Microsoft

《2022 年 Microsoft 数字防御报告》

阐明威胁格局和增强数字防御的能力。

目录

除非另有说明，否则本报告中的数据、见解和事件均来自 2021 年 7 月至 2022 年 6 月（Microsoft 2022 财年）。

为了获得查看和浏览此报告的最佳体验，建议使用 Adobe Reader，该程序可从 Adobe 网站上免费下载。

报告引言 02

网络犯罪现状 06

网络犯罪现状概述 07
引言 08
勒索软件和敲诈勒索：国家层面的威胁 09
来自一线响应者的勒索软件见解 14
网络犯罪即服务 18
不断演变的网络钓鱼威胁格局 21
Microsoft 通过早期协作破坏僵尸网络的时间线 25
网路犯罪分子滥用基础结构 26
黑客入侵是否成为常态? 28

国家层面威胁 30

国家层面威胁概述 31
引言 32
民族国家数据的背景 33
国家层面行为者及其活动的示例 34
不断演变的威胁格局 35
关键基础设施攻击趋势 36
IT 供应链作为数字生态系统的门户 37
快速漏洞利用 39
俄罗斯国家层面行为者的战时网络策略威胁着乌克兰及其他地区 41
中国扩大全球目标以获得竞争优势 44
伊朗在权力交接后行事愈发激进 46
朝鲜利用网络功能实现政权的三个主要目标 49
网络雇佣兵威胁网络空间的稳定性 52
实施网络安全规范，确保网络空间和平与安全 53

设备与基础结构 56

设备与基础结构概述 57
引言 58
政府纷纷采取行动提升关键基础设施安全性和复原能力 59
IoT 和 OT 设备暴露：趋势和攻击 62
供应链和固件黑客攻击 65
聚焦固件漏洞 66
基于侦察的 OT 攻击 68

网络影响行动 71

网络影响力行动概述 72
引言 73
网络影响力行动的趋势 74
聚焦 COVID-19 和俄罗斯入侵乌克兰期间的影响力行动 76
跟踪俄罗斯宣传指数 78
合成媒体 80
防范网络影响力行动的整体方法 83

网络复原能力 86

网络复原能力概述 87
引言 88
网络复原能力：互联社会的关键基础 89
实现系统和架构现代化的重要性 90
基本安全状况是高级解决方案有效性的决定性因素 92
保持身份健康是组织健康运作的基础 93
操作系统默认安全设置 96
软件供应链的集中性 97
建立针对新兴 DDoS、Web 应用程序和网络攻击的复原能力 98
开发平衡的数据安全方法和网络复原能力 101
针对网络影响力行动的复原能力：人文层面 102
通过技能强化人为因素 103
来自我们的勒索软件消除计划的见解 104
立即就量子安全问题采取行动 105
整合业务、安全性和 IT 资源以提高复原能力 106
网络复原能力钟形曲线 108

参与团队 110

客户安全与信任部、公司副总裁

Tom Burt 的引言

“我们分析的来自全球产品和服务生态系统的数万亿信号揭示了全球数字威胁的凶猛程度、范围和规模”

威胁格局简介 .....

威胁格局的范围和规模

密码攻击的数量已增加到估计每秒 921 次攻击 - 在短短一年内增加了 74%。

消除网络犯罪

到目前为止，Microsoft 已清除网络犯罪分子使用的 10,000 多个域和国家层面行为者使用的 600 多个域。

解决漏洞

93% 的勒索软件事件响应工作显示出，被攻击者对权限访问和横向移动的控制不足。

2022 年 2 月 23 日，网络安全世界进入一个新的时代，即混合战争时代。当天，在导弹发射和坦克越过边界的前几个小时，俄罗斯行动者以乌克兰政府、技术和金融行业为目标，发动了大规模的破坏性网络攻击。此第三版年度《Microsoft 数字防御报告》(MDDR) 的“国家层面威胁”一章中详细介绍了这些攻击以及从中获得的经验教训。在这些经验教训中，关键的一点是，云提供了针对网络攻击的最佳物理和逻辑安全保障，并在威胁情报和终结点保护方面取得了进步，其价值已在乌克兰得到验证。

虽然对今年网络安全发展的任何调查都必须从此处开始，但今年的报告提供了更深入的探讨。在本报告的第一章，我们将重点介绍网络犯罪分子的活动，然后在第二章介绍国家层面威胁。这两个群体都大大提高了攻击的复杂性，显著增加了其行动的影响。在俄罗斯占据新闻头条的同时，伊朗行动者在总统权力交接后升级了其攻击方式，对以色列发动了破坏性攻击，并针对美国的关键基础结构发动了勒索软件和“入侵并泄露”行动。中国还加强了在东南亚和南半球其他地区的间谍活动，试图对抗美国的影响力并窃取关键数据和信息。

如第三章所述，外国行为者也正在使用高效技术在全球各地区开展宣传影响行动。例如，俄罗斯一直在努力说服本国公民和许多其他国家 / 地区的公民，让他们相信其入侵乌克兰是正当的，同时也在西方散播抹黑 COVID 疫苗的宣传，并在国内宣传疫苗的有效性。此外，行动者越来越多地将物联网 (IoT) 设备或运营技术 (OT) 控制设备作为网络和关键基础结构的入口点，这点将在第四章中讨论。最后，在最后一章，我们回顾了今年在网络复原能力方面取得的进展，提供了过去一年中从抵御针对 Microsoft 和我们客户的攻击中获得的见解和教训。

每一章都提供了基于 Microsoft 独特优势的重要经验教训和见解。我们分析的来自全球产品和服务生态系统的数万亿信号，揭示了全球数字威胁的凶猛程度、范围和规模。Microsoft 正在采取行动，保护我们的客户和数字生态系统免受这些威胁。您将从下文了解我们的技术如何识别和阻止针对我们客户的数十亿网络钓鱼企图、身份盗窃和其他威胁。

Tom Burt 的引言
续

我们还使用法律和技术手段，查封和关闭网络犯罪分子和国家层面行为者使用的基础结构，并向受到国家层面行为者威胁或攻击的客户发送通知。我们致力于开发越来越有效的功能和服务，使用 AI/ML 技术识别和阻止网络威胁，安全专业人员也能够更快速、更有效地识别和防御网络入侵。

也许最重要的是，在整个 MDDR 中，我们针对个人、组织和企业可以采取的措施提供了切实建议，帮助他们抵御这些日益增长的数字威胁。采用良好的网络安全机制的做法是最有效的防御措施，可以显著降低网络攻击的风险。

网络犯罪现状

网络犯罪分子继续作为精明的盈利企业行事。攻击者正在适应并寻找实施其技术的新方法，从而增加了其攻击行动基础结构托管方式和位置的复杂性。与此同时，网络犯罪分子变得更加节俭。为了降低开销并提高合法性，攻击者正在入侵业务网络和设备，以托管网络钓鱼活动、恶意软件，甚至利用其计算能力来挖掘加密货币。

详情请参见第 6 页

“乌克兰混合战争中网络武器的部署，标志着一个新的冲突时代的到来。”

国家层面威胁

国家层面行为者正在发起越来越复杂的网络攻击，旨在逃避检测并进一步推进其战略重点。乌克兰混合战争中网络武器的部署，标志着一个新的冲突时代的到来。俄罗斯还通过信息影响行动支持战争，利用宣传来影响俄罗斯、乌克兰和全球的舆论。在乌克兰以外地区，国家层面行为者活动更加猖獗，开始利用自动化、云基础结构和远程访问技术方面的进步来攻击更广泛的目标。提供对最终目标访问权限的企业 IT 供应链经常遭到攻击。随着行为者迅速利用未修补的漏洞，使用复杂和暴力的技术来窃取凭据，并使用开源或合法软件混淆其行动，网络安全机制变得更加关键。此外，伊朗还加入了俄罗斯的行列，使用包括勒索软件在内的破坏性网络武器作为攻击的主要手段。

这些形势的发展迫切需要采用一致的全球框架、优先考虑人权并保护人们免受网上鲁莽的国家行为的伤害。所有国家 / 地区都应共同努力，实施负责任的国家 / 地区行为准则和规则。

详情请参见第 30 页

设备与基础结构

各类面向互联网的设备被迅速采用，再加上疫情的原因，成为加速数字化转型的一个组成部分，极大地增加了我们数字世界的攻击面。因此，网络犯罪分子和民族国家迅速乘机而入。虽然近年来 IT 硬件和软件的安全性得到了加强，但 IoT 和 OT 设备的安全性却没有跟上。威胁行为者正在利用这些设备在网络上建立访问并实现横向移动，在供应链中建立立足点，或破坏目标组织的 OT 运营。

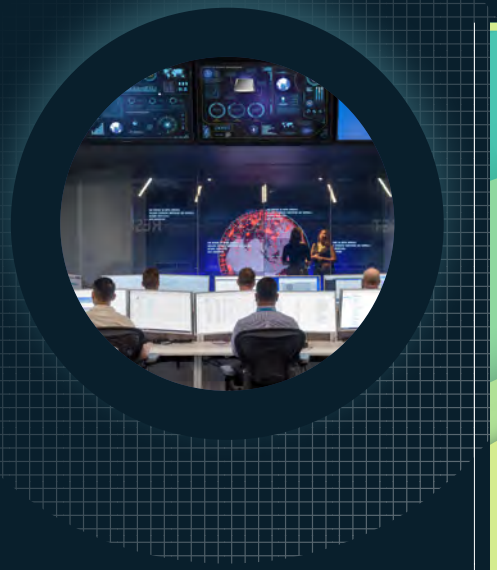
详情请参见第 56 页

Tom Burt 的引言
续

网络影响行动

国家层面越来越多地利用复杂的影响行动进行宣传，影响国内和国际的公众舆论。这些活动会削弱人民的信任感，加剧两极分化，并阻碍民主进程。熟练的 Advanced Persistent Manipulator 行为者正在使用传统媒体以及 Internet 和社交媒体来大幅增加其活动的范围、规模和效率，以及他们在全球信息生态系统中产生的巨大影响。在过去的一年里，我们看到这些行动被用作俄罗斯在乌克兰的混合战争的一部分，但也看到俄罗斯和包括中国和伊朗在内的其他国家，越来越多地部署由社交媒体驱动的宣传行动，以扩大他们在一系列问题上的全球影响力。

详情请参见第 71 页



网络复原能力

安全性是技术成功的重要推动因素。创新和提高工作效率只能通过引入使组织能够尽可能弹性抵御现代攻击的安全措施来实现。疫情迫使 Microsoft 调整安全实践和技术，以保护我们的员工，无论他们在哪里工作。去年，威胁行为者继续利用在疫情期间以及向混合工作环境转变期间暴露的漏洞。从那时起，我们面临的主要挑战便一直是应对各种普遍且复杂的攻击方法以及加剧的国家层面活动。在本章中，我们详细介绍了我们面临的挑战，以及我们与 15,000 多名合作伙伴为应对挑战而采取的防御措施。

详情请参见第 86 页

我们独特的优势

370 亿
拦截的电子邮件威胁数量

347 亿
拦截的身份威胁数量

43 万亿个
使用复杂的数据分析和 AI 算法每天合成的信号，来了解和防范数字威胁和犯罪网络活动。

25 亿
每天分析的端点信号数量

8,500 多个
遍布 77 个国家 / 地区的工程师、研究人员、数据科学家、网络安全专家、威胁搜寻者、地缘政治分析师、调查人员和一线响应者的数量。

15,000 多个
我们的安全生态系统中致力于提升客户网络复原能力的合作伙伴数量。

2021 年 7 月 1 日至 2022 年 6 月 30 日

Tom Burt 的引言
续

我们相信 Microsoft，无论在独立行动中，还是在与私营企业、政府和民间团体中的其他方的密切合作中，都有责任保护支撑我们社会结构的数字系统，并为每个人营造安全可靠的计算环境，无论他们身在何处。这一责任正是我们自 2020 年以来每年发布 MDDR 的原因。这份报告是 Microsoft 大量数据和全面研究的结晶。它包含我们对数字威胁格局如何演变的独特见解，以及我们可以立即采取以提高生态系统安全性的关键行动。

我们希望向读者灌输一种紧迫感，使其能够根据我们在这里以及全年在许多网络安全出版物中提供的数据和见解立即采取行动。当我们思考威胁对数字环境的严重性以及进而对物理世界产生的影响时，请务必记住，我们都有能力采取行动保护我们自己、我们的组织和企业免受数字威胁。

