשרם של מוצרי ושירותי ICT, החששות הגדולים ביותר הם אבטחת שרשרת אספקת תוכנה ואבטחת IoT.

- הנציבות האירופית הציעה את חוק חוסן הסייבר, שיקבע דרישות אבטחת סייבר לתוכנות עצמאיות ולמכשירים מחוברים ושירותים נלווים.[5] שיטות עבודה רלוונטיות עבור ספקי תוכנה כוללות מינוף מחזור חיים מאובטח של פיתוח תוכנה[6] ומתן 'עץ מוצר של תוכנה' (SBOM).[7] דרישות אבטחה חדשות יחולו על מכשירים מחוברים ועל כל היצרנים תוטל משימה לנהל תהליכי גילוי פגיעויות מתואמים[8] עבור מוצרים שהופצו.

קובעי המדיניות גם מיקדו את תשומת לבם בהתפשטות המתמשכת של מכשירי IoT ומכשירי OT המחוברים לרשת.

- בבריטניה, טיוטת הצעת החוק לאבטחת מוצרים ותשתיות טלקומוניקציה תחייב יצרנים של מוצרי צריכה הניתנים לחיבור, כגון טלוויזיות חכמות, להפסיק להשתמש בסיסמאות ברירת מחדל המהוות מטרה קלה לפושעי סייבר, לקבוע מדיניות גילוי פגיעויות (כגון דרך לקבל הודעה על ליקויי אבטחה), ולספק שקיפות לגבי משך הזמן המינימלי שבמהלכו הם יספקו עדכוני אבטחה.[9]
- באיחוד האירופי, תקנים או דרישות אבטחה חדשים מיושמים באמצעות כלי חקיקה מרובים, כולל חקיקת משנה להנחיית ציוד הרדיו החלה על מכשירים אלחוטיים ושואפת לשפר את עמידות הרשת, להגן על פרטיות הצרכנים ולהפחית את הסיכון להונאה כספית.[10] בנוסף, ייתכן שיידרש שימוש בתוכנית הסמכת ענן,[11] הנמצאת כעת בפיתוח כתוצאה מחוק אבטחת הסייבר של האיחוד האירופי משנת 2019.[12]

הצורך בעקביות

במקרים רבים, טווח הפעילות בין אזורים, מגזרים, טכנולוגיות ותחומי ניהול סיכונים תפעוליים מתבצע בו-זמנית, וכתוצאה מכך נוצרת חפיפה פוטנציאלית או חוסר עקביות בהיקף, בדרישות ובמורכבות עבור ארגונים המבקשים למנף הדרכה או להפגין תאימות. ללא הגדרה מקובלת אוניברסלית של IoT, ההיקף מאתגר במיוחד עבור תקנות מכשירי IoT ו-OT. הדוגמאות לעיל עשויות לחול על "מוצרים מחוברים ושירותים נלווים", "מוצרי צריכה הניתנים לחיבור" ו"מכשירים אלחוטיים". במקביל, ממשלות רבות שואפות ליישם משטרי הערכה חזקים יותר כדי להבין טוב יותר האם וכיצד ארגונים ומוצרים עומדים בדרישות הנוכחיות, החדשות והמתפתחות. ככל שהמגמות הללו יתמזגו, המורכבות תגדל. באופן מעודד, שאלות שהוצגו במהלך הייעוץ לחוק חוסן הסייבר של האיחוד האירופי בחנו כיצד רגולציה חדשה יכולה לתקשר באופן פוטנציאלי עם רגולציה קיימת של אבטחת סייבר, דבר המצביע על כוונה להימנע מדרישות אבטחת סייבר סותרות.

גישות איטרטיביות מבוססות סיכון ומוכוונות תוצאות או תהליכים (לעומת ספציפיות ליישום) יכולות לטפח אבטחת סייבר משופרת ושיפור מתמשך. באופן דומה, התמקדות בהפעלת יכולת פעולה הדדית בין מגזרים, אזורים ותחומי מדיניות עשויה להגביר באופן עקבי את אבטחת הסייבר בשרשראות אספקה גלובליות המחוברות ביניהן.

ממשלות הפועלות לשיפור האבטחה והעמידות של תשתיות חיוניות

המשך

יש מדיניות אבטחת סייבר מורכבת יותר ויותר של תשתיות חיוניות הנמצאת בפיתוח על פני אזורים, מגזרים ותחומי נושאים. פעילות זו מביאה איתה הזדמנויות גדולות ואתגרים משמעותיים. האופן שבו ממשלות ימשיכו הלאה יהיה חיוני לעתיד הטרנספורמציה הדיגיטלית ולאבטחת המערכת האקולוגית כולה.

האצת ההשקעות בכל המערכת האקולוגית באבטחת שרשרת אספקת התוכנה ובארכיטקטורת 'אפס אמון'

הצו הנשיאותי של ארה"ב (EO) 14028 בנושא שיפור אבטחת הסייבר היווה זרז להאצת היוזמות המתמשכות של Microsoft להשקיע באבטחת שרשרת האספקה שלנו ושל המערכת האקולוגית כולה ולאפשר ללקוחותינו לעמוד ביעדי 'אפס אמון'.

מזה זמן רב אנו מאמינים כי שיפור שרשרת אספקת התוכנה דורש שיתוף של למידה ושיטות עבודה מומלצות, החל מההפצה לציבור של 'מחזור החיים של פיתוח האבטחה של Microsoft' לפני כ-15 שנה.

בנוסף, אנו משתפים פעולה באופן הדוק עם 'מרכז המצוינות הלאומי לאבטחת סייבר' כדי להדגים גישות לארכיטקטורת 'אפס אמון' המיושמת הן בטכנולוגיה מקומית והן בטכנולוגיית ענן ומבססים יכולות מוצר חדשות, כולל היכולת לאכוף אימות עמיד בפני דיוג עבור סביבות היברידיות ומרובות עננים.

כיום, אנו הולכים מעבר לדרישות ה-EO כדי להפגין תאימות לדרישות האבטחה של שרשרת אספקת התוכנה ולספק מידע על 'עץ מוצר של תוכנה' (SBOM) בשתי דרכים:

1. ראשית, אנו משתפים גרסת קוד פתוח של מחולל ה-SBOM שלנו, שבנינו כך שישתלב בקלות עם ערוצי CI/CD התומכים בגרסאות Build בפלטפורמות Windows, Linux, Mac, iOS ו-Android.[13]
2. שנית, אנו תורמים לפיתוח תקני תעשייה לשלמות, שקיפות ואמון בשרשרת האספקה (SCITT). זה יאפשר החלפה אוטומטית של מידע שרשרת אספקה הניתן לאימות, כולל ממצאים המוכיחים תאימות לדרישות כגון אלה הנובעות מהנחיית שרשרת אספקת התוכנה של ה-EO.

תובנות מעשיות

1. יש לתכנן מחדש מוסדות רב-צדדיים כדי להתמודד עם האתגר הדחוף של מתקפות סייבר מדינתיות.
2. יש לפתח מדיניות אבטחת סייבר עקבית וניתנת לפעולה הדדית בין אזורים, מגזרים ותחומי נושאים.

קישורים למידע נוסף

- השקעות מתמשכות באבטחת שרשרת האספקה לתמיכה בצו הנשיאותי לאבטחת סייבר | Microsoft Tech Community
- ממשלת ארה"ב מגדירה אסטרטגיה ודרישות של ארכיטקטורת 'אפס אמון' | הבלוג של Microsoft Security
- צו נשיאותי בנושא סייבר | Microsoft Federal
- שלמות, שקיפות ואמון שרשרת האספקה | github.com
- יישום ארכיטקטורת 'אפס אמון' | NCCoE (nist.gov)

IoT ו-OT נחשפים: מגמות והתקפות

העולם הדיגיטלי המחובר יותר ויותר פירושו שמכשירים עוברים במהירות לאינטרנט, מתקשרים עם מערכות גדולות יותר, אוספים נתונים ויוצרים נראות על פני מרחבים שהוסתרו בעבר. מצב זה מביא עמו הזדמנויות לארגונים ולגורמי איום כאחד, כאשר עסקי פשעי הסייבר הופכים הן לתעשייה של מיליארדי דולרים והן לסיכון.

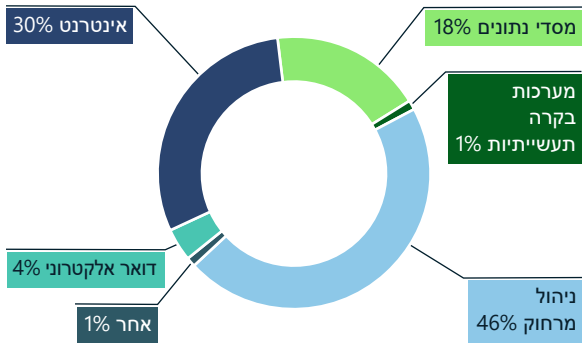
מכשירי IoT – כולל כל דבר, החל ממדפסות וכלה במצלמות אינטרנט, מכשירי בקרת אקלים ובקרות גישה לבניינים – מהווים סיכוני אבטחה ייחודיים לאנשים, ארגונים ורשתות. על אף שהם קריטיים לפעילותם של ארגונים רבים, הם עלולים להפוך במהירות לנטל ולסיכון אבטחה. האימוץ המהיר של פתרונות IoT כמעט בכל תעשייה הגדיל את מספר וקטורי התקיפה ואת סיכון החשיפה של ארגונים.

תוכנות זדוניות כשירות עברו לפעולות בקנה מידה גדול נגד תשתיות ושירותים אזרחיים (כולל בתי חולים, נפט וגז, רשתות חשמל, שירותי תחבורה ותשתיות חיוניות אחרות) כמו גם רשתות ארגוניות. גורמי איום נדרשים להשקיע מאמצי מחקר משמעותיים כדי לחשוף ולנצל את התצורה של סביבות הפעלה ומכשירי IoT ו-OT מוטמעים.

מכשירי IoT מהווים סיכוני אבטחה ייחודיים כנקודות כניסה וציר ברשת. מיליוני מכשירי IoT חשופים או אינם מתוקנים.

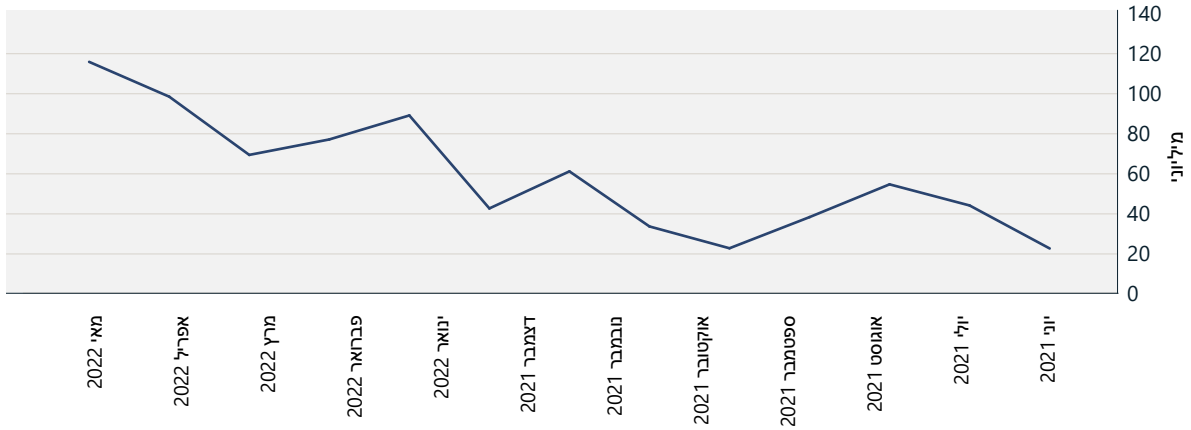
ניתן לגלות מכשירים חשופים באמצעות כלי חיפוש באינטרנט על ידי זיהוי שירותים המאזינים ביציאות רשת פתוחות. יציאות אלה משמשות בדרך כלל לניהול מרחוק של מכשירים. אם אינו מאובטח כראוי, מכשיר IoT חשוף יכול לשמש כנקודת ציר לשכבה אחרת של הרשת הארגונית מכיוון שמשתמשים לא מורשים יכולים לגשת מרחוק ליציאות. ראינו מגוון של גורמי איום המנסים לנצל פגיעויות במכשירים חשופים לאינטרנט, החל ממצלמות, דרך נתבים וכלה בתרמוסטטים. עם זאת, למרות הסיכון, מיליוני מכשירים נותרים ללא תיקון או חשופים.

סיכום סוגי ההתקפות על IoT/OT



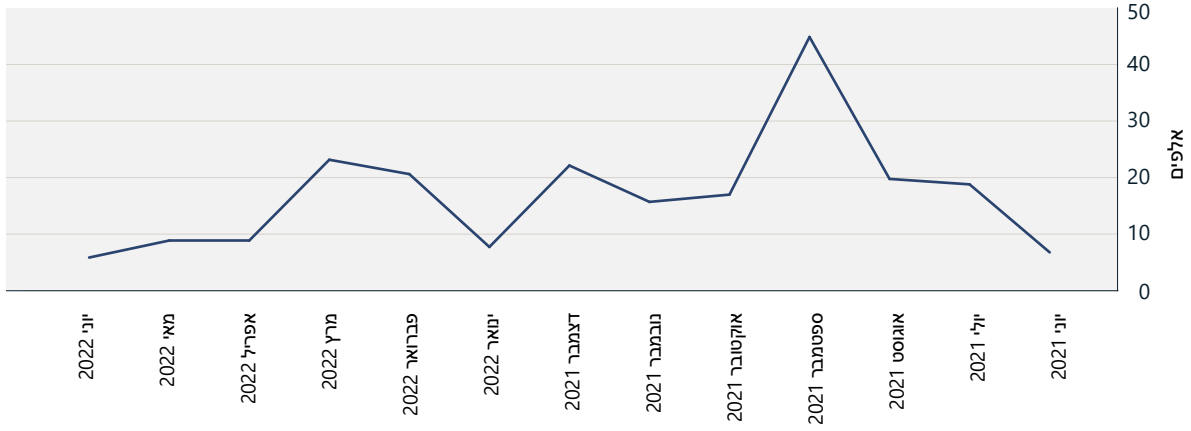
סוגי התקפות שנצפו דרך רשת חיישני MSTIC. הנפוצות ביותר היו התקפות נגד מכשירי ניהול מרחוק, התקפות דרך האינטרנט והתקפות על מסדי נתונים (מסוג brute force או נקודות תורפה).

התקפות נגד מכשירי ניהול מרחוק



התקפות הולכות וגוברות על יציאות ניהול מרחוק לאורך זמן, כפי שניתן לראות דרך רשת חיישני MSTIC.

התקפות אינטרנט נגד IoT ו-OT



נפח התקפות אינטרנט לאורך זמן, כפי שניתן לראות דרך רשת חיישני MSTIC. ככל שמספר המכשירים המחוברים ישירות לאינטרנט ממשיך לרדת, הסבירות שהתוקפים יחפשו אותם עשויה בסופו של דבר לפחות.

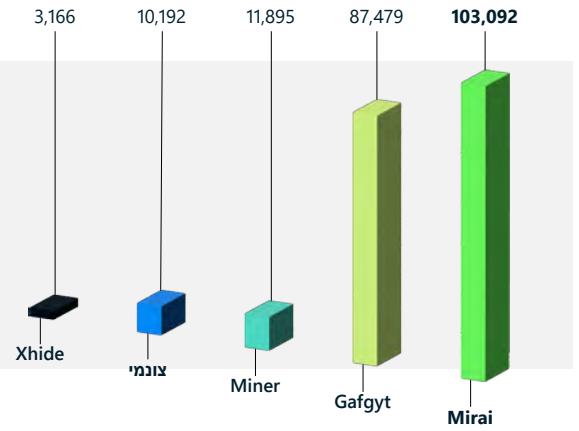
IoT ו-OT נחשפים: מגמות והתקפות

המשך

כלי שירות מחודש של תוכנות זדוניות

ככל שקבוצות פשעי סייבר התפתחו, כך התפתחו גם פריסת התוכנות הזדוניות ובחירת היעדים שלהם. בשנה האחרונה, ראינו התקפות נגד פרוטוקולי IoT נפוצים – כגון Telnet – פוחתות באופן משמעותי, במקרים מסוימים בשיעור של עד 60 אחוז. במקביל, קבוצות פשעי סייבר וגורמים מדינתיים שינו את ייעודם של רשתות ה-botnets. ההתמדה של תוכנות זדוניות, כגון Mirai, מדגישה את המודולריות של התקפות אלה ואת יכולת ההסתגלות של איומים קיימים.

התוכנות הזדוניות המובילות ל-IoT שזוהו בחוץ



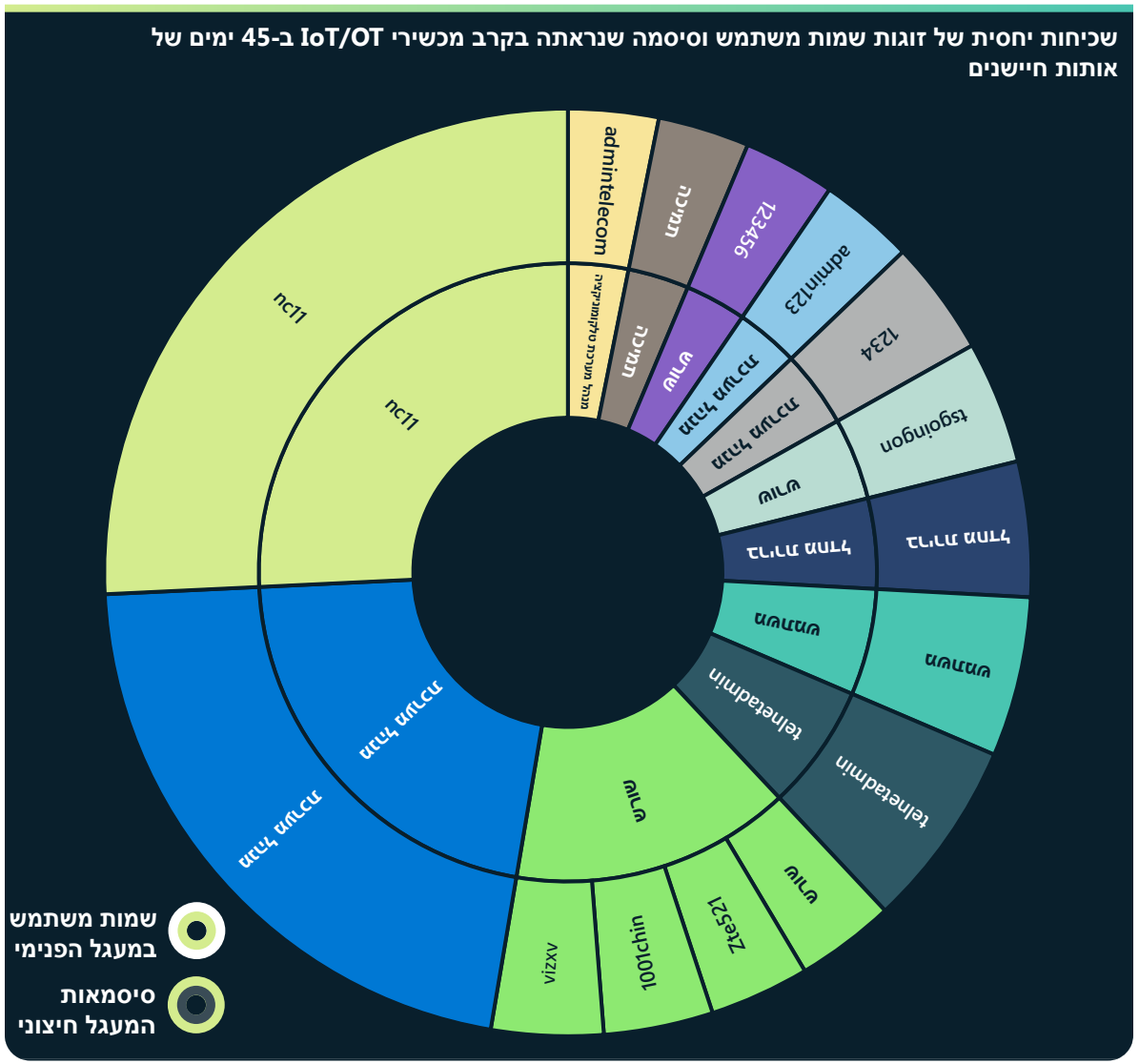
Mirai התפתחה כדי להדביק מגוון רחב של מכשירי IoT כולל מצלמות פרוטוקול אינטרנט, מקליטי וידאו דיגיטליים של מצלמות אבטחה ונתבים. וקטור התקיפה עקף בקרות אבטחה מדור קודם ומהווה סיכון לנקודות קצה ברשת על-ידי ניצול פגיעויות נוספות ותנועה רוחבית. Mirai עוצבה מחדש מספר פעמים, כאשר הגרסאות מסתגלות לארכיטקטורות שונות ומנצלות הן פגיעויות ידועות והן פגיעויות אפס-ימים כדי לפרוץ וקטורי תקיפה חדשים.

השימוש ב-Mirai גדל בקרב ארכיטקטורות CPU 32 ו-64 סיביות x86 במהלך השנה האחרונה, והתוכנה הזדונית קיבלה יכולות חדשות שאומצו במהירות על ידי קבוצות מדינתיות וקבוצות פשע. התקפות של מדינות ממנפות כעת גרסאות חדשות של רשתות botnet קיימות בהתקפות מסוג 'מניעת שירות מבוזרת' (DDoS) על יריבים זרים.

ככל שההכנסות מהתקפות נגד מכשירי IoT ירדו ב-2022, ראינו כמה קבוצות של גורמי איום מנצלות לרעה פגיעויות – כגון Log4j ו-Spring4Shell – כדי לספק מטען זדוני למכשירים כגון שרתים, להדביק אותם ולגייס אותם לרשתות botnet גדולות שמבצעות מתקפות DDoS. לכלי השירות המחודש של תוכנות זדוניות שנועד להתמקד במכשירי IoT פגיעים יש השלכות חמורות הן על ארגונים והן על מדינות, מכיוון שתנועה רוחבית עלולה לחשוף דלתות אחוריות למטענים נוספים ולמכשירים אחרים ברשתות.

> פרוטוקולים רבים של מערכות בקרה תעשייתיות אינם מפוקחים ולכן פגיעים להתקפות ספציפיות ל-OT. משמעות הדבר עלולה להיות סיכון מוגבר לתשתיות חיוניות.

שכיחות יחסית של זוגות שמות משתמש וסיסמה שנראתה בקרב מכשירי IoT/OT ב-45 ימים של אותות חיישנים



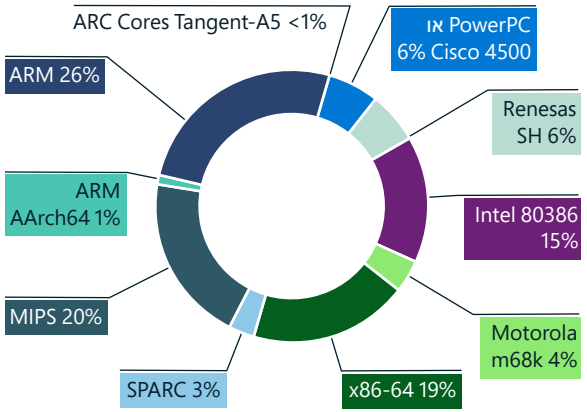
שימוש בזוגות נפוצים של שמות משתמש וסיסמה מגביר את הסיכון לפריצה. בהתבסס על גודל מדגם של מעל 39 מיליון מכשירי IoT ו-OT, אלה המשתמשים בשמות משתמש וסיסמאות זהים מייצגים כ-20 אחוזים.

IoT ו-OT נחשפים: מגמות והתקפות

המשך

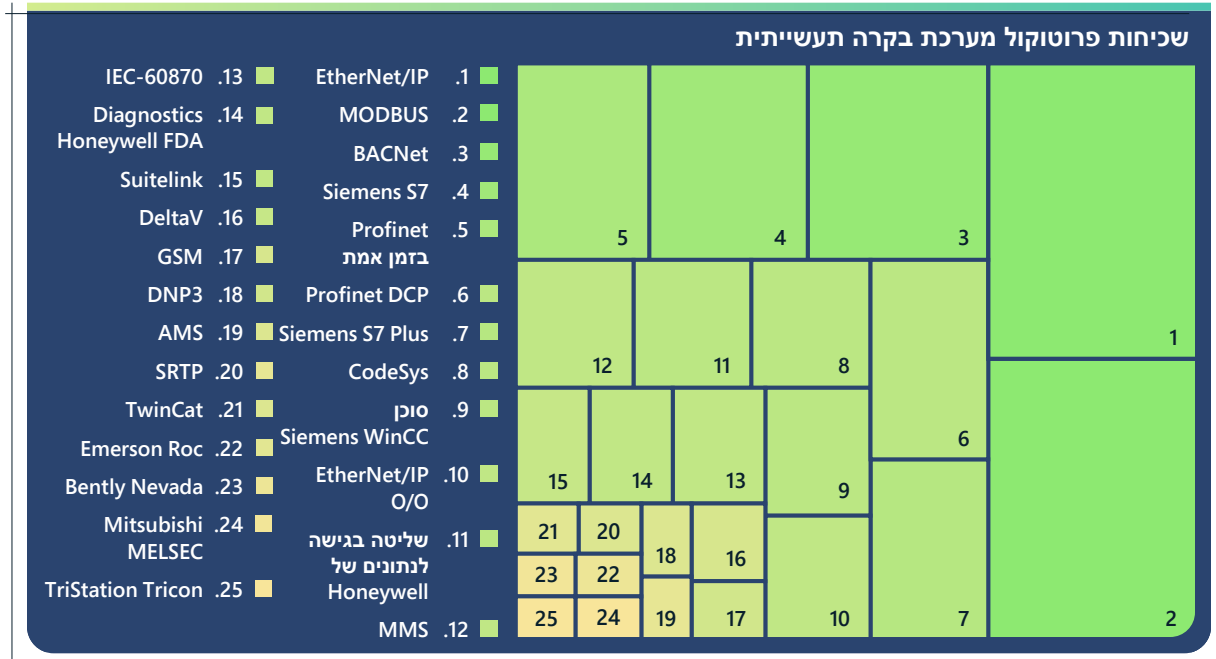
בעוד שתצורות חלשות ואישורי ברירת מחדל עדיין מהווים סיכון לרשתות, Microsoft הבחינה בנקודות תורפה מבוססות אינטרנט רבות המשתמשות ב-HTTP. ראינו עלייה זו בהתקפות על שירותים מבוססי אינטרנט המשתמשות ברשתות botnet מדור קודם. בינתיים, חלה ירידה במספר יציאות ה-Telnet הפתוחות באינטרנט, סימן חיובי לאבטחת הרשת שכן רשתות botnet שהיוו בעבר סיכון למכשירים מאבדות רלוונטיות. למרות ירידה זו ביציאות ה-Telnet הפתוחות, עדיין ראינו רשתות botnet שנשארות ברשתות חיישנים.

הפצה של תוכנות זדוניות של IoT על ידי ארכיטקטורת CPU



Microsoft הבחינה כי תוכנות זדוניות מתמקדות במכשירי IoT הפועלים על ARM במידה הרבה ביותר, ובעקבותיהם MIPS, X86-64, ומעבד 80386 של Intel.

שכיחות פרוטוקול מערכת בקרה תעשייתית



פגיעויות פרוטוקול מערכת הבקרה התעשייתית

בדקנו נתוני OT מהחיישנים שלנו המחוברים לענן, וחשפנו את פרוטוקולי מערכת הבקרה התעשייתית (ICS) הנפוצים ביותר. פרוטוקולים אלה מספקים תובנות לגבי טבעם של מכשירים אלה ומשטח התקיפה שלהם. זה רלוונטי במיוחד לאבטחת תשתיות חיוניות. מספר לקחים עיקריים הם:

1. רוב הפרוטוקולים המיוצגים הם קנייניים, כך שלכלי ניטור IT סטנדרטיים לא תהיה נראות אבטחה מספקת בכל המכשירים והפרוטוקולים הללו. כתוצאה מכך, רשתות נותרות ללא פיקוח ולכן פגיעות יותר להתקפות ספציפיות ל-OT.
2. יש מגוון גדול של פרוטוקולים ספציפיים לספק. משמעות הדבר היא שפתרונות אבטחה ספציפיים לספק לא יוכלו לכסות כראוי את כל הרשת. Microsoft מתעדפת גישה אגנוסטית לספקים, כדי לספק כיסוי אבטחה עבור מגוון רחב של מכשירים שונים.
3. ארגונים צריכים לוודא שפרוטוקולים אלה אינם חשופים ישירות לאינטרנט מהרשתות שלהם. חשיפה זו עלולה להוות סיכון אבטחה משמעותי בשל פגיעויות והאופי הלא מאובטח של פרוטוקולים אלה.

תוכנות זדוניות כמו Mirai ממשיכות להתקיים הודות לפיתוח יכולות חדשות והן מאומצות על ידי קבוצות פשעי סייבר וגורמים מדינתיים, תוך מינוף גרסאות חדשות של רשתות botnet קיימות בהתקפות DDoS על יריבים זרים.

תובנות מעשיות

1. יש לוודא שהמכשירים חזקים על-ידי החלת תיקונים, שינוי סיסמאות ברירת מחדל ויציאות SSH המוגדרות כברירת מחדל.
2. יש לצמצם את משטח התקיפה על ידי ביטול חיבורי אינטרנט ויציאות פתוחות מיותרים, הגבלת גישה מרחוק על ידי חסימת יציאות, מניעת גישה מרחוק ושימוש בשירותי VPN.
3. יש להשתמש בפתרון התומך ב-IoT/OT לגילוי ותגובה ברשת (NDR) ובפתרון מערכת לניהול מידע ואירועי אבטחה (SIEM)/תיאום ותגובה של אבטחה (SOAR) כדי לנטר מכשירים לאיתור התנהגויות חריגות או בלתי מורשות, כגון תקשורת עם מארחים לא מוכרים.
4. יש לפלח רשתות כדי להגביל את יכולתו של תוקף לנוע רוחבית ולפרוץ לנכסים לאחר חדירה ראשונית. יש לבודד מכשירי IoT ורשתות OT מרשתות IT ארגוניות באמצעות חומות אש.
5. יש לוודא כי פרוטוקולי ICS אינם חשופים ישירות לאינטרנט.

פריצת שרשראות אספקה וקושחה

כמעט לכל מכשיר המחובר לאינטרנט יש קושחה, שהיא תוכנה המוטמעת בחומרת המכשיר או במעגל המודפס. במהלך השנים האחרונות, ראינו התמקדות מוגברת בקושחה במטרה לבצע התקפות הרסניות. מכיוון שהקושחה צפויה להמשיך להיות מטרה רבת ערך עבור גורמי איום, ארגונים חייבים להגן מפני פריצת קושחה.

הקושחה אחראית לפונקציות העיקריות של המכשיר, כגון התחברות לרשת או אחסון נתונים. קושחה נמצאת בנתבים, מצלמות, טלוויזיות ומכשירים אחרים המשמשים בארגונים (IoT) יחד עם ציוד בקרה תעשייתי (OT) המשמש בתשתית חיונית. מבחינה היסטורית, הקושחה נכתבה עם קוד לא מאובטח, דבר שיוצר פגיעויות משמעותיות שניתן לנצל לצורך השתלטות על המכשיר או להחדרת קוד זדוני לקושחה.