感谢您抽出时间阅读今年的《Microsoft 数字防御报告》。我们希望您会发现它提供了宝贵的见解和建议，帮助我们共同捍卫数字生态系统。

Tom Burt 公司副总裁，客户安全与信任部

本报告有双重目标：

① 为我们的客户、合作伙伴和更广泛的生态系统中的利益相关者阐明不断演变的数字威胁格局，揭示新型网络攻击以及长期存在的威胁的发展趋势。

② 帮助我们的客户和合作伙伴提高网络复原能力，应对这些威胁。

网络犯罪现状

随着网络防御方法的改善以及越来越多的组织采取主动的预防方法，攻击者正在调整其采用的技术。

网络犯罪现状概述 07
引言 08
勒索软件和敲诈勒索：国家层面的威胁 09
来自一线响应者的勒索软件见解 14
网络犯罪即服务 18
不断演变的网络钓鱼威胁格局 21
网路犯罪分子滥用基础结构 26
黑客入侵是否成为常态? 28

网络犯罪

现状概述

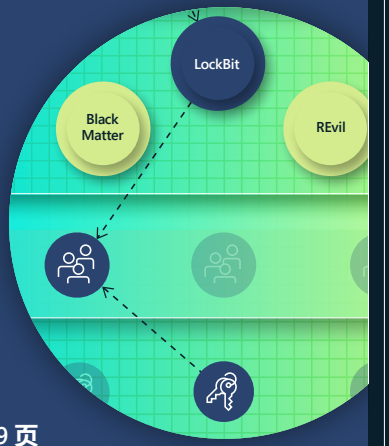
随着网络防御方法的改善以及越来越多的组织采取主动的预防方法，攻击者正在调整其采用的技术。

网络犯罪分子继续作为精明的盈利企业行事。攻击者正在适应并寻找实施其技术的新方法，从而增加了其攻击行动基础结构托管方式和位置的复杂性。与此同时，网络犯罪分子变得更加节俭。为了降低开销并提高合法性，攻击者正在入侵业务网络和设备，以托管网络钓鱼活动、恶意软件，甚至利用其计算能力来挖掘加密货币。

网络犯罪继续上升，因为网络犯罪经济的工业化通过提供更多的工具和基础结构，降低了网络犯罪入门的技能门槛。

详情请参见第 18 页

以政府、企业和关键基础设施为攻击目标的勒索软件和敲诈勒索的威胁正变得越来越猖狂。

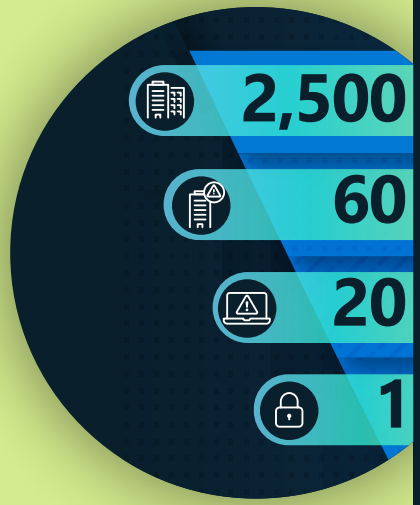


详情请参见第 9 页

攻击者越来越多地以披露敏感数据相威胁来获取赎金。

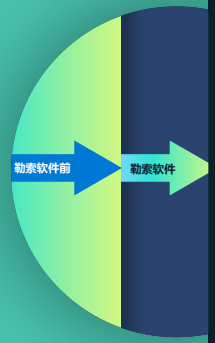
详情请参见第 10 页

人工勒索软件最为普遍，因为犯罪分子利用这些攻击成功入侵了三分之一的目标，其中的 5% 被成功勒索。



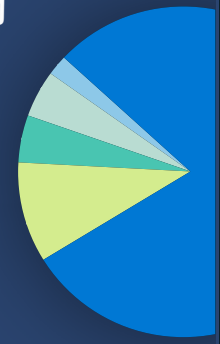
详情请参见第 9 页

针对勒索软件最有效的防御措施包括多重身份验证、频繁的安全修补程序以及跨网络体结构的零信任原则。



详情请参见第 13 页

不加区分地以所有收件箱为目标的凭据网络钓鱼计划呈上升趋势，包括发票欺诈在内的企业电子邮件入侵给企业带来了重大的网络犯罪风险。



详情请参见第 21 页

为了破坏网络犯罪分子和国家层面行为者的恶意基础结构，Microsoft 开始转向创新的法律手段以及公共和私人合作伙伴关系。

详情请参见第 25 页

引言

网络犯罪持续上升，随机攻击和有针对性攻击都在增加。

随着网络防御方法的改善，以及越来越多的政府和企业采取主动的预防方法，我们看到攻击者使用两种策略来获得实施网络犯罪所需的访问权限。一种方法是开展目标广泛、依靠数量的活动。另一种方法是使用监视和更有选择性的目标定位来提高回报率。即使创收不是目标（例如出于地缘政治目的的国家层面活动），也会使用随机和针对性的攻击。在过去的一年里，网络犯罪分子继续依靠社会工程并利用热门话题来最大限度地提高活动的成功率。例如，虽然以新冠病毒（COVID）为主题的网络钓鱼诱饵的使用频率下降，但我们观察到，为支持乌克兰公民而征集募捐的诱饵越来越多。

攻击者正在适应并寻找实施其技术的新方法，从而增加了其攻击行动基础结构托管方式和位置的复杂性。我们观察到，网络犯罪分子变得更加节俭，攻击者不再为技术付费。为了降低开销并提高合法性，部分攻击者越来越多地试图入侵企业，以托管网络钓鱼活动、恶意软件，甚至利用其计算能力来挖掘加密货币。

在本章中，我们还研究了黑客活动主义的兴起，这是一种由于普通公民为实现社会或政治目标而进行网络攻击所造成的破坏。自 2022 年 2 月以来，作为俄乌战争的一部分，世界各地数以千计的个人，无论是专家还是新手，已经动员起来发动攻击，例如瘫痪网站和泄露被盗数据。现在预测这种趋势在实际敌对行为结束后是否会继续下去还为时过早。

组织必须定期审查和加强访问控制，并实施安全策略以防范网络攻击。然而，他们能做的还不止于此。我们解释了我们的数字犯罪部门（DCU）如何利用民事案件来占据网络犯罪分子和国家层面行为者使用的恶意基础结构。我们必须通过公私合作来共同应对这一威胁。我们希望通过分享我们过去十年的经验，可以帮助其他人了解和思考他们可以采取的主动措施，以保护自己和更广泛的生态系统，免受不断增长的网络犯罪威胁。

Amy Hogan-Burney
数字犯罪部门总经理

勒索软件和敲诈勒索：国家层面的威胁

勒索软件攻击给所有个人带来了越来越大的危险，因为关键的基础设施、各种规模的企业以及州 / 省和地方政府都是利用日益增长的网络犯罪生态系统的犯罪分子的目标。

在过去两年中，高调的勒索软件事件（如涉及关键基础设施、医疗保健和 IT 服务提供商的事件）引起了公众的广泛关注。随着勒索软件攻击的范围变得越来越大胆，其影响也越来越广泛。以下是我们在 2022 年已经看到的攻击示例：

- 2 月份，一起针对两家公司的网络攻击影响了德国北部数百家加油站的支付处理系统。[1]
- 3 月，一起针对希腊邮政部门的攻击暂时中断了邮件传递，并影响了金融交易的处理。[2]
- 5 月下旬，一起针对哥斯达黎加政府机构的勒索软件攻击，导致医院关闭，海关和税收征收中断，迫使该国宣布进入紧急状态。[3]
- 同样在 5 月，一起攻击导致印度最大的航空公司之一的航班延误和取消，数百名乘客滞留。[4]

这些攻击的成功及其对现实世界的影响程度是网络犯罪经济工业化的结果，它使人们能够获得工具和基础结构，并通过降低入门的技能门槛扩大了网络犯罪的能力。

近年来，勒索软件已经从单一“团伙”开发和分发勒索软件有效负载的模式转变为勒索软件即服务 (RaaS) 模式。RaaS 使一个团体能够管理勒索软件有效负载的开发，并通过将数据泄露给其他网络犯罪分子（实际上是发起勒索软件攻击的网络犯罪分子）来为付款和勒索提供服务，这些网络犯罪分子被称为“联盟公司”，从利润中分成。这种网络犯罪经济的特许经营扩大了攻击者的数量。网络犯罪工具的工业化使攻击者更容易执行入侵、泄露数据和部署勒索软件。

人工勒索软件[5] - 这个由 Microsoft 研究人员创造的术语用来描述由人类驱动的威胁。他们根据在目标网络中发现的内容在攻击的每个阶段做出决策，并描述商品勒索软件攻击的威胁。此类威胁仍然是各组织面临的重大威胁。

基于 Microsoft Defender for Endpoint (EDR) 数据的模型（2022 年 1 月至 6 月）。

勒索软件敲诈勒索：国家层面的威胁

接上页

随着采用双重勒索货币化策略成为一种标准做法，勒索软件攻击变得更加有影响力。这包括从被入侵的设备中窃取数据，对设备上的数据进行加密，然后公开或威胁要公开发布被盗的数据，从而迫使受害者支付赎金。

虽然大多数勒索软件的攻击者会投机地将勒索软件部署到他们能够访问的任何网络，但有些人会利用访问代理和勒索软件运营商之间的联系，从其他网络犯罪分子那里购买访问权限。

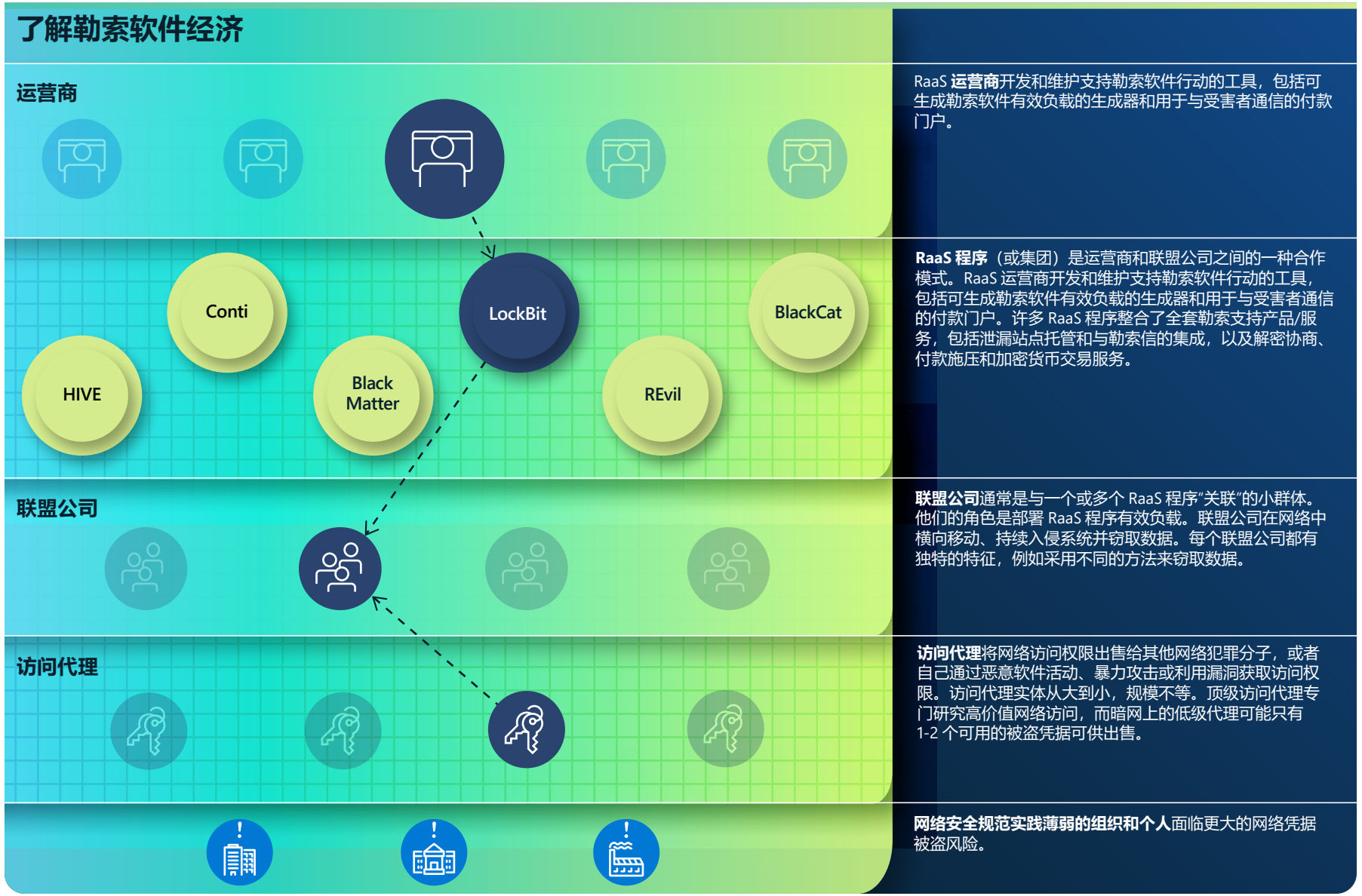
我们独特而广泛的信号情报来自多个来源（身份、电子邮件、终结点和云），并提供了对不断增长的勒索软件经济的见解，此外还有一个包含专门针对技术上不太熟练的攻击者设计的工具附属系统。

专业网络犯罪分子之间不断扩大的关系提高了勒索软件攻击的速度、复杂程度和成功率。这促使网络犯罪生态系统演变为拥有不同技术、目标和技能组合的互联参与者，这些参与者在初始访问目标、支付服务、解密或发布工具或网站方面相互支持。

勒索软件操作员现在可以在线购买对组织或政府网络的访问权限，或者通过与代理的人际关系获取凭据和访问权限，而代理的主要目标仅仅是将他们获得的访问权限变现。

然后，操作员使用购买的访问权限来部署通过暗网市场或论坛购买的勒索软件有效负载。在许多情况下，与受害者的谈判由 RaaS 团队进行，而不是由操作员自己进行。这些犯罪交易是无缝的。由于暗网的匿名性和跨国执法的困难，参与者几乎不可能被逮捕和指控。

要持续、成功地应对这一威胁，就需要与私营部门密切合作，实施一项政府整体战略。



与媒体有时描述的勒索软件不同，单一的勒索软件变体很少由一个端到端的“勒索软件团伙”进行管理。相反，有独立的实体构建恶意软件，获取对受害者的访问权限，部署勒索软件并处理勒索谈判。犯罪生态系统的工业化已导致：

- 入侵和交接访问权限（访问即服务）的访问代理。
- 恶意软件开发人员出售攻击工具。
- 犯罪分子和联盟公司实施入侵。
- 加密和勒索服务提供商，从联盟公司手中接管货币化（RaaS）。

所有人工勒索软件活动都对安全漏洞具有共同的依赖关系。具体而言，攻击者通常利用组织糟糕的网络安全机制状况，这通常包括不经常安装补丁和未实施多重身份验证（MFA）。

案例研究：Conti 的解散

Conti 是过去两年中最大的勒索软件变体之一，于 2022 年中开始关闭运营，Microsoft 威胁情报中心 (MSTIC) 观察到其活动在 3 月底和 4 月初显著减少。我们在 4 月中旬观察到了最后一次 Conti 勒索软件部署。然而，就像其他勒索软件运营的关闭一样，Conti 的解散对勒索软件的部署并没有产生重大影响，因为 MSTIC 观察到，Conti 的联盟公司正在部署其他勒索软件有效负载，包括 BlackBasta、Lockbit 2.0、LockbitBlack 和 HPE。这与前几年的数据一致，表明该勒索软件团伙解体后，又在几个月后重新出现，或将其技术能力和资源重新分配给新的团伙。

Microsoft 威胁情报团队根据勒索软件威胁行为者使用的特定工具将他们作为各个团体进行跟踪（标记为 DEV），而不是根据他们使用的恶意软件进行跟踪。这意味着，当 Conti 的联盟公司分散时，我们能够通过使用其他工具或 RaaS 套件来继续跟踪这些 DEV。例如：

- 隶属于 Trickbot 的 DEV-0230 一直是 Conti 的多产用户。4 月下旬，MSTIC 使用 QuantumLocker 对其进行了观察。
- DEV-0237 从 Conti 的勒索软件套件转移到了 HIVE 和 Nokoyawa，包括在 5 月 31 日针对哥斯达黎加政府机构的攻击中使用了 HIVE。
- MSTIC 观察到另一个多产的 Conti 勒索软件套件用户 DEV-0506 正在使用 BlackBasta。

在 RaaS 程序之间快速切换的联盟公司 (DEV-0237) 示例

在 Conti 等 RaaS 程序关闭后，勒索软件联盟公司几乎立即转移到另一个程序 (Hive)。

RaaS 发展了勒索软件生态系统并阻碍归因

由于人工勒索软件由操作员个人驱动，因此攻击模式因目标而异，并在整个攻击过程中交替变化。过去，我们观察到在单个勒索软件毒株的每个活动中，初始进入媒介、工具和勒索病毒有效负载选择之间具有密切的关系。这使得归因变得更容易。然而，RaaS 联盟模型分离了这种关系。因此，Microsoft 跟踪在特定攻击中部署有效负载的勒索软件联盟，而不是将勒索软件有效负载开发人员作为运营商进行跟踪。

换句话说，我们不再假设 HIVE 开发人员是 HDE 勒索软件攻击的幕后操纵者；它更有可能是一个联盟公司。

网络安全行业一直难以充分把握开发人员和运营商之间的这种界限。该行业仍然经常以有效负载的名称报告勒索软件事件，给人一种错误的印象，即使用该特定勒索软件有效负载的所有攻击背后都是一个单一实体或勒索软件团伙，而与之相关的所有事件都共享共同的技术和基础结构。为了支持网络防御者，重要的是要详细了解不同的联盟公司展开攻击之前的阶段（如数据泄露和其他持久性机制）以及可能存在的检测和保护机会。

与恶意软件相比，攻击者更需要凭据来实现成功操作。整个组织能否成功地感染人工勒索软件，取决于对高特权帐户的访问权限。

聚焦人工勒索软件攻击

在过去的一年里，Microsoft 的勒索软件专家对 100 多个人工勒索软件事件进行了深入调查，以跟踪攻击者的技术，并了解如何更好地保护我们的客户。

请务必注意，我们在此处共享的分析数据仅适用于已注册的托管设备。未注册的非托管设备是组织硬件资产中最不安全的部分。

最流行的勒索软件阶段技术：

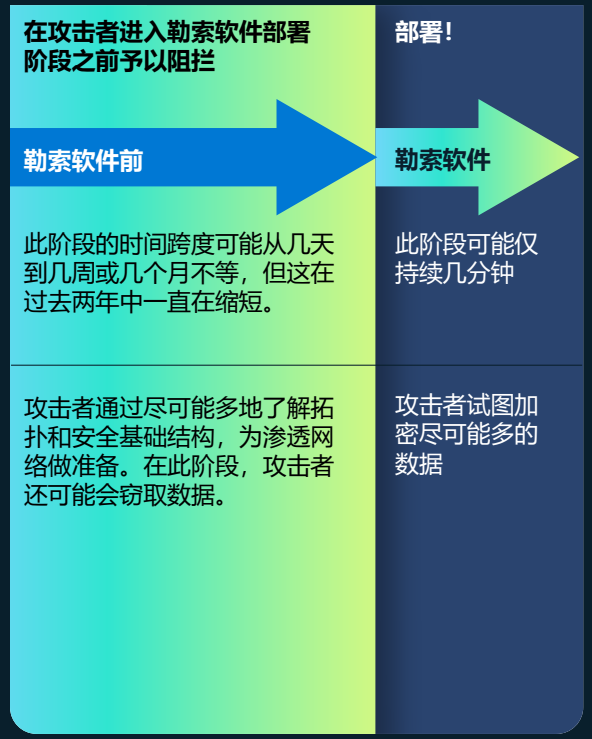
75%
使用管理工具。

75%
使用获取的提升的被入侵用户帐户，通过 SMB 协议传播恶意有效负载。

99%
试图使用 OS 内置工具篡改已发现的安全和备份产品。

典型的人为攻击

人工勒索软件攻击可分为勒索软件前阶段和勒索软件部署阶段。在勒索软件前阶段，攻击者准备通过了解组织的拓扑和安全基础结构来渗透网络。



我们的调查发现，人工勒索软件攻击背后的大多数行为者都利用了类似的安全漏洞，并共享常见的攻击模式和技术。

持久的安全策略

打击和预防这种性质的攻击需要转变组织的思维方式，使其专注于提供所需的综合性保护，以便在攻击者从勒索软件前阶段转移到勒索软件部署阶段之前，减缓和阻止攻击者的行动。

企业必须始终如一且积极主动地将安全最佳实践应用于其网络，以缓解各种类型的攻击。由于人为决策，这些勒索软件攻击可能会生成多个看似不同的安全产品警报，这些警报很容易丢失或无法及时响应。警报疲劳是真实存在的，安全运营中心 (SOC) 可以通过研究警报中的趋势或将警报分组为事件来了解全局，从而减少其工作量。然后，SOC 可以使用攻击表面减少规则等强化功能来缓解警报。针对常见威胁的强化功能不仅可以减少警报量，还可以阻止许多攻击者访问网络。

组织必须保持持续的高标准安全态势和网络安全机制，以保护自己免受人工勒索软件攻击。

切实可行的见解

勒索软件攻击者的行为动机是轻松获利，因此通过加强安全保护来增加攻击成本是破坏网络犯罪经济的关键。

1. 建立凭据清洁机制。与恶意软件相比，攻击者更需要凭据来实现成功操作。整个组织能否成功地感染人工勒索软件，取决于对高特权帐户（如域管理员）的访问权限或编辑组策略的能力。
2. 审核凭据暴露。
3. 优先部署 Active Directory 更新。
4. 优先考虑云强化。
5. 减少攻击面。
6. 强化面向 Internet 的资产，了解你的边界。
7. 通过强化网络以减少警报数量并为高优先级事件预留带宽，减少 SOC 警报疲劳。

更多信息的链接

- RaaS：了解网络犯罪零工经济以及如何保护自己 | Microsoft 安全博客
- 人工勒索软件攻击：可预防的灾难 | Microsoft 安全博客

来自一线响应者的勒索软件见解

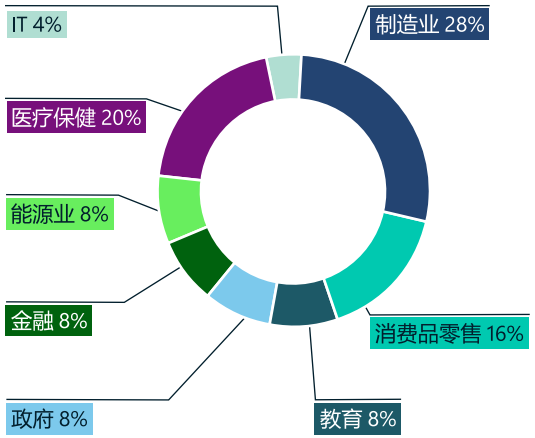
从 2019 年开始，世界各地的组织都经历了人工操作勒索软件攻击的稳步增长。不过，去年的执法行动和地缘政治事件对网络犯罪组织产生了重大影响。

Microsoft 的安全服务热线针对整个网络攻击为客户提供支持，从调查到成功遏制，再到恢复活动。响应和恢复服务通过两个高度集成的团队提供，一个团队专注于调查及恢复的基础工作，第二个团队专注于遏制和恢复。本节总结了过去一年基于勒索软件攻击的调查结果。