סיכון זה מחמיר כשמדובר בשרשרת האספקה. רוב המכשירים נבנים באמצעות רכיבי תוכנה וחומרה של יצרנים רבים, כמו גם ספריות קוד פתוח. במקרים רבים למפעילי המכשירים אין אפשרות לראות את עץ המוצר (H/SBOM) של החומרה והתוכנה כדי שיוכלו להעריך את סיכון שרשרת האספקה של המכשירים ברשת שלהם. ביוני 2020, נחשפו פגיעויות בערימת הרשת המשמשת יצרנים רבים ושונים ומשפיעה על מאות מיליוני מכשירי IoT במרחב הצרכני ובמרחב הציוד התעשייתי.[14] במקרים מסוימים, ערימת הרשת מותגה מחדש על ידי ספקים אחרים ולא הייתה שום אינדיקציה לכך שהמכשיר פגיע. אנו רואים איום הולך וגובר של גורמים זדוניים המתמקדים בשרשרת אספקת תוכנה וחומרה זו של מכשירי IoT/OT כדי לפרוץ לארגונים.

תהליך עדכון הקושחה משתנה במידה רבה בין מכשירים, והמורכבות והאתגר הלוגיסטי של ביצועו משפיעים על תדירות העדכון. לא תמיד ניתן לקבוע אם מכשיר מפעיל את הקושחה העדכנית ביותר, עובדה המקשה על מומחי אבטחה לנטר ולוודא את מערך האבטחה במכשירי ה-IoT וה-OT שלהם. בנוסף, למכשירים מסוימים יש קושחה שאינה חתומה באמצעות הצפנה, כך שניתן לעדכן אותם ללא אימות מהמשתמש. חולשות אלה פותחות עוד יותר את המכשירים להתקפות שרשרת אספקה לאורך כל שרשרת הייצור וההפצה.

כדי להתמודד עם איומים אלה, Microsoft משקיעה באופן משמעותי בדאגה לאבטחת הקושחה ולשלמותה בזמן שהיא עוברת בשלבים השונים של שרשרת האספקה, ובאישור בכל עת שלא חיבלו בה במהלך קליטת נתונים או לאורך הדרך. זה יאפשר לנו לאמת את האמון בין כל מקטע בערוץ ולספק שרשרת משמורת מאושרת וניתנת להוכחה מקצה לקצה עבור כל רכיב שאנו שולחים ללקוחות. אנו עובדים עם השותפים שלנו כדי להביא את אבטחת מהשבב לענן זו לכל המכשירים ברשת הארגון וה-OT.

"ספקי תשתיות טכנולוגיות מידע ותקשורת (ICT) יותר ויותר מהווים יעדים מכיוון שהם מאפשרים שכפול נרחב של התקפה יחידה. במקביל, החקיקה, הרגולציה ודרישות הלקוחות הגלובליות לאבטחה ועמידות של שרשרת האספקה נמצאות במגמת עלייה, ולעתים קרובות הן שונות בדרישותיהן.

הפתרון הוא שותפות. יחד עם ספקים וממשלות גלובליות, Microsoft מחויבת לטפל באבטחה בכל המערכת האקולוגית של שרשרת האספקה שלנו, תוך חריגה מדרישות הלקוחות והרגולטורים כאחד. לשם כך, אנו מקדמים גישה מקיפה לאבטחה ולעמידות תפעולית הנפרסת באופן גמיש לאורך שרשרת האספקה.

קידום שלמות הקושחה מהתכנון ועד לתפעול המכשיר הוא המפתח לגישה הקולקטיבית שלנו. הבטחת תהליכי SDL של ספקים ופריסת חדשנות בסיס חומרה של אמון הן דוגמאות לאופן שבו אנו יכולים 'לבנות' תקינות שרשרת אספקה.

הקהילה שלנו ממנפת מחקר ופיתוח קולקטיביים המתפרשים על פני טכניקות חדשות נגד חבלה ומנגנוני הצפנה חדשים, בשילוב עם ניטור שוטף וזיהוי חריגות. יחד, אנו מתקדמים במזעור הפיתוי של שרשרת האספקה כמשטח תקיפה".

עדנה קונוויי,
סגנית נשיא, מנהלת אבטחה וסיכונים, תשתיות ענן

זרקור על פגיעויות קושחה

התוקפים ממנפים יותר ויותר פגיעויות בקושחת מכשירי IoT כדי לחדור לרשתות ארגוניות. בניגוד לנקודות קצה מסורתיות של IT המשתמשות בסוכני זיהוי ותגובה מורחבים (XDR) לזיהוי חולשות, זיהוי פגיעויות במכשירי IoT/OT הוא הרבה יותר חמקמק.

סקר שנערך לאחרונה על ידי Microsoft ומכון Ponemon מדגיש הן את ההזדמנות והן את אתגר האבטחה של מכשירי IoT/OT בארגון.[15] בעוד ש-68 אחוזים מהנשאלים מאמינים שאימוץ IoT/OT הוא קריטי לטרנספורמציה הדיגיטלית האסטרטגית שלהם, 60 אחוזים מכירים בכך שאבטחת IoT/OT היא אחד ההיבטים הפחות מאובטחים של תשתית ה-IT/OT.

דוגמה לתוקפים המשתמשים בפגיעויות בקושחת מכשירי IoT כדי לחדור לרשת היא הסוס הטרויאני Trickbot שמינף סיסמאות ברירת מחדל ופגיעויות בנתבי Mikrotik[16] כדי לעקוף מערכות הגנה ארגוניות. האתגר הבסיסי עם קושחת מכשירי IoT הוא חוסר הנראות למערך האבטחה ולפגיעויות של מכשירים.

בעוד שישנם פתרונות זמינים לבניית מכשירים מאובטחים, ישנם מיליארדי מכשירים שכבר קיימים בשוק ופרוסים בארגונים. אלה ידועים בשם מכשירי סביבה בשלה (Brownfield). בשנת 2021, Microsoft רכשה את ReFirm Labs כדי לשפוך אור על אבטחת מכשירי הסביבה הבשלה (Brownfield) ולאפשר לבוני מכשירים לשפר את אבטחת מוצריהם. ReFirm Labs מנתחת את תמונת הקושחה הבינארית של מכשיר ומפיקה דוח מפורט על חולשות אבטחה פוטנציאליות.[17] טכנולוגיה זו משולבת במהדורה עתידית של Microsoft Defender עבור IoT.

במהלך השנה האחרונה בחנו את התוצאות המצטברות של הקושחה הייחודית שנסרקה על ידי לקוחותינו. בעוד שלא כל חולשה שמתגלה עשויה להיות ניתנת לניצול, קיומן מדגיש את האתגר הבסיסי של אבטחת קושחת המכשיר.

הערה: סוגי החולשות הקיימים במכשירי IoT/OT לעולם לא יהיו מקובלים בנקודות קצה מסורתיות של Windows או Linux.

- סיסמאות חלשות: עשרים ושבעה אחוזים מתמונות הקושחה שנסרקו הכילו חשבונות עם סיסמאות המקודדות באמצעות אלגוריתמים חלשים (MD5/DES), אשר נפרצים בקלות על ידי התוקפים.
- פגיעויות ידועות: כמו מערכות אחרות, קושחת מכשירי IoT/OT מינפה באופן נרחב ספריות קוד פתוח. עם זאת, לעתים קרובות מכשירים נשלחים עם גרסאות לא עדכניות של רכיבים אלה. בניתוח שלנו, 32 אחוז מהתמונות הכילו לפחות 10 פגיעויות ידועות (CVEs) שדורגו כקריטיות (9.0 ומעלה). ארבעה אחוז הכילו לפחות 10 פגיעויות קריטיות בנות יותר משש שנים.
- אישורים שפג תוקפם: אישורים משמשים לאימות חיבורים וזהויות, וכן להגנה על נתונים רגישים, אך 13 אחוז מהתמונות שנותחו הכילו לפחות 10 אישורים שתוקפם פג לפני יותר משלוש שנים.
- רכיבי תוכנה: שלושים ושישה אחוזים מהתמונות מכילים רכיבי תוכנה ש-Microsoft ממליצה לא לכלול במכשירי IoT כגון כלי לכידת מנות (tcpdump, libpcap), שניתן למנף לצורך איסוף זדוני ברשת כחלק משרשרת התקפה.

חולשות אבטחה בתמונות קושחה שנותחו

התקפות קושחה שקיימות

Viasat: שימוש בפגיעות קושחה כדי להתמקד בתקשורת לוויינית

בפברואר 2022, תקרית רשת לוויינית ניתקה רשת תקשורת אסטרטגית עם השפעות שהורגשו ברחבי אירופה. מערכת KA-SAT של Viasat קיבלה כמות גדולה של תעבורה שניתקה מודמים רבים והחלה מתקפת מניעת שירות מבוזרת נגד הרשת. כאשר הפס הרחב הקבוע שובש, אלפי טורבינות רוח הפכו לבלתי נגישות מרחוק למפעילים ותוכנות זדוניות שמבצעות מחיקה נפרסו במודמים המושפעים. השיבוש השפיע על יותר מ-30,000 מסופי לוויין המשמשים חברות וארגונים לתקשורת.

Cyclops Blink: שימוש במתקפת שרשרת אספקה של קושחה כדי להתמקד בשערי חומת אש

עבור גורמי איום, הפיתוח וההרחבה של תשתיות שליטה ובקרה (C2) והתקפה הם מרכיב מכריע בהצלחה. ככל שהצורך בתשתית C2 יציבה גדל, נתבים הפכו לווקטור תקיפה נחשק בשל תיקונים בתדירות נמוכה והיעדר פתרונות אבטחה מקיפים המאפיינים אותם.

Microsoft משתפת פעולה עם הממשלה והתעשייה בטכנולוגיית ניתוח קושחה כדי להביא נראות מעמיקה יותר לאבטחת המכשיר ולספק אבטחה מחזור חיים מלא עבור בוני מכשירים ומפעילים.

מאז יוני 2019, קבוצת איום מתמיד מתקדם (APT) המזוהה עם מדינה השתמשה בתוכנה הזדונית המודולרית Cyclops Blink כדי להתמקד בהתקני חומת האש הפגיעים של WatchGuard ובנתבי ASUS על ידי ביצוע עדכוני קושחה זדוניים וגיוסם לרשת botnet גדולה. התוכנה הזדונית מדביקה בהצלחה מכשירים על ידי ניצול פגיעות ידועה המאפשרת הסלמת הרשאות, ומאפשרת לגורמי האיום לנהל את המכשיר. לאחר ההדבקה, התוכנה הזדונית מאפשרת התקנת מודולים נוספים ומתחמקת מעדכוני קושחה. מכשירים שנפרצו נצפו מתחברים לשרתי C2 המתארחים במכשירי WatchGuard אחרים. מפעילי Cyclops Blink, שהנפיקו אישורי SSL רבים עבור ה-C2 שלהם ביציאות TCP שונות, השיגו גישה מורשית מרחוק לרשתות על ידי ביצוע עדכוני קושחה זדוניים ועל ידי התחמקות משיטות אבטחה מסורתיות כגון סריקה.

כיצד Microsoft משפרת את אבטחת שרשרת האספקה

Microsoft משתפת פעולה עם הממשלה והתעשייה כדי להתמודד עם אתגרי אבטחת מכשירי IoT ו- OT אלה (ראה את הדיון בעמוד 66). התרומה שלנו תכלול מינוף טכנולוגיית ניתוח הקושחה כדי לספק למפעילי מכשירים נראות לגבי מערך האבטחה של המכשירים ברשת שלהם. זה יאפשר ללקוחות לזהות ולתעדף מכשירים שזקוקים להגנות נוספות, שדרוגים או החלפה – ויגביר את הדרישה מבוני מכשירים להשקיע באבטחת מכשירים. במקביל, אנו תומכים בבונים עם פתרונות מקיפים לתכנון מכשירים מאובטחים ולאימוץ אבטחת מחזורי חיים של פיתוח.

רכיב מרכזי נוסף הוא אספקת תשתית חזקה לבונים ולמפעילים כדי לאפשר עדכון של קושחת המכשיר כאשר בעיות אבטחה מתגלות ונפתרות. Microsoft משלבת ניתוח קושחה ו-Defender עבור IoT עם עדכון מכשירים עבור IoT Hub כדי לספק פתרון לטיפול במחזור החיים המלא של אבטחת מכשירי IoT ו-OT. אלה הם שלבים חשובים במימוש החזון שלנו שהלקוחות יאבטחו את התשתית על ידי אימוץ מכשירים התומכים בגישת 'אפס אמון' לפתרונות ה-IoT וה-OT שלהם.[18]

התוקפים מתמקדים יותר ויותר בפגיעויות בקושחת מכשירי IoT כדי לחדור לרשתות ארגוניות.

תובנות מעשיות

1. יש לקבל נראות עמוקה יותר למכשירי IoT/OT ברשת הארגון ולתעדף אותם לפי סיכון לארגון אם הם נפרצים.
2. יש להשתמש בכלי סריקת קושחה כדי להבין חולשות אבטחה פוטנציאליות ולעבוד עם ספקים כדי לזהות כיצד להפחית את הסיכונים עבור מכשירים בסיכון גבוה.
3. יש להשפיע באופן חיובי על האבטחה של מכשירי IoT/OT על-ידי דרישה לאימוץ שיטות עבודה מומלצות למחזור חיי פיתוח מאובטח על-ידי הספקים.

קישורים למידע נוסף

- יש לבצע הערכה של שרשראות האספקה הקריטיות התומכות בתעשיית טכנולוגיית המידע והתקשורת בארה"ב

התקפות OT מבוססות איסוף זדוני

שרשראות אספקה מורכבות משתמשות במידע עיצובי ספציפי לצורך תכנון המערכת בפועל. מבין שלל הנכסים המרכיבים מידע עיצובי זה, הרגיש ביותר הוא קובץ הפרויקט, המגדיר את הסביבה ואת נכסיה. קובץ זה הוא יעד אסטרטגי חיוני עבור גורמי איום השואפים להשיג גישה ולבצע התקפה מוצלחת המותאמת לחלוטין לסביבה.

התמקדות במערכות תעשייתיות כדי לשבש תהליכים תפעוליים כרוכה בשני שלבים.

1. ראשית, על התוקף להשיג גישה לרשת ה-OT. ניתן לעשות זאת על ידי כניסה דרך מכשירי IoT בצד של הארגון ברשת (מודל Purdue רמה 4) וחציית גבול ה-IT-OT, המופרד באופן מסורתי על ידי חומות אש וציוד רשת, לרמות התפעול והבקרה.
2. שנית, יש לזהות את מכשירי הרשת. מערכות תעשייתיות משתמשות במכשירים ורכיבים סטנדרטיים בארכיטקטורות מותאמות אישית שתוכננו במיוחד עבור הסביבות שלהן. אחד ממכשירים סטנדרטיים אלה הוא בקר לוגיקה לתכנות (PLC). כל יצרן מפתח ממשקים ופונקציות ייחודיים עבור בקרי ה-PLC שלו, המהווים מרכיב חיוני במערכות תעשייתיות, ותצורתם של מכשירים אלה עוברת הגדרה נוספת באמצעות סכמות מותאמות אישית שתוכננו במיוחד עבור סביבות הלקוח.

התצורה הייחודית של כל PLC מתוארת בקובץ הפרויקט, המכיל את הגדרת הסביבה ונכסיה, לוגיקת הסולם ועוד.

ברוב הסביבות המציגות ראיות להתקפה, הניתוח מראה שציר הזמן שקדם להתקפה עולה בהרבה על אורך זמן ההתקפה עצמה. גורמי איום משקיעים לעתים קרובות חודשים בהדמיית הסביבה ונכסיה מרחוק, ועושים ניסיונות רבים לבניית מודל ולהכנת המתקפה הממוקדת שלהם. כאשר סביבות משתנות ללא הרף ומשלבות מכשירים חדשים, פגיעויות נוצרות במיוחד סביב הנתונים בקובצי הפרויקט והתצורה. גניבת קובץ פרויקט יכולה לקדם התקפה בשבועות או חודשים ולאפשר לתוקפים ליצור מודל של סביבת היעד במהירות ובדיוק, ובכך להגביר את הקושי באיתור פעילות זדונית.

Incontroller-ו Industroyer

ראינו עלייה בהתקפות על ארגונים, תשתיות חיוניות ומטרות ממשלתיות על ידי גורמים בחסות המדינה באמצעות תוכנות זדוניות מודולריות ומסגרות תקיפה. ניסיונות חדשים לשבש פעולות קריטיות באוקראינה מדגישים את האיום הגובר של התקפות OT מבוססות איסוף זדוני המותאמות במיוחד לסביבות היעד שלהן. שלבי האיסוף הזדוני והמחקר המורחבים המבוצעים על ידי גורמי סייבר מדינתיים מצביעים על אסטרטגיה של שימוש בלוחמת סייבר לצורך פגיעה בתשתיות מרחוק כדי לעמוד ביעדים אסטרטגיים או תפעוליים ספציפיים בפעולות סייבר-קינטיות משולבות ובאסטרטגיה פוליטית.

ראינו איום הולך וגובר של התקפות OT מבוססות איסוף זדוני המותאמות במיוחד לסביבות היעד שלהן.

התקפות OT מבוססות איסוף זדוני

המשך

בתחילת 2022 זוהו שתי התקפות OT קריטיות הניתנות להתאמה. מתקפת סייבר פיזית על תחנות משנה וממסרי הגנה באוקראינה בוצעה באמצעות תוכנות זדוניות מותאמות אישית, וכללה גרסה של Industroyer, תוכנה זדונית שידוע כי גרמה להפסקות חשמל באוקראינה לאחר פריסתה בשנת 2016.

Industroyer2 היא הפריסה מחדש הידועה הראשונה של תוכנות זדוניות לתקיפת OT זדונית על יעד חדש. היא השתמשה בתוסף פרוטוקול IEC104 (פרוטוקול סטנדרטי לניטור ובקרה של מערכות חשמל) שפותח עבור Industroyer והתמקד בעיקר ביחידות מסוף מרוחקות הדומות ל-PLC עם מספר דגם ABB RTU540/560. הכותב של תוכנה זדונית זו השתמש בידע על סביבת הקורבן כדי להוציא פקודות שוב ושוב לתפוקות שנקבעו מראש, תוך דאגה לכך שלא ניתן יהיה להפעיל אותן באופן ידני. כך הובטח שהפסקות החשמל יהיו ארוכות יותר והשפעתן תהיה מזיקה יותר.

Incontroller, מסגרת תקיפה מודולרית שזוהתה באותה תקופה, היא ערכת כלים מודולרית שמקצרת משמעותית את זמן ביצוע החדירה והתקיפה של מכשירי OT, תוך עקיפת פתרונות אבטחה מדור קודם. ערכת הכלים לשימוש כללי כוללת יכולות איסוף נתונים, איסוף זדוני ותקיפה הניתנות להתאמה אישית רבה לסביבות שונות ויכולות להשפיע מאוד על שלב המחקר לקראת התקפת OT, להפחית את הזמן הדרוש לביצוע האיסוף הזדוני, ולתמוך בסימולציה של סביבות על ידי חילוץ מידע על מכשירים ותצורותיהם.

מסגרת Incontroller תומכת בפרוטוקולים עבור בקרי PLC של Schneider Electric ו-Omron ואוספת מידע, כגון גרסת הקושחה, סוג הדגם ומכשירים מחוברים. ערכת הכלים יכולה להוציא פקודות לשינוי תצורות ולהפעלה וכיבוי של תפוקות. לאחר שהושגה גישה לסביבה, המסגרת תומכת בהשתלת דלתות אחוריות במכשירים למסירת מטענים נוספים, הנפקת פגיעויות להגדלת כמות נקודות הגישה, העלאת לוגיקת סולם והיכולת לבצע התקפות DoS. האופי הגנרי של ערכת הכלים מאפשר לגורם האיום לתקוף סביבה במהירות ללא צורך לכתוב התקפות חדשות עבור כל PLC או מיקום. זה מאפשר לגורם לתקשר בקלות עם סוגים שונים של מכונות על פני תעשיות רבות באופן פוטנציאלי.

תובנות מעשיות

1. יש להימנע מהעברת קבצים המכילים הגדרות מערכת דרך ערוצים לא מאובטחים, או לאנשי צוות שאינם חיוניים.
2. כאשר העברת קבצים כאלה היא בלתי נמנעת, יש להקפיד לפקח על הפעילות ברשת ולוודא שהנכסים מאובטחים.
3. יש להגן על עמדות הנדסה על-ידי ניטור באמצעות פתרונות EDR.
4. יש לבצע באופן יזום תגובה לאירועים עבור רשתות OT.
5. יש לפרוס ניטור רציף, כגון Defender עבור IoT.

הערות סיום

1. ראה למשל, הוראה מתוקנת בנושא אבטחת רשתות ומערכות מידע (NIS2) | עיצוב העתיד הדיגיטלי של אירופה (europa.eu); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&r id=1; חוק לתיקון חקיקת ביטחון (הגנה על תשתיות חיוניות), התשפ"ב-2022 (homeaffairs.gov.au); צ'ילה: הצעת חוק לאבטחת סייבר ותשתיות מידע חיוניות שהוצגה בסנאט | פוסט חדשות | DataGuidance; יפן העבירה הצעת חוק לביטחון כלכלי לשמירה על טכנולוגיה רגישה | The Japan Times; סקירת חוק אבטחת הסייבר ועדכון לקוד הנוהג של אבטחת סייבר עבור CIIs (csa.gov.sg); הצעה לחקיקה לשיפור עמידות הסייבר של בריטניה— GOV.UK (www.gov.uk); חוק טלקומוניקציה (אבטחה), התשפ"א-2021 (legislation.gov.uk); עדכון מסגרת אבטחת הסייבר של NIST – מסע אל NIST | CSF 2.0
2. Cert-In – דף הבית
3. ייזום התייעצות בנושא הנהגת חובת דיווח על מתקפות סייבר (admin.ch)
4. ראה, למשל, ללא כותרת (house.gov)
5. חוק חוסן הסייבר | מעצבים את העתיד הדיגיטלי של אירופה (europa.eu)
6. ראה,למשל, מחזור החיים של פיתוח האבטחה של Microsoft
7. ראה, למשל, יצירת 'עצי מוצר של תוכנה' (SBOMs) באמצעות SPDX ב Microsoft -Microsoft Engineering@; ראה גם, לדוגמה, הרכיבים המינימליים עבור עץ מוצר של תוכנה (SBOM) | מנהל התקשורת והמידע הלאומי (ntia.gov)
8. ראה, למשל, https://www.microsoft.com/en-us/msrc/cvd
9. הצעת החוק לאבטחת מוצרים ותשתית טלקומוניקציה (PSTI) – גיליון מידע על אבטחת מוצרים – GOV.UK (www.gov.uk)
10. הנציבות מחזקת את אבטחת הסייבר של מכשירים ומוצרים אלחוטיים (europa.eu)
11. תוכנית הסמכת ענן: בניית שירותי ענן מהימנים ברחבי אירופה – ENISA (europa.eu)
12. הסמכה – ENISA (europa.eu)
13. "https://github.com/microsoft/sbom-tool" GitHub - כלי Microsoft/sbom: כלי SBOM הוא כלי מדרגי מאוד ומוכן לארגון ליצירת SBOMs תואמי SPDX 2.2 עבור כל מגוון של חפצים.
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years- to-come
15. חדשנות IoT/OT קריטית אך מגיעה עם סיכונים משמעותיים (דצמבר 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. חשיפת השימוש של Trickbot במכשירי IoT בתשתית C2 (מרץ 2022): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. תוכנית IoT בערוץ 9 פרק על סריקת קושחת IoT (מאי 2022): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. כיצד ליישם גישת 'אפס אמון' בפתרונות ה-IoT שלך (מאי 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

מבצעי השפעה בסייבר

מבצעי ההשפעה הזרה של ימינו משתמשים בשיטות ובטכנולוגיות חדשות, דבר שהופך את הקמפיינים שלהם שנועדו לשחוק את האמון ליעילים ואפקטיביים יותר.

סקירה כללית על

מבצעי השפעה בסייבר

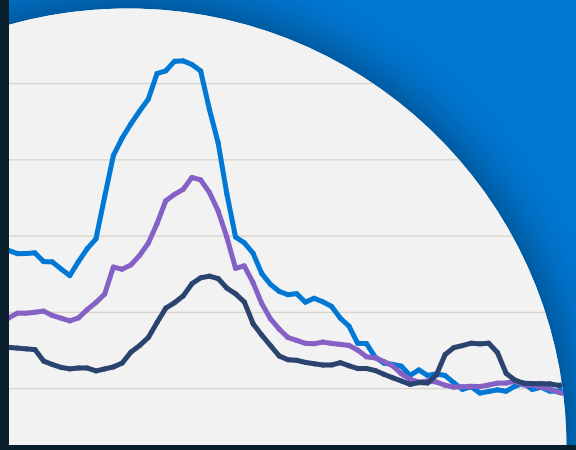
מבצעי ההשפעה הזרה של ימינו משתמשים בשיטות ובטכנולוגיות חדשות, דבר שהופך את הקמפיינים שלהם שנועדו לשחוק את האמון ליעילים ואפקטיביים יותר.

מדינות משתמשות יותר ויותר במבצעי השפעה מתוחכמים כדי להפיץ תעמולה ולהשפיע על דעת הקהל הן מקומית והן בזירה הבינלאומית. הקמפיינים האלה שוחקים את האמון, מגבירים את הקיטוב ומאיימים על תהליכים דמוקרטיים. גורמים מניפולטיביים מיומנים ומתקדמים בעלי יכולת התמדה משתמשים במדיה המסורתית בשילוב עם האינטרנט והמדיה החברתית כדי להגדיל במידה ניכרת את ההיקף, קנה המידה והיעילות של הקמפיינים שלהם, ואת ההשפעה הנרחבת שיש להם במערכת האקולוגית העולמית של המידע. בשנה האחרונה ראינו את הפעולות הללו בשימוש כחלק מהמלחמה ההיברידית של רוסיה באוקראינה, אך גם ראינו את רוסיה ומדינות אחרות, כולל סין ואיראן, פונות יותר ויותר לפעולות תעמולה המופעלות על ידי המדיה החברתית כדי להרחיב את השפעתן העולמית.

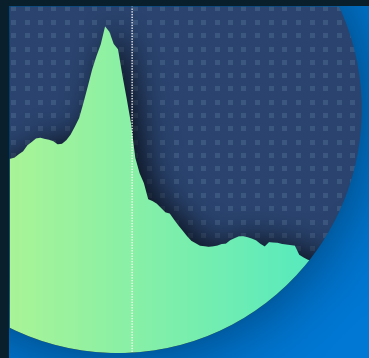
מבצעי השפעה בסייבר הופכים מתוחכמים יותר ויותר ככל שיותר ממשלות ומדינות משתמשות במבצעים אלה כדי לעצב דעות, להכפיש יריבים ולקדם מחלוקת.

מידע נוסף בעמוד 74

הפלישה הרוסית לאוקראינה מדגימה מבצעי השפעה בסייבר המשולבים עם מתקפות סייבר מסורתיות יותר ומבצעים צבאיים קינטיים כדי למקסם את ההשפעה.



מידע נוסף בעמוד 76



רוסיה, איראן וסין השתמשו במסעות תעמולה והשפעה לאורך תקופת מגפת הקורונה, לעתים קרובות כמכשיר אסטרטגי להשגת יעדים פוליטיים רחבים יותר.

מידע נוסף בעמוד 76

מדיה סינתטית הופכת נפוצה יותר בשל ריבוי הכלים היוצרים בקלות תמונות, קטעי וידאו ושמע מלאכותיים ומציאותיים מאוד ומפיצים אותם. טכנולוגיית מקור דיגיטלית המאשרת את מקור נכסי המדיה טומנת בחובה הבטחה להילחם בשימוש לרעה.

מידע נוסף בעמוד 80

גישה הוליסטית להגנה מפני מבצעי השפעה בסייבר

Microsoft בונה על תשתית מודיעין איומי הסייבר שלה שכבר בשלה כדי להילחם במבצעי השפעה בסייבר. האסטרטגיה שלנו היא לזהות, לשבש, להגן ולהרתיע מסעות תעמולה של פולשים זרים.

מידע נוסף בעמוד 83

מבוא

דמוקרטיה זקוקה למידע אמין כדי לפרוח. תחום מרכזי שבו מתמקדת Microsoft הוא מבצעי ההשפעה המפותחים ומונצחים על ידי מדינות. הקמפיינים האלה שוחקים את האמון, מגבירים את הקיטוב ומאיימים על תהליכים דמוקרטיים.

מבצעי השפעה זרים תמיד היוו איום על המערכת האקולוגית של המידע. עם זאת, מה ששונה בעידן האינטרנט והמדיה החברתית הוא ההיקף, קנה המידה והיעילות הגדולים בהרבה של הקמפיינים, וההשפעה הנרחבת שעלולה להיות להם על המערכת האקולוגית העולמית של המידע.

הפתגם עתיק היומין ש"שקר מגיע למחצית הדרך מסביב לעולם לפני שלאמת יש הזדמנות לנעול את נעליה", נתמך כעת בנתונים. מחקר של המכון הטכנולוגי של מסצ'וסטס (MIT)[1] מצא כי לשקרים יש סיכוי גבוה ב-70% להיות מצויצים מחדש מאשר לאמת, והם מגיעים ל-1,500 האנשים הראשונים פי שישה מהר יותר. המערכת האקולוגית של המידע הפכה עכורה יותר ויותר ככל שמסעות תעמולה משגשגים באינטרנט וברשתות החברתיות ומערערים את האמון בערוצי החדשות המסורתיים. במחקר משנת 2021,[2] רק שבעה אחוזים מהמבוגרים בארה"ב אמרו שיש להם "מידה רבה" של אמון וביטחון בדיווחי חדשות בעיתונים, בטלוויזיה וברדיו, בעוד ש-34 אחוזים דיווחו "בכלל לא".

Microsoft פועלת כדי לזהות את הגורמים, האיומים והטקטיקות העיקריים במרחב ההשפעה הזרה בסייבר ולשתף לקחים שנלמדו. ביוני השנה פרסמנו דוח מקיף על הלקחים שנלמדו מאוקראינה, שכלל סקירה מפורטת של מבצעי ההשפעה בסייבר של רוסיה.[3]

אנחנו גם חוקרים כיצד טכנולוגיות מתקדמות כמו דיפ-פייק יכולות לשמש כנשק ולערער את אמינותם של עיתונאים. בנוסף, אנו עובדים עם התעשייה, הממשלה והאקדמיה כדי לפתח דרכים טובות יותר לזיהוי מדיה סינתטית ולשיקום האמון – כגון מערכות בינה מלאכותית (AI) שיכולות לזהות זיופים.

האופי המשתנה במהירות של המערכת האקולוגית של המידע והתעמולה המדינתית המקוונת, כולל המיזוג של מתקפות סייבר מסורתיות עם מבצעי השפעה וההתערבות בבחירות דמוקרטיות, מחייבים גישה של כלל החברה למיתון האיומים המקוונים והלא מקוונים על הדמוקרטיה.

Microsoft מחויבת לתמוך במערכת אקולוגית בריאה של מידע שבה חדשות ומידע מהימנים משגשגים. אנו מפתחים כלים ויכולות זיהוי איומים כדי להילחם בסיכון המתפתח והמתרחב של מבצעי השפעה המונעים על ידי מדינות. כדי לאפשר עבודה זו, רכשנו לאחרונה את Miburo Solutions, אנו משתפים פעולה עם מאמתי צד שלישי כגון ה-Global Disinformation Index ו-NewsGuard, ואנו משתפים ולעתים מובילים שותפויות עם מספר בעלי עניין, כולל The Coalition למקור תוכן ואותנטיות (C2PA). רק על ידי עבודה משותפת נוכל להצליח להתמודד עם אלה המבקשים לערער תהליכים ומוסדות דמוקרטיים.