93%

勒索软件恢复行动期间进行的 Microsoft 调查表明，特权访问权限和横向移动控制不足。

按行业划分的勒索软件事件和恢复活动

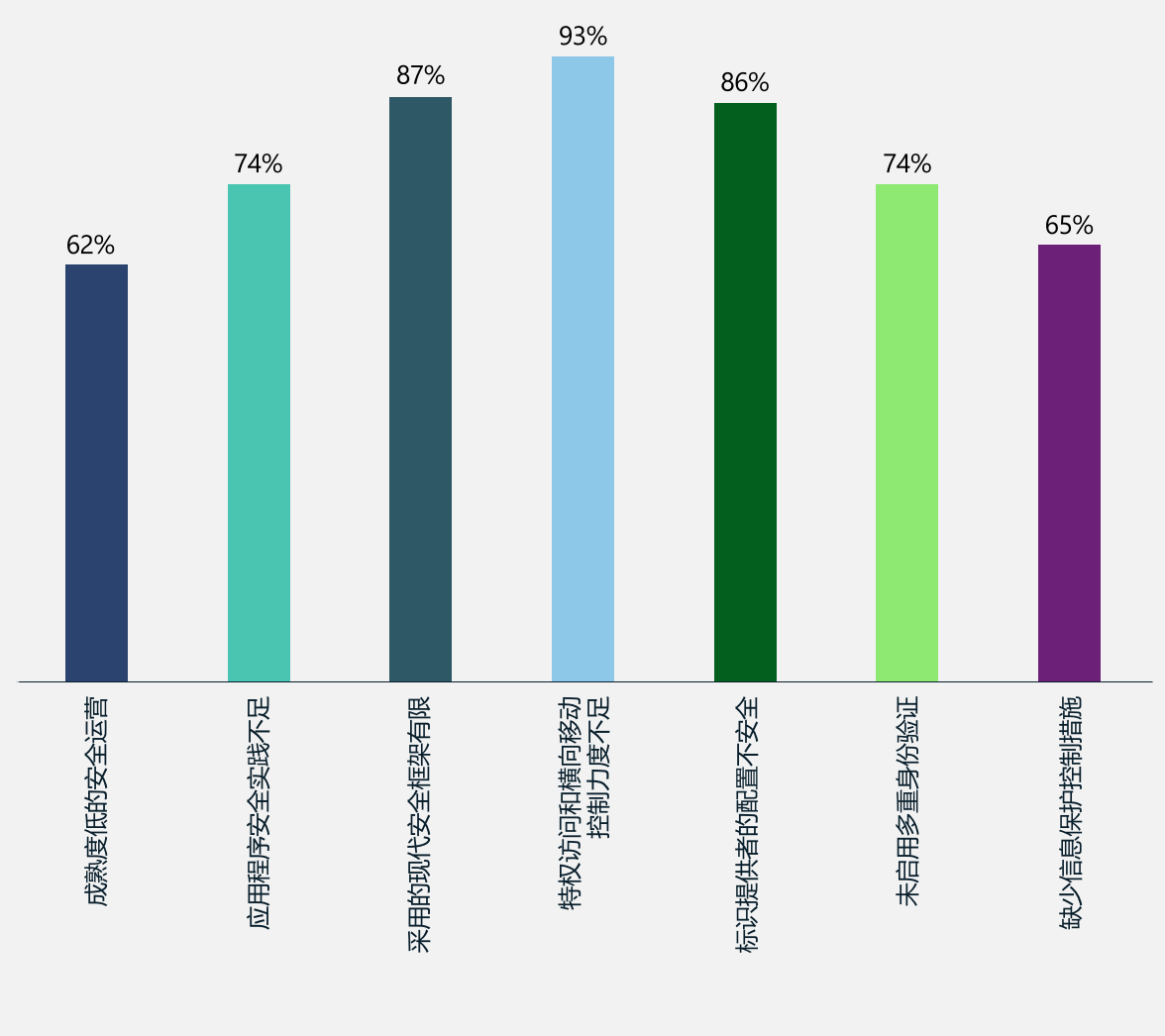


随着新的小型团体和威胁的出现，防御团队必须意识到不断演变的勒索软件威胁，同时防范以前未知的勒索软件恶意软件系列。犯罪团体使用的快速开发方法促进了智能勒索软件的创建，包装在易于使用的套件中。这使得他们在对数量更多的目标发起广泛攻击时具有更大的灵活性。

以下几页深入分析了导致薄弱的勒索软件防范的最常见因素，调查结果分为以下三类：

1. 薄弱的身份控制
2. 无效的安全运营
3. 有限的数据保护

勒索软件响应行动中最常见发现的摘要



勒索软件事件响应行动中，最常见的发现是特权访问权限和横向移动控制的不足。

来自一线响应者的勒索软件见解

接上页

我们在现场响应行动中发现的三个主要促成因素：

① **薄弱的身份控制：凭据盗窃攻击仍然是主要促成因素之一**

② **无效的安全运营流程不仅为攻击者提供了机会窗口，还明显地影响了恢复时间**

③ **归根结底在于数据 - 组织难以实施符合其业务需求的有效的数据保护策略**

① 薄弱的身份控制

人工勒索软件不断发展，并采用传统上与针对性攻击相关的凭据盗窃和横向移动方法。成功的攻击通常是长期运行的活动的结果，这些活动涉及入侵 Active Directory（AD）等身份系统，允许人类操作员窃取凭据、访问系统并在网络中保持持久性。

Active Directory (AD) 和 Azure AD 安全性

88%

的受影响客户没有采用 AD 和 Azure AD 安全最佳实践。这已成为常见的攻击媒介，因为攻击者利用关键身份系统中的错误配置和较薄弱的安全状况来获得对企业的更广泛访问并加大对企业的影响。

最低特权访问以及特权访问工作站 (PAW) 的使用

没有一个受影响的组织在管理其关键身份和高价值资产（如专有系统和业务关键型应用程序）期间通过专用工作站实施适当的管理凭据隔离和最低特权访问原则。

特权帐户安全性

88%

的行动中，未针对敏感和高特权帐户实施 MFA，从而为攻击者留下了安全漏洞，使他们可以利用合法凭据入侵凭据并进行进一步攻击。

84%

84% 的组织中的管理员未使用特权身份控制措施（如即时访问）来防止进一步恶意地使用泄露的特权凭据。

来自一线响应者的勒索软件见解

接上页

② 无效的安全运营

我们的数据显示，遭受勒索软件攻击的组织在安全运营、工具和信息技术资产生命周期管理方面存在重大差距。基于现有数据，观察到最多的差距如下：

修补：

68%

的受影响组织没有有效的漏洞和修补程序管理流程，对手动流程和自动修补的高度依赖为攻击者带来了关键的可乘之机。制造业和关键基础设施继续努力维护和修补传统运营技术（OT）系统。

缺乏安全运营工具：

大多数组织表示，由于缺乏安全工具或错误配置了安全工具，其缺乏端到端的安全可见性，因此导致检测和响应效果下降。

60%

的组织表示未使用 EDR[6] 工具，这是一种用于检测和响应的基本技术。

60%

没有对安全信息和事件管理 (SIEM) 技术进行投资，从而导致监控孤岛，检测端到端威胁的能力有限以及安全运营效率低下。自动化仍然是 SOC 工具和流程中的一个关键差距，迫使 SOC 工作人员花费大量时间来研究安全遥测。

84%

的受影响组织无法将其多云环境集成到其安全运营工具中。

响应和恢复流程：

76%

我们观察到，在 76% 的受影响组织中，缺乏有效的响应计划是一个关键方面，阻碍了组织做好适当的危机准备，并对响应和恢复速度产生了负面影响。

③ 有限的数据保护

许多遭到入侵的组织缺乏适当的数据保护流程，从而对恢复时间和恢复业务运营的能力产生了严重影响。他们遇到的最常见差距包括：

不可变备份：

44%

的组织没有为受影响系统进行不可变的备份。数据还显示，管理员没有针对 AD 等关键资产制定备份和恢复计划。

数据丢失防护：

攻击者通常会通过利用组织中的漏洞、泄露关键数据以进行勒索、知识产权盗窃或变现来入侵系统。

92%

的受影响组织没有实施有效的数据丢失防护控制措施来降低这些风险，从而导致严重的数据丢失。

勒索软件在某些地区有所下降，在其他地区有所增加

今年，我们发现北美和欧洲的响应团队收到的勒索软件案例举报总数与去年相比有所下降。与此同时，拉丁美洲举报的案例有所增加。

对这一观察结果的一种解释是，网络犯罪分子从被认为更有可能触发执法审查的区域转向要求更宽松的目标。由于 Microsoft 并未观察到全球企业网络安全性的显著改善，无法解释勒索软件相关支持电话的减少，我们认为最可能的原因是 2021 年和 2022 年的执法活动增加了犯罪活动的成本，此外还有 2022 年的一些地缘政治事件。

最盛行的 RaaS 行动之一属于一个名为 REvil（邪恶，也称为 Sodinokibi）的俄语犯罪团伙，该团伙自 2019 年以来便一直活跃。2021 年 10 月，作为国际执法行动 GoldDust 的一部分，REvil 的服务器被关闭。[7] 2022 年 1 月，俄罗斯逮捕了 14 名所谓的 REvil 成员，并突击搜查了 25 个与之相关的地点。[8] 这是俄罗斯首次对其境内的勒索软件运营商采取行动。

虽然执法活动可能会降低 2022 年的攻击频率，但威胁行为者可能会制定新的策略，以避免在未来被抓获。此外，俄罗斯和美国在俄罗斯入侵乌克兰问题上的紧张关系，似乎终结了俄罗斯在全球打击勒索软件方面刚刚开始的合作。在 REvil 成员被捕后一段短暂的不确定性之后，美国和俄罗斯停止了在追捕勒索软件行为者方面的合作，这意味着网络犯罪分子可能会再次将俄罗斯视为避风港。

展望未来，我们预测勒索软件活动的速度将取决于以下关键问题的结果：

1. 政府是否会采取行动，阻止勒索软件犯罪分子在其境内开展行动，或设法干扰在外国境内活动的行为者？
2. 勒索软件团体是否会改变策略，不再使用勒索软件，转而诉诸勒索式攻击？
3. 组织是否能够比犯罪分子利用漏洞更快地实现 IT 运营的现代化和转型？
4. 跟踪赎金支付方面的进展是否会迫使赎金接收者改变策略和谈判？

虽然执法活动可能会降低 2022 年的攻击频率，但威胁行为者可能会制定新的策略，以避免在未来被抓获。

2X

勒索软件攻击在某些地区有所减少，但索取的赎金增加了一倍多。

切实可行的见解

1. 专注于整体安全策略，因为所有勒索软件系列都利用相同的安全漏洞来影响网络。
2. 更新和维护安全基础，以提高深度防御的基本保护水平，并实现安全运营的现代化。通过迁移到云，你可以更快地检测威胁和做出响应。

更多信息的链接

- 保护组织免受勒索软件影响 | Microsoft 安全
- 强化环境抵御入侵的 7 种方法 | Microsoft 安全博客
- 改进基于 AI 的防御措施，破坏人工勒索软件 | Microsoft 365 Defender 研究团队
- Security Insider：探索最新的网络安全见解和更新 | Microsoft 安全

网络犯罪即服务

网络犯罪即服务（CaaS）是对全球客户的日益增长和不断演变的威胁。Microsoft 数字犯罪部门 (DCU) 观察到 CaaS 生态系统持续增长，在线服务数量不断增加，助长了各种网络犯罪，包括 BEC 和人工勒索软件。网络钓鱼仍是首选的攻击方法，因为网络犯罪分子可以通过成功窃取和销售被盗帐户的访问权限而获得重大价值。

为了应对不断扩大的 CaaS 市场，DCU 改进了其侦听系统，以检测和识别整个 Internet 生态系统、深网、经过审查的论坛、[9] 专门的网站、在线讨论论坛和消息传递平台中的 CaaS 产品 / 服务。

网络犯罪分子现在正在跨时区和语言进行协作，以取得特定的成果。例如，一个由亚洲个人管理的 CaaS 网站在欧洲开展行动，并在非洲创建恶意帐户。这些行动的多司法管辖区性质带来了复杂的法律和执法挑战。为此，DCU 将其工作重点放在瘫痪用于促进 CaaS 攻击的恶意犯罪基础结构上，并与世界各地的执法机构合作，以追究罪犯的责任。

网络犯罪分子越来越多地使用分析来最大限度地扩大覆盖面、范围和收益。与合法企业一样，CaaS 网站必须确保产品和服务的有效性，以保持良好的声誉。例如，CaaS 网站通常会自动访问遭到入侵的帐户，以确保被盗凭据的有效性。当密码被重置或漏洞被修补后，网络犯罪分子将停止销售特定帐户。我们发现，越来越多的 CaaS 网站为买家提供按需验证作为质量控制过程。因此，买家可以确信 CaaS 网站出售的是有效帐户和密码，同时降低了在被盗凭据在出售前已修复的情况下 CaaS 商家需要承担的潜在成本。

DCU 还观察到，CaaS 网站为买家提供了从特定地理位置、指定的在线服务提供商以及特定的个人、职业和行业购买遭入侵帐户的选项。频繁订购的帐户集中在处理发票的专业人员或部门，如 CFO 或“应收账款”。同样，由于通过公开招标过程提供的信息量很大，参与公开承包的行业往往会受到攻击。

DCU 对 CaaS 的调查揭示了一些关键的趋势：

服务的数量和复杂性正在上升。

一个示例是 Web 外壳的演变，它通常由用于自动进行网络钓鱼攻击的被入侵的 Web 服务器组成。DCU 观察到，CaaS 经销商通过专门的 Web 仪表板简化了网络钓鱼套件或恶意软件的上传。随后，CaaS 销售人员通常会试图通过仪表板向威胁行为者出售其他服务，如垃圾邮件服务以及基于定义属性（包括地理位置或职业）的特定垃圾邮件收件人列表。在某些情况下，我们观察到单个 Web 外壳被用于多个攻击活动，这表明威胁行为者可能保留对被入侵服务器的持久访问权限。我们还发现，作为 CaaS 生态系统的一部分提供的匿名服务以及为虚拟专用网络 (VPN) 和虚拟专用服务器 (VPS) 帐户提供的服务有所增加。在大多数情况下，提供的 VPN/VPS 最初是通过被盗信用卡购买的。CaaS 网站还提供了大量的远程桌面协议 (RDP)、安全外壳 (SSH) 和 cPanel，用作协调网络犯罪攻击的平台。CaaS 商家使用适当的工具和脚本配置 RDP、SSH 和 cPanel，以促进各种类型的网络攻击。

同构域创建服务越来越多地要求使用加密货币付款。

同构域通过使用与一个字符外观相同或几乎相同的另一个字符来模拟合法域名。其目的是欺骗观众，使其认为同构域是真正的域。这些域是无处不在的威胁，也是大量网络犯罪的门户。CaaS 站点现在出售自定义同构域名，允许买家请求特定的公司和域名进行模拟。收到付款后，CaaS 商户将使用同构文字生成器工具选择域名，然后注册恶意同构文字。这项服务的付款几乎全部使用加密货币。

2,750,000 个

DCU 今年成功阻止了网站的注册，提前制止了犯罪分子利用这些站点进行全球网络犯罪。

网络犯罪即服务

续

CaaS 卖家越来越多地提供泄露的凭据供买家购买。

泄露的凭据会导致用户帐户遭到未经授权的访问，其中包括电子邮件消息服务、企业文件共享资源和 OneDrive for Business。如果管理员凭据遭到泄露，未经授权的用户可以访问机密文件、Azure 资源和公司用户帐户。在许多情况下，DCU 的调查发现，在多个服务器之间未经授权使用相同的凭据是一种自动验证凭据的方法。此模式表明，遭到入侵的用户可能是多次网络钓鱼攻击的受害者，或者其设备恶意软件允许僵尸网络按键记录器收集凭据。

为了避免被检测到，具有增强功能的 CaaS 服务和产品正在出现。

一位 CaaS 卖家提供的网络钓鱼套件具有更高的复杂性和更强大的匿名化功能，旨在绕过检测和预防系统，成本只需每天 6 美元。该服务提供一系列重定向，在允许流量到达下一层或站点之前执行检查。其中一项是对设备进行 90 多次指纹识别检查，包括它是否是虚拟机，收集有关所用浏览器和硬件的详细信息，等等。如果所有检查都通过，流量将被发送到用于网络钓鱼的登录页面。

端到端网络犯罪服务正在向托管服务销售订阅。

通常，如果操作安全性较差，实施网络犯罪的每个步骤都可能会暴露威胁行为者。如果从多个 CaaS 站点购买服务，则暴露和识别的风险会增加。DCU 在暗网中观察到一个令人担忧的趋势，即现在有越来越多的服务通过匿名化软件代码和泛化网站文本来减少暴露。端到端网络犯罪订阅服务提供商管理所有服务并保证结果，从而进一步降低订阅 OCN 的暴露风险。降低的风险提高了这些端到端服务的受欢迎程度。

网络钓鱼即服务 (PhaaS) 是端到端网络犯罪服务的一个示例。PhaaS 是先前被称为完全不可检测服务 (FUD) 的进化，以订阅的方式提供。典型的 PhaaS 条款包括将网络钓鱼网站保持活跃一个月时间。

DCU 还发现了一家以订阅模式提供分布式拒绝服务 (DDoS) 的 CaaS 商户。此模式将发起攻击所需的僵尸网络的创建和维护工作外包给 CaaS 商户。每个 DDoS 订阅客户都会收到加密服务，以提高操作安全性，并获得一年的全天候支持。DDoS 订阅服务提供不同的体系结构和攻击方法，因此购买者只需选择要攻击的资源，销售人员就可以为其提供对僵尸网络上一系列遭到入侵的设备的访问权限，以便购买者发起攻击。DDoS 订阅的成本仅为 500 美元。

PhaaS，网络犯罪分子在单个订阅中提供多种服务。
一般来说，购买者只需采取三个操作：

1. 从提供的数百个网络钓鱼站点模板/设计中进行选择。
2. 提供电子邮件地址来接收从网络钓鱼受害者处获得的凭据。
3. 以加密货币的形式向 PhaaS 商家付款。

完成这些步骤后，PhaaS 商家将创建具有三层或四层重定向和托管资源的服务来针对特定用户发起攻击。随后，他们将发动攻击活动、获取和验证受害者的凭据并将其发送到购买者提供的电子邮件地址。为了获得额外收入，许多 PhaaS 商家提供在公有区块链上托管网络钓鱼站点的服务，这样就可以通过任何浏览器访问这些站点并可通过重定向将用户指向分布式账本上的资源。

DCU 正在开发可识别和破坏 CaaS 网络犯罪分子行动的工具和技术。CaaS 服务的发展带来了重大挑战，尤其是在影响加密货币支付方面。

加密货币用于犯罪

随着采用加密货币成为主流，犯罪分子越来越多地使用它来逃避执法和反洗钱 (AML) 措施。这加大了执法部门跟踪向网络犯罪分子进行的加密货币付款的难度。

在过去四年中，全球在区块链解决方案上的支出增长了约 340%，而新的加密货币钱包增长了约 270%。全球有超过 8,300 万个独特的钱包，截至 2022 年 7 月 28 日，所有加密货币的总市值约为 1.1 万亿美元。[10]

来源：Twitter.com - @PeckShieldAlert（PeckShield 是一家总部位于中国的区块链安全公司）。

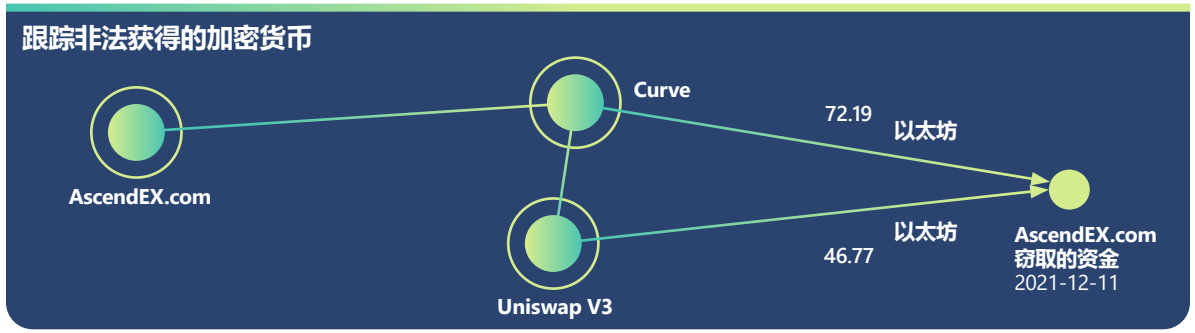
跟踪勒索软件付款

勒索软件是非法获取加密货币的最大来源之一。为了破坏勒索软件攻击中使用的恶意技术基础结构（例如于 2022 年 4 月破坏 Zloader）[11]，Microsoft DCU 开始跟踪犯罪钱包，以实现加密货币跟踪和恢复功能。

DCU 调查人员观察到，勒索软件行为者不断发展与受害者的沟通策略，以掩盖资金踪迹。最初，网络犯罪分子在勒索信中包含比特币地址。然而，这使得在区块链上跟踪支付交易变得很容易，因此勒索软件行为者不再提供钱包地址，而是将电子邮件地址或链接附加到聊天网站，以向受害者传达赎金付款地址。一些行为者甚至为每个受害者创建了独特的网页和登录名，以防止安全研究人员和执法部门假装是受害者，从而获得犯罪分子的钱包地址。尽管犯罪分子努力隐藏其踪迹，但通过与可跟踪金钱在区块链上的移动的执法部门和加密分析公司合作，仍然可以追回一些赎金。

趋势：DEX 洗钱活动

网络犯罪分子的一个关键问题是将加密货币转换为法定货币。网络犯罪分子有几种潜在的转化途径，每种途径都有不同程度的风险。一种降低风险的方法是通过去中心化交易所 (DEX) 洗钱，然后通过可用的套现方案进行套现，如中心化交易所 (CEX)、点对点 (P2P) 和场外交易 (OTC) 交易所。



通过使用加密货币调查工具 Chainalysis，Microsoft 数字犯罪部门发现，AcendEX 黑客除了在 Uniswap 上，还在一个名为 Curve 的小型 DEX 上交换了窃取的资金。此图说明了数字犯罪部门发现的洗钱路线。每个圆圈代表一组钱包，每行上的数字代表以洗钱为目的传输的以太坊的总额。

DEX 是一个有吸引力的洗钱地点，因为它们通常不遵循 AML 措施。

2021 年 12 月，黑客攻击了全球加密货币交易平台 AscendEx，窃取了属于客户的约 7,770 万美元加密货币。[12]AscendEx 聘请了区块链分析公司，并联系了其他 CEX，以便将接收被盗资金的钱包列入黑名单。此外，发送代币的地址在以太坊区块链浏览器 Etherscan 上进行了相应的标记。[13] 为了规避警报和黑名单，黑客于 2022 年 2 月 18 日向全球最大的 DEX 之一 Uniswap 发送了 150 万美元的以太坊。[14]

DEX 采取更严厉的 AML 措施，可能会削弱其平台上的洗钱活动，并迫使网络犯罪分子使用其他混淆手段，如代币翻滚或无证交易所。例如，Uniswap 最近宣布将开始使用黑名单来阻止已知参与非法活动的钱包在交易所进行交易。[15]

切实可行的见解

1. 如果你是网络犯罪的受害者，并使用加密货币向犯罪分子付款，请联系当地执法部门，他们可能能够帮助跟踪和追回丢失的资金。
2. 选择 DEX 时，务必熟悉已实施的应用程序生命周期管理（ALM）措施。

更多信息的链接

- 针对日益复杂的加密货币挖矿黑客的基于硬件的威胁防御 | Microsoft 365 Defender 研究团队

不断演变的网络钓鱼威胁格局

凭据网络钓鱼计划正在不断增加，仍然对各地用户构成重大威胁，因为它们不加区分地以所有收件箱为攻击目标。在我们的研究人员跟踪和防御的威胁中，网络钓鱼攻击的数量比所有其他威胁都要大几个数量级。

使用 Defender for Office 中的数据，我们可以发现恶意电子邮件和盗窃身份活动。Azure Active Directory 标识保护通过盗窃身份事件警报提供更多信息。使用 Defender for Cloud Apps，我们可以发现盗窃身份数据访问事件，而 Microsoft 365 Defender (M365D) 可提供跨产品关联。横向移动指标则来自 Defender for Endpoint（攻击行为警报和事件）、Defender for Office（恶意电子邮件）以及 M365D（用于提供跨产品关联）。

7.1 亿

每周拦截的网络钓鱼电子邮件数量。

1 小时 12 分钟

如果您成为网络钓鱼电子邮件的受害者，攻击者访问您的私人数据所需的平均时间。[16]

1 小时 42 分钟

一旦设备遭到入侵，攻击者开始在您的公司网络内横向移动的平均时间。[17]

Microsoft 365 凭据仍然是攻击者最抢手的帐户类型之一。一旦登录凭据遭到入侵，攻击者就可以登录到与企业连接的计算机系统，以促进恶意软件和勒索软件的感染，通过访问 SharePoint 文件窃取机密的公司数据和信息，并通过使用 Outlook 发送额外的恶意邮件等行为继续网络钓鱼的传播。

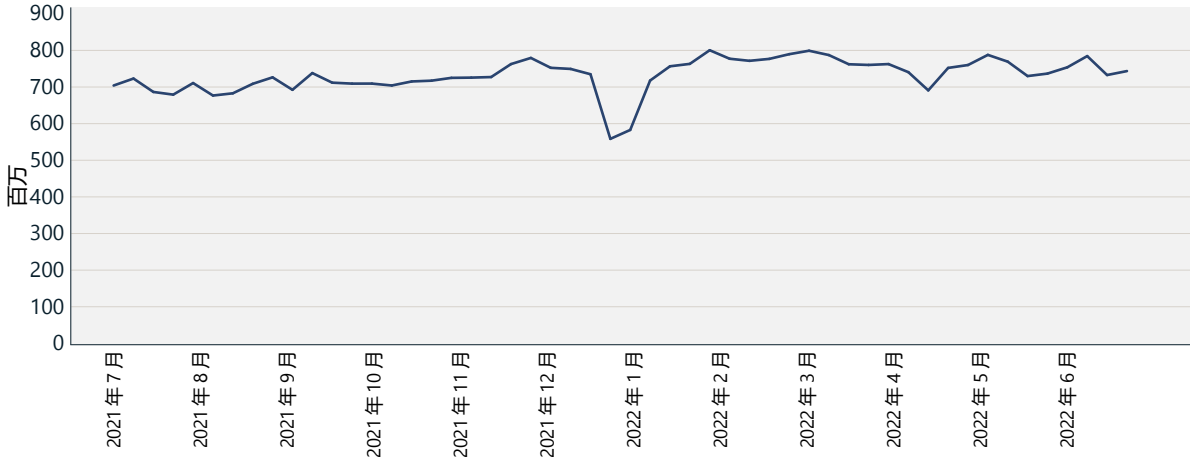
除了针对更广泛目标发起的活动以及以获取凭据、捐款和个人信息为目的的网络钓鱼外，攻击者还将特定的企业作为攻击目标以获取更多付款。为获得经济利益而针对企业开展的电子邮件网络钓鱼攻击统称为 BEC 攻击。Microsoft 每月检测数百万封 BEC 电子邮件，相当于观察到的所有网络钓鱼电子邮件的 0.6%。IC3 于 2022 年 5 月发布的一篇报告[18] 表明，BEC 攻击造成的暴露损失呈上升趋势。