תרזה האטסון

סגנית נשיא, טכנולוגיה ואחריות תאגידית

מגמות במבצעי השפעה בסייבר

מבצעי השפעה בסייבר הופכים מתוחכמים יותר ויותר ככל שהטכנולוגיה מתפתחת בקצב מהיר. אנו רואים חפיפה והרחבה של הכלים המשמשים במתקפות סייבר מסורתיות המיושמים במבצעי השפעה בסייבר. בנוסף, אנו רואים יותר תיאום והתגברותו בין מדינות הלאום.

Microsoft השקיעה השנה במאבק במבצעי השפעה זרה על ידי רכישת Miburo Solutions, חברה המתמחה בניתוח מבצעי השפעה זרה. בשילוב של אנליסטים אלה עם מנתחי הקשר האיומים של Microsoft, Microsoft הקימה את המרכז לניתוח איומים דיגיטליים (DTAC). DTAC מנתח ומדווח על איומי מדינות, כולל מתקפות סייבר ומבצעי השפעה, ומשלב מידע ומודיעין איומים עם ניתוח גיאופוליטי כדי לספק תובנות וליידע לגבי תגובה יעילה והגנות.

יותר משלושה רבעים מהאנשים ברחבי העולם אמרו שהם מודאגים מהשימוש במידע כנשק,[4] והנתונים שלנו תומכים בחששות אלה. Microsoft ושותפיה עוקבים אחר האופן שבו גורמים מדינתיים משתמשים במבצעי השפעה להשגת היעדים האסטרטגיים והמטרות הפוליטיות שלהם. בנוסף למתקפות סייבר הרסניות ולמאמצי ריגול סייבר, משטרים אוטוריטריים משתמשים יותר ויותר במבצעי השפעה בסייבר כדי לעצב דעות, להכפיש יריבים, לעורר פחד, לקדם מחלוקת ולעוות את המציאות.

למבצעי השפעה זרה בסייבר אלה יש בדרך כלל שלושה שלבים:

הצבה מראש

בדומה למיצוב מראש של תוכנות זדוניות בתוך רשת המחשבים של הארגון, מבצעי השפעה זרה בסייבר מציבים מראש נרטיבים כוזבים ברשות הרבים באינטרנט. טקטיקת המיצוב מראש סייעה זה מכבר לפעילויות סייבר מסורתיות יותר, במיוחד אם מנהלי IT סורקים את פעילות הרשת העדכנית ביותר שלהם. תוכנות זדוניות הנמצאות במצב רדום במשך זמן ממושך ברשת יכולות להפוך את השימוש בהן ליעיל יותר בהמשך. נרטיבים שקריים שנמצאים מבלי משים באינטרנט יכולים לגרום לאזכורים שיבואו בעקבותיהם להיראות אמינים יותר.

השקה

לעתים קרובות בזמן המועיל ביותר להשגת המטרות של הגורם, קמפיין מתואם מושק כדי להפיץ נרטיבים באמצעות כלי תקשורת וערוצי מדיה חברתית הנתמכים על ידי הממשלה ומושפעים ממנה.

הגברה

לבסוף, כלי תקשורת ושליחים הנשלטים על ידי המדינה מגבירים את עוצמת הנרטיבים בתוך קהלי היעד. לעתים קרובות, גורמים טכנולוגיים תמימים מרחיבים את טווח ההגעה של הנרטיבים. לדוגמה, פרסום מקוון יכול לעזור במימון פעילויות ומערכות אספקת תוכן מתואמות יכולות להציף מנועי חיפוש.

גישה תלת-שלבית זו יושמה בסוף 2021 כדי לתמוך בנרטיב השקרי הרוסי שסבב סביב נשק ביולוגי ומעבדות ניסויים ביולוגיים הקיימים לכאורה באוקראינה. הנרטיב הזה הועלה לראשונה ל-YouTube ב-29 בנובמבר 2021 כחלק ממופע קבוע בשפה האנגלית על ידי גולה אמריקאי ממוסקבה שטען כי מעבדות לניסויים ביולוגיים במימון אמריקאי הנמצאות באוקראינה קשורות לנשק ביולוגי. הסיפור נעלם כמעט מעיני הציבור במשך חודשים. ב-24 בפברואר 2022, בדיוק כשטנקים רוסיים חצו את הגבול, הנרטיב נשלח לקרב. צוות ניתוח נתונים ב-Microsoft זיהה 10 אתרי חדשות בשליטת רוסיה או בהשפעה רוסית, שפרסמו בו זמנית דיווחים ב-24 בפברואר, שהצביעו על "הדוח של השנה שעברה" וביקשו לתת בו אמון. בנוסף, גורמים במשרד החוץ הרוסי קיימו מסיבות עיתונאים שזרעו עוד טענות שקריות על מעבדות ניסויים ביולוגיים אמריקאיות בסביבת המידע. צוותים בחסות רוסית החלו בשלב זה לעבוד על הגברת עוצמת הנרטיב ברשתות החברתיות ובאתרי האינטרנט באופן רחב יותר.

אנו רואים משטרים אוטוריטריים ברחבי העולם עובדים יחד כדי לזהם את המערכת האקולוגית של המידע לטובתם ההדדית. לדוגמה, במהלך מגפת הקורונה השתמשו רוסיה, איראן וסין בפעולות תעמולה ובמבצעי השפעה תוך שימוש בתערובת של שיטות הפצה גלויות, סמויות למחצה וסמויות כדי לפגוע בדמוקרטיות ולקדם מטרות גיאופוליטיות נוספות (נדון בהרחבה בעמוד 76). שלושת המשטרים שיחקו במערכות האקולוגיות של המסרים והמידע זה של זה כדי לקדם נרטיבים מועדפים. חלק ניכר מסיקור זה כלל ביקורת או תיאוריות קונספירציה על ארצות הברית ובעלות בריתה, שהושמעו על ידי אנשי ממשל בהצהרות רשמיות תוך קידום החיסונים והתגובות שלהם לנגיף הקורונה כעדיפים על אלו של ארצות הברית ודמוקרטיות אחרות. על ידי הגברת עוצמה הדדית, כלי תקשורת המופעלים על ידי המדינה יצרו מערכת אקולוגית שבה סיקור שלילי של דמוקרטיות – או סיקור חיובי של רוסיה, איראן וסין – שהופק על ידי כלי תקשורת ממלכתי אחד קיבל חיזוק על ידי אחרים.

התקדמות מבצעי השפעה זרה בסייבר[5]

המחשה לאופן שבו נרטיבים על מעבדות לניסויים ביולוגיים ונשק ביולוגי אמריקאיים הופצו באמצעות שלושת השלבים הרחבים של מבצעי השפעה זרה רבים – הצבה מראש, השקה והגברה.

מגמות במבצעי השפעה בסייבר

המשך

כדי להוסיף לאתגר, גופי טכנולוגיה במגזר הפרטי עשויים לאפשר את הקמפיינים הללו מבלי משים. גורמים מאפשרים יכולים לכלול חברות שרושמות תחומים באינטרנט, מארחות אתרים, מקדמות חומרים ברשתות חברתיות ובאתרי חיפוש, מנתבות תעבורה ועוזרות לשלם עבור תרגילים אלה באמצעות פרסום דיגיטלי. על ארגונים להיות מודעים לכלים ולשיטות שבהם משתמשים משטרים אוטוריטריים למבצעי השפעה בסייבר כדי שיוכלו לזהות ולאחר מכן למנוע את התפשטות הקמפיינים. יש גם צורך גובר לעזור לצרכנים לפתח יכולת מתוחכמת יותר לזיהוי מבצעי השפעה זרה ולהגביל את המעורבות עם הנרטיבים או התוכן שלהם.

מבצעי השפעה בסייבר, כולל תעמולה אוטוריטרית, מהווים איום על דמוקרטיות ברחבי העולם מכיוון שהם שוחקים את האמון, מגבירים את הקיטוב ומאיימים על תהליכים דמוקרטיים.

יש צורך בהגברת התיאום ושיתוף המידע בין הממשלה, המגזר הפרטי והחברה האזרחית כדי להגביר את השקיפות ולחשוף ולשבש את קמפיינים למטרות השפעה אלו.

ברחבי העולם, יותר משלושה רבעים מהאנשים מודאגים מהאופן שבו המידע משמש כנשק.

זרקור על מבצעי השפעה במהלך מגפת הקורונה ופלישת רוסיה לאוקראינה

מדינות שביקשו לשלוט בסביבת המידע לאורך המגפה ובמהלך הפלישה הרוסית לאוקראינה מספקות דוגמאות בולטות לאופן שבו משטרים אוטוריטריים משלבים פעולות סייבר ומידע.

תעמולת הקורונה

רוסיה, איראן וסין הפעילו מסעות תעמולה והשפעה לאורך מגפת הקורונה. הקורונה כיכבה בקמפיינים אלה בשתי דרכים מרכזיות:

1. ייצוגים של המגפה עצמה.
2. קמפיינים שהשתמשו בקורונה כמכשיר אסטרטגי להשגת יעדים פוליטיים רחבים יותר.

המטרה הרחבה של קמפיינים מסוג זה היא כפולה: ראשית, לערער דמוקרטיות, מוסדות דמוקרטיים ואת תדמיתן של ארצות הברית ובעלות בריתה בזירה העולמית; ושנית, לחזק את מעמדם באופן מקומי ובינלאומי.

דוגמה לכך ניתן לראות בהודעות של חשבונות רוסיים ידועים וארגוני תקשורת המכוונים לקוראי השפה האנגלית לעומת האופן שבו ממשלת רוסיה תקשרה עם אנשיה בנוגע לחיסון ולחומרת מגפת הקורונה.

הנושאים המכוסים על ידי 10 הסיפורים הנצפים ביותר בנושא נגיף הקורונה ב-RT.com
(אוקטובר 2021 - אפריל 2022)

תעמולה נגד חיסונים מכוונת לקוראים שאינם רוסים

רוסית (תורגם למטה לאנגלית)	אנגלית
"סגרים וחיסוני ובוסטר מונעים הדבקה"	"החיסונים לא מצליחים לבלום את ההדבקה ואינם יעילים נגד זנים חדשים"
"אנשי ציבור רוסיים נמצאו חיוביים"	"לחיסון של פייזר יש תופעות לוואי מסוכנות"
"מספרי מקרי התחלואה והמוות הולכים וגדלים ברוסיה"	"חיסון המוני מונע ממניעים פוליטיים"
"החיסון ספוטניק V יעיל ביותר"	"פייזר ומודרנה עורכות ניסויים לא מפוקחים"
"דרושה הוכחת חיסון בתחבורה הציבורית"	

העברת הודעות הנוגעות לקורונה ברוסית המשתנות לפי שפה.

קמפיינים שביקשו לטשטש את מקורו של נגיף הקורונה מציעים דוגמה נוספת. מאז תחילת המגפה, תעמולות הקורונה הרוסית, האיראנית והסינית הגבירו את הסיקור מהאחרים כדי להעצים את הנושאים המרכזיים הללו. חלק גדול מהסיקור הזה כלל קידום ביקורת או תיאוריות קונספירציה על ארצות הברית. על ידי הגברת עוצמה הדדית קבועה, כלי תקשורת המופעלים על ידי המדינה פיתחו מערכת אקולוגית שבה סיקור שלילי של דמוקרטיות או סיקור חיובי של רוסיה, איראן וסין על ידי כלי תקשורת ממלכתי אחד קיבל חיזוק על ידי האחרים שוב ושוב.

אחת הדוגמאות לכך היא הטענה המוקדמת של התקשורת הממלכתית הרוסית והאיראנית, לפיה נגיף הקורונה עשוי להיות נשק ביולוגי שנוצר על ידי ארצות הברית. טענה זו הופצה באתרי קונספירציה שוליים בתחילת המגפה לאחר ראיון עם פרופסור למשפטים שטען כי הוא מאמין שנגיף הקורונה נוצר כנשק.[6] לאחר שהריאיון פורסם בכמה אתרי אינטרנט עם תפוצה מוגבלת, הסיפור נאסף על ידי כלי תקשורת בבעלות המדינה. PressTV, אתר אירני בשפה האנגלית והצרפתית בחסות ממשלת איראן,[7] פרסם בפברואר 2020 סיפור בשפה האנגלית שכותרתו "האם נגיף הקורונה הוא נשק לוחמה ביולוגית אמריקאי כפי שפרנסיס בויל מאמין?" המאמר רמז כי ארצות הברית עמדה מאחורי התפרצות נגיף הקורונה, ונכתב כי "בכל מלחמות ארה"ב נעשה שימוש בכלי נשק רדיולוגיים, כימיים, ביולוגיים ונשקים אסורים אחרים, הגובים מחיר הרסני מאנשים באזורים שהיוו יעד להתקפה".[8] כלי תקשורת ממלכתיים רוסיים ודיווחים ממשלתיים סיניים הדהדו את דעה זו. Russia Today (RT) כלי תקשורת בבעלות המדינה הידוע בתפקידו בהפצת תעמולת הקרמלין[9] – פרסם לפחות סיפור אחד שקידם התבטאויות של בכירים איראנים שטענו כי נגיף הקורונה עשוי להיות "תוצר של 'מתקפה ביולוגית' אמריקאית המכוונת נגד איראן וסין"[10] ופרסם פוסטים ברשתות החברתיות המרמזים על כך. לדוגמה, בציוץ של RT מ-27 בפברואר 2020 נכתב: "הרימו ידיים, מי לא יתפלא אם אי פעם יתגלה ש-coronaviru#הוא נשק ביולוגי?"[11]

המלחמה באוקראינה – תעמולה כנשק מלחמתי

הפלישה הרוסית לאוקראינה מספקת דוגמה מובהקת לאופן שבו ניתן לשלב מבצעי השפעה בסייבר עם מתקפות סייבר מסורתיות יותר ופעולות צבאיות בשטח כדי למקסם את השפעתן.

לקראת הפלישה לאוקראינה, מנתחי מודיעין בתחום האיומים של Microsoft ראו לפחות שישה גורמים נפרדים המזוהים עם רוסיה מבצעים יותר מ-237 מתקפות סייבר נגד אוקראינה. קמפיינים אלה שאפו לפגוע בשירותים ובמוסדות, לשבש את גישתם של האוקראינים למידע אמין ולזרוע ספקות לגבי הנהגת המדינה.

זרקור על מבצעי השפעה במהלך מגפת הקורונה ופלישת רוסיה לאוקראינה

המשך

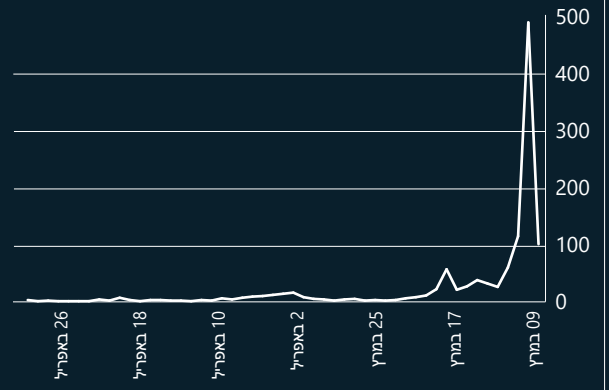
בדוח של Microsoft שפורסם באפריל 2022, הצגנו כיצד בניסיון לכאורה לשלוט בסביבת המידע בקייב, רוסיה שיגרה מתקפת טילים על מגדל טלוויזיה בקייב באותו יום שבו שיגרה תוכנה זדונית הרסנית נגד חברת מדיה אוקראינית גדולה.[12]

בדוגמה נוספת לאופן שבו מתקפות סייבר ומבצעי השפעה מתמזגים, גורם איום רוסי שלח לאזרחים אוקראינים הודעות דואר אלקטרוני שהתיימרו להיות מתושבי מריופול, שבהן האשים את ממשלת אוקראינה בהסלמת המלחמה וקרא לבני ארצם להתקומם נגד הממשלה. הודעות דואר אלקטרוני אלה פנו באופן ספציפי (בשמם) לנמענים, דבר המעיד על כך שייתכן שהמידע שלהם נגנב במתקפת סייבר קודמת הקשורה לריגול. לא נכללו קישורים זדוניים, עובדה המרמזת על כך שהכוונה הייתה מבצעי השפעה טהורים.

הצגת חומר שלכאורה נפרץ, הודלף או רגיש בדרך אחרת היא טקטיקה נפוצה המשמשת גורמים רוסים במבצעי השפעה. לאורך המלחמה באוקראינה, ערוצי מדיה חברתית פרו-רוסיים קידמו את מה שלטענתם היה חומרים שהודלפו או חומרים רגישים באופן אחר ממקורות אוקראינים. חומר שהודלף או רגיש משמש ערוצי מדיה חברתית וכלי תקשורת פרו-רוסיים כחלק מאסטרטגיית השפעה רחבה יותר שמטרתה לפגוע באמון במוסדות ולהטיל ספק בנרטיבים מרכזיים. ניתן לתמרן מידע זה כדי ליצור תעמולה המכוונת נגד אוקראינה והמערב, להפחית את האמון בביטחון הדיגיטלי ולשחוק את התמיכה בסיוע מערבי לאוקראינה.

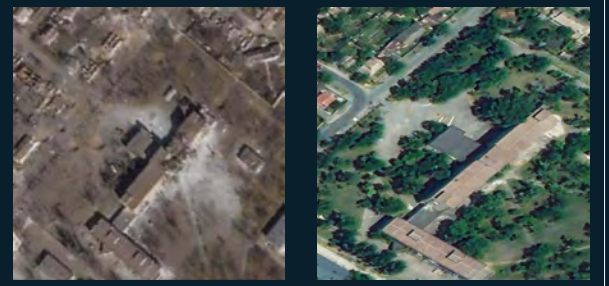
רוסיה השתמשה בהתקפות מידע אחרות כדי לעצב את דעת הקהל לאחר אירועים בשטח כדי לטשטש או לערער עובדות. לדוגמה, ב-7 במרץ, רוסיה הציבה מראש נרטיב באמצעות הגשת תביעה רשמית לאו"ם (UN) כי בית חולים ליולדות במריופול, אוקראינה, רוקן ומשמש כאתר צבאי. ב-9 במרץ הפציצה רוסיה את בית החולים. לאחר פרסום הידיעה על ההפצצה צייץ נציג רוסיה באו"ם, דמיטרי פוליאנסקי, כי סיקור ההפצצה הוא "פייק ניוז" וציטט טענות קודמות של רוסיה בנוגע לשימוש שנעשה בו לכאורה כאתר צבאי. רוסיה דחפה את הנרטיב הזה באופן נרחב באתרי אינטרנט שבשליטתה במשך שבועיים בעקבות המתקפה על בית החולים.

תחומים עם תעבורה
(9 במרץ 2022-30 באפריל 2022)



אתרי תעמולה פרסמו סיפורים על בית החולים ליולדות במשך כשבועיים עם התחדשות קצרה שהחלה ב-1 באפריל 2022. מקור: הבינה המלאכותית של Microsoft ל- Good Lab.

תמונות לוויין של בית חולים פרינטלי במריופול בפברואר ובמרץ 2022



ניתוח תמונת הלוויין של Microsoft עצמה הראה כי בית החולים הפרינטלי הופצץ. התמונה הראשונה היא מה-24 בפברואר 2022 והשנייה היא מה-24 במרץ 2022. מקור הצילום: Planet Labs.

טיוח הזוועות על ידי רוסיה נמשך ככל שהמלחמה התקדמה. לדוגמה, בסוף יוני 2022, כלי תקשורת ומשפיענים רוסיים הציגו את הפצצת הקניון כמוצדקת והכרחית, וטענו באופן שקרי שהוא אינו בשימוש כקניון, אלא משמש כמחסן נשק עבור כוחות ההגנה הטריטוריאליים האוקראינים.[13] מספר בלוגרים התומכים בקרמלין ב-Telegram פרסמו והעצימו תכנים המחזקים את נרטיב "הדגל הכוזב", כאשר בלוגרים הצביעו על אינדיקטורים לכאורה של זיוף, כולל נוכחותם של אנשים במדי צבא בצילומים מהזירה[14] והיעדרן של נשים מהצילומים.[15] רוסיה השיקה קמפיינים תוך הסתמכות על מערכת מובנית של שליחי ואמצעי תעמולה. העצמתם של סיפורים אלה ברשת מספקת לרוסיה את היכולת להסיט את האשמה על הבמה הבינלאומית ולהימנע מנטילת אחריות.

מדינות כמו רוסיה מבינות את ערך השימוש במידע המגיע ממקורות סגורים כדי להשפיע על תפיסות הציבור, ומשתמשות בקמפיינים של "פריצה והדלפה" כדי להפיץ נרטיבים נגדיים ולזרוע חוסר אמון.

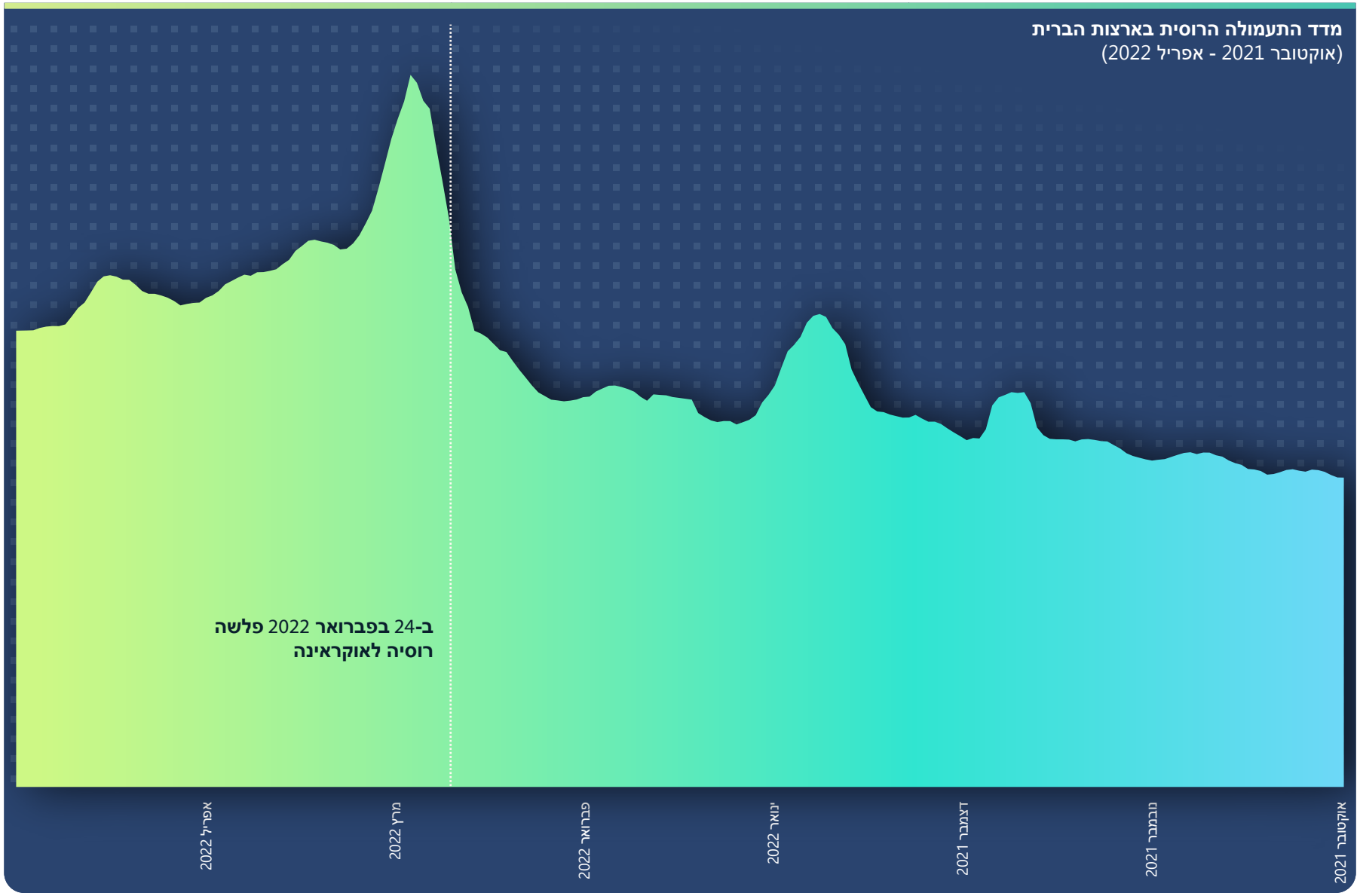
קישורים למידע נוסף

- הגנה על אוקראינה: לקחים ראשונים ממלחמת הסייבר | Microsoft On the Issues
- סקירה כללית של פעילות תקיפות הסייבר של רוסיה באוקראינה | דוח מיוחד של Microsoft
- שיבוש מתקפות סייבר המכוונות לאוקראינה | Microsoft On the Issues

מעקב אחר מדד התעמולה הרוסית

בינואר 2022, כמעט אלף אתרים אמריקאים הפנו תנועה לאתרי תעמולה רוסיים. הנושאים הנפוצים ביותר באתרי תעמולה רוסיים המכוונים לקהל אמריקאי היו המלחמה באוקראינה, הפוליטיקה הפנימית בארה"ב (פרו-טראמפ או פרו-ביידן) ונרטיבים הקשורים לנגיף הקורונה ולחיסונים.

מדד התעמולה הרוסי (RPI) עוקב אחר זרימת החדשות מכלי תקשורת ומגורמים המתפקדים כמגברים שבשליטת המדינה הרוסית ובחסותה כשיעור מכלל תעבורת החדשות באינטרנט. ניתן להשתמש ב-RPI כדי לשרטט את צריכת התעמולה הרוסית ברחבי האינטרנט ובאזורים גיאוגרפיים שונים על ציר זמן מדויק. עם זאת, Microsoft מציינת כי אנו יכולים לצפות רק בתעמולה הרוסית שפורסמה באתרי אינטרנט שזוהו בעבר. אין לנו תובנות לגבי תעמולה בסוגים אחרים של אתרים, כולל אתרי חדשות סמכותיים, אתרים לא מזוהים וקבוצות של רשתות חברתיות.



מעקב אחר מדד התעמולה הרוסית

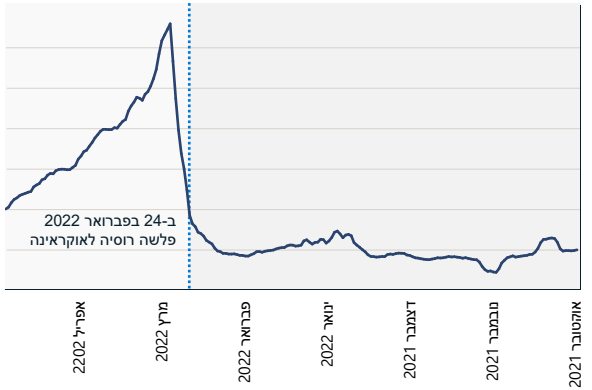
המשך

מדד התעמולה הרוסית: אוקראינה

כשהחלה המלחמה באוקראינה, ראינו עלייה של 216 אחוזים בתעמולה הרוסית, שהגיעה לשיאה ב-2 במרץ. התרשים שלהלן מראה כיצד העלייה הפתאומית הזו התרחשה במקביל לפלישה. שני הגרפים מראים כיצד התעמולה הרוסית זינקה זמן קצר לאחר תחילת הפלישה.

RPI, אוקראינה

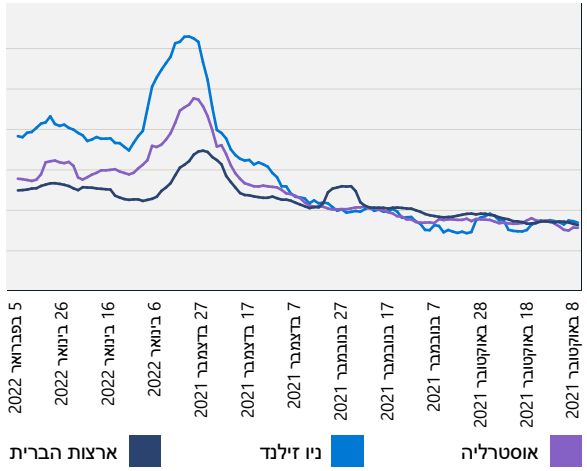
(7 באוקטובר 2021-30 באפריל 2022)



מדד התעמולה הרוסית: ניו זילנד לעומת אוסטרליה וארצות הברית

הערכה של ה-RPI בניו זילנד הראתה זינוק בסוף 2021 שהיה קשור לתעמולה בנושא נגיף הקורונה. זינוק זה בצריכת התעמולה הרוסית בניו זילנד קדם לעלייה במחאה הציבורית בתחילת 2022 בוולינגטון. זינוק שני היה קשור בבירור לפלישה הרוסית לאוקראינה ועלה על מדדי ה-RPI של אוסטרליה וארצות הברית.

RPI, ניו זילנד לעומת אוסטרליה וארצות הברית



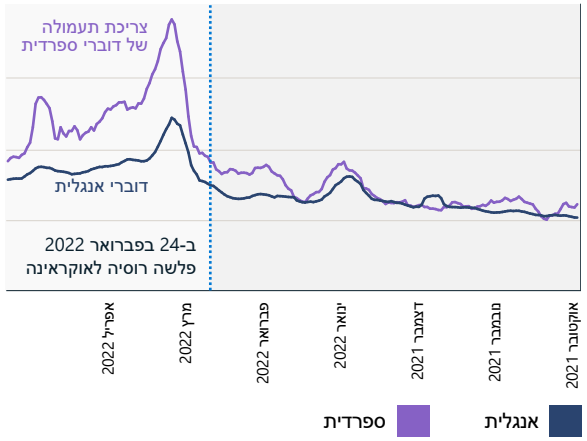
צריכת התעמולה הרוסית בניו זילנד דמתה לצריכה באוסטרליה עד השבוע הראשון של דצמבר 2021. לאחר דצמבר, צריכת התעמולה הרוסית בניו זילנד עלתה ביותר מ-30 אחוזים ביחס לצריכה באוסטרליה ובארצות הברית.

מדד התעמולה הרוסית בארצות הברית: אנגלית וספרדית

ה-RPI גם עוקב אחר תעמולה בשפות שונות. מספר ערוצי תקשורת, כולל RT ו-Sputnik News, זמינים ביותר מ-20 שפות. אלה כוללות אנגלית, ספרדית, גרמנית, צרפתית, יוונית, איטלקית, צ'כית, פולנית, סרבית, לטבית, ליטאית, מולדבית, בלארוסית, ארמנית, אוסטיאנית, גיאורגית, אזרבייג'נית, ערבית, טורקית, פרסית ודארי.

הגרף הבא מראה כי ה-RPI עבור חדשות בשפה הספרדית בארצות הברית הוא הרבה יותר גבוה מאשר עבור חדשות בשפה האנגלית.

צריכת התעמולה הרוסית גבוהה פי 2 בקרב דוברי ספרדית



צריכת התעמולה הרוסית בארצות הברית גבוהה פי שניים בקרב דוברי ספרדית.

צריכת התעמולה הרוסית גבוהה באמריקה הלטינית

RT בספרדית הוא אתר החדשות הבינלאומי עם המספר הגבוה ביותר של צפיות בדף ועוקבים ב-Facebook.

מקור: הבינה המלאכותית של Microsoft ל-Good Research Lab

מדיה סינתטית

אנו נכנסים לעידן הזהב של יצירת מדיה מבוססת בינה מלאכותית ותמרונה. אנליסטים של Microsoft מציינים כי הדבר מונע על-ידי שתי מגמות מרכזיות: ריבוי הכלים והשירותים הקלים לשימוש ליצירה מלאכותית של תמונות, סרטוני וידאו, קטעי שמע וטקסט סינתטיים ומציאותיים ביותר, והיכולת להפיץ במהירות תוכן הממוטב לקהלים ספציפיים.

אף אחת מהתפתחויות אלו אינה בעייתית מיסודה בפני עצמה. ניתן להשתמש בטכנולוגיה מבוססת בינה מלאכותית ליצירת תוכן דיגיטלי מהנה ומלהיב, בין אם ביצירת חומרים סינתטיים לגמרי או בשיפור חומרים קיימים. כלים אלה נמצאים בשימוש נרחב על ידי ארגונים לפרסום ותקשורת ועל ידי אנשים פרטיים ליצירת תוכן מרתק עבור העוקבים שלהם. עם זאת, למדיה סינתטית, כאשר היא נוצרת ומופצת מתוך כוונה לפגוע, יש פוטנציאל לגרום נזק חמור לאנשים, לחברות, למוסדות ולחברה. Microsoft הייתה כוח מניע בפיתוח טכנולוגיות ושיטות עבודה, הן באופן פנימי והן ברחבי המערכת האקולוגית הרחבה יותר של המדיה, כדי לצמצם נזק זה.

סעיף זה בוחן תובנות מניתוח של Microsoft לגבי הטכנולוגיה המתקדמת ביותר ליצירת תוכן סינתטי מזיק, הנזקים שעלולים להיווצר אם תוכן זה מופץ באופן נרחב ואמצעי צמצום טכניים שיכולים להגן מפני איומי סייבר מבוססי מדיה סינתטית.

יצירת מדיה סינתטית

תחום הטקסט והמדיה הסינתטיים מתקדם במהירות מדהימה מכיוון שטכניקות שפעם היו אפשריות רק עם משאבי המחשוב העצומים של אולפני סרטים גדולים משולבות כיום באפליקציות טלפון. במקביל, כלים הופכים קלים יותר לשימוש ויכולים ליצור תוכן עם רמה של ריאליזם שיכול להטעות אפילו מומחי מדיה פורנזיים. אנחנו קרובים מאוד להגיע לנקודה שבה כל אחד יוכל ליצור סרטון וידאו סינתטי של כל אחד אומר או עושה משהו. זה לא בלתי סביר להאמין שאנחנו נכנסים לעידן שבו כמות משמעותית של התוכן שאנחנו רואים באינטרנט הוא סינתטי באופן מלא או חלקי ונוצר באמצעות טכניקות AI.

> עם הזמינות של כלים מתוחכמים יותר, קלים לשימוש וזמינים באופן נרחב, יצירת תוכן סינתטי נמצאת במגמת עלייה ובקרוב לא ניתן יהיה להבחין בינה לבין המציאות.

ישנם הרבה כלים מסחריים איכותיים לעריכת תמונות, וידאו ושמע בחינם. ניתן להשתמש בכלים אלה כדי לבצע שינויים פשוטים אך מזיקים פוטנציאלית לתוכן דיגיטלי כגון הוספת טקסט מטעה, החלפת פנים והסרה או שינוי של הקשר. "זיופים זולים" כאלה נמצאים בשימוש נרחב להפצת תוכן זדוני, לקידום אידיאולוגיות פוליטיות ולפגיעה במוניטין. דוגמה ידועה לכך היא הסרטון משנת 2019[16] שבו נראית יו"ר בית הנבחרים של ארה"ב, ננסי פלוסי, מדברת בצורה עילגת ונראית שיכורה. אף על פי שנקבע במהרה כי הסרטון הואט כדי ליצור את האפקט, "הזיוף הזול" התפשט למרחקים לפני שהסרטון וההקשר המקוריים עלו על פני השטח.

גישות מתוחכמות יותר לשינוי תוכן מדיה כוללות יישום של טכניקות AI מתקדמות כדי (א) ליצור מדיה סינתטית גרידא, ו-(ב) לבצע עריכות מתוחכמות יותר של מדיה קיימת. המונח דיפ-פייק משמש לעתים קרובות למדיה סינתטית שנוצרה באמצעות טכניקות AI מתקדמות (השם מגיע מרשתות עצביות עמוקות שבהן משתמשים לעתים). טכנולוגיות אלה מפותחות כאפליקציות, כלים ושירותים עצמאיים ומשולבות בכלי עריכה מסחריים וקוד פתוח מבוססים.

טכנולוגיות כאלה משמשות כנשק על ידי גורמים רעים בתקווה לפגוע באנשים ובמוסדות. דוגמאות לטכניקות דיפ-פייק כוללות:

- **החלפת פנים (וידאו, תמונות)** – החלפת פנים בסרטון וידאו באחרים. ניתן להשתמש בטכניקה זו כדי לנסות להפעיל סחיטה על אדם, חברה או מוסד, או כדי למקם אנשים במקומות או במצבים מביכים.
- **הפעלת בובות (וידאו, תמונות)** – שימוש בסרטון וידאו כדי להנפיש תמונת סטילס או סרטון וידאו שני. כך ניתן ליצור מצב שבו נראה כאילו אדם אמר משהו מביך או מטעה.
- **רשתות יריבות יצירתיות (וידאו, תמונות)** – משפחה של טכניקות ליצירת תמונות פוטוריאליסטיות.
- **מודלי טרנספורמר (וידאו, תמונות, טקסט)** – יצירת תמונות עשירות מתיאורי טקסט.

כיום, טכניקות מתקדמות כאלה המבוססות על בינה מלאכותית עדיין אינן נמצאות בשימוש נרחב במבצעי השפעה בסייבר, אך אנו צופים שהבעיה תגדל ככל שהכלים יהפכו לקלים יותר לשימוש וזמינים יותר.

השפעת המניפולציה של מדיה סינתטית

השימוש בפעולות מידע כדי לגרום נזק או להרחיב את ההשפעה אינו חדש. עם זאת, המהירות שבה מידע יכול להתפשט, וחוסר היכולת שלנו למיין במהירות עובדה מתוך בדיה, פירושם שההשפעה והנזק הנגרמים על ידי זיופים ומדיה זדונית אחרת שנוצרו באופן סינתטי יכולים להיות גדולים בהרבה, כפי שהודגם בדוגמה של פלוסי.

ישנן מספר קטגוריות של נזק שאנו לוקחים בחשבון: הרצת מניות, הונאת תשלומים, vishing (דיוג קולי), התחזות, נזק למותג, פגיעה במוניטין ורשתות botnet. רבות מהקטגוריות הללו דיווחו באופן נרחב על דוגמאות מהעולם האמיתי, דבר שעלול לערער את היכולת שלנו להפריד בין עובדה לבדיה.

איום ארוך-טווח וחתרני יותר הוא על ההבנה שלנו לגבי מה נכון אם איננו יכולים לסמוך עוד על מה שאנחנו רואים ושומעים. מסיבה זו, כל תמונה, קטע שמע או סרטון פוגעניים של דמות ציבורית או פרטית ניתן לדחות כמזויפים – תוצאה הידועה בשם "הדיבידנד של השקרן".[17] מחקר שנערך לאחרונה[18] מראה כי שימוש לרעה זה בטכנולוגיה כבר משמש לתקיפת מערכות פיננסיות, אם כי תרחישים רבים אחרים של שימוש לרעה מתקבלים על הדעת.

מדיה סינתטית

המשך

זיהוי מדיה סינתטית

נעשים מאמצים בתחומי התעשייה, הממשלה והאקדמיה לפתח דרכים טובות יותר לזיהוי ולצמצום המדיה הסינתטית ולשיקום האמון. ישנם מספר נתיבים מבטיחים להמשך הדרך, כמו גם חסמים המחייבים התחשבות.

גישה אחת היא לבנות מערכות מבוססות בינה מלאכותית שיכולות לזהות זיופים – למעשה אלו הן מערכות AI "הגנתיות" כדי להתמודד עם מערכות ה-AI ההתקפיות. זהו תחום של מחקר פעיל שבו המערכות הנוכחיות ליצירת אודיו ווידאו סינתטיים משאירות ממצאים הניתנים לזיהוי על ידי כלים אוטומטיים ואנליסטים פורנזיים מיומנים של מדיה.

למרבה הצער, בעוד שבזיופים הנוכחיים יש פגמים חושפים, הממצאים המדויקים נוטים להיות ספציפיים לכלי או לאלגוריתם מסוים. משמעות הדבר היא שהדרכה על זיופים ידועים אינה כוללת בדרך כלל אלגוריתמים אחרים כפי שהוכח בתחרות פתוחה בשנת 2020 לבניית גלאי תמונות דיפ-פייק.[19] מפתה להגדיל את ההשקעה בפיתוח גלאים מתקדמים יותר, אך Microsoft סקפטית מאוד שהדבר יביא לשיפורים משמעותיים משתי סיבות:

ראשית, יש לנו מודלים פיזיים מצוינים המשקפים את העולם האמיתי. יוצרי הזיופים הנוכחיים מעגלים פינות, והתוצאה היא ממצאים הניתנים לזיהוי, אך דגמים חדשים יותר יהפכו מציאותיים יותר ויותר. אין שום דבר מיוחד במהותו בסצנה מהעולם האמיתי שצולמה במצלמה שלא ניתן ליצור מודל שלה במחשב.

שנית, אלגוריתמים מתקדמים ליצירת זיופים משתמשים בטכניקה הנקראת רשתות יריבות יצירתיות (GANs) כחלק מתהליך היצירה. GAN מפעיל שתי מערכות AI אחת נגד השנייה באמצעות מחולל ליצירת הזיוף ומפלה (discriminator) לזיהוי תמונות מזויפות ולאימון המחולל. כל השקעה בפיתוח גלאי טוב יותר רק תאפשר למחולל לשפר את איכות הזיופים.

נוף המדיה הסינתטית

גורמים מחסום נמוך לכניסה	**כלים קלים לשימוש**	**כלים מתוחכמים יותר**	**קל להפצה**	
מפיקים שימושים טובים ומזיקים	**ארגונים ומוסדות**	**אנשים פרטיים וצרכנים**	**גורמים זדוניים שיגרמו נזק**	
הפצה מהירות חסרת תקדים	**הגברה במדיה החברתית**	**הודעות דואר אלקטרוני ופרסומות ממוקדות**	**קובצי שמע באמצעות דואר קולי**	**ישירות מהמקור**
השפעות שחיקת האמון	**פגיעה במוניטין האישי**	**הונאה ונזקים כספיים אחרים**	**נזק לארגון או למותג**	**הרצת מניות**
צמצום פתרונות מבטיחים	**מערכות AI מתקדמות לזיהוי**	**מקור דיגיטלי**	**מאמצים חוצי תעשיות**	

מדיה סינתטית

המשך

מקור לנכסים דיגיטליים

אם לא ניתן לסמוך על זיהוי זיופים, מה אפשר לעשות כדי להגן מפני השימושים המזיקים של מדיה סינתטית? טכנולוגיה מתפתחת חשובה אחת היא מקור דיגיטלי – מנגנון המאפשר ליוצרי מדיה דיגיטלית את היכולת לאשר נכס ומסייע לצרכנים לזהות אם הנכס הדיגיטלי טופל שלא כדין. מקור דיגיטלי הינו חשוב במיוחד בהקשר של רשתות המדיה החברתית של ימינו בהתחשב במהירות שבה תוכן יכול לנוע באינטרנט ובהזדמנות עבור גורמים רעים לתמרן תוכן בקלות.

טכנולוגיית מקור דיגיטלי היא גרסה מודרנית של חתימת מסמכים קריפטוגרפית, שנועדה לתעד את המקור, היסטוריית העריכה והמטא-נתונים של אובייקטים בזמן שהם זורמים באינטרנט של ימינו. החזון והשיטות הטכניות כדי לאפשר סוג זה של הסמכת מדיה מקצה לקצה המוגנת מפני שימוש שלא כדין פותחו על-ידי צוותי חוקרים ומדענים ב-Microsoft. אנו מובילים במשותף שותפות חוצת תעשיות שמטרתה להפיח חיים בטכנולוגיית מקור המדיה ב-Project Origin (שנוסדה על-ידי Microsoft, BBC, CBC/Radio-Canada וה-New York Times) ועוסקים ביוזמת אותנטיות התוכן (שנוסדה על-ידי Adobe). Microsoft גם עבדה עם שותפים בשירותי הטכנולוגיה והמדיה כדי להקים את The Coalition למקור תוכן ואותנטיות (C2PA). C2PA הוא ארגון תקנים שפרסם לאחרונה את מפרט המקור הדיגיטלי המתקדם ביותר לשימוש עם נכסי מדיה הכוללים תמונות, קטעי וידאו, אודיו וטקסט.

אובייקט התומך ב-C2PA נושא מניפסט המגן על האובייקט ועל המטה-נתונים מפני טיפול שלא כדין, והאישור הנלווה מזהה את המפרסם.

המדיה הסינתטית לא נועדה במקור לגרום נזק, אך היא מנוצלת על ידי גורמים רעים כדי לערער את האמון באנשים ובמוסדות.

מקור דיגיטלי הוא טכנולוגיה מתפתחת ומבטיחה שיש לה פוטנציאל לעזור לשקם את האמון של אנשים בתוכן מדיה מקוון על ידי אישור מקורו של נכס מדיה.

פתרונות הזמינים לציבור המבוססים על מפרט C2PA מופיעים כתכונה חדשה במוצרים קיימים או כאפליקציות ושירותים עצמאיים חדשים. אנו מצפים שרוב כלי הלכידה, העריכה והיצירה הנפוצים יתמכו ב-C2PA בעוד מספר שנים. הדבר מהווה הזדמנות עבור ארגונים לקבוע את הצרכים והשימושים שלהם למקור דיגיטלי כיום, ולדרוש את שכבת הגנה נוספת זו בכלים שבהם הם משתמשים בזרימות עבודה קיימות.

תובנות מעשיות

1. יש לנקוט צעדים יזומים כדי להגן על הארגון מפני איומי מידע מטעה באמצעות התחשבות יזומה בתגובות יחסי הציבור והתקשורת.
2. יש להשתמש בטכנולוגיית מקור כדי להגן על תקשורת רשמית.

קישורים למידע נוסף

- צעד מבטיח קדימה בנושא הדיסאינפורמציה | Microsoft On the Issues
- אבן דרך שהושגה, ב-31 בינואר 2022
- Microsoft ALT Innovation | Project Origin
- הקואליציה למען מקור תוכן ואותנטיות (C2PA)
- גילוי פרטים טכניים אודות המערכת ש-Project Origin משתמש בה לאימות מדיה | Microsoft ALT Innovation

900%

עלייה משנה לשנה בהתפשטות הדיפ-פייק מאז 2019.[20]

גישה הוליסטית להגנה מפני מבצעי השפעה בסייבר

Microsoft בונה על תשתית מודיעין איומי הסייבר שלה שכבר בשלה כדי לפתח תצוגה רחבה וכוללת יותר של מבצעי השפעה בסייבר.

אנו משתמשים במסגרת לאסטרטגיות תגובה וצמצום מוצעות כדי להילחם באיום הנשקף ממבצעים, שניתן לחלק לארבעה עמודי תווך מרכזיים: גילוי, שיבוש, הגנה והרתעה.

בנוסף, Microsoft אימצה ארבעה עקרונות כדי לעגן את העבודה שלנו במרחב זה. הראשון הוא מחויבות לכבד את חופש הביטוי ולשמור על יכולתם של לקוחותינו ליצור, לפרסם ולחפש מידע באמצעות הפלטפורמות, המוצרים והשירותים שלנו. השני הוא שאנו פועלים באופן יזום למניעת השימוש בפלטפורמות ובמוצרים שלנו לצורך הגברת עוצמתם של אתרים ותכנים של השפעה זרה בסייבר. השלישי הוא שלא נרוויח במכוון מתכנים או גורמים של השפעה זרה בסייבר. והאחרון הוא שאנו נותנים עדיפות להצפת תוכן כדי להתמודד עם מבצעי השפעה זרה בסייבר על ידי שימוש בנתונים פנימיים ומהימנים של צד שלישי על המוצרים שלנו.

זיהוי

כמו בהגנת סייבר, הצעד הראשון בהתמודדות עם מבצעי השפעה זרה בסייבר הוא פיתוח היכולת לזהות אותם. אף חברה או ארגון יחידים לא יכולים לקוות להשיג בכוחות עצמם את ההתקדמות הנדרשת. שיתוף פעולה חדש ורחב יותר במגזר הטכנולוגי יהיה חיוני, כאשר ההתקדמות בניתוח מבצעי השפעה בסייבר ודיווח עליהם תישען במידה רבה על תפקידה של החברה האזרחית, כולל במוסדות אקדמיים ובארגונים ללא כוונת רווח.

מתוך הכרה בתפקיד זה, החוקרים ג'ייק שפירו ואלישיה וואנלס מאוניברסיטת פרינסטון וקרן קרנגי לשלום בינלאומי, בהתאמה, מיפו את התוכניות להשקת "המכון לחקר סביבת המידע" (IRIE) החדש.
בתמיכת Microsoft, ה-Knight Foundation ו-Craig Newmark Philanthropies, ה-IRIE ייצור מוסד מחקר כולל עם בעלי עניין רבים במודל של הארגון האירופי למחקר גרעיני (CERN). הוא ישלב מומחיות בעיבוד וניתוח נתונים כדי להאיץ ולהרחיב תגליות חדשות במרחב זה. הממצאים ישותפו כדי ליידע את קובעי המדיניות, חברות הטכנולוגיה והצרכנים באופן רחב יותר.

הגנה

עמוד התווך האסטרטגי השני הוא חיזוק ההגנה הדמוקרטית, עדיפות ארוכת שנים הזקוקה להשקעה ולחדשנות. עליו לקחת בחשבון את האתגרים שהטכנולוגיה הציבה לדמוקרטיה, ואת ההזדמנויות שהטכנולוגיה יצרה להגנה על חברות דמוקרטיות בצורה יעילה יותר.

מסגרת האסטרטגיה של Microsoft נועדה לסייע לבעלי עניין חוצי-מגזרים לזהות, לשבש, להגן ולהרתיע מפני תעמולה – במיוחד קמפיינים של תוקפים זרים.

ראוי להתחיל עם אחד האתגרים הטכנולוגיים הגדולים של תקופתנו – השפעת האינטרנט והפרסום הדיגיטלי על העיתונות המסורתית. מאז המאה ה-18, עיתונות חופשית ועצמאית מילאה תפקיד מיוחד בתמיכה בכל דמוקרטיה על פני כדור הארץ – חשפה שחיתויות, תיעדה מלחמות והאירה את האתגרים החברתיים הגדולים ביותר של זמן זה וכל זמן אחר. עם זאת, האינטרנט פגע בחדשות המקומיות בכך שטרף את ההכנסות מפרסום ופיתה את המנויים בתשלום. עיתונים מקומיים רבים קרסו.
אחת התובנות הרבות מעבודתנו האחרונה היא שעיירות שאין בהן עיתון חשופות ללא ידיעתן ובאופן בלתי נמנע לנפח גדול מהממוצע של תעמולה זרה. מסיבות אלה, אחד מעמודי המגן הקריטיים של הדמוקרטיה חייב לחזק את העיתונות המסורתית ואת העיתונות החופשית, במיוחד ברמה המקומית. זה דורש השקעה מתמשכת וחדשנות שחייבות לשקף את הצרכים המקומיים של מדינות ויבשות שונות. בעיות אלה אינן קלות, והן דורשות גישות של ריבוי בעלי עניין, ש-Microsoft וחברות טכנולוגיה אחרות תומכות בהן יותר ויותר.

אנחנו צריכים גם חידושים חדשים במדיניות הציבורית, שצריכה להיות בראש סדר העדיפויות הציבורי. זה יכול לכלול חוקים המאפשרים למפרסמים לנהל משא ומתן על הכנסות מפרסום באופן קולקטיבי עם חברות טכנולוגיה, וחקיקה המספקת זיכויי מס כדי לשחרר את חדרי החדשות המקומיים מחלק ממסי השכר שלהם לעיתונאים שהם מעסיקים. עיתונאים זקוקים לכלים רבים אחרים למלאכתם, כולל היכולת להפריד בין תוכן ממקורות לגיטימיים לתוכן ממקורות מזויפים.

יש גם צורך שמתפתח במהירות לעזור לצרכנים לפתח יכולת מתוחכמת יותר לזיהוי פעולות מידע המונחות על ידי מדינות. בעוד שאולי זה נראה מרתיע, זה דומה לעבודה שמגזר הטכנולוגיה עושה זה זמן רב כדי להילחם באיומי סייבר אחרים. לדוגמה, חינוך הצרכנים להסתכל בקפידה רבה יותר על כתובת דואר אלקטרוני כדי לעזור לזהות דואר זבל (ספאם) או תקשורת מזויפת אחרת. יוזמות בארצות הברית – כגון ה-News Literacy Project (פרויקט אוריינות החדשות) וה-Trusted Journalism (העיתונות המהימנה).

איום ארוך-טווח וחתרני יותר הוא הנזק להבנה שלנו לגבי מה נכון אם איננו יכולים לסמוך עוד על מה שאנחנו רואים ושומעים.

גישה הוליסטית להגנה מפני מבצעי השפעה בסייבר

המשך

Program – עוזרים לפתח צרכנים מושכלים יותר של חדשות ומידע. ברחבי העולם, טכנולוגיה חדשה כמו תוסף הדפדפן של NewsGuard יכולה לעזור לקדם את המאמץ הזה הרבה יותר מהר.

זה גם צריך להזכיר לנו שחלק מהבסיס לדמוקרטיה הוא חינוך לאזרחות. כמו תמיד, המאמץ הזה צריך להתחיל בבתי הספר. אבל אנחנו חיים בעולם שדורש מאיתנו לקבל חינוך מתמשך לאזרחות לאורך כל חיינו. ההתחייבות החדשה ל'אזרחות בעבודה', בהובלת 'המרכז ללימודים אסטרטגיים ובינלאומיים', וש-Microsoft הייתה חתומה ושותפה ראשונה בה, מבקשת להמריץ מחדש את אוריינות האזרחות בתוך קהילות ארגוניות. זוהי דוגמה טובה להיקף ההזדמנויות לחיזוק ההגנות הדמוקרטיות שלנו.

לשבש

בשנים האחרונות, היחידה לפשעי מחשב (DCU) של Microsoft שיכללה טקטיקות ופיתחה כלים לשיבוש איומי סייבר, החל מתוכנות כופר ועד רשתות botnet והתקפות של מדינות. למדנו לקחים קריטיים רבים, החל מתפקיד השיבוש האקטיבי בהתמודדות עם מגוון רחב של מתקפות סייבר.

כאשר אנו חושבים על התמודדות עם מבצעי השפעה בסייבר, שיבוש עשוי לשחק תפקיד חשוב אף יותר והגישה הטובה ביותר לשיבוש הולכת ומתבהרת. התרופה היעילה ביותר להונאה רחבת היקף היא שקיפות. זו הסיבה ש-Microsoft הגדילה את יכולתה לזהות ולשבש מבצעי השפעה מדינתיים על ידי רכישת Miburo Solutions, חברה מובילה לניתוח ומחקר איומי סייבר המתמחה באיתור ותגובה למבצעי השפעה זרה בסייבר.

הניסיון שלנו הראה שממשלות, חברות טכנולוגיה וארגונים לא ממשלתיים צריכים לייחס מתקפות סייבר בזהירות ועם ראיות רבות. הבנת ההשפעה של שיבוש כזה היא חיונית ויכולה לסייע אף יותר בשיבוש השפעה בסייבר. אנו עדים לשיתוף המידע של ממשלת ארה"ב לקראת הפלישה הרוסית לאוקראינה, שהפך שקיפות לפעולה יעילה – כגון חשיפת תוכניות רוסיות, כולל קמפיינים ספציפיים כמו מזימה להשתמש בסרטון גרפי מזויף.

כפי שניתן לראות בפרסום של מכון CyberPeace בז'נבה בקיץ שעבר על מתקפות סייבר מתמשכות בתוך אוקראינה ומחוצה לה, יש הזדמנות למגוון רחב של ארגוני חברה אזרחית וארגונים במגזר הפרטי לקדם שקיפות בכל הנוגע למבצעי השפעה בסייבר. דיווחים אמינים על פעולות חדשות שהתגלו ומתועדות היטב יכולים לעזור לציבור להעריך טוב יותר את מה שהוא קורא, רואה ושומע, במיוחד באינטרנט. לשם כך, Microsoft תתבסס ותרחיב את דוחות הסייבר הקיימים שלה ותפרסם דוחות, נתונים ועדכונים חדשים הקשורים למה שאנו מגלים על מבצעי השפעה בסייבר, כולל הצהרות ייחוס בעת הצורך. אנו נפרסם דוח שנתי המשתמש בגישה מבוססת נתונים כדי לבחון את השכיחות של פעולות מידע זרות ברחבי החברה ואת הצעדים הבאים להבטחת שיפור מצטבר. כמו כן, נשקול צעדים נוספים הנשענים על סוג זה של שקיפות.

תפקידו של הפרסום הדיגיטלי חשוב במיוחד, למשל, שכן פרסום יכול לסייע במימון פעולות זרות ובמקביל ליצור מראית עין של לגיטימציה לאתרי תעמולה בחסות זרה. יהיה צורך במאמצים חדשים כדי לשבש את התזרימים הפיננסיים הללו.

הרתעה

לבסוף, איננו יכולים לצפות ממדינות לשנות התנהגות אם אין נטילת אחריות על הפרת הכללים הבינלאומיים. אכיפת אחריות כזו היא אחריות ממשלתית ייחודית. עם זאת, באופן הולך וגובר, פעולה של בעלי עניין מרובים ממלאת תפקיד חשוב בחיזוק ובהרחבה של נורמות בינלאומיות. יותר מ-30 פלטפורמות מקוונות, מפרסמים ובעלי אתרים – כולל Microsoft – חתמו על 'קוד הנוהג' של 'הנציבות האירופית' בנושא דיסאינפורמציה שעודכן לאחרונה, והסכימו להתחייבויות מחוזקות להתמודדות עם אתגר הולך וגדל זה. בדומה לקריאת פריז (Paris Call) האחרונה, קריאת קרייסטצ'רץ' (Christchurch Call) וה'הצהרה על עתיד האינטרנט', פעולה רב-צדדית ורבת בעלי עניין יכולה להפגיש בין ממשלות וציבור בין מדינות דמוקרטיות. לאחר מכן, ממשלות יכולות לבנות על הנורמות והחוקים הללו לקידום נטילת האחריות שהדמוקרטיות בעולם זקוקות וראויות לה.

באמצעות שקיפות רדיקלית מהירה, ממשלות וחברות דמוקרטיות יכולות להקהות ביעילות קמפיינים של השפעה על ידי ייחוס המקור להתקפות מדינתיות, יידוע הציבור ובניית אמון במוסדות.

הגדלנו את היכולת הטכנית לזיהוי ולשיבוש מבצעי השפעה זרה ואנו מחויבים לדווח בשקיפות על מבצעים אלה כמו שאנו מדווחים על מתקפות סייבר.

תובנות מעשיות

1. יש להטמיע שיטות עבודה חזקות להיגיינה דיגיטלית ברחבי הארגון.
2. יש לשקול דרכים להפחתת כל הפעלה לא מכוונת של מבצעי השפעה בסייבר על ידי העובדים או על ידי שיטות העבודה העסקיות. זה כולל צמצום האספקה לאתרי תעמולה זרים ידועים.
3. יש לתמוך בקמפיינים של אוריינות מידע ומעורבות אזרחית כמרכיב מרכזי כדי לעזור לחברות להתגונן מפני תעמולה והשפעה זרה.
4. יש ליצור קשר ישיר עם קבוצות רלוונטיות לתעשייה הפועלות לטיפול במבצעי השפעה.

הערות סיום

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. הגנה על אוקראינה: לקחים ראשונים ממלחמת הסייבר (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. דוברת משרד החוץ הרוסי Maria Zakharova: 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. טענות קרמנצ'וג של רוסיה מול הראיות – bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. בדיקת עובדות: הסרטון של ננסי פלוסי "שיכורה" עובר מניפולציה | 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. תוצאות אתגר זיהוי דיפ-פייק: יוזמה פתוחה לקידום בינה מלאכותית (facebook.com)
20. דיפ-פייק 2020: נקודת המפנה (The Tipping Point), יוהנס טמקאנד, ג'ון תומאס וכריסטיאן פיטרסון, אוקטובר 2020

עמידות סייבר

הבנת הסיכונים והתגמולים של המודרניזציה הופכת להיות חיונית לגישה הוליסטית לעמידות.

סקירה כללית על

עמידות סייבר

אבטחת סייבר היא גורם מאפשר עיקרי להצלחה טכנולוגית. ניתן להגיע לחדשנות ופרודוקטיביות משופרת רק על ידי הטמעת אמצעי אבטחה שהופכים ארגונים לעמידים ככל האפשר מפני התקפות מודרניות.

המגפה אתגרה אותנו ב-Microsoft לשנות את נוהלי וטכנולוגיות האבטחה כדי להגן על העובדים שלנו בכל מקום שבו הם עובדים. בשנה האחרונה המשיכו גורמי האיום לנצל את הפגיעויות שנחשפו במהלך המגפה והמעבר לסביבת עבודה היברידית. מאז, האתגר העיקרי שלנו הוא ניהול השכיחות והמורכבות של שיטות תקיפה שונות ושל פעילות מדינתית מוגברת.

עמידות סייבר יעילה דורשת גישה הוליסטית ואדפטיבית כדי לעמוד באיומים המתפתחים על שירותי ותשתיות הליבה.

מידע נוסף בעמוד 89

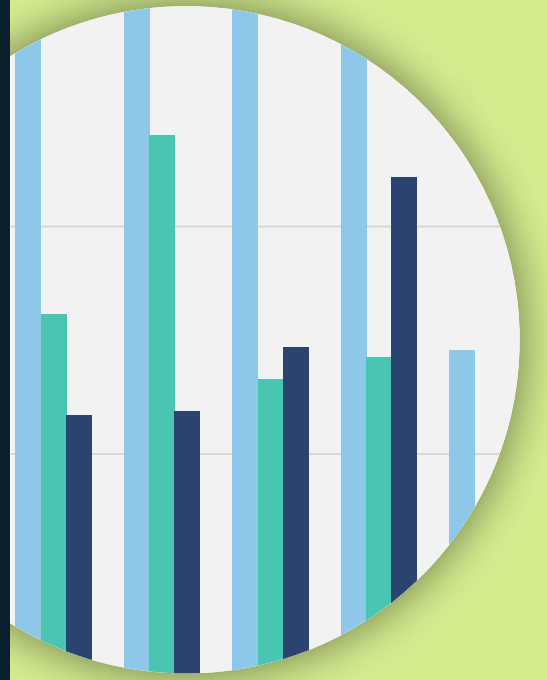
מערכות וארכיטקטורה מודרניות חשובות לניהול איומים בעולם היפר-מחובר.

מידע נוסף בעמוד 90

מערך אבטחה בסיסי הוא גורם מכריע ביעילות פתרונות מתקדמים.

מידע נוסף בעמוד 92

בעוד שהתקפות מבוססות סיסמה הן עדיין המקור העיקרי לחשיפת זהויות, סוגים אחרים של מתקפות צצים.



מידע נוסף בעמוד 93

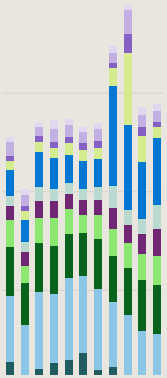
הממד האנושי של עמידות למבצעי השפעה בסייבר הוא היכולת שלנו לעבוד יחד ולשתף פעולה.