网络钓鱼攻击中使用的技术的复杂性持续攀升。为了应对反制措施，攻击者调整了新的方式以实施其技术并增加其攻击行动基础结构托管方式和位置的复杂性。这意味着组织必须定期重新评估其实施安全解决方案的策略，以阻止恶意电子邮件并加强对单独用户帐户的访问控制。

531,000 个

除了 Defender for Office 阻止的 URL 之外，我们的数字犯罪部门还指示删除了在 Microsoft 之外托管的 531,000 个唯一的网络钓鱼 URL。

检测到的网络钓鱼电子邮件



每周检测到的网络钓鱼数量继续增加。12 月至 1 月的下降是预期的季节性下降，这在去年的报告中也有说明。来源：Exchange Online Protection 信号。

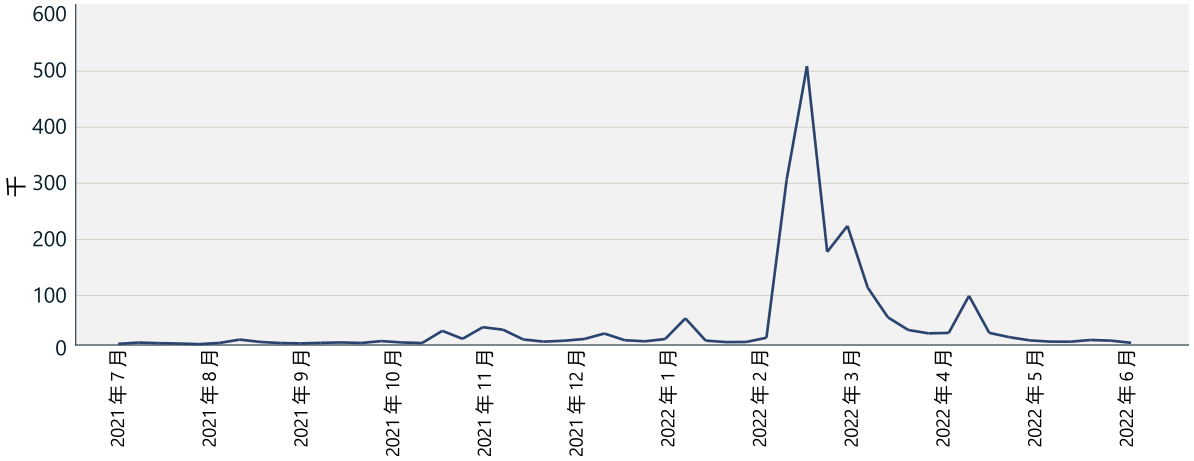
不断演变的网络钓鱼威胁格局

接上页

我们继续观察到网络钓鱼电子邮件逐年稳步增加。2020 年和 2021 年向远程工作的转变使得旨在利用不断变化的工作环境而获利的网络钓鱼攻击大幅增加。网络钓鱼运营商可以迅速采用新的电子邮件模板，使用的诱饵与全球重大事件（如 COVID-19 疫情）相关，使用的主题与协作和生产力工具（如 Google 云端硬盘或 OneDrive 文件共享）相关。虽然 COVID-19 主题有所减少，但乌克兰战争在 2022 年 3 月初开始成为一种新的诱饵。我们的研究人员发现，冒充合法组织的电子邮件数量激增，这些电子邮件以比特币和以太坊的形式征求加密货币捐款，据称是为了支持乌克兰公民。

在 2022 年 2 月下旬乌克兰战争爆发的几天内，企业客户遭遇的包含以太坊地址的网络钓鱼电子邮件数量急剧增加。在 3 月的第一周，收到的网络钓鱼电子邮件数量达到峰值，当时有 50 万封网络钓鱼电子邮件包含以太坊钱包地址。在战争开始之前，被检测为网络钓鱼的其他电子邮件的以太坊钱包地址数量显著减少，平均每天几千封电子邮件。

使用以太坊钱包地址的网络钓鱼电子邮件



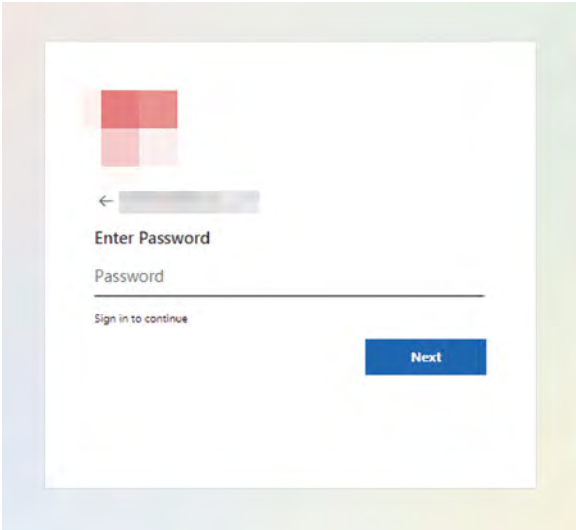
在乌克兰 - 俄罗斯冲突开始时，检测为包含以太坊钱包地址的网络钓鱼的电子邮件总数增加，在最初推送后逐渐减少。

网络钓鱼者比以往任何时候都更依赖于合法的基础结构来运营，从而推动旨在破坏企业运营各个方面的网络钓鱼活动的增长，使网络钓鱼者不必自己购买、托管或运营。例如，恶意电子邮件可能源自遭到入侵的发件人帐户。攻击者可从这些电子邮件地址中受益，因为这些地址具有较高的信誉评分，比新创建的帐户和域更值得信任。在一些更高级的网络钓鱼活动中，我们观察到攻击者更喜欢从使用“无需操作”策略错误设置了 DMARC[19] 的域发送电子邮件和实施欺骗，这为电子邮件欺骗打开了大门。

大型网络钓鱼行动往往使用云服务和云虚拟机 (VM) 来实施大规模攻击。攻击者可以使用 SMTP 电子邮件中继或云电子邮件基础结构，完全自动执行从 VM 部署和传递电子邮件的过程，从而受益于这些合法服务的高传递率和良好声誉。如果恶意邮件被允许通过这些云服务发送，则防御者必须依靠强大的电子邮件筛选功能来阻止电子邮件进入其环境。

Microsoft 帐户仍然是网络钓鱼运营商的首要目标，大量假冒 Microsoft 365 登录页面的网络钓鱼登录页面就证明了这一点。例如，网络钓鱼者试图通过生成针对收件人自定义的唯一 URL 来匹配其网络钓鱼套件中的 Microsoft 登录体验。此 URL 指向为获取凭据而开发的恶意网页，但 URL 中的参数将包含特定收件人的电子邮件地址。一旦目标导航到页面，网络钓鱼套件将预先填充用户登录数据和为电子邮件收件人自定义的公司徽标，镜像目标公司自定义的 Microsoft 365 登录页面的外观。

使用动态内容假冒 Microsoft 登录页面的网络钓鱼页面

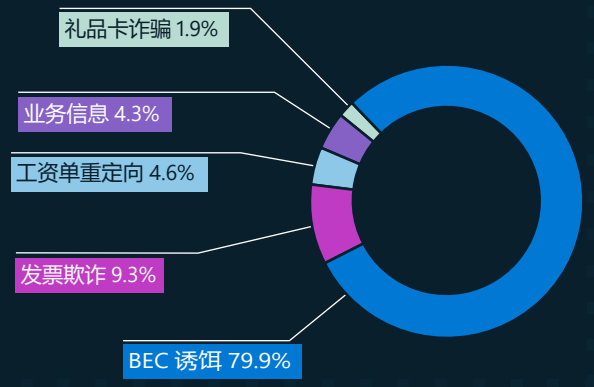


聚焦企业电子邮件入侵

网络犯罪分子正在开发越来越复杂的方案和技术，破坏安全设置，并将目标对准个人、企业和组织。为此，我们正在投入大量资源，进一步加强我们的 BEC 执法计划。

BEC 是代价最高的金融网络犯罪，估计 2021 年的调整后损失将达到 24 亿美元，占全球五大 Internet 犯罪损失的 59% 以上。[20] 为了了解问题的范围以及如何更好地保护用户免受 BEC 攻击，Microsoft 安全研究人员一直在跟踪攻击中最常使用的主题。

BEC 主题（2022 年 1 月至 6 月）



按发生次数比例划分的 BEC 主题

BEC 趋势

作为切入点，BEC 攻击者通常会试图与潜在受害者展开对话，以建立融洽的关系。攻击者会冒充同事或生意上的熟人，逐渐将对话引导到资金转移的方向。我们追踪到，作为 BEC 诱饵的自我介绍电子邮件占检测到的 BEC 电子邮件的近 80%。Microsoft 安全研究人员在过去一年中发现的其他趋势包括：

- 2022 年观察到的 BEC 攻击中最常用的技术是欺骗 [21] 和假冒。[21]
- 对受害者造成最大经济损失的 BEC 子类型是发票欺诈（根据我们进行的 BEC 活动调查发现的数量和要求支付的美元金额）。
- 商业信息盗窃（如应付账款报告和客户联系人）使攻击者能够发起令人信服的发票欺诈。
- 大多数工资重定向请求都来自免费的电子邮件服务，很少来自遭到入侵的帐户。来自这些来源的电子邮件数量在每个月的 1 号和 15 号左右激增，这是最常见的发薪日。
- 尽管礼品卡诈骗是众所周知的欺诈途径，但在检测到的 BEC 攻击中，礼品卡诈骗仅占 1.9%。

切实可行的见解

防范网络钓鱼

为了减少您的组织遭受网络钓鱼的风险，建议 IT 管理员实施以下策略和功能：

1. 要求在所有帐户中使用 MFA 以限制未经授权的访问。
2. 为高特权帐户启用条件访问功能，以阻止来自通常不会在贵组织中生成流量的国家、地区和 IP 的访问。
3. 考虑为高管、参与付款或购买活动的员工及其他特权帐户采用物理安全密钥。
4. 强制使用支持 Microsoft SmartScreen 等服务的浏览器来分析 URL 中的可疑行为，并阻止对已知恶意网站的访问。[23]
5. 使用基于机器学习的安全解决方案，在电子邮件到达收件箱之前，隔离高概率网络钓鱼并引爆沙盒中的 URL 和附件，例如 Microsoft Defender for Office 365。[24]
6. 在整个组织中启用假冒和欺骗防护功能。
7. 配置域密钥识别邮件 (DKIM) 和基于域的消息身份验证、报告和一致性 (DMARC) 操作策略，以防止传递可能欺骗声誉良好的发件人的未经身份验证的电子邮件。
8. 审核租户和用户创建的允许规则，删除广域和基于 IP 的异常。这些规则通常具有优先级，可以通过电子邮件筛选允许已知的恶意电子邮件。
9. 定期运行网络钓鱼模拟器，以评估整个组织面临的潜在风险，并识别和告知易受攻击的用户。

更多信息的链接

- 从 Cookie 盗窃到 BEC：攻击者使用 AiTM 网络钓鱼站点作为进一步财务欺诈的切入点 | Microsoft 365 Defender 研究团队，Microsoft 威胁情报中心 (MSTIC)

同构文字欺骗

BEC 和网络钓鱼是常见的社会工程策略。社会工程在犯罪中发挥着重要作用，它通过获得信任来说服目标与犯罪分子进行互动。

在实体商业中，商标用于确保客户对产品或服务来源的信任，而假冒产品是对商标的滥用。与之类似，网络犯罪分子在网络钓鱼攻击中伪装成目标所熟悉的联系人，使用同构文字欺骗潜在受害者。

同构文字是在 BEC 中用于电子邮件通信的域名，其中一个字符被外观上相同或几乎相同的字符替换，以达到欺骗目标的目的。

BEC 尝试中使用的同构技术

BEC 通常有两个阶段，第一个阶段涉及凭据泄露。这些类型的凭据泄露可能是网络钓鱼攻击或大型数据泄露的结果。然后，凭据在暗网上被出售或交易。

第二个阶段是欺诈阶段，在此阶段，攻击者使用泄露的凭据和同构电子邮件域进行复杂的社会工程。

BEC 攻击的发展

技术	显示出该同构技术的域的百分比
用 l 代替 I	25%
用 i 代替 l	12%
用 q 代替 g	7%
用 rn 代替 m	6%
用 .cam 代替 .com	6%
用 0 代替 o	5%
用 ll 代替 l	3%
用 ii 代替 i	2%
用 vv 代替 w	2%
用 I 代替 ll	2%
用 e 代替 a	2%
用 nn 代替 m	1%
用 ll 代替 I，用 I 代替 i	1%
用 o 代替 u	1%