מידע נוסף בעמוד 102

את הרוב המכריע של מתקפות הסייבר המוצלחות ניתן היה למנוע על ידי שימוש בהיגיינת אבטחה בסיסית.

מידע נוסף בעמוד 108

בשנה האחרונה חווה העולם פעילות DDoS חסרת תקדים בהיקף, במורכבות ובתדירות.



מידע נוסף בעמוד 98

מבוא

המגפה אתגרה אותנו ב-Microsoft לשנות את נוהלי וטכנולוגיות האבטחה כדי להגן על העובדים שלנו בכל מקום שבו הם עובדים. בשנה האחרונה המשיכו גורמי האיום לנצל את הפגיעויות שנחשפו במהלך המגפה והמעבר לסביבת עבודה היברידית. מאז, האתגר העיקרי שלנו הוא ניהול השכיחות והמורכבות של שיטות תקיפה שונות ושל פעילות מדינתית מוגברת.

פעילות האיומים הדיגיטליים ורמת התחכום של מתקפות הסייבר עולה מדי יום. רבות מההתקפות המורכבות של ימינו מתמקדות בפגיעה בארכיטקטורות של זהויות, בשרשראות אספקה ובגורמי צד שלישי עם דרגות שונות של בקרות אבטחה. בפרט, ראינו שהתקפות דיוג זהות הן איום ברור ונוכח. עם זאת, סוגים אלה של התקפות אינם מצליחים בדרך כלל עם ניהול זהויות טוב, בקרה מפני דיוג ושיטות עבודה לניהול נקודות קצה. כתוצאה מכך, עלינו לזכור את היסודות: תשעים ושמונה אחוזים מההתקפות ניתנות לעצירה באמצעות אמצעי היגיינה בסיסיים. ב-Microsoft, אנו מנהלים זהויות ומכשירים כחלק מגישת 'אפס אמון' שלנו, הכוללת גישה עם הרשאות מינימליות ואישורים עמידים בפני דיוג כדי לעצור ביעילות את גורמי האיום ולשמור על הנתונים שלנו מוגנים.

כיום, אפילו גורמי איום חסרי כישורים טכניים מתוחכמים יכולים לבצע התקפות הרסניות להפליא, כאשר הגישה לטקטיקות, טכניקות ונהלים מתקדמים הופכת לזמינה באופן נרחב בכלכלת פשעי הסייבר. המלחמה באוקראינה המחישה כיצד גורמים מדינתיים הסלימו את פעולות הסייבר ההתקפי שלהם באמצעות שימוש מוגבר בתוכנות כופר. תוכנות כופר הן כיום תעשייה מתוחכמת עם גורמי איום המשתמשים בטקטיקות סחיטה כפולות או משולשות כדי לחלץ תשלום ומפתחים המציעים תוכנות כופר כשירות (RaaS). עם RaaS, גורמי איום משתמשים ברשת שותפה כדי לבצע התקפות, מורידים את חסם הכניסה עבור פושעי סייבר פחות מיומנים, ובסופו של דבר, מרחיבים את מאגר התוקפים.

כתוצאה מכך, Microsoft תכננה תוכנית לחיסול תוכנות כופר. מטרת התוכנית היא לתקן פערים בבקרות ובכיסוי, לתרום לשיפורים בתכונות עבור שירותים, ולפתח מדריכי שחזור עבור מרכז תפעול האבטחה וצוותי ההנדסה שלנו למקרה של מתקפת כופר.

ההתקפות האחרונות על שרשרת האספקה וספקים של צד שלישי מצביעות על נקודת מפנה משמעותית בתעשייה. ההפרעה שהתקפות אלה גורמות ללקוחות, לשותפים, לממשלות שלנו ול-Microsoft ממשיכה לגבור, וממחישה את החשיבות של מיקוד תשומת הלב בעמידות הסייבר ובשיתוף הפעולה בין בעלי עניין באבטחה. יריבים מתמקדים גם במערכות מקומיות, ומחזקים את הצורך של ארגונים לנהל פגיעויות שמציגות מערכות מדור קודם על-ידי מודרניזציה והעברת תשתיות לענן, שבו האבטחה איתנה יותר.

אנו חיים בעידן שבו אבטחה היא גורם מפתח להצלחה טכנולוגית. ניתן להגיע לחדשנות ופרודוקטיביות משופרת רק על ידי הטמעת אמצעי אבטחה שהופכים ארגונים לעמידים ככל האפשר מפני התקפות מודרניות. ככל שהאיומים הדיגיטליים גדלים ומתפתחים, חיוני לבנות עמידות סייבר במארג של כל ארגון.

ברט ארסנולט
מנהל אבטחת מידע ראשי

עמידות סייבר: יסוד חיוני של חברה מחוברת

המהפכה בטכנולוגיה הדיגיטלית גרמה לארגונים להפוך למחוברים יותר ויותר הן באופן שבו הם פועלים והן בשירותים שהם מציעים. ככל שהאיומים בנוף הסייבר מתרבים, בניית עמידות סייבר במארג הארגון היא קריטית לא פחות מהעמידות הפיננסית והתפעולית.

הטרנספורמציה הדיגיטלית שינתה לעד את האופן שבו ארגונים מקיימים אינטראקציה עם לקוחות, שותפים, עובדים ובעלי עניין אחרים. טכנולוגיות חדשות מספקות הזדמנויות עצומות ליצירת קשר עם אנשים, לחולל שינוי במוצרים ולמטב את התפעול. המגפה האיצה את הטרנספורמציה הדיגיטלית על ידי הנעת טכנולוגיות חדשניות המאפשרות לאנשים לשתף פעולה בדרכים חדשות ומכל מקום.

ככל שאיומי הסייבר הופכים אנדמיים, מניעת פגיעתם בארגונים הופכת לקשה יותר בעולמנו "המחובר תמיד". עמידות סייבר מייצגת את יכולתו של הארגון להמשיך לפעול ולשמור על צמיחה מואצת למרות מטחי ההתקפות. מניעה חייבת להיות מאוזנת עם יכולות הישרדות והתאוששות וממשלות וארגונים מפתחים מודלים מקיפים החורגים מעבר לאבטחה ופרטיות כדי להגן על נכסים, נתונים ומשאבים אחרים כחלק מעמידות הסייבר.

פיתוח גישה הוליסטית לעמידות סייבר

עמידות סייבר דורשת גישה הוליסטית, אדפטיבית וגלובלית שיכולה להתמודד עם האיומים המתפתחים על שירותי ותשתיות הליבה, כולל:

- היגיינת סייבר בסיסית כפי שמתוארת בעקומת הפעמון של עמידות הסייבר שלנו.
- הבנה וניהול פשרות הסיכון/תגמול של טרנספורמציה דיגיטלית.
- יכולות תגובה בזמן אמת המאפשרות זיהוי יזום של איומים ופגיעויות.
- הגנה מפני התקפות ידועות ופעילות מונעת מפני וקטורים חדשים וצפויים של התקפה, כולל יכולת תיקון אוטומטי.
- צמצום ההשפעה של התקפות ואסונות באמצעות בידוד ופילוח תקלות.
- שחזור ויתירות אוטומטיים במקרה של שיבוש.
- מתן עדיפות לבדיקות תפעוליות כדי למצוא פערים ולהבין את תחומי האחריות ויחסי התלות המשותפים במשאבים חיצוניים, כגון פתרונות אבטחה מבוססי ענן.

תוכנית יעילה לעמידות סייבר מתחילה ביסודות המשאבים כגון הבנת השירותים הזמינים והחזקה בקטלוג אמין של משאבים שניתן לפנות אליו במקרה של שיבוש. בהסתמך על בסיס זה, על התוכנית להיות מסוגלת להעריך את האפקטיביות שלה, למדוד את ביצועי השירותים הקריטיים ואת יחסי התלות שלהם, לבדוק ולאמת יכולות בשירותים המקומיים ובשירותי ענן, ולהזין שיפור מתמיד לאורך מחזור החיים הדיגיטלי של הארגון.

כדי לספק גישה הוליסטית, אנו משתפים פעולה עם ארגונים כדי לזהות את השירותים המקומיים והמקוונים הקריטיים ביותר שלהם, התהליכים העסקיים, יחסי התלות, כוח האדם, המוכרים והספקים. כמו כן, אנו שואפים לזהות נכסים ומשאבים הקשורים לציפיות הלקוחות והשוק, התחייבויות רגולטוריות וחוזיות ותפעול פנימי. כאשר משאבים קריטיים אלה מזוהים, מאמצים מקבילים צריכים לזהות ולנטר איומים, שיבושים, וקטורים פוטנציאליים של תקיפה ופגיעויות במערכת ובתהליך. היכולת לעשות זאת תחת המחסור הנוכחי במיומנויות דורשת קפדנות בתעדוף המבוסס על הסיכון הכולל הנשקף לארגון.

סוג זה של גישה הוליסטית צריך להיות אדפטיבי על רקע נוף האיומים המתפתח ללא הרף, במטרה להניע שיפור ביצועים מדיד, קיצור הזמן הנדרש לזיהוי, תגובה והתאוששות, והפחתת רדיוס ההשפעה במקרה של שיבוש. הגישה חייבת גם להכיר בקישוריות הגוברת של האיומים. לדוגמה, תוצאתו של אירוע אבטחה עלולה להיות פריצת נתונים עם השלכות על הפרטיות, שתחייב שיתוף פעולה בין צוותים פנימיים וחיצוניים רבים כדי להגיב במהירות ולמזער את ההשפעה.

> עמידות סייבר היא היכולת של הארגון להמשיך בפעילות ולשמור על האצת הצמיחה למרות השיבושים, כולל מתקפות סייבר.

תובנות מעשיות

1. יש לבנות ולנהל מערכות טכנולוגיות המגבילות את ההשפעה של פריצה ומאפשרות להן להמשיך לפעול בצורה מאובטחת ויעילה, גם אם הפריצה מצליחה. יש להתמקד בנכסים קריטיים נפוצים, בתמיכה בזריזות וארכיטקטורה ליכולת הסתגלות (לדוגמה, היברידית ומרובת עננים, מרובת פלטפורמות), לצמצם משטחי תקיפה (לדוגמה, הסרת אפליקציות שאינן בשימוש והקצאת יתר של זכויות גישה), להניח שמשאבים נפרצו ולצפות שהיריבים יתפתחו.
2. בעת תכנון פרויקטים דיגיטליים, יש להביא בחשבון איומים פוטנציאליים לצד הזדמנויות, ותחומי אחריות משותפים לעמידות לאורך שרשרת האספקה של הטכנולוגיה הדיגיטלית, כולל פתרונות אבטחה מבוססי ענן.
3. יש לבנות מערכות להטמעת אבטחה לפי תכנון ולנקוט צעדים כדי לצפות, לזהות, להתמודד, להסתגל ולהגיב לאיומים מתפתחים עתידיים.
4. יש לוודא שמנהיגים עסקיים מתייעצים עם צוותי אבטחה לפי הצורך כדי להבין את הסיכונים הכרוכים בהתפתחויות חדשות. כמו כן, צוותי אבטחה צריכים להביא בחשבון מטרות עסקיות ולייעץ למנהיגים כיצד לפעול להשגתן בצורה מאובטחת.
5. יש לוודא כי קיימים שיטות עבודה ונהלים תפעוליים ברורים לעמידות ארגונית במקרה של אירועי סייבר.

חשיבות המודרניזציה של מערכות וארכיטקטורה

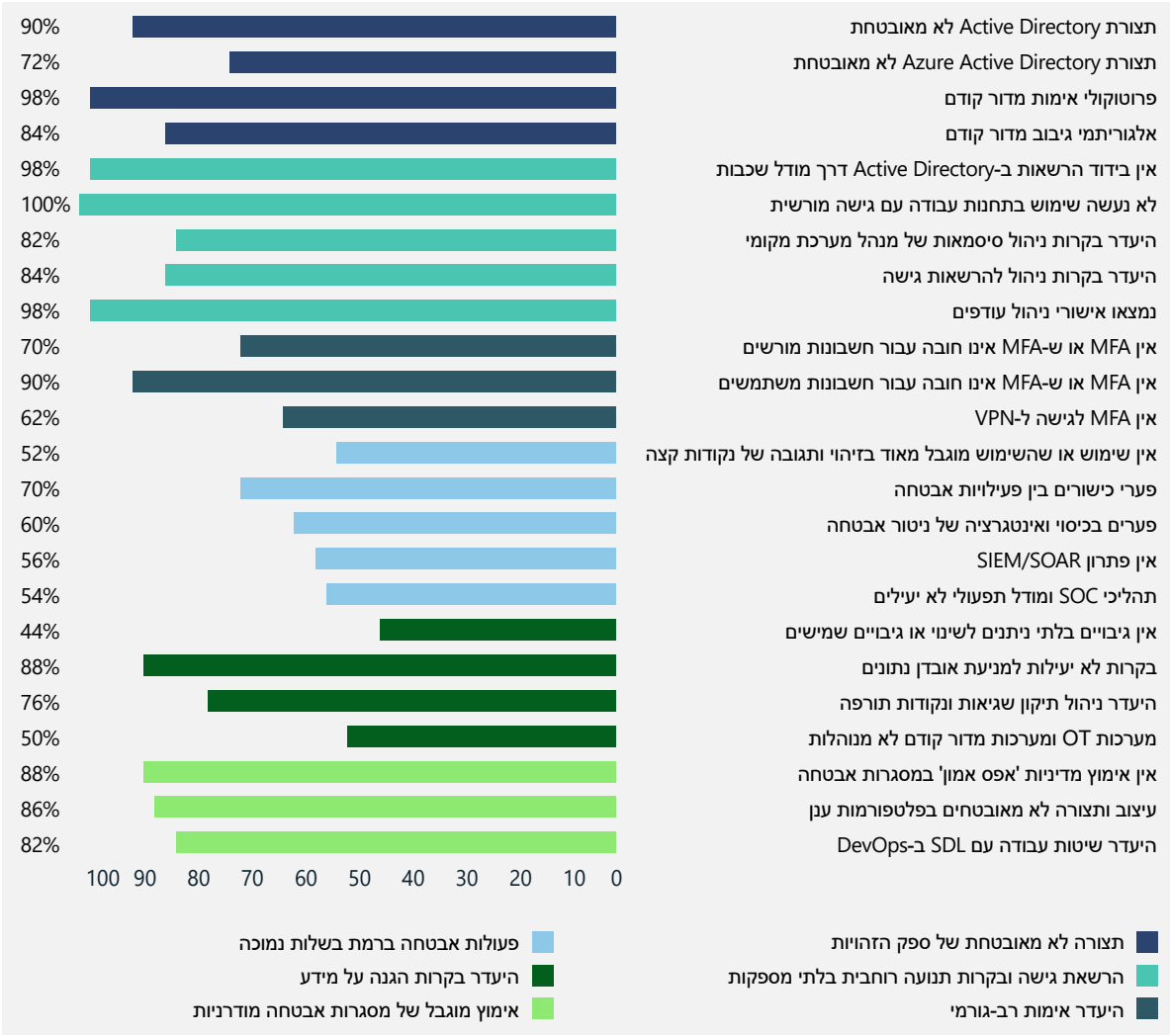
כאשר אנו מפתחים יכולות חדשות לעולם היפר-מחובר, עלינו לנהל את האיומים הנשקפים ממערכות ותוכנות מדור קודם.

מערכות מדור קודם – אלה שפותחו לפני שכלי קישוריות מודרניים כגון טלפונים חכמים, טאבלטים ושירותי ענן הפכו לנורמה – מייצגים סיכון לארגונים שעדיין משתמשים בהם. חשיפה זו לסיכונים מקבלת חיזוק על-ידי הממצאים של צוות שירותי האבטחה של Microsoft לתגובה לאירועים, קבוצה של מומחי אבטחה שעוזרת ללקוחות להגיב להתקפות ולהתאושש מהן.

במהלך השנה האחרונה, בעיות שנמצאו בקרב לקוחות שהתאוששו מהתקפות היו קשורות לשש קטגוריות כפי שמוצג בתרשים בדף זה. הדף הבא מתאר צעדים מעשיים שיש לנקוט לשיפור העמידות.

ניתן לייחס למעלה מ-80 אחוז מאירועי האבטחה לכמה אלמנטים חסרים הניתנים לטיפול באמצעות גישות אבטחה מודרניות.

סוגיות מרכזיות המשפיעות על עמידות הסייבר



תרשים זה מציג את אחוז הלקוחות המושפעים שחסרים להם בקרות אבטחה בסיסיות שהן קריטיות להגברת עמידות הסייבר הארגונית. הממצאים מבוססים על התקשרויות של Microsoft בשנה האחרונה.

"מנהיגים צריכים לחשוב על עמידות סייבר כהיבט קריטי של עמידות עסקית. עליהם להתכונן לשיבושים בסייבר באותו אופן שבו הם מתכוננים לאסונות טבע או לאירועים בלתי צפויים אחרים ולקבץ יחדיו בעלי עניין פנימיים מתחומים כגון תפעול, תקשורת, משפט ועוד, כדי לעצב אסטרטגיות. פעולה זו תסייע להבטיח שארגונים יחזירו את המערכות העסקיות הקריטיות שלהם לפעולה במהירות האפשרית כדי לחזור לפעילות עסקית רגילה.

אבל זה לא עוצר שם. מכיוון שארגונים רבים מסתמכים על ספקים ונותני שירותים צד שלישי, מנהיגים צריכים להרחיב את תכנון עמידות הסייבר לשרשרת הערך שלהם מקצה לקצה כדי להבטיח עוד יותר המשכיות עסקית ועמידות".

אן ג'ונסון,
סמנכ"לית אבטחה, תאימות, זהויות וניהול פיתוח עסקי

חשיבות המודרניזציה של מערכות וארכיטקטורה

המשך

ישנם תחומים ברורים שארגונים יכולים לטפל בהם כדי להפוך את הגישה שלהם למודרנית ולהתגונן מפני איומים:

בעיה	צעדים מעשיים
תצורה לא מאובטחת של ספק הזהויות תצורה שגויה וחשיפה של פלטפורמות זהויות ומרכיביהן הן וקטור נפוץ להשגת גישה לא מורשית להרשאות גבוהות.	יש לעקוב אחר קווי הבסיס לתצורת האבטחה ושיטות עבודה מומלצות בעת פריסה ותחזוקה של מערכות זהויות כגון תשתית AD ו-Azure AD. יש ליישם הגבלות גישה על-ידי אכיפת הפרדת הרשאות, הרשאת גישה מינימליות ושימוש בתחנות עבודה עם גישה מורשית (PAW) לניהול מערכות זהויות.
הרשאת גישה ובקרות תנועה רוחבית בלתי מספקות למנהלי מערכת יש הרשאות מוגזמות ברחבי הסביבה הדיגיטלית והם חושפים לעתים קרובות אישורי ניהול בתחנות עבודה הנתונים לסיכוני אינטרנט ופרודוקטיביות.	יש לאבטח ולהגביל את הגישה הניהולית כדי להפוך את הסביבה לעמידה יותר ולהגביל את היקף ההתקפה. יש להשתמש בבקרות ניהול להרשאות גישה כגון גישת 'בדיוק בזמן' וניהול 'במידה הדרושה'.
היעדר אימות רב-גורמי (MFA) התוקפים של היום לא פורצים פנימה, הם מתחברים.	MFA היא בקרת גישה קריטית ובסיסית למשתמשים שכל הארגונים צריכים להפעיל. בשילוב עם גישה מותנית, MFA יכול להיות בעל ערך רב במאבק באיומי סייבר.
פעולות אבטחה ברמת בשלות נמוכה רוב הארגונים שהושפעו השתמשו בכלים מסורתיים לזיהוי איומים ולא היו להם תובנות רלוונטיות לתגובה ותיקון בזמן.	אסטרטגיית זיהוי איומים מקיפה דורשת השקעות בזיהוי ותגובה מורחבים (XDR) ובכלים מודרניים מקוריים בענן המשתמשים בלמידת מכונה כדי להפריד בין רעש לאותות. יש להפוך את כלי פעולות האבטחה למודרניים על-ידי שילוב XDR שיכול לספק תובנות אבטחה עמוקות בנוף הדיגיטלי.
היעדר בקרות הגנה על מידע ארגונים ממשיכים להיאבק כדי להרכיב בקרות הוליסטיות להגנה על מידע שיש להן כיסוי מלא בכל מיקומי הנתונים והן נשארות יעילות לאורך כל מחזור החיים של המידע ותואמות את הקריטיות העסקית של נתונים.	יש לזהות את הנתונים העסקיים הקריטיים והיכן הם ממוקמים. יש לסקור תהליכי מחזור חיים של מידע ולאכוף הגנה על נתונים תוך הבטחת ההמשכיות העסקית.
אימוץ מוגבל של מסגרות אבטחה מודרניות זהות היא מערך האבטחה החדש, המאפשר גישה לסביבות מחשוב ולשירותים דיגיטליים שונים. שילוב עקרונות 'אפס אמון', אבטחת אפליקציות ומסגרות סייבר מודרניות אחרות מאפשר לארגונים לנהל סיכונים באופן יזום שאחרת ארגונים היו מתקשים לחזותם.	מסגרות 'אפס אמון' אוכפות מושגים של הרשאות מינימליות, אימות מפורש של כל הגישה, ותמיד מניחות פריצה. ארגונים צריכים גם ליישם שיטות עבודה ובקרות אבטחה ב-DevOps ובתהליכי מחזור החיים של אפליקציות לקבלת רמות אבטחה גבוהות יותר במערכות העסקיות שלהם.

מערך אבטחה בסיסי הוא גורם מכריע ביעילות פתרונות מתקדמים

באמצעות הניתוח שלנו, גילינו שכיחות של שטחים מתים נפוצים בהגנות ארגוניות המאפשרים לתוקפים לקבל גישה ראשונית, להשיג דריסת רגל וליישם התקפה, גם בנוכחותם של פתרונות אבטחה מתקדמים.

במקרים רבים, התוצאה של מתקפת סייבר נקבעת הרבה לפני שהמתקפה מתחילה. תוקפים ממנפים סביבות פגיעות כדי להשיג גישה ראשונית, לבצע מעקב ולזרוע הרס באמצעות תנועה רוחבית והצפנה או חילוץ נתונים. עצירת תוקף בשלב מוקדם מגדילה באופן ניכר את ההזדמנות להפחתת הפגיעה הכוללת.

Microsoft בחנה תצורות ספציפיות במערכי אבטחה כדי לזהות את החסרונות הנפוצים ביותר בסביבות אלה בפועל. זה אפשר לנו לראות את הפגיעויות הנפוצות ביותר שנוצלו במהלך מתקפות כופר המופעלות על ידי בני אדם, שאפשרו לגורמי האיום להשיג גישה ולעבור דרך הרשת מבלי שזוהו.

תצורות אבטחה בסיסיות חייבות להיות מופעלות

מכשירים של ארגון שאינם משולבים או מיושנים (הן ביחס לפגיעויות והן ביחס לסטטוס סוכן אבטחה) משמשים כנקודות כניסה פוטנציאליות ודרכים לביסוס גישה עבור התוקפים. מצאנו כי בעוד שווידוא שמכשירים ארגוניים אכן משולבים עם זיהוי ותגובה של נקודות קצה[1] (EDR) מעודכן ועם פתרון פלטפורמת ההגנה על נקודות קצה[2] (EPP) הוא צעד חשוב, זה אינו מבטיח את עצירת תוכנות כופר.

פתרונות מתקדמים כגון EDR ו-EPP הם קריטיים בזיהוי מוקדם של תוקף בזרימת התקיפה ומאפשרים תיקון והגנה אוטומטיים. עם זאת, מכיוון שפתרונות מתקדמים אלה מסתמכים על יכולת בסיסית לזהות התקפה, הם דורשים הפעלת תצורות אבטחה בסיסיות. למעשה, ראינו שכיחות של תרחישים עם פתרונות מתקדמים מיושמים שהתערערו בשל היעדר תצורות אבטחה בסיסיות.

שיטות עבודה מומלצות בתצורות אבטחה הן אינדיקטור טוב יותר לעמידות מאשר זמן התגובה של אנליסטים במרכז תפעול האבטחה (SOC)

ראינו הפחתה של 70 אחוז בזמן שנדרש לאנליסט SOC לראות ולפעול על פי התראה רלוונטית במשך תקופה של שישה חודשים באוכלוסיית הלקוחות והשותפים שלנו. מודעות מוגברת זו היא סימן טוב. עם זאת, בעוד שנראות תצורת האבטחה שיפרה את ביצועי האנליסטים של ה-SOC, הפעלת נראות המוצר על-ידי קליטה ועדכון של מכשירי הארגון הייתה מנבא טוב יותר למניעה מוצלחת.

סיכון הנשקף ממכשירים לא מוכרים

בניגוד לרשתות ענן, שבהן הלקוחות יודעים אילו נכסים פועלים באילו מערכות הפעלה, רשתות מקומיות יכולות להכיל מגוון רחב של מכשירים כגון IoT, מחשבים שולחניים, שרתים ומכשירי רשת שאינם מנוטרים או מנוהלים על ידי הארגון.

לרשת ארגונית ממוצעת יש יותר מ-3,500 מכשירים מחוברים שאינם מוגנים על-ידי סוכן EDR וייתכן שיש להם גישה למשאבים ארגוניים או אפילו לנכסים בעלי ערך גבוה. Microsoft Defender עבור נקודת קצה (MDE) משתמש בבדיקת רשת כדי לגלות מכשירים ולספק מידע אודות סיווגי מכשירים עבור אלה המחוברים לרשת, כגון שם המכשיר, הפצת מערכת ההפעלה וסוג המכשיר.

3,500

המספר הממוצע של מכשירים מחוברים בארגון שאינם מוגנים על-ידי סוכן זיהוי ותגובה של נקודות קצה.

עבור מכשירים שאינם נתמכים על ידי סוכן EDR, יש להיות מודעים לפחות לקיומם ולפעול כדי להגן עליהם על ידי הערכת פגיעויות, כמו גם הגבלת הגישה לרשת.

תובנות מעשיות

1. אפילו פתרונות מתקדמים יכולים להתערער כתוצאה מהיעדר תצורות אבטחה בסיסיות.
2. יש להשקיע בשיטות עבודה מומלצות בתצורות של מערך האבטחה כדי להתגונן מפני התקפות עתידיות. הגדרות בסיסיות אלה מייצרות החזר השקעה עצום במונחים של יכולת הארגון להתגונן מפני התקפות.
3. יש לצרף את כל המכשירים הרלוונטיים לפתרון EDR.
4. יש להקפיד לעדכן את סוכני האבטחה ולהבטיח הגנה מפני חבלה כדי לאפשר נראות רבה יותר ויתרונות הגנה מלאים יותר של מוצרים.

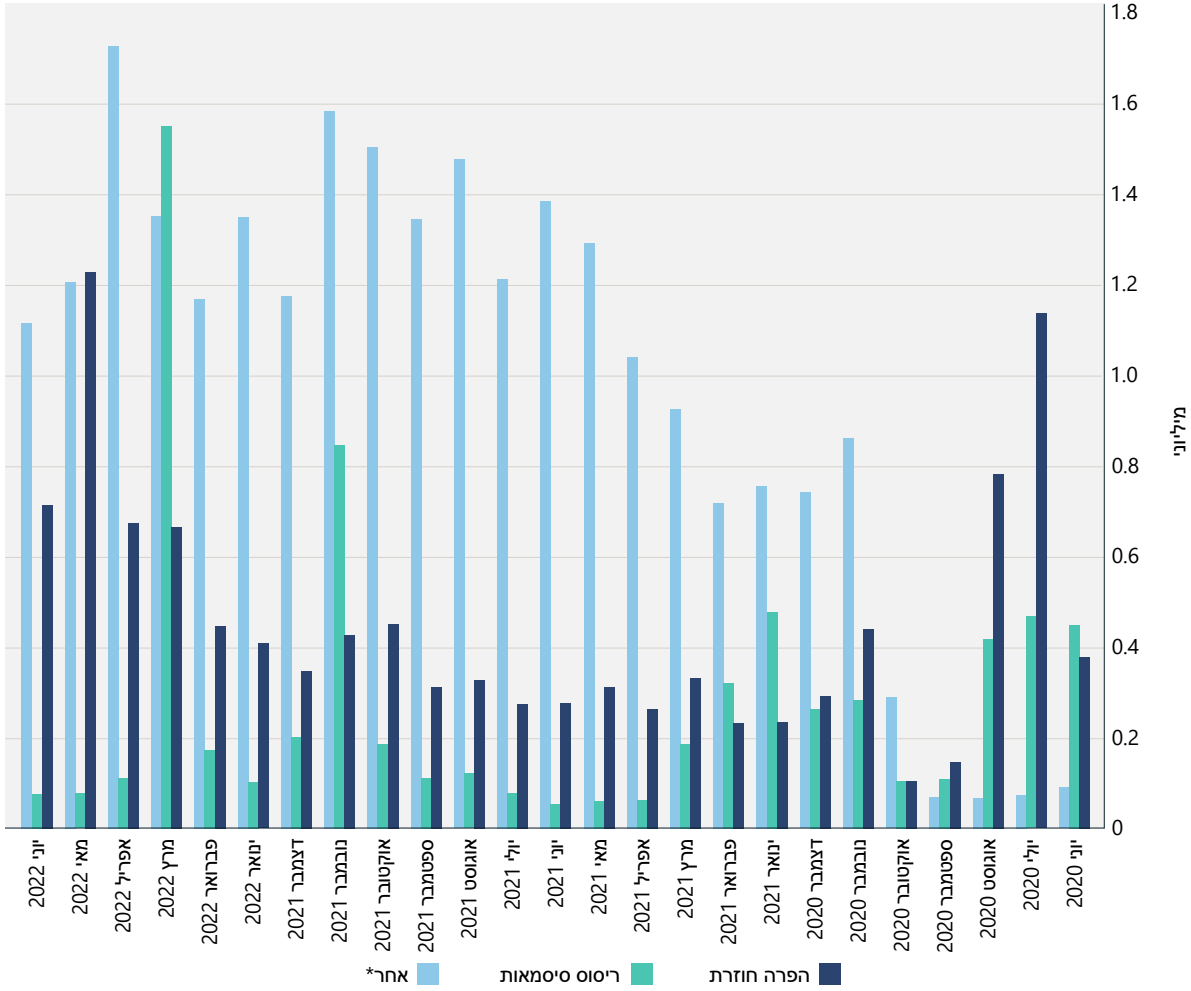
שמירה על תקינות הזהות היא בבסיס הרווחה הארגונית

אבטחת הזהות חשובה היום יותר מאי פעם. בעוד שהתקפות מבוססות סיסמה הן עדיין המקור העיקרי לחשיפת זהויות, סוגים אחרים של מתקפות צצים. נפח ההתקפות המתוחכמות ממשיך לגדול ביחס לנורמה הקודמת של ריסוס סיסמאות ופריצה חוזרת.

התקפות מבוססות סיסמה עדיין נפוצות, ויותר מ-90 אחוז מהחשבונות שנפרצו באמצעות שיטות אלה אינם מוגנים באמצעות אימות חזק. אימות חזק משתמש ביותר מגורם אימות אחד, לדוגמה סיסמה + SMS ומפתחות אבטחה של FIDO2.

ראינו עלייה בהתקפות ריסוס סיסמאות ממוקדות, עם עליות חדות מאוד בנפח תעבורת התוקפים המפוזרת על פני אלפי כתובות IP.

משתמשים שנפגעו לפי קטגוריית התקפה



משתמשים שנפגעו חודשית לפי קטגוריית התקפה נפחי ההתקפות מסוג ריסוס סיסמאות היו תנודתיים מאוד, כפי שניתן לראות בעליות החדות בנובמבר 2021 ובמרץ 2022. עליות אלו מייצגות אלפי משתמשים ואלפי כתובות IP שנפגעו. *"אחר" מציין התקפות שונות מהתקפות ריסוס סיסמאות ופריצה חוזרת, בכללן דיוג, תוכנות זדוניות, 'אדם בתווך', פגיעה במנפיק אסימונים מקומי ועוד. מקור: Azure AD Identity Protection.

4,500

בזמן שלוקח לקרוא את ההצהרה הזו, התגוננו מפני 4,500 התקפות של סיסמאות.

שמירה על תקינות הזהות היא בבסיס הרווחה הארגונית

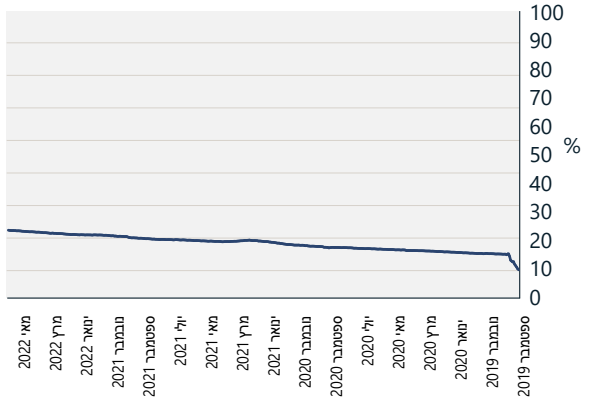
המשך

אימוץ של אימות חזק

בנימה חיובית, אנו רואים צמיחה מתמדת באימוץ אימות חזק בקרב בסיס הלקוחות הארגוני של Azure Active Directory (Azure AD). עבור Azure AD, מספר המשתמשים הפעילים בחודש (MAU) באימות חזק גדל מ-19 אחוז ל-26 אחוז בשנה האחרונה, בעוד ש-MAU באימות חזק עבור חשבונות מנהלי מערכת גדל מ-30 אחוז לכ-33 אחוז.

מגמה זו חיובית, אך עדיין יש צורך בגדילה משמעותית כדי להגיע לכיסוי של רוב המשתמשים באימות חזק; לקוחות שאינם משתמשים עדיין באימות חזק בסביבותיהם צריכים להתחיל בתכנון ובפריסה של אימות חזק כדי להגן על המשתמשים שלהם.[3] בעת תכנון פריסת אימות חזק, יש לשקול שימוש באימות נטול סיסמאות מכיוון שהוא מציע את החוויה השימושית המאובטחת ביותר, תוך ביטול הסיכון להתקפות סיסמאות.

שימוש באימות חזק
(ספטמבר 2019 עד מאי 2022)

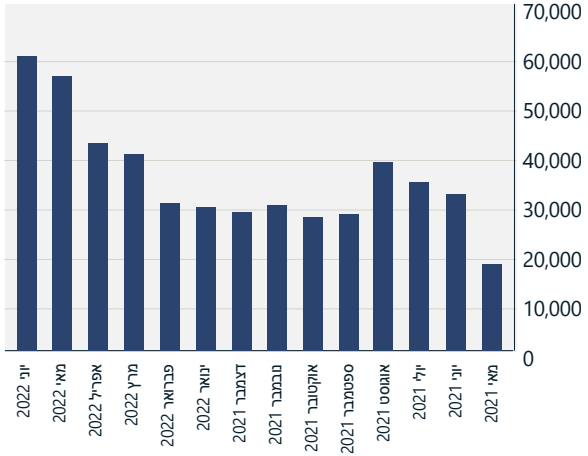


בעוד שהשימוש באימות חזק הוכפל מאז 2019, רק 26 אחוז מהמשתמשים ו-33 אחוז ממנהלי המערכת משתמשים באימות חזק. מקור: Azure Active Directory.

עלייה מתמדת בהתקפות הפעלה חוזרת של אסימונים

חלקן של צורות תקיפה אחרות גדל בשנת 2022. ראינו עלייה בהתקפות ממוקדות שנמנעות באופן ספציפי מאימות מבוסס סיסמה כדי להפחית את הסיכוי לזיהוי. התקפות אלה ממנפות קובצי Cookie של כניסה יחידה (SSO) בדפדפן או אסימוני רענון שהושגו באמצעות תוכנות זדוניות, דיוג ושיטות אחרות. במקרים מסוימים, התוקפים בוחרים תשתית במיקומים הסמוכים למיקום הגיאוגרפי של משתמש היעד כדי להפחית עוד יותר את סיכויי הזיהוי. ראינו עלייה מתמדת בהתקפות הפעלה חוזרת של אסימונים, שהגיעו ליותר מ-40,000 זיהויים בחודש ב-Azure AD Identity Protection.
הפעלה חוזרת של אסימונים היא השימוש באסימונים שהונפקו למשתמש לגיטימי על ידי תוקף שיש לו החזקה באסימונים האמורים. אסימונים מושגים בדרך כלל באמצעות תוכנות זדוניות, למשל על ידי חילוץ קובצי ה-Cookie מהדפדפן של המשתמש או באמצעות שיטות דיוג מתקדמות.

נפח של התקפות הפעלה חוזרת של אסימונים שזוהו



התקפות הפעלה חוזרת של אסימונים שזוהו לחודש מקור: Azure AD Identity Protection, הפעלות ייחודיות שסומנו על-ידי זיהוי האסימון החריג.

שמירה על תקינות הזהות היא בבסיס הרווחה הארגונית

המשך

חילוץ אסימונים

יותר מתוכנות זדוניות, התוקפים זקוקים לאישורים כדי להשיג את מטרותיהם. למעשה, 100 אחוז מכל מתקפות הכופר המופעלות על ידי בני אדם כוללות אישורים גנובים. חדירות מתוחכמות רבות כוללות אישורים שנרכשו מהרשת האפלה, שנגנבו תחילה מתוכנות זדוניות לא מתוחכמות לגניבת אישורים הנמצאות בתפוצה רחבה. סוג זה של תוכנות זדוניות התפתח כדי לגנוב אסימונים, כולל מידע על הפעלות ותביעות MFA. משמעות הדבר היא כי הידבקויות במערכות ביתיות, שבאמצעותן משתמשים נכנסים לנכסים ארגוניים, יכולות להוביל לאירועים חמורים ברשתות ארגוניות.

תוקפים יכולים גם לחלץ אסימונים ממכשירי הקורבנות באמצעות התקפות מסוג 'אדם בתווך', שבהן הקורבן לוחץ על קישור זדוני בדואר אלקטרוני או בהודעה מיידית של דיוג ומופנה לאתר אינטרנט שנראה כמו דף הכניסה הלגיטימי של ספק הזהויות. במציאות, זהו שירות אינטרנט שמופעל על ידי התוקף שמעביר ומיירט את כל התעבורה בין המשתמש לספק הזהויות. התוקף מסוגל ליירט את שם המשתמש והסיסמה וגם להעביר אתגרי MFA; אסימונים שנוצרו על-ידי ספק הזהויות ויורטו על-ידי התוקף עשויים להכיל תביעות MFA שהתוקף יכול להשתמש בהן כדי לעמוד בדרישות ה-MFA.

Microsoft Defender עבור אפליקציות ענן זיהה בממוצע 895 התקפות כאלה בחודש מאז תחילת 2022. ניתן למנוע צורה זו של התקפה באמצעות שימוש בגורמים עמידים בפני דיוג של MFA, כגון אימות מבוסס אישורים, Windows Hello לעסקים או מפתחות אבטחה של FIDO2.

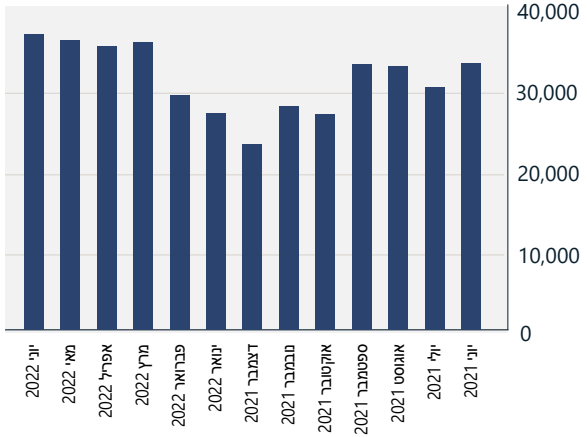
התקפות מבוססות סיסמה הן השיטה העיקרית שבה חשבונות נפרצים.

עייפות MFA

באמצעות שימוש במושג "עייפות MFA", התוקפים יוצרים בקשות מרובות עבור MFA למכשיר של הקורבן, בתקווה שהקורבן יקבל את הבקשה בשוגג או כתוצאה מעייפות. ניתן למנוע התקפה זו על-ידי שימוש באפליקציות אימות מודרניות כגון Microsoft Authenticator בשילוב עם תכונות כגוןהתאמת מספרים[4] וכאפשור הקשר נוסף.[5] Azure AD Identity Protection העריך כי קיימות 30,000 התקפות מסוג עייפות MFA בחודש.

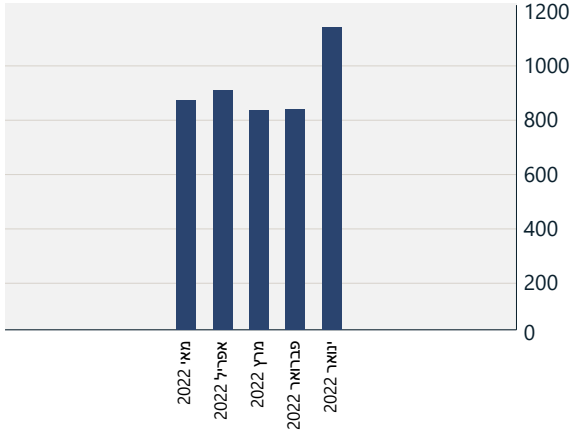
חלקן של המתקפות המתוחכמות ממשיך לגדול, עובדה שמדגישה את הצורך בגורמים עמידים בפני דיוג של אימות רב-גורמי.

מופעים משוערים של התקפות עייפות MFA



מקור: Azure AD Identity Protection.

מופעים של דיוג ובעקבותיהם התקפות 'אדם בתווך'



מקור: Microsoft Defender עבור אפליקציות בענן.

תובנות מעשיות

1. יש לוודא שכל החשבונות ברחבי הארגון מוגנים על-ידי אמצעי אימות חזקים.
2. אימות ללא סיסמה מציע את החוויה המאובטחת והידידותית ביותר למשתמש, ומבטל את הסיכון להתקפות סיסמאות.
3. יש להשבית אימות מדור קודם ברחבי הארגון כולו.
4. יש להגן על חשבונות בעלי ערך גבוה וחשבונות מנהלי מערכת באמצעות צורות עמידות בפני דיוג של אימות חזק.
5. יש לבצע מודרניזציה מספק זהויות מקומי לספק זהויות בענן ולחבר את כל האפליקציות לספק זהויות מבוסס ענן לקבלת חוויית משתמש ואבטחה עקביות.

קישורים למידע נוסף

- יום הסיסמאות העולמי הקרוב הוא הזמן לשקול לוותר לחלוטין על סיסמאות | Microsoft Security

הגדרות האבטחה המוגדרות כברירת מחדל של מערכת ההפעלה

עם נוף איומי האבטחה המתפתח ללא הרף, אנו רואים צורך הולך וגובר באבטחת מחשבים המוגדרת כברירת מחדל לשיפור עמידות הסייבר. בעוד שאבטחת מערכת ההפעלה דחופה, מורכבת וקריטית לעסקים יותר מאי פעם, לעשות את זה ולנהל אותה נכון יכול להיות עניין מאתגר.

בעבר, אבטחת מחשבים ומכשירים כללה תכונות אבטחה מובנות שהלקוח או מומחה ה-IT היה צפוי להגדיר לרמה הרצויה לו. גישה זו אינה מספקת עוד, מכיוון שהתוקפים משתמשים בכלים מתקדמים יותר באוטומציה, תשתיות ענן וטכנולוגיות גישה מרחוק כדי להשיג את מטרותיהם. זה הפך להיות קריטי שכל שכבות האבטחה, מהשבב ועד הענן, מוגדרות כברירת מחדל. Microsoft התפתחה כדי להגדיר את אבטחת מערכת ההפעלה Windows כברירת מחדל.[6]

לקוחות שמאמצים את ההגנה – לעומק, כולל מערך אבטחה שכבתי, תכונות אבטחה חדשות, תיקונים ועדכונים קבועים ועקביים, כמו גם הדרכה ומודעות לאבטחה כדי לדווח על דיוג והונאות אחרות – יכולים לצפות לפחות תוכנות זדוניות.

כדי לפשט את ההגנה לעומק, Windows 11 כוללת הגנות חומרה ותוכנה משולבות היטב המופעלות כברירת מחדל, כולל שלמות זיכרון, אתחול מאובטח ומודול פלטפורמה מהימנה (TPM) 2.0. גם משתמשי Windows 10 עם חומרה מותאמת יכולים להפעיל תכונות אלה באפליקציית ההגדרות של Windows או בתפריט ה-BIOS.

למכשירים ישנים יותר באופן כללי אין לעתים קרובות התאמה חזקה כל כך בין אבטחת חומרה לטכניקות אבטחת תוכנה. עבור מכשירים שבהם האבטחה אינה מופעלת כברירת מחדל, יש לקבוע את תצורתם באופן ידני בהגדרות במידת האפשר.[7]

יש לפעול באופן יזום לגבי החלת עדכונים ותיקוני אבטחה רציפים של מערכת ההפעלה המסייעים לספק הגנה לאורך כל מחזור החיים של החומרה והתוכנה.

עבור מכשירים שבהם האבטחה אינה מופעלת כברירת מחדל, Microsoft ממליצה לקבוע את תצורתם באופן ידני בהגדרות במידת האפשר.

תובנות מעשיות

1. יש להשתמש בפתרון ללא סיסמה המאגד אישורי כניסה במודול הפלטפורמה המהימנה, ולחפש באופן ספציפי פתרון ללא סיסמה העומד בתקן התעשייה Fast Identity Online (FIDO) Alliance.[8]
2. יש לבצע ניקוי בזמן של כל קובצי ההפעלה שאינם בשימוש ומיושנים הנמצאים במכשירים של ארגונים.
3. יש להגן מפני מתקפות קושחה מתקדמות על-ידי הפעלת שלמות זיכרון, אתחול מאובטח ומודול פלטפורמה מהימנה 2.0, אם אינם מופעלים כברירת מחדל, אשר מקשיחים את האתחול באמצעות יכולות המובנות במעבדים מודרניים.
4. יש להפעיל הצפנת נתונים והגנה על אישורים.
5. יש להפעיל אמצעי בקרה לאפליקציות ולדפדפן לקבלת הגנה משופרת מפני אפליקציות לא מהימנות והגנות מובנות אחרות מפני ניצול לרעה.
6. יש להפעיל הגנה על גישה לזיכרון כדי לסייע בהגנה מפני התקפות פיזיות מזדמנות, כגון מישהו שמחבר התקן זדוני ליציאות הנגישות מבחוץ.

קישורים למידע נוסף

- ספר האבטחה של Windows | מסחרי
- תכונות אבטחה חדשות עבור Windows 11 יעזרו להגן על עבודה היברידית | הבלוג של Microsoft Security

ריכוזיות שרשרת האספקה של התוכנות

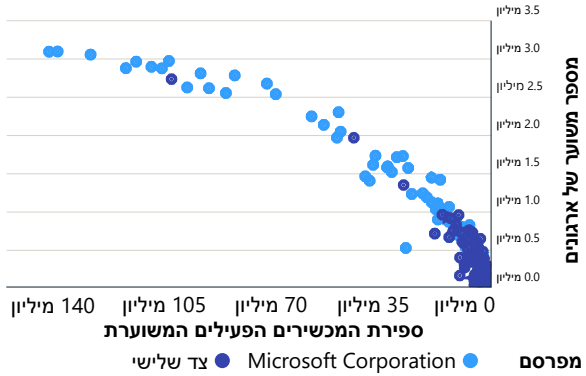
התקפות על אפליקציות, תוספים והרחבות של צד שלישי עלולות לשחוק את אמון הלקוחות בספקים הממלאים תפקיד מרכזי במערכת האקולוגית של האספקה. השימוש בתורת הרשתות לבחינת מרכזיות התוכנה עוזר להאיר את הקריטיות של ביצוע התיקונים, במיוחד עבור אפליקציות מרכזיות.

רשת האפליקציות של Windows, הכוללת 18 מיליון קובצי הפעלה של אפליקציות, מותקנת ונמצאת בשימוש על ידי חמישה מיליון ארגונים, ומספקת תצוגה ברמה הגבוהה ביותר של המערכת האקולוגית של התוכנה שלנו. מתוך 100,000 האפליקציות הנפוצות ביותר, 97 אחוז מיוצרות על-ידי ארגוני צד שלישי שהעדכונים ותיקוני האבטחה שלהן מתוחזקים על-ידם. עובדה זו ממחישה שתי תכונות חשובות של המערכת האקולוגית של האפליקציות המסחריות שלנו.

תכונה ראשונה, יש מרכזיות במערכת האקולוגית של האפליקציות המסחריות של Windows. רק 100,000 האפליקציות המובילות (מתוך 18 מיליון) נמצאות בשימוש ב-1,000 מכשירים או יותר. במילים אחרות, למעט יותר ממחצית האחוז מאפליקציות אלה יש השפעה רחבה מסוג זה בקרב המערכת האקולוגית של המכשירים.

תכונה שנייה, יש גיוון ביכולת הניהול של אפליקציות אלה, כאשר 10,000 ספקי האפליקציות המובילות מנהלים את העדכונים ואת תיקוני האבטחה של אפליקציות מסחריות אלה הנמצאות בשימוש הרב ביותר. עובדה זו מדגימה את התלות ההדדית שיש לחברה במערך מגוון של בקרות אבטחה, תאימות וניהול של ספקי תוכנה.

חדירה מסחרית של האפליקציות הנפוצות ביותר



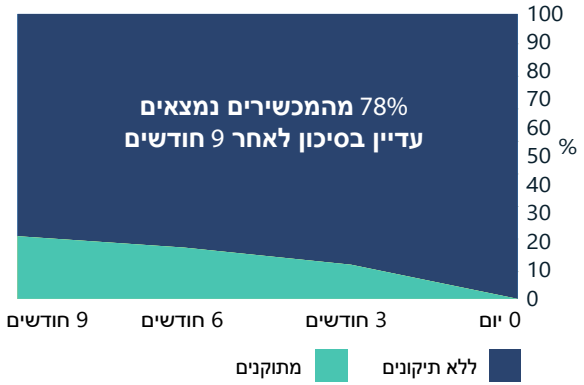
האפליקציות המובילות משמשות מיליוני ארגונים ועשרות מיליוני מכשירים. מכיוון שהן נמצאות כמעט בכל מקום, יריבים עומדים על המשמר באופן מתמיד כדי לנצל פגיעויות באפליקציות מובילות אלה, דבר שעלול להשפיע על מיליוני מכשירים בבסיס המשתמשים.

אנו רואים מיליוני מכשירים מסחריים שעדיין משתמשים בגרסאות אפליקציות פגיעות חודשים רבים לאחר פרסום התיקון או אפילו שנים לאחר סיום התמיכה במוצר. לדוגמה, קיימים יותר ממיליון מכשירים מסחריים פעילים של Windows שבהם פועלת גרסה של קורא PDF שאינה נתמכת מאז 2017.

> גרסאות ישנות של אפליקציות שאינן נתמכות נשארות בשימוש פעיל במיליוני מכשירים מסחריים. כתוצאה מכך, ארגונים נמצאים בסיכון נשיאת פגיעויות שלא יתוקנו.

עבור גרסאות אפליקציות שבתמיכה, אנו רואים דריכה במקום מבחינת מהירות אימוץ תיקונים קריטיים, שהיא מגמה הפוכה מהמגמה שתניע עמידות. במקום זאת, העקומה צריכה להראות עלייה אקספוננציאלית בקצב אימוץ התיקונים מחודש לחודש, כדי להשיג את העמידות הדרושה.

קצב פריסת התיקונים הקריטיים



לאחר שבחנו פגיעות קריטית שהשפיעה על 134 גרסאות של קבוצת דפדפנים, מצאנו ש-78 אחוז, או מיליוני מכשירים, עדיין השתמשו באחת הגרסאות שהושפעו תשעה חודשים לאחר פרסום התיקון.

השתמשנו בערכת הכלים InterpretML[9] כדי לזהות מאפיינים התואמים לארגונים שסביר יותר שיהיו להם מכשירים עם גרסאות אפליקציה ישנות יותר. החשובים מבין המנבאים הללו כללו: מעט שעות של התעסקות במכשירים; אזורים גיאוגרפיים כגון אסיה והאוקיינוס השקט ואמריקה הלטינית; ותעשיות כגון רכב, כימיקלים, טלקומוניקציה, תחבורה ולוגיסטיקה, משלמי בריאות (מטפלים בתביעות) וביטוח.

> תחזוקת עמידות תוכנה צריכה לכלול השבתה או הסרת התקנה באופן קבוע של אפליקציות שאינן בשימוש.

> האבטחה והתאימות של הארגון תלויים במאמציו ובמאמצי ספקי התוכנה שלו.

תובנות מעשיות

1. יש לבצע עדכונים בזמן לכל האפליקציות ונקודות הקצה דרך הארגון.
2. יש לבצע ניקוי בזמן של כל קובצי ההפעלה שאינם בשימוש ומיושנים הנמצאים במכשירים של ארגונים.

קישורים למידע נוסף

- תיעוד של Microsoft Intune | Microsoft Docs
- ניהול אפליקציות | Microsoft Docs
- Microsoft Defender עבור נקודת קצה | Microsoft Security
- OSS מסגרת שרשרת אספקה מאובטחת | הנדסת אבטחה של Microsoft
- מסגרת שרשרת האספקה המאובטחת של תוכנת הקוד הפתוח של Microsoft | GitHub

בניית עמידות בפני התקפות DDoS, אפליקציות אינטרנט ורשת מתפתחות

טרנספורמציה דיגיטלית מואצת הביאה את קיצו של מודל הרשת ומערך האבטחה המסורתי. המעבר לענן פירושו שארגונים חייבים לאמץ אבטחת רשת מקורית בענן כדי להגן על נכסים דיגיטליים.

מורכבות ההתקפות, תדירותן ונפחן ממשיכות לגדול ואינן מוגבלות עוד לעונות החגים, עובדה המעידה על מעבר להתקפות לאורך כל השנה. זה מדגיש את חשיבותה של הגנה מתמשכת מעבר לעונות תעבורת השיא המסורתיות.

מתקפות מניעת שירות מבוזרת (DDoS)

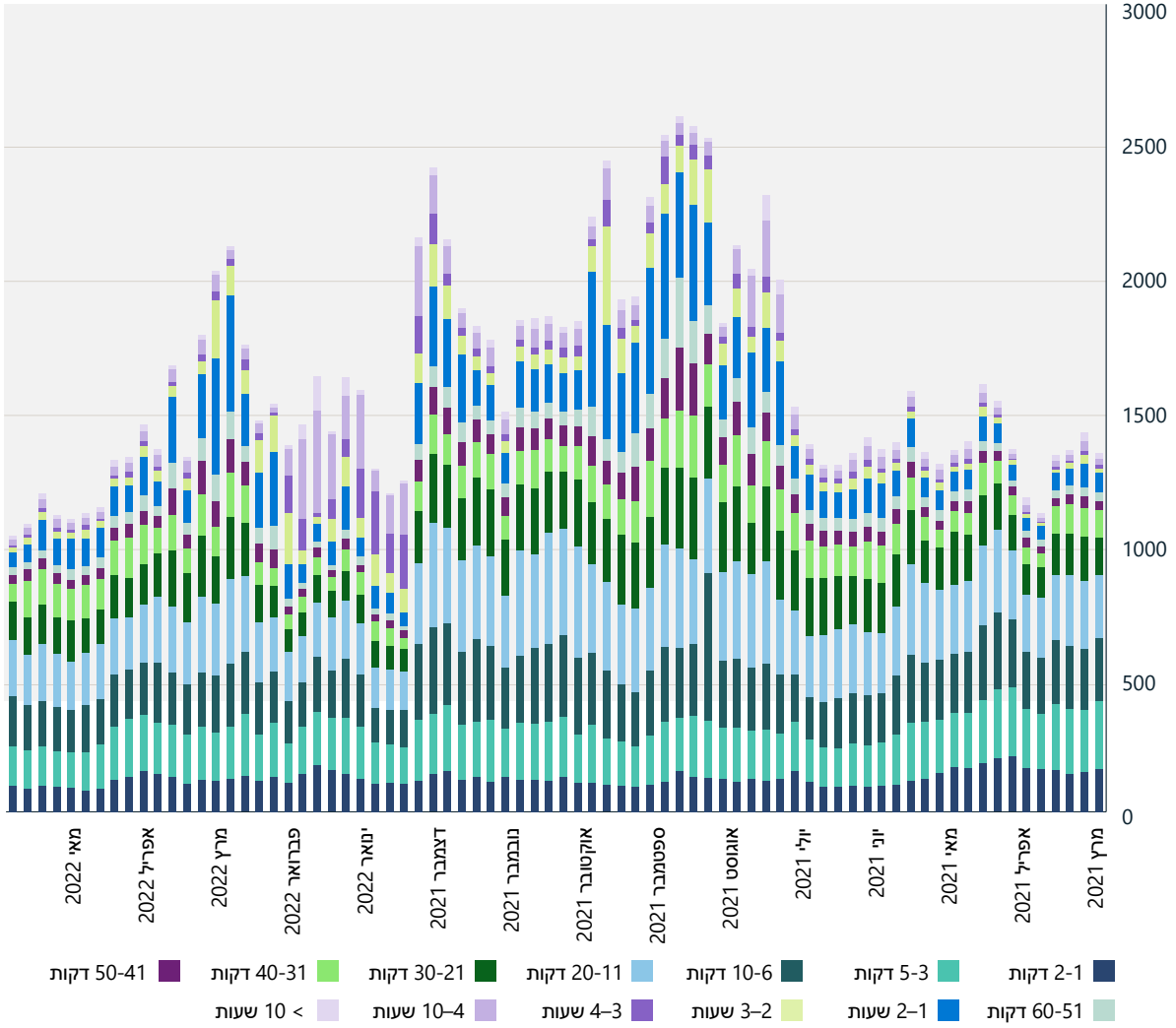
בשנה האחרונה חווה העולם פעילות DDoS חסרת תקדים בהיקף, במורכבות ובתדירות. התפוצצות מתקפות DDoS זה הונע על ידי עלייה משמעותית בהתקפות מדינתיות והמשך התפשטותם של שירותי DDoS להשכרה בעלות נמוכה. Microsoft צמצמה בממוצע 1,955 התקפות ביום, עלייה של 40 אחוז לעומת השנה הקודמת. בעבר, מספר השיא של ההתקפות התרחש בדרך כלל בעונת החגים של סוף השנה. השנה, לעומת זאת, מספר ההתקפות הגבוה ביותר שתועד ביום אחד היה ב-10 באוגוסט 2021. נתון זה עשוי להצביע על מעבר להתקפות לאורך כל השנה ומדגיש את החשיבות של הגנה מתמשכת מעבר לעונות תעבורת השיא המסורתיות.

בנובמבר 2021, Microsoft סיכלה מתקפת DDoS נפחית עם תפוקה של 3.4 טרה-ביט לשנייה (Tbps) מכ-10,000 מקורות המשתרעים על פני מספר מדינות. התקפות נפחיות דומות בנפח גבוה של מעל 2+Tbps צומצמו בשנת 2022 והדגישו כי לא רק המורכבות ותדירות ההתקפות הולכות וגדלות, אלא גם הנפח (רוחב הפס) של ההתקפה.

משך ההתקפה

רוב ההתקפות שנצפו בשנה האחרונה היו קצרות מועד. כ-28 אחוז מההתקפות נמשכו פחות מ-10 דקות, 26 אחוז נמשכו 10-30 דקות ו-14 אחוז נמשכו 31-60 דקות. שלושים ושניים אחוז מההתקפות נמשכו יותר משעה.

מספר התקפות ה-DDoS והתפלגות משך הזמן
(מרץ 2021 - מאי 2022)



רוב ההתקפות בשנה האחרונה היו קצרי מועד. כ-28 אחוז מההתקפות נמשכו פחות מ-10 דקות.

בניית עמידות בפני DDoS מתפתחים, התקפות על אפליקציות אינטרנט והתקפות רשת

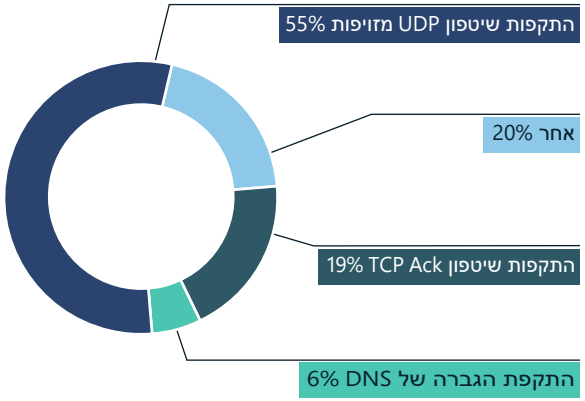
נמשכו

וקטורים של התקפות DDoS

בשנה האחרונה, וקטורי התקיפה הנפוצים היו מסוג User Datagram Protocol (UDP) השתקפות ביציאה 80 באמצעות פרוטוקול גילוי שירות פשוט (SSDP), connectionless lightweight directory access protocol (CLDAP), מערכת שמות תחומים (DNS) ופרוטוקול זמן רשת (NTP) המהווים שיא אחד ויחיד. ראינו גם עלייה בהתקפות DDoS בשכבת האפליקציה המתמקדות באתרים, עם 16.3 מיליון RPS שיא (בקשות לשנייה) ותעבורת שיא של 9.89 Tbps.

בשנת 2022, Microsoft צמצמה כמעט 2,000 התקפות DDoS מדי יום וסיכלה את מתקפת ה-DDoS הגדולה ביותר שדווחה אי פעם בהיסטוריה.

וקטורים של התקפות DDoS



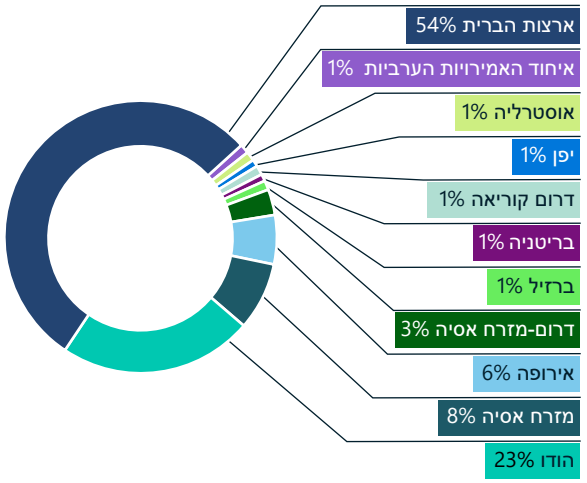
התקפות שיטפון UDP מזויפות הגיעו לווקטור העליון במחצית הראשונה של 2022, מ-16 אחוז ל-55 אחוז. התקפות שיטפון TCP Ack פחתו מ-54 אחוז ל-19 אחוז.