分析了 2022 年 1 月至 7 月之间的 1,700 多个同构域。虽然使用了 170 种同构技术，但 75% 的域仅使用了 14 种技术。

同构攻击的实际应用

攻击者在邮件服务提供商处注册了一个看起来与受害者认识的邮件域相同的同构域，并且用户名也一模一样。然后，攻击者从被劫持的域发送了一封被劫持的电子邮件，其中包含新的付款说明。

利用开源情报以及对电子邮件线程的访问，犯罪分子确定了负责开具发票和付款的个人。然后，他们假冒发送发票的个人的电子邮件地址。这种假冒形式包括创建相同的用户名，并对真正发件人的邮件域进行同构。

攻击者复制包含合法发票的电子邮件链，然后将发票更改为包含自己的银行详细信息。然后，他们从假冒的同构电子邮箱将此修改过的新发票重新发送到目标。因为上下文合乎情理并且电子邮箱看起来是真实的，所以目标人员通常会遵循欺诈性指示。

切实可行的见解

1. 强制使用支持分析 URL 服务的浏览器，来发现可疑行为并阻止对已知恶意网站（例如 Safe Links 和 SmartScreen）的访问。[25]
2. 使用基于机器学习的安全解决方案，在电子邮件到达收件箱之前，隔离高概率网络钓鱼并引爆沙盒中的 URL 和附件。

更多信息的链接

- 互联网犯罪投诉中心 (IC3) | 商业电子邮件入侵 : 430 亿美元诈骗案
- 欺骗性智能见解 - Office 365 | Microsoft Docs
- 冒名顶替洞察 - Office 365 | Microsoft Docs

Microsoft 通过早期协作破坏僵尸网络的时间线

十多年来，DCU 一直致力于主动制止产生 26 种恶意软件并造成国家层面破坏的网络犯罪。随着 DCU 团队不断采用更先进的策略和工具来停止这些非法行为，我们看到网络犯罪分子也在改进攻击方法，试图保持领先。下面是一个时间线，显示了 DCU 破坏的僵尸网络示例以及 Microsoft 为关闭它们而采取的策略。

2008 年

Conficker 僵尸网络

描述：一种以 Windows 操作系统为目标的快速传播的蠕虫病毒，感染了公共网络中数百万台计算机和设备，造成全球网络中断。

协作：成立 Conficker 工作组，这是同类组织中的第一个联盟。Microsoft 与全球 16 家组织合作，战胜了该僵尸网络程序。

Microsoft 响应：该工作组在多个国际司法管辖区开展合作，并成功打败了 Conficker。

2009 年

Waledac 僵尸网络

描述：这是一种包含美国域名的复杂垃圾邮件僵尸网络，它会收集电子邮件地址并分发垃圾邮件，感染了全世界多达 90,000 台计算机。[26]

协作：建立了另一个联盟 Microsoft 恶意软件防护中心 (MMPC)，重点与学术界密切合作。[27]

Microsoft 响应：Microsoft 使用了 C2 的分层破坏方法，并在没有通知的情况下夺取了美国域名，让恶意行为者出其不意。[28]Microsoft 对 Waledac 服务器使用的近 280 个域名授予临时所有权。

2011 年

Microsoft 数字犯罪部门已成立

协作：通过汇集由调查人员、律师和工程师组成的团队，阻止会影响 Microsoft 生态系统的网络犯罪。

Microsoft 方法：目标是更好地了解各种恶意软件的技术方面，并向 Microsoft 的法律团队提供这些见解，以制定有效的中断策略。

2013 年

Rustock 僵尸网络

描述：这是一种使用 Internet 提供商作为主要 C2 的后门木马垃圾电子邮件程序，用于销售药品。

协作：Microsoft 与 Pfizer Pharmaceuticals 建立了合作关系，以了解 Rustock 销售的药物，同时与荷兰执法官员密切合作。[29]

Microsoft 响应：Microsoft 与美国马歇尔大学和荷兰执法部门合作，关闭了该国的 C2 服务器。此外，还注册并阻止了将来所有的域生成器算法 (DGA)。

Sirefef/Zero Access 僵尸网络

描述：这是一种广告僵尸网络，用于将人们引导至会安装恶意软件或窃取个人信息的危险网站；感染的计算机已超过 200 万台，广告商每月因此损失超过 270 万美元；主要涉及美国和西欧。

协作：与 FBI 和欧洲刑警组织网络犯罪中心密切合作，以破坏点对点基础结构。

Microsoft 响应：加入 Zero Access 网络，替换了犯罪分子的 C2 服务器，并成功夺取了下载服务器域。

2019 年

Trickbot 僵尸网络

描述：这是一种复杂的僵尸网络，在全球范围内设有零散的基础结构，其目标是金融服务行业，入侵 IoT 设备。

协作：Microsoft 与金融服务信息共享和分析中心 (FS-ISAC) 合作，摧毁 Trickbot。[30]

Microsoft 响应：DCU 构建了一个系统来识别和跟踪自动程序的基础结构，并为活跃的 Internet 提供商生成通知，同时考虑到各个国家 / 地区的特定法律。

持续专注于破坏行动

描述：Microsoft 在过去一年中破坏了七个威胁行为者的基础结构，成功阻止他们分发更多恶意软件、控制受害者的计算机以及将更多受害者作为目标。

协作：在与 Internet 服务提供商、政府、执法部门和私营企业的合作中，Microsoft 分享了大量信息，以补救全球各地超过 1,700 万的恶意软件受害者。

2022 年

展望未来

DCU 不断创新，并希望利用其在破坏僵尸网络方面的丰富经验来开展超越恶意软件的联合行动。要想持续取得成功，我们需要进行创造性工程设计、信息共享、创新的法律理论并实现公私企业合作。

网路犯罪分子滥用基础结构

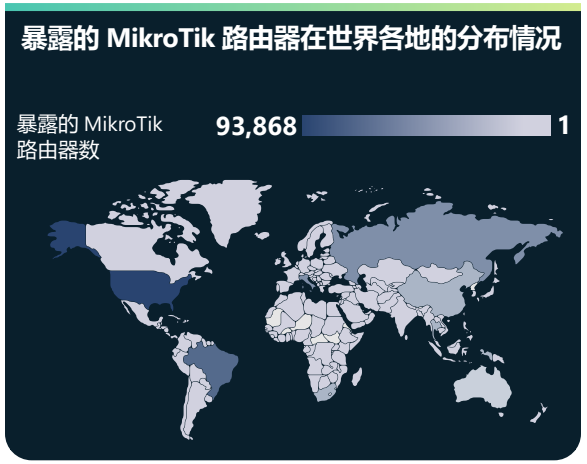
使用 Internet 网关作为犯罪命令与控制基础结构

对于使用广泛僵尸网络的网络犯罪分子而言，IoT 设备越来越成为其青睐的攻击目标。当路由器未安装补丁并直接暴露在 Internet 上时，威胁行为者会滥用它们来访问网络、执行恶意攻击，甚至支持其运营。

Microsoft Defender for IoT 团队对各种设备进行了研究，从传统的工业控制系统控制器到前沿的 IoT 传感器，不一而足。该团队调查了 IoT 和 OT 特定的恶意软件，为共享的威胁指标列表增添了相关内容。

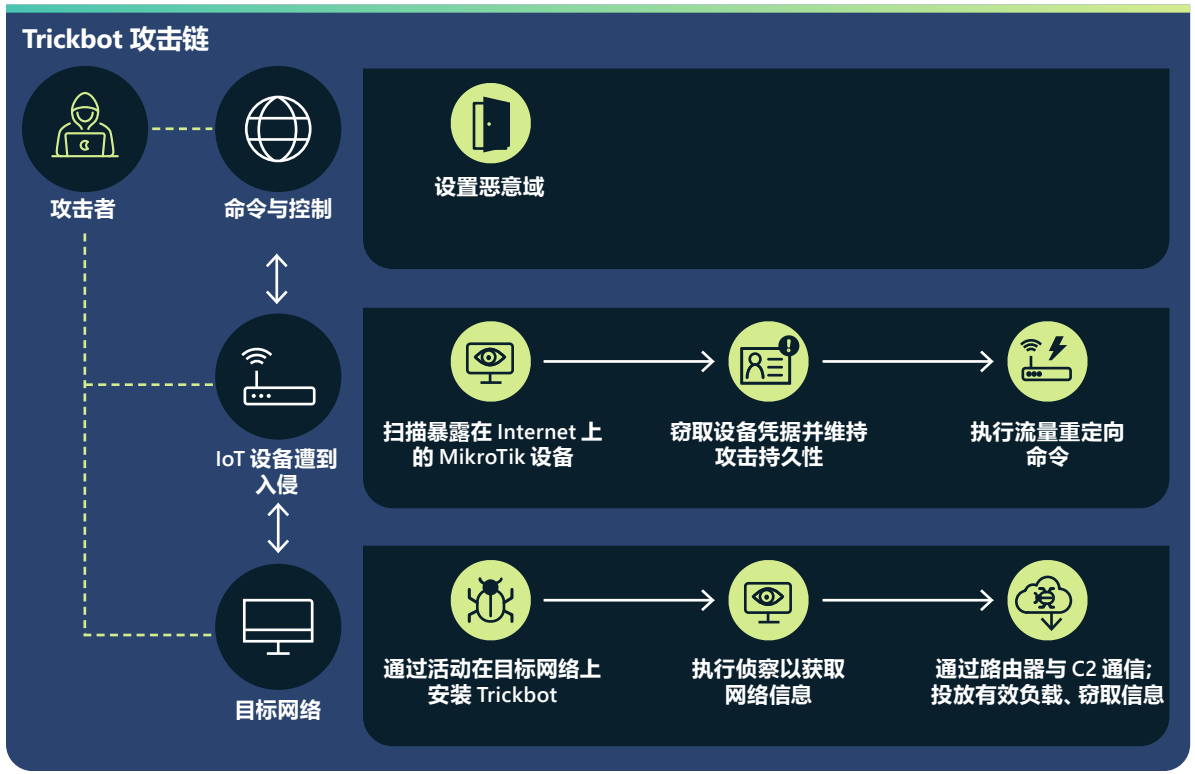
路由器是特别容易受到攻击的媒介，因为它们在连接 Internet 的家庭和组织中无处不在。我们一直在跟踪 MikroTik 路由器（这是一款在全球住宅和商业领域常用的路由器）的活动，确定它们如何被用于命令与控制 (C2)、域名系统 (DNS) 攻击和加密货币挖掘劫持。

更具体地说，我们确定了 Trickbot 行动者如何利用遭到入侵的 MikroTik 路由器，并对其进行重新配置以作为其 C2 基础结构的一部分。这些设备的普及加剧了 Trickbot 滥用它们的严重性，而其独特的硬件和软件使威胁行为者能够逃避传统安全措施，扩展其基础结构，并危及更多的设备和网络。



暴露的路由器存在潜在漏洞被利用的风险。

通过跟踪和分析包含安全外壳 (SSH) 命令的流量，我们观察到攻击者在获得设备的合法凭据后会使用 MikroTik 路由器与 Trickbot 基础结构进行通信。这些凭据可通过暴力攻击、使用现成的补丁利用已知漏洞以及使用默认密码来获得。一旦设备遭到访问，攻击者就会发出一个独特命令，在路由器的两个端口之间重定向流量，从而在受 Trickbot 影响的设备和 C2 之间建立通信线路。



Trickbot 攻击链显示使用 MikroTik IoT 设备作为 C2 的代理服务器。

我们已经将对攻击 MikroTik 设备（不仅仅是 Trickbot）的各种方法的相关信息以及已知的常见漏洞和暴露 (CVE) 汇总到一个针对 MikroTik 设备的开源工具中，该工具可提取与攻击这些设备相关的取证工件。[31]

充当恶意软件 C2 反向代理的设备不仅限于 Trickbot 和 MikroTik 路由器。通过与 Microsoft RiskIQ 团队合作，我们追溯到所涉及的 C2，并通过观察 SSL 证书，最终确定 Ubiquiti 和 LigoWave 设备也受到了影响。[32] 这充分表明 IoT 设备正在成为国家层面联合攻击的活跃组成部分，同时也是使用广泛的僵尸网络的网络犯罪分子的热门攻击目标。

滥用 IoT 设备的加密犯罪分子

随着已知漏洞的数量逐年持续增长，网关设备日益成为威胁行为者有价值的攻击目标。攻击者利用网关设备进行加密货币挖掘和其他类型的恶意活动。

随着加密货币的日益普及，许多个人和组织对路由器等设备中的计算能力和网络资源进行投资，以在区块链中挖掘货币。然而，挖掘加密货币是一个耗费时间和资源的过程，并且成功几率很低。为了提高挖出货币的几率，挖掘者在分布式合作网络中汇集在一起，接收与他们使用互联资源成功挖掘出的货币百分比相关的哈希值。