תעשיית הגיימינג ממשיכה להיות המטרה העיקרית של מתקפות DDoS, בעיקר ממוטציות של רשת הבוטים Mirai והתקפות פרוטוקול UDP בנפח נמוך. מכיוון ש-UDP נמצא בשימוש נפוץ ביישומי גיימינג ובאפליקציות סטרימינג, רוב מוחץ של וקטורי התקיפה היו התקפות שיטפון UDP מזויפות, בזמן שחלק קטן היו התקפות שיקוף והגברת UDP.

אזורי יעד גיאוגרפיים

מתוך מתקפות ה-DDoS שזוהו בשנה האחרונה, 54 אחוז בוצעו נגד יעדים בארצות הברית, מגמה שאולי מוסברת בחלקה על ידי העובדה שרוב לקוחות Azure ו-Microsoft נמצאים בארצות הברית. ראינו גם עלייה חדה בהתקפות נגד הודו, מ-2 אחוז בלבד מכלל ההתקפות במחצית השנייה של 2021 ל-23 אחוז במחצית הראשונה של 2022. מזרח אסיה, הונג קונג בפרט, ממשיכה להיות יעד פופולרי עם 8 אחוז. באירופה ראינו ריכוזי התקפות נגד האזורים אמסטרדם, וינה, פריז ופרנקפורט.

יעד מתקפת DDoS

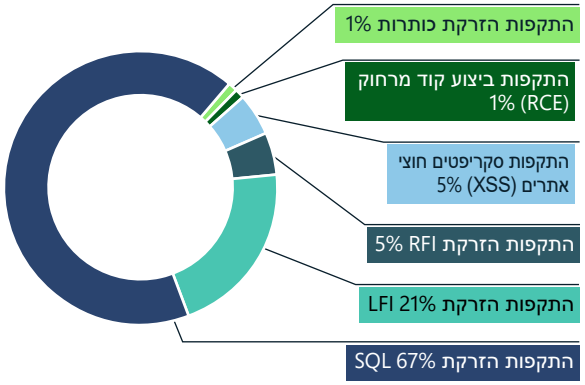


אנו מייחסים את הנפח הגבוה של ההתקפות באסיה לטביעת הרגל העצומה של האזור בתחום הגיימינג, במיוחד בסין, יפן, דרום קוריאה והודו. טביעת רגל זו תמשיך להתרחב ככל שחדירה גוברת של טלפונים חכמים תניע את הפופולריות של משחקים לטלפון הנייד, דבר המרמז על כך שיעד גיאוגרפי זה רק ימשיך לגדול.

ניצול לרעה של אפליקציות אינטרנט

חומת אש של אפליקציות אינטרנט (WAF), בשילוב עם הגנה מפני מתקפות DDoS, מהווה חלק בלתי נפרד מאסטרטגיית ההגנה המעמיקה להגנה על נכסי ממשק תכנות באינטרנט ובאפליקציות (API). Microsoft הבחינה ביותר מ-300 מיליארד כללי WAF שהופעלו מדי חודש באמצעות WAFs של Azure.

התפלגות סוגי ההתקפות הנפוצים ביותר



Azure WAF מזהה מיליארדי התקפות Open Web Application Security Project (OWASP) Top 10[10] מדי יום. על פי האותות שלנו, התוקפים ניסו לבצע התקפות הזרקת SQL במידה הרבה ביותר ואחריהן התקפות הזרקת קבצים מקומית והתקפות הזרקת קבצים מרחוק. זה עולה בקנה אחד עם רשימת עשרת המובילים של OWASP המציגה התקפות הזרקה כסוג השלישי הנפוץ ביותר של התקפות אינטרנט.

כמו כן, חלה עלייה בהתקפות בוטים נגד אפליקציות אינטרנט של Azure, עם ממוצע של 1.7 מיליארד בקשות בוטים בחודש ו-4.6 אחוז מהתעבורה הזו מורכבת מבוטים רעים.

בניית עמידות בפני התקפות DDoS, אפליקציות אינטרנט ורשת מתפתחות

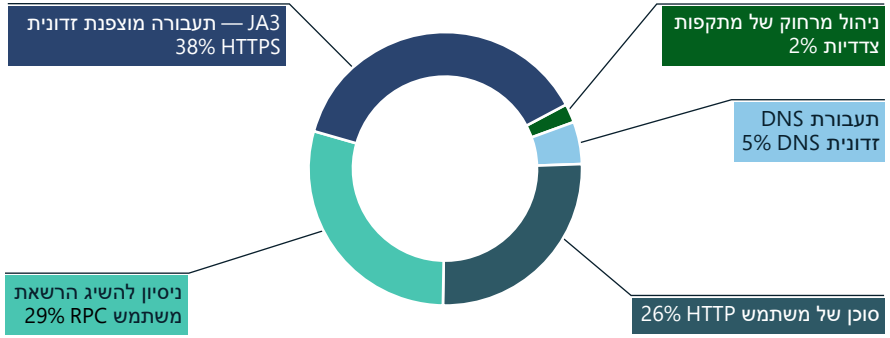
המשך

בשל מספר גדל והולך של בוטים המבצעים התקפות מילוי אישורים, הונאות בכרטיסי אשראי, מבצעי השפעה בסייבר והתקפות שרשרת אספקה, אנו מצפים לראות עלייה מתמדת בהתקפות בוטים נגד אפליקציות אינטרנט.

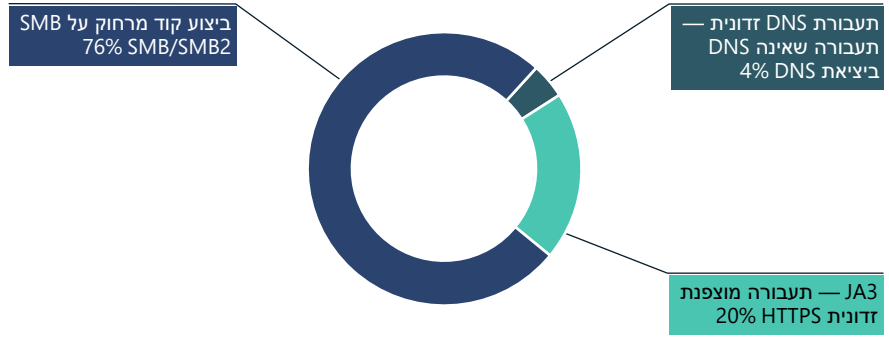
פריצות לרשת: איתור ומניעה

ראינו עלייה משמעותית בניצול לרעה של שכבת הרשת, במיוחד תוכנות זדוניות, בשנת 2022. מערכת איתור ומניעת חדירות של חומת האש של Azure (IDPS) חסמה יותר מ-150 מיליון חיבורים בחודש יוני בלבד.

סיבת דחיית תעבורה של IDPS



סיבות להתראה על תעבורה של IDPS



ניתוח של התראה ומניעת תעבורה של IDPS מראה את הגישות הבאות המשמשות את התוקפים. בדחיית תעבורה, אנו רואים תוקפים המשתמשים ב-SSL כדי להסתיר את פעילותם והתקפות ביצוע מרחוק הופכות נפוצות יותר. בתעבורת התראות, אנו רואים פרוטוקולי SMB/SMB2 המשמשים לביצוע התקפות ביצוע מרחוק.

תובנות מעשיות

1. יש לבדוק את כל התעבורה בין מערכות בתוך מרכז נתונים או שירות ענן, ותעבורה המבקשת לגשת אליהם.
2. יש לפתח אסטרטגיית תגובת אבטחת רשת חזקה לאורך כל השנה.
3. יש להשתמש בשירותי אבטחה מקוריים בענן כדי ליישם מערך אבטחה חזק של 'אפס אמון' ברשת.

קישורים למידע נוסף

- יש לשפר את הגנות האבטחה מפני התקפות של תוכנות כופר באמצעות חומת האש של Azure | בלוג ועדכונים של Microsoft Azure
- אנטומיה של התקפת הגברת DDoS | הבלוג של Microsoft Security
- הגנה חכמה על אפליקציות מהקצה לענן באמצעות חומת האש של Azure Web Application | בלוג ועדכונים של Azure | Microsoft Azure

פיתוח גישה מאוזנת לאבטחת מידע ועמידות סייבר

הטרנספורמציה הדיגיטלית הניעה התרחבות עצומה של נכסי נתונים ועלייה בסיכוני אבטחה, תאימות ופרטיות. ארגונים עמידים לסייבר חייבים לאזן בין השקעות בהגנה על נתונים, תאימות ויכולות שחזור ולשלב אותן עם תהליכי תגובה רגולטוריים מיוחדים כדי לטפל בסוגים שונים של פריצות.

השאלה איננה האם יקרו פריצות לנתונים, אלא מתי. המחקר "עלות של פריצות לנתונים, 2021" של IBM ו-Ponemon Institute מדווח על עלות גלובלית ממוצעת של פריצות לנתונים של $4.24 מיליון דולר (עלייה של 10% לעומת השנה הקודמת) ו$9.05- מיליון דולר בארצות הברית. כשלי תאימות נמצאו כגורם המוביל להגברת העלויות. לעומת זאת, הפחתת עלויות הפריצה הייתה קשורה לשיטות עבודה מומלצות כגון תכנון תגובה לתקריות (IR), בשלות הפריסה של 'אפס אמון', בינה מלאכותית ואוטומציה של אבטחה ושימוש בהצפנה.

פריצות לנתונים הן בלתי נמנעות. ארגונים הנוקטים בגישת עמידות מאוזנת יפחיתו את התדירות, ההשפעה והעלות של פריצות.

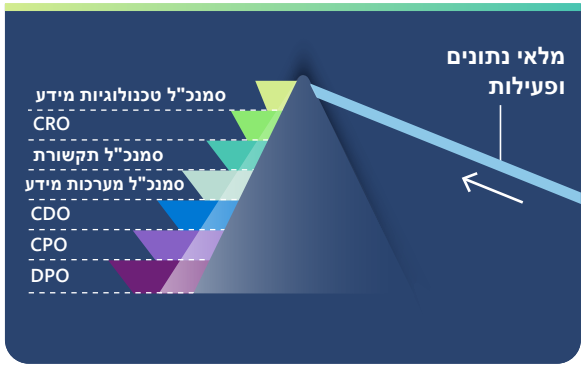
פיקוח על נתונים, אבטחה, תאימות ופרטיות תלויים זה בזה

בשנים האחרונות אנו רואים שנתונים זוכים לחשיבות כמנוע יצירת ערך חיוני עבור ארגונים. בה בעת, עלייתן של תקנות הפרטיות המחייבות הן פיקוח על נתונים והן אבטחה טשטשו את הגבולות בין תפקידי סיכון. בעוד שלתפקידים חדשים יותר ברמת C, כגון סמנכ"ל הנתונים (CDO) או סמנכ"ל הפרטיות (CPO) יש אינטרס באבטחה ובתאימות, היישום והתפעול של הגנת הנתונים מסתמכים לעתים קרובות על צוותים בראשות קציני המידע הראשיים (CIO) ו/או מנהל אבטחת המידע הראשי (CISO). זה לא חד כיווני, מכיוון שליוזמות פיקוח על נתונים בהובלת מנהלי CDO יש גם יתרונות אבטחה. כתוצאה מקשרים הדדיים אלה, צוותי IT, פיקוח על נתונים, אבטחה, תאימות ופרטיות צריכים לעבוד באופן הדוק יותר ויותר כדי להשיג יעילות ולנהל סיכונים.

פלטפורמות ניהול סיכוני נתונים מאוחדות עבור נכסי הנתונים של הארגון כולו הן העתיד

קשה לישר קו בין תהליכי ניהול ה-IT, הפיקוח על הנתונים, האבטחה, התאימות והפרטיות בסביבה של אפליקציות מותאמות אישית עבור כל דיסציפלינה וכיסוי לא עקבי על-פני פיזור הנתונים ההיברידי מרובה העננים הטיפוסי של הארגון. אנו מאמינים שארגונים זקוקים ל"חלון זכוכית יחיד" כדי לאתר ולדעת את הנתונים שלהם, להגן על הנתונים שלהם, לפקח על הגישה, השימוש ומחזור החיים של הנתונים ולמנוע אובדן נתונים בכל נכסי הנתונים.

עבודה מאותו מלאי נתונים ופרטי פעילות מקלה על תהליכים חוצי צוותים, מניבה תמונת סיכונים מקיפה יותר ומאפשרת לארגונים להתכונן טוב יותר ולייעל את תגובתם לפריצה.



"חלון הזכוכית היחיד" צריך לשמש כפריזמה. צוותים שיש להם עניין באבטחת נתונים, תאימות ופרטיות זקוקים לתצוגות שונות אך עקביות של אותו מלאי נתונים ופעילות כדי ליישר קו ולשתף פעולה. פעילות נתונים כוללת אירועי גישה לנתונים, שינוי ותנועה, שהם חלק חשוב ממשוואת אבטחת הנתונים.

פיקוח יעיל על נתונים, אבטחה, תאימות ופרטיות תלויים זה בזה ודורשים שיתוף פעולה בין צוותים.

תובנות מעשיות

1. יש לאזן בין הגנה לשחזור ולצמצם את השפעת פריצות הנתונים על-ידי השקעה ביכולות תאימות, הגנה על נתונים ותגובה.
2. יש לפתח ולאמץ תהליכים וכלים שחוצים ממגורות של סיכוני נתונים ומכסים את נכסי הנתונים המלאים.

קישורים למידע נוסף

- Microsoft Purview – פתרונות להגנה על נתונים | Microsoft Security
- העתיד של תאימות ופיקוח על נתונים כבר כאן: היכרות עם Microsoft Purview | הבלוג של Microsoft Security

עמידות למבצעי השפעה בסייבר: הממד האנושי

במהלך חמש השנים האחרונות, ההתקדמות בגרפיקה ובלמידת מכונה הציגה כלים קלים לשימוש המסוגלים ליצור במהירות תוכן איכותי ומציאותי שיכול להתפשט באופן נרחב ברחבי האינטרנט תוך שניות.

כשמדובר באירועים המדווחים באמצעות טקסט, אודיו ותוכן חזותי, הגענו לנקודה שבה לא בני אדם ולא אלגוריתמים יכולים להבחין באופן אמין בין עובדה לבדיה. התפשטותם של כלים אלה ותפוקותיהם מטילה בספק את אמינותם של כל אמצעי המדיה הדיגיטלית, ומשבשת את ההבנות שלנו לגבי אירועים מקומיים ועולמיים. לצורות חדשות של פעולות השפעה המתאפשרות על ידי התקדמות הטכנולוגיה יש השלכות חמורות על תהליכים דמוקרטיים.[11]

עולות שאלות לגבי מה אנו יכולים לעשות כדי להתכונן לעתיד עמיד יותר נגד מבצעי השפעה בסייבר האלה. הטכנולוגיה היא רק חלק אחד של התמונה. זה ידרוש מאמצים רבים, כולל חינוך המכוון לאוריינות מדיה, מודעות ודריכות, השקעות בעיתונות איכותית – עם כתבים מהימנים בזירה, המקומית, הארצית והבינלאומית – רשתות של שיתוף והתרעה על מבצעי השפעה, וסוגים חדשים של תקנות שמענישות גורמים זדוניים המייצרים או מתמרנים מדיה דיגיטלית במטרה להונות.

אנו גם מכירים בכך ששיקום האמון בתוכן דיגיטלי הוא יעד שאפתני שידרוש נקודות מבט מגוונות והשתתפות. אין חברה, או מוסד, או ממשלה אחת שיכולים לפתור את האיומים האלה בכוחות עצמם. כוח העל שלנו כבני אדם הוא היכולת שלנו לעבוד יחד ולשתף פעולה. זה חשוב במיוחד עכשיו כי זה יחייב את כולם – ממשלות גלובליות, תעשיות, אקדמיה, ובמיוחד ארגוני חדשות, חברה ומדיה – לעבוד יחד למען שיפור ובריאות החברה שלנו.

קישורים למידע נוסף

- אפליקציות לבינה מלאכותית במשימות סייבר של משרד ההגנה | Microsoft On the Issues
- בינה מלאכותית ואבטחת סייבר: אתגרים עולים וכיוונים מבטיחים. שימוע על יישומי בינה מלאכותית למבצעים במרחב הסייבר בפני ועדת המשנה לאבטחת סייבר, של ועדת הכוחות המזוינים של הסנאט, הקונגרס ה-17 (3 במאי 2022; עדותו של אריק הורביץ)

חיזוק הגורם האנושי באמצעות מיומנויות

טיפול בגורם האנושי הוא מרכיב מרכזי בכל אסטרטגיית מיומנות אבטחת סייבר. על פי המחקר "המרכיב האנושי באבטחת IT" של Kaspersky,[12] 46 אחוז מאירועי אבטחת הסייבר כוללים צוות רשלני או במדים שסייע בשוגג למתקפה.

צוות החינוך והמודעות של Microsoft בארגון האבטחה והעמידות הדיגיטליים אחראי על חיזוק הגורם האנושי של אבטחת הסייבר על-ידי העצמת העובדים לאבטחת המערכות והנתונים שלנו ושל לקוחותינו.
המטרות שלנו הן:

- להפחית את הסיכון ל-Microsoft וללקוחותינו על-ידי בניית מערך מיומנויות אבטחה מרכזי, כלל-ארגוני וריכוזי בקרב אוכלוסיית העובדים.
- לחזק את הידע על אבטחת עובדים באמצעות גישה רב-שלבית לחיזוק ההדרכה כדי לתמוך בתוצאות ההתנהגות הרצויות.
- לעודד שינוי תרבותי על-ידי הפיכתה של חשיבה אבטחתית לחלק מהותי מהתרבות של Microsoft באמצעות הדרכות ואירועי אבטחה הנדרשים מדי שנה.
- לקדם משאב אינטרנט ריכוזי במקום אחד לקבלת שיטות עבודה מומלצות, מידע על מדיניות החברה ודיווח על אירועים עבור כל מה שקשור לאבטחת סייבר.

תוכנית מיומנות ממוקדת ומרוכזת בתחום אבטחת הסייבר מגיעה לכל עובד של Microsoft לפחות פעם בשנה. הצעות ההדרכה ממוטבות כדי לתמוך ביוזמות אבטחת הסייבר הנוכחיות ולספק תוצאות התנהגות הניתנות למדידה. המועצה לניהול סיכוני מידע (IRMC) של Microsoft ממלאת תפקיד מרכזי בזיהוי תוצאות חשובות של שינוי התנהגות אבטחת סייבר שיש לטפל בהן באמצעות הדרכה.

בכל תוכניות מיומנות אבטחת הסייבר שלנו, אנו מודדים את היעילות, האפקטיביות והתוצאות של הפתרון במידת האפשר. לדוגמה, להצעת המיומנות שלנו לאיומים פנימיים יש תאימות הדרכה של 95 אחוז, שביעות רצון יוצאת דופן של הלומדים, והיא הביאה לעלייה משמעותית בדווחי מנהלים על מקרי איומים פנימיים אפשריים באמצעות הכלי Report It Now (דווח על זה עכשיו) של החברה. התכנית כוללת:

יסודות האבטחה: הדרכת מודעות ותאימות לאבטחת סייבר מרוכזת וכלל-ארגונית, העוסקת בשיטות עבודה בסיסיות של אבטחה ופרטיות. סדרת הדרכות זו שרבים ציפו לה, משתמשת במודל בידור חינוכי (edutainment) כדי להפוך את הלמידה על אבטחת סייבר למרתקת ומעניינת.

STRIKE: ההדרכה הטכנית הנדרשת של Microsoft עבור מהנדסים שבונים ומתחזקים פתרונות עסקיים. הדרכה זו שהיא בהזמנה בלבד עוסקת בתחומים עדכניים וקריטיים של שיטות עבודה מומלצות להיגיינת אבטחת סייבר ומשתמשת במודל העברה היברידי בשידור חי המותאם לצורכי הקהל.

תוכניות ספציפיות: תוכניות הדרכה ממוקדות התומכות ביוזמות ספציפיות של אבטחת סייבר, כולל Shadow IT, Insider Threat ו-Microsoft Federal. הצעות אלה משולבות באופן הדוק באסטרטגיית המעורבות הכוללת של יוזמות אבטחת הסייבר שלהן בהתאמה באמצעות חסות ההנהלה ודיווח על גבי כרטיסי ניקוד כדי למנוע גישת הדרכה של "סמן את התיבה".

MSProtect: משאב האינטרנט הריכוזי של Microsoft המספק שיטות עבודה מומלצות, מידע על מדיניות החברה ודיווח על אירועים עבור כל מה שקשור לאבטחת סייבר. משאב לפי דרישה זה הוא המועדף על עובדים מחוץ להצעות ההדרכה הרשמיות.

> אין לראות במיומנויות אבטחה פעילות של תאימות וסימון תיבות. במקום זאת, יש להתמקד בשינוי התנהגות כדי לאפשר ניטור תוצאות על פני התנהגויות יעד מזוהות, ולהקים מערכות הקשבה כדי לקבוע את השפעת ההצעות.

תובנות מעשיות

1. יש לספק הדרכה ומשאבי אבטחה לעובדים בזמן ובמקום שבהם הם זקוקים להם.
2. יש לפתח אסטרטגיית מיומנויות מרוכזת המעודכנת על-ידי בעלי עניין מכל רחבי הארגון.
3. יש לוודא שהשפעת ההדרכה נמצאת במעקב ומנותחת ליעילות (כמות), אפקטיביות (איכות) ותוצאות (השפעה עסקית).

קישורים למידע נוסף

- Microsoft משיקה את השלב הבא של יוזמת מיומנויות לאחר שעזרה ל-30 מיליון אנשים

תובנות מהתוכנית שלנו לחיסול תוכנות כופר

Microsoft פועלת בחמש השנים האחרונות במסע לקראת מודל אבטחהשל[13] 'אפס אמון' משלה כדי לוודא שבריאותם של זהויות ומכשירים נשמרת והם מנוהלים היטב. ככל שהסיכון לתוכנות כופר גדל, פיתחנו ראייה עמוקה שתתמוך בגישה שלנו להגנה על עצמנו ועל לקוחותינו.

לאחר הערכה פנימית מעמיקה, בנינו תוכנית לחיסול תוכנות כופר כדי לתקן פערים בבקרות ובכיסוי, לתרום לשיפורי תכונות עבור שירותים כגון Defender עבור נקודות קצה, Azure ו-M365, ולפתח מדריכים עבור צוותי ה-SOC וההנדסה שלנו לגבי אופן ההתאוששות במקרה של מתקפת תוכנת כופר.

הצעד הראשון היה להבין את היקף ההגנה שלנו מפני מתקפת כופר המכוונת כלפי Microsoft. המאמצים כבר היו בעיצומם כדי לפרוס את Defender עבור נקודת קצה ולהבטיח שכל המכשירים מנוהלים ותואמים למדיניות ה'אפס אמון' שלנו, אך היינו צריכים למצוא דרך להבין את כל ההיבטים של השאלה הגדולה יותר – האם נוכל להתאושש ביעילות מהתקפה. כדי לקבל תובנות, הערכנו את NIST 8374: ניהול סיכוני תוכנות כופר: פרופיל מסגרת אבטחת סייבר (CSF),[14] אשר מיישר קו עם המדיניות הארגונית הכוללת שלנו מול רשימת הבקרות הידועה שלנו. ניתוח זה זיהה במהירות פערים בכיסוי.

לאחר מכן, תיעדפנו פערים בין הפונקציות 'זהה', 'אתר', 'הגן', 'הגב' ו'שחזר' של ה-CSF. מצאנו התאמה אסטרטגית ל'אפס אמון' ולתוכניות אחרות וגם גילינו פערים שלא הייתה להם זרימת עבודה קיימת. לאחר שהערכנו את כמות העבודה והמאמץ הדרושים לתיקון פערים אלה, הפרדנו אותם לשני עמודי תווך:

- **הגנה על הארגון (PtE):** הגדרת פריטי עבודה שעלינו לעשות כארגון כדי להגן על עצמנו ולהיות מסוגלים להתאושש מהתקפות, אם אחת מהן תצליח.
- **הגנה על הלקוח (PtC):** בניית יכולות בהצעות שלנו כדי להגן על לקוחותינו כמו גם על העסק שלנו.

הטמעת ממצאים בארגון שלנו

כדי לתקן את הסיכונים העיקריים ולהגן על השירותים הקריטיים שלנו מפני מתקפת תוכנות כופר, אנו מתכננים למקד את ההשקעות במהלך 6 עד 12 החודשים הבאים בהשגת חמשת התרחישים הבאים כחלק מתוכנית כופר ייעודית. ברגע שנצליח בכל אחד מתרחישים אלה, נרחיב בהדרגה את היקף התוכנית כדי להגיע לכל חלקי הארגון.

תרחיש 1: חברי צוות האבטחה מבינים את הסיכון הכולל הקשור למתקפת כופר ויש להם תהליך שהוקם כדי לספק מודעות למנהלים על פערי בקרה וסטטוס הסיכון.

תרחיש 2: לחברי צוות האבטחה יש גישה למדריכים שנועדו לעזור להם ולצוותים אחרים ב-Microsoft להגיב למתקפת תוכנת כופר ולשחזר שירותים קריטיים שנפגעו כתוצאה ממנה.

תרחיש 3: לחברי צוות העמידות הארגונית יש תקן שיש לפעול לפיו לגיבוי מערכות קריטיות. מדריכים קיימים ותרגילים קבועים של גיבוי ושחזור נעשים כדי לוודא שניתן יהיה לשחזר נתונים במקרה של מתקפת תוכנות כופר.

תרחיש 4: בעלי שירותים מבינים ומיישמים את הבקרות והמדיניות הנדרשות בתחום האבטחה והתפעול כדי להגן על השירות, נתוני הלקוחות, נקודות הקצה ונכסי הרשת שלהם מפני התקפות של תוכנות כופר, תוך התמקדות מיוחדת בשירותים המתועדפים כשירותים קריטיים של Microsoft.

תרחיש 5: כל העובדים יכולים לגשת למשאבי למידה והדרכה המתארים כיצד לזהות מתקפת כופר וכיצד להודיע לצוות האבטחה ולהפעיל את התגובה.

תובנות מעשיות

1. יש לתעד ולאמת פעילויות שחזור ותיקון מקצה לקצה הקשורות למתקפות של תוכנות כופר נגד שירותים קריטיים.
2. יש לשתף את בעלי העניין בעדכון המדריכים של ניהול המשברים הארגוניים כך שיכללו פעילויות ספציפיות לתוכנות כופר ותהליך החלטה והדרכה כדי לקבוע אם/מתי לשלם עבור תוכנות כופר.
3. יש לשפר את כיסוי הזיהוי וההגנה על-ידי הפעלת היכולות הזמינות במוצרי האבטחה שנפרסו (לדוגמה, כללי צמצום משטח התקיפה של Defender עבור נקודות קצה).
4. יש לעבוד עם צוות תקני האבטחה להגדרת תוכנית בסיסית להגנה מפני מתקפת תוכנות כופר, ולספק הדרכה ותיעוד לצוותי ההנדסה על אופן ההתגוננות מפני מתקפת תוכנת כופר.
5. יש להשתמש באוטומציה כדי להקל על צוותי ה-DevOps את הפריסה של מדיניות האבטחה והתפעול ולהבטיח שאם מערכת סוטה מהתאימות, היא תסומן ותתוקן במהירות.

קישורים למידע נוסף

- שיתוף האופן שבו Microsoft מגנה מפני תוכנות כופר | Microsoft Inside Track

לפעול עכשיו לפי השלכות אבטחה קוונטית

הלחץ גובר לנהל את האיום שמחשוב קוונטי מציב לקריפטוגרפיה של ימינו ולכל מה שהיא מגינה עליו. התזכיר של מחלקת הביטחון הלאומי של מערכות קהילת המודיעין וההגנה שפורסם לאחרונה על שיפור אבטחת הסייבר[15] מתבסס על צו נשיאותי 10428 האמריקאי[16] לשיפור אבטחת הסייבר של האומה ומדגיש את אבטחת שרשרת אספקת התוכנה כקריטית לטיפול בהתקפות מדינתיות עתידיות.

מהם מחשבים קוונטיים?

מחשבים קוונטיים הם מכונות המשתמשות בתכונות של פיזיקה קוונטית לאחסון נתונים ולביצוע חישובים. זה יכול להיות בעל יתרון עצום עבור משימות מסוימות שבהן הם יכולים להשיג ביצועים טובים בהרבה אפילו ממחשבי העל הטובים ביותר שלנו. מחשוב קוונטי כבר פותח אופקים חדשים להצפנת נתונים ועיבודם. מחקרים צופים כי מחשוב קוונטי יהפוך לתעשייה קוונטית של מיליארדי דולרים כבר בשנת 2030.[17] למעשה, מחשוב קוונטי ותקשורת קוונטית צפויים להיות בעלי השפעה טרנספורמטיבית על פני מגוון רחב של תעשיות, החל מבריאות ואנרגיה ועד לפיננסים וביטחון.

מחשוב קוונטי הוא איום על הקריפטוגרפיה של ימינו ועל כל מה שהיא מגינה עליו.

האיום על הקריפטוגרפיה של ימינו

עם אלגוריתם שור משנת 1994 ומחשב קוונטי בקנה מידה תעשייתי של יותר מכמה מיליוני קיוביטים פיזיקליים, ניתן יהיה לשבור ביעילות את כל האלגוריתמים הקריפטוגרפיים עם מפתח ציבורי הנוכחיים שלנו, הפרוסים באופן נרחב. זהו עניין קריטי לשקול, להעריך ולתקנן מערכות הצפנה "בטוחות קוונטית" שהן יעילות, זריזות ובטוחות מפני התקפה מבוססת קוונטית יריבה. העברת תוכנה ל"קריפטוגרפיה פוסט-קוונטית", כלומר אלגוריתמים קלאסיים קיימים ופרוטוקולים חזקים יותר לתקיפה קוונטית, תדרוש שנים – אם לא עשור או יותר – להשגתה.[18]

משמעות הדבר היא שהלחץ גובר לנהל את האיום על הקריפטוגרפיה של ימינו ועל כל מה שהיא מגינה עליו. יריבים יכולים לתעד נתונים מוצפנים כעת ולנצל אותם מאוחר יותר ברגע שיהיה מחשב קוונטי זמין. אם נמתין להגעתו של מחשב קוונטי לפני שנתייחס להשלכות הקריפטוגרפיות שלו, זה יהיה מאוחר מדי.

מכיוון שנעשה שימוש בקריפטוגרפיה בכל המערכת האקולוגית של הסייבר, משמעות הדבר היא ששירותי האבטחה מבוססי הקריפטוגרפיה שלנו עלולים להיפרץ. לדוגמה, זה כולל שירותים לתקשורת (TLS, IPSec), העברת הודעות (דואר אלקטרוני, שיחות ועידה באינטרנט), ניהול זהויות וגישה, גלישה באינטרנט, חתימת קוד, עסקאות תשלום ושירותים אחרים התלויים בקריפטוגרפיה להגנה.

ככל שמחשבים קוונטיים הופכים למציאות, רכיבי תוכנה של צד שלישי המכילים יישומים של אלגוריתמים ויכולות קריפטוגרפיים ידרשו בדיקה נוספת גם כן. זה מחייב את כל הארגונים לאורך שרשרת הערך לעשות את חלקם כדי להבטיח שהשרשרת תישאר מאובטחת. גופים בתעשייה וממשלות מגבירים את המאמצים להגדיר את דרישות האבטחה של שרשרת אספקת התוכנה, ובמקרים מסוימים, מציגים מנדטים חדשים לאבטחת השרשרת. מזכר הביטחון הלאומי NSM-8[19] קובע דרישות ולוחות זמנים ליישום קריפטוגרפיה פוסט-קוונטית במערכות ביטחון לאומי (NSS). הוא מפרט את ציפיות התזמון תוך 180 יום ל"תכנון מודרניזציה, שימוש בהצפנה לא נתמכת, פרוטוקולים מאושרים ייחודיים למשימה, פרוטוקולים עמידים קוונטית ותכנון לשימוש בקריפטוגרפיה עמידה קוונטית במידת הצורך".

סטנדרטיזציה היא פעילות שדורשת זמן ממושך לביצועה במעבר לקריפטוגרפיה בטוחה קוונטית. ארגוני תקינה שעובדים על תקנים באמצעות קריפטוגרפיה של מפתח ציבורי חייבים להתחיל להתנסות באלגוריתמים פוסט-קוונטיים ולהסתגל אליהם עכשיו.

אלגוריתמים חדשים של קריפטוגרפיה פוסט-קוונטית (PQC) – אלגוריתמים קלאסיים שנחשבים חזקים למתקפה קוונטית – נמצאים כעת תחת בדיקה באמצעות פרויקט הסטנדרטיזציה הפוסט-קוונטית של NIST.[20] עבודה זו תשפיע על המאמצים הגלובליים בתוך ארגוני תקינה. על אף שתהיה חפיפה מסוימת עם בחירות האלגוריתמים של ממשלת ארה"ב, בחירות שונות של גופים לאומיים/רגולטוריים עבור אלגוריתמים תואמים עשויות להציב אתגרים בינלאומיים. פיצול זה יסבך בתורו את הנדסת המוצרים והשירותים.

אלגוריתמים חדשים של קריפטוגרפיה פוסט-קוונטית נמצאים בבדיקה באמצעות תוכנית הסטנדרטיזציה של קריפטוגרפיה פוסט-קוונטית של NIST. עבודה זו תשפיע על המאמצים הגלובליים בתוך ארגוני תקינה.

תובנות מעשיות

לצד SAFECode וחברים שותפים, על התעשייה לנקוט פעילויות מיידיות לטווח קצר יותר כדי להתכונן למעבר ל-PQC.[21] אלה כוללות:

1. יש לערוך רשימת מלאי של המוצרים/קודים המשתמשים בקריפטוגרפיה.
2. יש ליישם אסטרטגיית זריזות קריפטו ברחבי הארגון הכוללת צמצום נטישת הקוד הנדרשת כאשר הקריפטוגרפיה תשתנה.
3. לבצע פיילוט לשימוש באלגוריתמים המועמדים כבטוחים מבחינה קוונטית במוצרים או בשירותים המשתמשים בקריפטוגרפיה.
4. לוודא מוכנות לשימוש באלגוריתמים שונים של מפתח ציבורי להצפנה, פרוטוקול שיתוף מפתח (key exchange) וחתימות.
5. יש לבדוק את האפליקציות מבחינת ההשפעה של גדלי מפתח, צפנים וחתימות גדולים מאוד.

קישורים למידע נוסף

- Microsoft הדגימה את הפיזיקה הבסיסית הנדרשת ליצירת סוג חדש של קיוביטים | Microsoft Research

שילוב עסקים, אבטחה ו-IT לעמידות רבה יותר

עמידות סייבר חזקה תלויה במנהיגים עסקיים שעובדים עם צוותי אבטחה כדי ליישם אבטחה. מניסיונה של Microsoft, מנהיגות אבטחה היא דיסציפלינה מאתגרת הדורשת תמיכה ממנהיגים ארגוניים כדי להגן על הארגון בצורה היעילה ביותר.

מנהיגי אבטחה מנווטים בספקטרום של אתגרים דינמיים המתפרשים על פני נושאים הקשורים לסיכונים, טכנולוגיה, כלכלה, תהליכים ארגוניים, מודלים עסקיים, שינוי תרבות, אינטרסים גיאופוליטיים, ריגול וציות לסנקציות בינלאומיות. כל אחד מאלה נושא ניואנסים שיש להבין ולנהל היטב.

על מנהלי האבטחה מוטלת גם המשימה לסכל הן תוקפים אנושיים אינטליגנטיים, ממומנים היטב ובעלי מוטיבציה גבוהה, והן פושעי סייבר בעלי מיומנות נמוכה, אך יעילים. הצוותים שלהם חייבים להגן על נכסים טכניים מורכבים שנבנו לעתים קרובות בהדרגה במשך 30 שנה או יותר, כאשר האבטחה הייתה בעדיפות נמוכה או לא קיימת. החלטות שהתקבלו לפני שנים יכולות להוות סיכון היום עד שנשלם את החוב הטכני ונטפל בפערי האבטחה.

למנהיגים ארגוניים ולקובעי מדיניות יכולה להיות השפעה חיובית משמעותית על האבטחה על-ידי תמיכה פעילה במנהלי האבטחה וסיוע בבניית גשר בין אבטחה משולבת לבין שאר הארגון. כאשר Microsoft עובדת עם לקוחות בעלי התאמה זו, אנו רואים שהם בונים ארגון עמיד יותר וגם משפרים את זריזותם לצורך הסתגלות וחדשנות.

מנהיגות ארגונית יכולה לתמוך במנהלי אבטחה על ידי התמקדות בשלושה תחומים מרכזיים:

1. בניית אבטחה מתוכננת

אבטחה נתפסת לעתים כמכשול או כדבר שנעשה במחשבה שנייה בתהליכים עסקיים, ולעתים קרובות נשקלת בהחלטות רק כאשר מאוחר מדי להימנע מסיכון או לתקן בזול ובקלות.

מנהיגים ארגוניים וקובעי מדיניות צריכים לוודא שהם:

כוללים אבטחה בשלב מוקדם של יוזמות חדשות. על יוזמות דיגיטליות חדשות ואימוץ ענן לתעדף את האבטחה כדי לוודא שהסיכון הארגוני לא יגדל עם כל אפליקציה או יכולת דיגיטלית חדשות. לאחר שהאבטחה כלולה באופן מהימן, ניתן להשתמש בתהליכים אלה כדי להפוך מערכות מדור קודם למודרניות לקבלת יתרונות אבטחה ופרודוקטיביות בו-זמנית.

מנרמלים את התחזוקה המונעת לצורך אבטחה. יש לוודא שלתחזוקת האבטחה הבסיסית – כגון החלת עדכוני ותיקוני אבטחה ותצורות מאובטחות – מוקצית תמיכה ארגונית מלאה (כולל תקציבים, זמן השבתה מתוזמן, דרישות רכישה לתמיכה במוצרים של הספק).

למרבה הצער, ארגונים רבים מעכבים, דוחים או מיישמים שיטות עבודה נפוצות אלה באופן חלקי בלבד. זה מספק הזדמנויות נרחבות לניצול על ידי תוקפים. הצורך בנרמול האבטחה מתועד ב-NIST 800-40 של ארה"ב.[22]

2. לעסוק באבטחה

מנהיגים ארגוניים צריכים להשתתף באופן פעיל ולתת חסות לתהליכי אבטחה מרכזיים כדי להבטיח תעדוף של משאבים ומוכנות לאסונות אבטחתיים. זה כולל עיסוק ב:

זיהוי נכסים עסקיים קריטיים. מנהלי וצוותי אבטחה צריכים לדעת אילו נכסים הם קריטיים לעסק כדי למקד את משאבי האבטחה בדברים החשובים ביותר. לעתים קרובות זהו תרגיל חדש הכולל שאילת שאלות חדשות שלא טופלו בעבר ומתן מענה להן.

תרגילי המשכיות עסקית של אבטחת סייבר והתאוששות מאסונות מתקפות סייבר יכולות להפוך לאירועים מרכזיים שמשבשים או עוצרים את רוב הפעולות העסקיות או את כולן. הקפדה על מוכנות הצוותים ברחבי הארגון להתמודד עם מצבים אלה תקצר את הזמן לשחזור הפעולות העסקיות, תצמצם את הנזק לארגון ותסייע לשמור על האמון והביטחון של הלקוחות, האזרחים והבוחרים. זה צריך להיות משולב בתהליך ההמשכיות העסקית וההתאוששות מאסון הקיים.

החלטות על סיכוני אבטחה מתקבלות בצורה הטובה ביותר על ידי בעלי עסקים או משימות שיש להם תמונה מלאה של כל הסיכונים וההזדמנויות.

שילוב עסקים, אבטחה ו-IT לעמידות רבה יותר

המשך

3. מיקום האבטחה בצורה נכונה

האופן שבו ארגונים בונים אחריות לסיכוני אבטחה גורם להם לעתים קרובות לקבלת החלטות לקויה בנוגע לסיכוני אבטחה. החלטות לגבי סיכונים מתקבלות בצורה הטובה ביותר על-ידי בעלי עסקים או משימות שיש להם את התמונה המלאה לגבי כל הסיכונים וההזדמנויות. אך במקום זאת, לעתים קרובות ארגונים מקצים אחריות (במרומז או במפורש) על סיכוני האבטחה למומחים לנושא בצוות האבטחה. הדבר מטיל נטל לא בריא על צוותי האבטחה תוך שלילת הנראות והשליטה של בעלי עסקים על סיכון מרכזי לעסק שלהם. ארגונים יכולים לתקן זאת על ידי:

הכנת בעלי העסקים: ללמד את בעלי העסקים לגבי סיכוני אבטחה באופן כללי וכיצד איומים אלה יכולים להשפיע על העסק שלהם ואף יעשו זאת. שילוב ישיר של צוותי אבטחה במאמץ זה גם מגביר את הקשר השיתופי עם האבטחה והזריזות העסקית הכוללת.

הקצאת סיכוני האבטחה לבעלי עסקים: ככל שבעלי העסקים מקבלים מספיק מידע כדי להבין ולקבל את סיכוני האבטחה, על הארגון להעביר אליהם במפורש את האחריות על סיכוני האבטחה, תוך המשך הטלת האחריות על צוותי האבטחה לניהול סיכון זה ולמתן מומחיות והדרכה מושכלות לבעלים.

"עמידות הסייבר היא בסולם נע בין המשכיות עסקית קלאסית והתאוששות מאסון, החל מגיבוי נתונים טוב; התקדמות ליכולות שחזור של תהליכים, טכנולוגיה ויחסי התלות שלהם (כולל אנשים וצדדים שלישיים); ומעבר לשירותים הפועלים תמיד, בעלי יכולת ריפוי עצמי, עמידות עבור תפקידים קריטיים וכשלים עבור צדדים שלישיים קריטיים. הארגונים העמידים ביותר מקדמים אינטגרציה בין IT, מנהלי עסקים ומומחי אבטחה. עמידות נהדרת כוללת תכנון לעמידות מההתחלה, ניהול שינויים בטוח ובידוד תקלות פרטני. עמידות סייבר היא רק תרחיש אחד בתוכנית תכנון טובה של כל הסיכונים. ככל שסיכוני הסייבר גדלים והמפגש בין אבטחת סייבר לעמידות הופך לחשוב יותר, החיבור של סמנכ"ל אבטחת המידע (CISO) לתוכנית העמידות הארגונית מתחזק. בכל שנה, יותר מנהלי CISO לוקחים בעלות על העמידות של החברה כולה".

ליסה רשאור
מנהלת כללי, ניהול סיכונים, Microsoft

קישורים למידע נוסף

- מעמידות להתמדה דיגיטלית: כיצד ארגונים משתמשים בטכנולוגיה דיגיטלית כדי להשתפר בזמנים חסרי תקדים | הבלוג הרשמי של Microsoft
- כיצד צוותי IT ואבטחה יכולים לעבוד יחד כדי לשפר את אבטחת נקודות הקצה | Microsoft Security

עקומת הפעמון של עמידות הסייבר

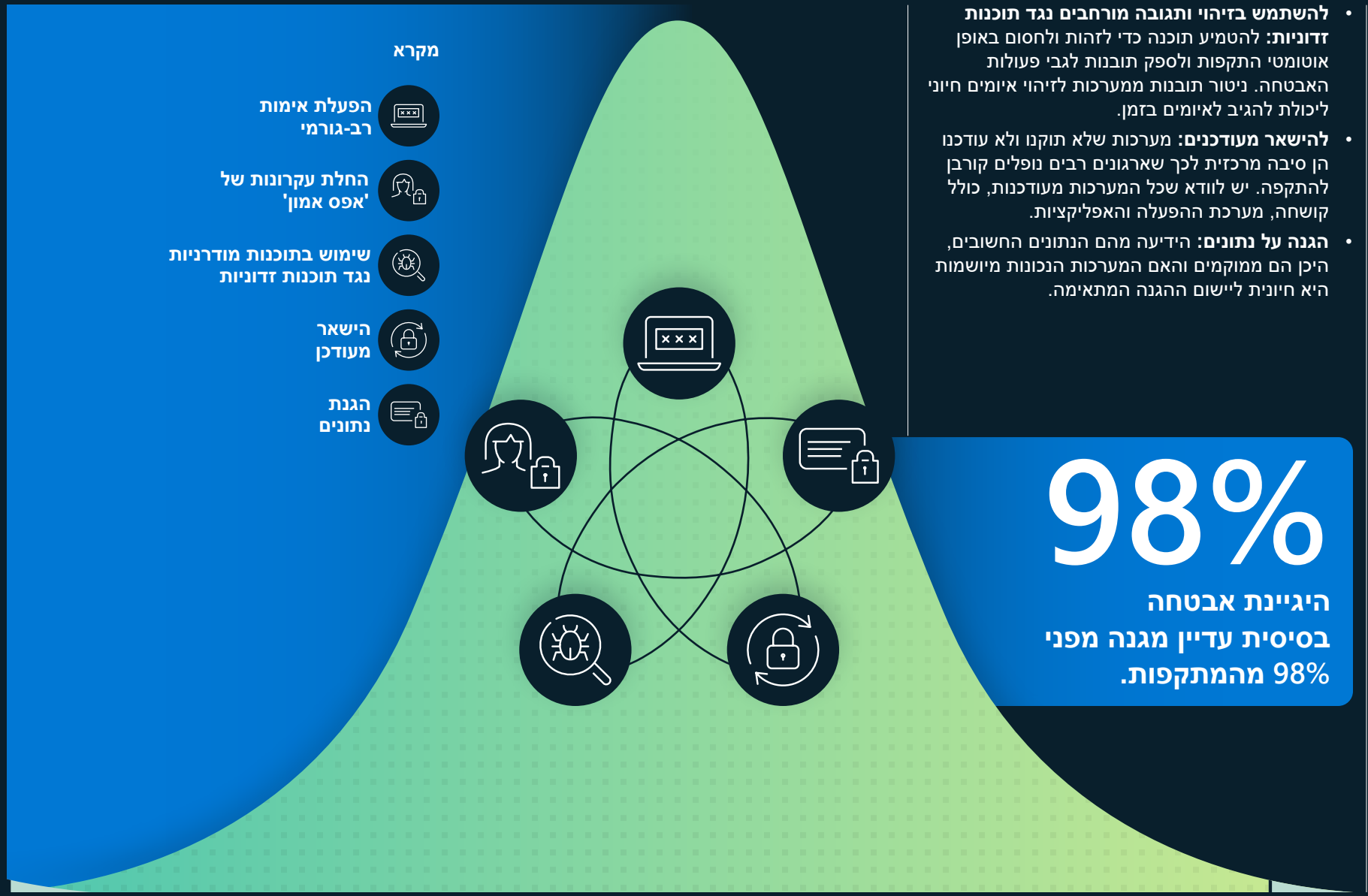
גורמי הצלחה לעמידות שכל ארגון צריך לאמץ

כפי שראינו, מתקפות סייבר רבות מצליחות פשוט משום שלא הקפידו על היגיינת אבטחה בסיסית.
הסטנדרטים המינימליים שכל ארגון צריך לאמץ הם:

- **לאפשר אימות רב-גורמי (MFA):** כדי להגן מפני סיסמאות משתמש שנפרצו ומסייע לספק עמידות נוספת לזהויות.
- **להחיל את עקרונות 'אפס אמון':** אבן הפינה של כל תוכנית עמידות המגבילה את ההשפעה על הארגון. עקרונות אלה הם:

1. – אימות מפורש – לוודא שהמשתמשים והמכשירים נמצאים במצב טוב לפני שמאפשרים גישה למשאבים.
2. – להשתמש בהרשאת גישה מינימלית – לאפשר רק את ההרשאה הדרושה לצורך גישה למשאב ולא יותר.
3. – להניח שמתרחשת פריצה – להניח שהגנות המערכת נפרצו ושיתכן כי המערכות יפרצו. משמעות הדבר היא ניטור מתמיד של הסביבה להתקפה אפשרית.

- **להשתמש בזיהוי ותגובה מורחבים נגד תוכנות זדוניות:** להטמיע תוכנה כדי לזהות ולחסום באופן אוטומטי התקפות ולספק תובנות לגבי פעולות האבטחה. ניטור תובנות ממערכות לזיהוי איומים חיוני ליכולת להגיב לאיומים בזמן.
- **להישאר מעודכנים:** מערכות שלא תוקנו ולא עודכנו הן סיבה מרכזית לכך שארגונים רבים נופלים קורבן להתקפה. יש לוודא שכל המערכות מעודכנות, כולל קושחה, מערכת ההפעלה והאפליקציות.
- **הגנה על נתונים:** הידיעה מהם הנתונים החשובים, היכן הם ממוקמים והאם המערכות הנכונות מיושמות היא חיונית ליישום ההגנה המתאימה.



98%

היגיינת אבטחה בסיסית עדיין מגנה מפני 98% מהמתקפות.

הערות סיום

1. זיהוי נקודות קצה ומתן תגובה (EDR) היא פלטפורמת אבטחה לנקודות קצה ארגוניות המיועדת לעזור לרשתות ארגוניות למנוע, לאתר, לחקור ולהגיב לאיומים מתקדמים. יכולות הזיהוי והתגובה של נקודות קצה מספקות זיהויי התקפות מתקדמים, כמעט בזמן אמת כך שניתן לפעול לגביהם. מנתחי אבטחה יכולים לתעדף התראות ביעילות, לקבל נראות לגבי ההיקף המלא של הפריצה ולנקוט פעולות תגובה כדי לתקן איומים.
2. פלטפורמת הגנה על נקודות קצה (EPP) היא פתרון הפרוס במכשירי נקודות קצה כדי למנוע תוכנות זדוניות מבוססות קבצים, לזהות ולחסום פעילות זדונית מאפליקציות מהימנות ולא מהימנות ולספק את יכולות החקירה והתיקון הדרושות כדי להגיב באופן דינמי לאירועי אבטחה והתראות.
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. ספר האבטחה של Windows: מסחרי
7. תכונות אבטחה חדשות עבור Windows 11 יעזרו להגן על עבודה היברידית | הבלוג של Microsoft Security
8. ברית FIDO: תקני אימות פתוח מאובטחים יותר מסיסמאות
9. https://interpret.ml/
10. עשרת הגדולים של OWASP | קרן 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. צו נשיאותי 14028 לשיפור אבטחת הסייבר של המדינה
17. https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth
18. "הדרך הארוכה לפנינו למעבר לקריפטוגרפיה פוסט-קוונטית," 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

צוותים משתתפים

צוותים משתתפים

הנתונים והתובנות בדוח זה סופקו על-ידי קבוצה מגוונת של אנשי מקצוע הממוקדים באבטחה, העובדים בצוותים רבים ושונים של Microsoft. ביחד, מטרתם היא להגן על Microsoft, על לקוחותיה ועל העולם כולו מפני האיומים של מתקפות הסייבר. אנו גאים לשתף את התובנות הללו ברוח השקיפות עם מטרה משותפת להפוך את העולם למקום בטוח יותר עבור כולם.

AI for Good Research Lab: רתימת העוצמה של נתונים ובינה מלאכותית כדי להתמודד עם רבים מהאתגרים בעולם. המעבדה משתפת פעולה עם ארגונים מחוץ ל-Microsoft ומיישמת בינה מלאכותית לשיפור הפרנסה והסביבה. תחומי ההתמקדות כוללים בטיחות באינטרנט (דיסאינפורמציה, אבטחת סייבר, בטיחות ילדים), תגובה לאסונות, קיימות ובינה מלאכותית לבריאות.

Enterprise & OS ,Azure Edge & Platform Security: אחראית על אבטחת הליבה של מערכת ההפעלה והפלטפורמה ב-Windows, Azure ומוצרים אחרים של Microsoft. הצוות בונה פתרונות אבטחה וחומרה מובילים בתעשייה בפלטפורמות של Microsoft כדי לצמצם את הפריצה לנקודות תורפה, לזהויות ואת הפריצה עם תוכנות זדוניות מהשבב לענן. יוצרי פלטפורמת הליבה המאובטחת של Microsoft במחשב, ב-Edge ובשרת, במעבד האבטחה של Microsoft Pluton ועוד.

Azure Networking ,Core: צוות עבודה ברשת בענן המתמקד ב-Microsoft WAN, רשתות Datacenter ותשתית הרשת המוגדרת על-ידי התוכנה של Azure, כולל פלטפורמת DDoS, פלטפורמת קצה הרשת ומוצרי אבטחת רשת כגון Azure WAF, חומת האש של Azure ו-Azure DDoS Protection Standard.

Microsoft Defender Experts: הארגון הגלובלי הגדול ביותר של Microsoft, המורכב מחוקרי אבטחה ממוקדי מוצרים, מדענים יישומיים ומנתחי מודיעין בתחום האיומים. צוות Defender Experts מספק יכולות זיהוי ותגובה חדשניות במוצרי האבטחה של Microsoft 365 והשירותים המנוהלים של Microsoft Defender Experts.

Microsoft Defender עבור IoT: צוות המורכב מחוקרים מומחי תחום המתמחים בהנדסה לאחור של תוכנות זדוניות, פרוטוקולים וקושחה של IoT/OT. הצוות צד אחר איומי IoT/OT כדי לחשוף מגמות וקמפיינים זדוניים.

One Engineering System (1ES): צוות שמטרתו לספק כלים ברמה עולמית כדי לעזור למפתחים של Microsoft להיות פרודוקטיביים ומאובטחים ככל האפשר. הצוות מוביל את האסטרטגיה המרכזית לאבטחת שרשרת אספקת התוכנה מקצה לקצה של Microsoft.

אבטחה דיגיטלית ועמידות (DSR): ארגון המוקדש לאפשר ל-Microsoft לבנות את המכשירים והשירותים המהימנים ביותר, תוך שמירה על בטיחות החברה שלנו, ועל נתוני החברה והלקוחות שלנו מוגנים.

אבטחת M365: ארגון המפתח פתרונות אבטחה, כולל Microsoft Defender עבור נקודות קצה (MDE), Microsoft Defender עבור זהות (MDI) ואחרים, כדי לאבטח לקוחות ארגוניים.

אבטחת זהות וגישה לרשת (IDNA): צוות שעובד כדי להגן על כל לקוחות Microsoft מפני גישה לא מורשית והונאה. IDNA Security הוא צוות חוצה דיסציפלינות של מהנדסים, מנהלי מוצר, מדעני נתונים וחוקרי אבטחה.

אמון ואבטחת לקוחות (CST): צוות המקדם שיפור מתמשך של אבטחת הלקוחות במוצרים ובשירותים המקוונים של Microsoft. צוות CST משתף פעולה עם צוותי הנדסה ואבטחה בכל רחבי החברה ומשימתו היא להבטיח את רמת התאימות ולשפר את האבטחה והשקיפות כדי להגן על הלקוחות ולקדם אמון גלובלי ב-Microsoft.

ארגון ואבטחה: צוות המתמקד במתן פלטפורמה מודרנית, מאובטחת וניתנת לניהול עבור הענן החכם והקצה החכם.

דיפלומטיה דיגיטלית: צוות בינלאומי של דיפלומטים לשעבר, קובעי מדיניות ומומחים משפטיים הפועלים לקידום מרחב סייבר שליו, יציב ומאובטח לנוכח הסכסוך הגובר בין מדינות.

הבינה המלאכותית, האתיקה וההשפעות בהנדסה ובמחקר של Microsoft (AETHER): ועדה מייעצת ב-Microsoft שמטרתה להבטיח שטכנולוגיות חדשות יפותחו ויעובדו באופן אחראי.

החיפוש וההפצה של Microsoft Bing: צוות שמטרתו לספק מנוע חיפוש אינטרנטי ברמה עולמית, המאפשר למשתמשים ברחבי העולם למצוא תוצאות חיפוש ומידע מהימנים במהירות, כולל מעקב אחר נושאים וסיפורים טרנדיים החשובים להם, תוך מתן שליטה למשתמשים על פרטיותם.

היחידה לפשעים דיגיטליים (DCU): צוות של עורכי דין, חוקרים, מדעני נתונים, מהנדסים, אנליסטים ואנשי עסקים המסורים למאבק בפשעי סייבר בקנה מידה עולמי באמצעות טכנולוגיה, זיהוי פלילי, תביעות אזרחיות, תביעות פליליות ושותפויות ציבוריות ופרטיות כאחד.

המרכז למודיעין על איומים תפעוליים (OpTIC): הצוות האחראי על ניהול והפצה של מודיעין איומי סייבר התומך במשימה של מרכז תפעול הגנת הסייבר (CDOC) של Microsoft להגן על Microsoft ועל לקוחותינו.

המרכז לניתוח איומים דיגיטליים (DTAC): צוות מומחים המנתח ומדווח על איומי מדינות, כולל מתקפות סייבר ומבצעי השפעה. הצוות משלב מידע ובינה איומי סייבר עם ניתוח גיאופוליטי כדי לספק תובנות ללקוחות שלנו ול-Microsoft לצורך יידוע לגבי תגובה יעילה והגנות.

צוותים משתתפים

המשך

הצלחת לקוחות: צוותי אבטחה ב'הצלחת לקוחות' עובדים ישירות עם לקוחות כדי לשתף שיטות עבודה מומלצות, לקחים שנלמדו והדרכה כדי להאיץ את הטרנספורמציה והמודרניזציה של האבטחה. צוות זה מרכיב ומארגן שיטות עבודה מומלצות ולקחים שנלמדו מהמסע של Microsoft – כמו גם של הלקוחות שלנו – לאסטרטגיות ייחוס, ארכיטקטורות ייחוס, תוכניות ייחוס ועוד.

יוזמת Democracy Forward: צוות של Microsoft הפועל לשימור, הגנה וקידום של יסודות הדמוקרטיה על-ידי קידום מערכת אקולוגית בריאה של מידע, שמירה על תהליכים דמוקרטיים פתוחים ומאובטחים וקידום אחריות אזרחית תאגידית.

יחידת האבטחה הדיגיטלית (DSU): צוות של עורכי דין ואנליסטים בתחום אבטחת הסייבר המספקים מומחיות משפטית, גיאופוליטית וטכנית כדי להגן על Microsoft ולקוחותיה. DSU בונה אמון בהגנות האבטחה הארגוניות של Microsoft מפני יריבי סייבר מתקדמים ברחבי העולם.

מדיניות אבטחת סייבר גלובלית: צוות שעובד עם ממשלות, ארגונים לא ממשלתיים ושותפים בתעשייה כדי לקדם מדיניות ציבורית בנושא אבטחת סייבר המעצימה את הלקוחות לחזק את האבטחה והעמידות שלהם כשהם מאמצים את הטכנולוגיה של Microsoft.

מודיעין האיומים של Microsoft Defender (RiskIQ): צוות שמייצר מודיעין טקטי באמצעות ניתוח של אוסף הטלמטריה החיצונית הנרחב של Microsoft, מתווה את נוף האיומים עם התפתחותו כדי לגלות תשתית איומים שלא הייתה ידועה קודם לכן, ומוסיף הקשר לגורמי איום ולקמפיינים. הצוות מפרסם באופן קבוע מחקרים עדכניים וייחודיים כדי לספק מודיעין טקטי חיוני למגנים.

מרכז המודיעין לגבי איומים של Microsoft (MSTIC): צוות המתמקד בזיהוי, מעקב ואיסוף מודיעין הקשור ליריבים המתוחכמים ביותר המשפיעים על לקוחותיה של Microsoft, כולל איומים ברמת מדינה, תוכנות זדוניות ודיוג.

מרכז התגובה לאבטחה של Microsoft (MSRC): צוות המעורב בחוקרי אבטחה שפועלים להגן על הלקוחות ועל המערכת האקולוגית של השותפים של Microsoft. MSRC, המהווה חלק בלתי נפרד ממרכז התפעול להגנת סייבר (CDOC) של Microsoft, מקבץ יחדיו מומחים למתן תגובה לתקריות אבטחה כדי לזהות איומים ולהגיב להם בזמן אמת.

מרכז התפעול להגנת סייבר (CDOC): מתקן אבטחת הסייבר וההגנה של Microsoft הוא כור היתוך שמקבץ יחדיו מומחי אבטחה מכל רחבי החברה כדי להגן על התשתית הארגונית ועל תשתית הענן שלנו שנגישה עבור הלקוחות. מומחים המגיבים לתקריות משתפים פעולה עם מדעני נתונים ומהנדסי אבטחה מכל קבוצות השירותים, המוצרים והמכשירים של Microsoft כדי לעזור לזהות איומים, להגיב להם ולהתגונן מפניהם מסביב לשעון.

ניהול סיכונים ארגוניים: צוות העובד בין יחידות עסקיות כדי לתעדף דיוני סיכונים עם ההנהגה הבכירה של Microsoft. ERM מחבר צוותי סיכונים תפעוליים מרובים, מנהל את מסגרת הסיכונים הארגוניים של Microsoft ומקל על הערכת האבטחה הפנימית של החברה באמצעות מסגרת אבטחת הסייבר NIST.

ניידות ארגונית: צוות שעוזר לספק את מקום העבודה המודרני ואת הניהול המודרני כדי לשמור על אבטחת הנתונים, בענן ובסביבה המקומית. מנהל נקודות הקצה כולל את השירותים והכלים שבהם Microsoft והלקוחות משתמשים כדי לנהל ולנטר מכשירים ניידים, מחשבים שולחניים, מכונות וירטואליות, מכשירים מוטמעים ושרתים.

פתרונות של Microsoft ללקוחות ולשותפים: ארגון מסחרי מאוחד של Microsoft לנושא יציאה לשוק, האחראי על תפקידי שטח דוגמת מומחי אבטחה ומכירות טכניות ויועצים.

צוות המחקר אבטחת ענן: על-ידי אבטחת הענן של Microsoft, בניית תכונות ומוצרי אבטחה חדשניים ועריכת מחקר, צוות זה מגן על לקוחות Microsoft ומאפשר להם לחולל שינוי מאובטח בארגונים שלהם.

צוות הפיתוח העסקי של Microsoft Security: צוות שמוביל את אסטרטגיית הצמיחה, השותפויות וההשקעות האסטרטגיות של Microsoft בתחום אבטחת הסייבר.

שירותי האבטחה של Microsoft לתגובה לאירועים: צוות של מומחי אבטחת סייבר המסייעים ללקוחות לעבור את מתקפת הסייבר כולה, החל מהחקירה ועד לפעילויות מוצלחות הקשורות לבלימה ושחזור. השירותים מוצעים באמצעות שני צוותים משולבים ביותר, הצוות לזיהוי ותגובה (DART) עם דגש על החקירה ועבודת השטח לשחזור, ונוהל האבטחה לשחזור מפריצה (CRSP), המתמקד בהיבטי הבלימה והשחזור.

Microsoft

הארת נוף האיומים והעצמת ההגנה הדיגיטלית.

מידע נוסף: https://microsoft.com/mddr

מידע מפורט יותר: https://blogs.microsoft.com/on-the-issues/

הישאר מחובר: @msftissues ו- @msftsecurity