在过去的一年中，Microsoft 观察到越来越多的攻击滥用路由器来重定向加密货币挖掘工作。网络犯罪分子会入侵连接到货币挖掘池的路由器，并通过 DNS 中毒攻击将货币挖掘流量重定向到其关联的 IP 地址，从而改变目标设备的 DNS 设置。受影响的路由器会将错误的 IP 地址注册到至给定域名，将其货币挖掘资源（或哈希值）发送到威胁行为者使用的池中。这些池可能会挖掘与犯罪活动相关的匿名货币，或者使用货币挖掘者生成的合法哈希值来获取他们挖掘的一定比例的货币，从而获得回报。

2021 年发现的已知漏洞中有半数以上没有补丁，更新和保护企业及专用网络上的路由器对于设备所有者和管理员来说仍然是一项重大挑战。

网关设备的 DNS 中毒会危及合法的采矿活动，并将资源重定向到犯罪的采矿活动。

使用虚拟机作为犯罪基础结构

在向云广泛迁移的过程中，网络犯罪分子会利用通过网络钓鱼或分发恶意软件凭据窃取者从不知情的受害者那里获得的私人资产。许多网络犯罪分子选择在基于云的虚拟机 (VM)、容器和微服务上设置其恶意基础结构。

当网络罪犯分子获得访问权限后，他们会执行一系列事件来设置基础结构，例如通过编写脚本和自动化流程设置一系列虚拟机。这些脚本化的自动化流程用于启动恶意活动，包括大规模电子邮件垃圾邮件攻击、网络钓鱼攻击和托管恶意内容的网页。它甚至包括建立一个可扩展的虚拟环境来进行加密货币挖掘，最终受害者在月底会收到数十万美元的账单。

网络犯罪分子明白他们的恶意活动生命周期有限，很快就会被发现和关闭。因此，他们扩大了规模，现在积极主动地运营，并把突发事件放在首位。据观察，他们会提前准备受入侵的帐户并监控其环境。一旦有帐户（使用数十万个虚拟机设置）被检测到，他们就会遍历到下一个帐户（已经通过脚本做好了准备，可立即激活），从而确保其恶意活动可以几乎无中断地持续进行。

与云基础结构一样，本地基础结构可用于对本地用户未知的虚拟本地环境进行攻击。这需要将初始接入点保持开放和可访问状态。网络犯罪分子也会滥用本地私有资产来启动云基础结构的前向链，设置用于混淆其来源以规避对可疑基础结构创建活动的侦察。

切实可行的见解

1. 实施良好的网络安全机制，并为员工提供网络安全培训以及避免遭受社交工程改造的指导。
2. 通过大规模检测定期执行自动用户活动异常检查，以帮助减少此类攻击。
3. 更新和保护公司及专用网络上的路由器。

黑客入侵是否成为常态？

虽然黑客入侵并不是一种新现象，但在乌克兰战争中，黑客志愿者数量激增，其中不乏一些受政府指示部署网络工具以损害政治对手、组织甚至国家层面的声誉或资产的黑客。

2022 年 2 月，乌克兰政府号召世界各地的平民加入其强大的 300,000 “IT 军”，对俄罗斯进行网络攻击。[33] 与此同时，该政府建立了 Anonymous、Ghostsec、Against the West、Belarusian Cyber Partisans 和 RaidForum2 等黑客激进分子团体开始支持乌克兰进行攻击。包括一些 Conti 勒索软件团伙在内的其他团体则站在俄罗斯一边。[34]

在接下来的几个月里，Anonymous 的活动非常引人注目。黑客以该组织的名义（或其附属机构的名义）暂时关闭了数千个俄罗斯和白俄罗斯网站，泄露了数百 GB 的被盗数据，入侵了俄罗斯电视频道以播放亲乌克兰内容，甚至提出为投降的俄罗斯坦克支付比特币。

平民黑客的崛起

在社交媒体平台的推动下，成千上万的潜在平民黑客迅速组织和动员起来，在相关指导下进行易于执行的攻击（例如 DDoS 攻击）。组织者利用 Twitter、Telegram 和私人论坛来召集黑客、组织行动并传播黑客入侵指导手册。

然而，大部分此类黑客可能掌握的技能有限，即使有相关指导也是如此。这暗示了两种可能的未来情形：一种情形是成百上千具有基本技术能力的个人会使用攻击模板在将来对目标进行联合攻击或由黑客激进分子进行个人攻击，另一种情形是在乌克兰敌对行动最终结束后，他们会将黑客入侵行动抛在脑后，至少在下一个政治或社会问题出现之前，不会采取行动。

黑客政治化

这种政治动员带来的更大风险是部署精通技术的黑客，他们可能会持续针对外国政府目标进行网络攻击，以支持自己国家的优先任务；他们可能是自发组织的，也可能是在政府要求下组织的。

伊朗、中国和俄罗斯已经将黑客活动用作其国家黑客组织的招募渠道。例如，2022 年 4 月，亲俄黑客组织 Killnet 对捷克铁路、地区机场和捷克的公务员服务器发起了 DDoS 攻击，但是捷克并未直接参与战争。[35] 与此同时，一些政府可能使用黑客入侵为传统的网络间谍或蓄意破坏行动打掩护 - 例如，伊朗针对以色列发起的行动。

在与黑客入侵相关的 DDoS 攻击不断加剧的环境中，技术行业面临挑战，他们必须快速破译流向网站的正常和异常流量之间的差异。Microsoft 及其合作伙伴开发了一系列工具，可区分恶意 DDoS 流量并追溯其来源。此外，Microsoft 的 Azure 平台可以识别出平台上产生异常高水平出站流量的计算机并将其关闭。

抗议软件的问世

抗议软件的出现直接源于对俄罗斯与乌克兰之间的战争的情绪反应。一些开源软件开发人员利用其软件的普及性，来发表声明或采取行动以应对不断发展的地缘政治局势。这包括在桌面或浏览器上打开无害的文本文件来传播和平信息，但也包括基于 IP 地址地理定位进行针对性攻击以及采取破坏性行动（如擦除硬盘驱动器）。随着其他全球事件的不断发展，我们将来还会再次见到抗议软件。由于这些行为通常是受人尊敬的开源维护者决定使用自己的开源组件发表个人声明的情况，因此目前没有相应的保护措施来阻止源文件包中发生此类更改，用户务必应注意其潜在影响。

在社交媒体平台的推动下，成千上万的潜在平民黑客组织和动员起来，在相关指导下进行易于执行的攻击（例如 DDoS 攻击）。

切实可行的见解

1. 技术行业必须齐心协力，制定应对这一新威胁的万全对策。
2. 包括 Microsoft 在内的领先技术公司拥有识别与 DDoS 攻击相关的恶意流量并禁用负责计算机的工具。
3. 在地缘政治冲突时期，开源用户应保持高度警惕。

尾注

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. 端点检测和响应 (EDR)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 是一个在线讨论论坛，在添加新成员时需要有现有成员为其提供担保。
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. 数据来源：Defender for Office（恶意电子邮件 / 盗用身份活动）、Azure Active Directory 标识保护（盗用身份事件 / 警报）、Defender for Cloud Apps（盗用身份数据访问事件）和 M365D（跨产品关联）。
17. 数据来源：Defender for Endpoint（攻击行为警报 / 事件）、Defender for Office（恶意电子邮件）和 M365D（跨产品关联）。
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. 基于域的消息身份验证、报告和一致性：这是一种电子邮件身份验证、策略和报告协议，可使电子邮件域的所有者保护其域免遭未经授权的使用。
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.Feb 22, 2010)。
27. 参见 Bowden, Mark.Worm: The First Digital World War.Grove/Atlantic, Inc., 2011 年 9 月 27 日。
28. 具体而言，《联邦民事诉讼规则》第 65 条允许一方在以下情况下寻求此类补救：1) 如果不给予救济，该方将立即遭受无法弥补的损害，以及 2) 该方试图及时向另一方发出通知。此外，法律要求应用平衡试验，平衡被告的通知权与对公众造成的伤害程度。
29. Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D.Wa.Feb 9, 2011)。
30. Microsoft Corp. v. Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist.LEXIS 258143, 在 *1（E.D.Va. Aug. 12, 2021).
31. https://github.com/microsoft/routeros-scanner
32. RiskIQ: Ubiquiti 设备遭到破坏并用作恶意软件 C2 反向代理 | RiskIQ Community Edition
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

国家层面威胁

国家层面行为者正在发起越来越复杂的网络攻击，旨在逃避检测并进一步推进其战略重点。

国家层面威胁概述 31
引言 32
民族国家数据的背景 33
国家层面行为者及其活动的示例 34
不断演变的威胁格局 35
关键基础设施攻击趋势 36
IT 供应链作为数字生态系统的门户 37
快速漏洞利用 39
俄罗斯国家层面行为者的战时网络策略威胁着乌克兰及其他地区 41
中国扩大全球目标以获得竞争优势 44
伊朗在权力交接后行事愈发激进 46
朝鲜利用网络功能实现政权的三个主要目标 49
网络雇佣兵威胁网络空间的稳定性 52
实施网络安全规范，确保网络空间和平与安全 53

国家层面威胁

概述

国家层面行为者正在发起越来越复杂的网络攻击，旨在逃避检测并进一步推进其战略重点。乌克兰混合战争中网络武器的部署，标志着一个新的冲突时代的到来。

俄罗斯还通过信息影响行动支持战争，利用宣传来影响俄罗斯、乌克兰和全球的舆论。这场第一次全面的混合冲突还给我们上了另外的重要一课。首先，通过迁移到云端，可以充分保护数字操作和数据的安全，无论是在网络空间还是物理空间均不例外。俄罗斯在最初攻击时使用 Wiper 恶意软件将本地服务作为攻击目标，并使用第一批发射的导弹之一将物理数据中心作为目标。

乌克兰的回应是将工作负载和数据快速迁移到托管在乌克兰境外数据中心内的超大规模云中。其次，网络威胁情报和终结点保护由云中的数据和高级 AI 和 ML 服务提供支持，这些技术进步帮助乌克兰抵御了俄罗斯的网络攻击。

在其他地区，国家层面行为者活动更加猖獗，逐步利用自动化、云基础结构和远程访问技术方面的进步来攻击更广泛的目标。提供对最终目标访问权限的企业 IT 供应链经常遭到攻击。随着行为者迅速利用未修补的漏洞，使用复杂和暴力的技术来窃取凭据，并使用开源或合法软件混淆其行动，网络安全机制变得更加关键。并且，伊朗加入了俄罗斯的行列，采用包括勒索软件在内的破坏性网络武器作为攻击的主要手段。

这些形势的发展迫切需要采用一致的全球框架，优先考虑人权并保护人们免受网上鲁莽的国家行为的伤害。所有国家 / 地区都应共同努力，实施协商一致的负责任的国家 / 地区行为准则和规则。

保卫乌克兰：网络战争早期阶段的经验教训 - Microsoft 对这些问题的看法

针对关键基础结构（尤其是 IT 部门、金融服务、交通系统和通信基础结构）的攻击更为猖獗。

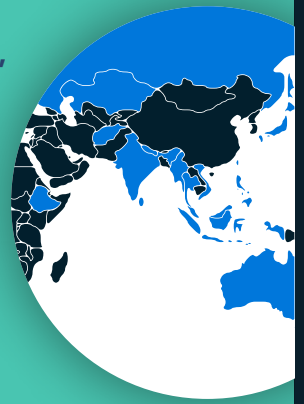
详情请参见第 35 页

使用 IT 供应链作为访问攻击目标的网关。

NOBELIUM

详情请参见第 36 页

中国扩大全球目标，特别是东南亚的小国，以获得情报和竞争优势。

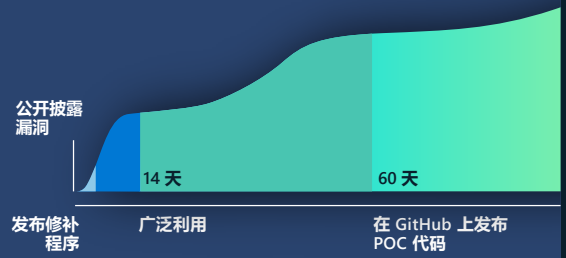


详情请参见第 44 页

伊朗在权力交接后行事愈发激进，将勒索软件攻击从地区敌对者扩大到美国和欧盟的受害者，并将美国备受瞩目的关键基础设施作为攻击目标。

详情请参见第 46 页

发现和快速利用未修补的漏洞已成为一项关键策略。快速部署安全更新则是防御的关键。



详情请参见第 39 页

朝鲜将国防和航空航天公司、加密货币、新闻媒体、叛逃者和援助组织作为攻击目标，以实现政权目标：稳固国防、促进经济和确保国内稳定。

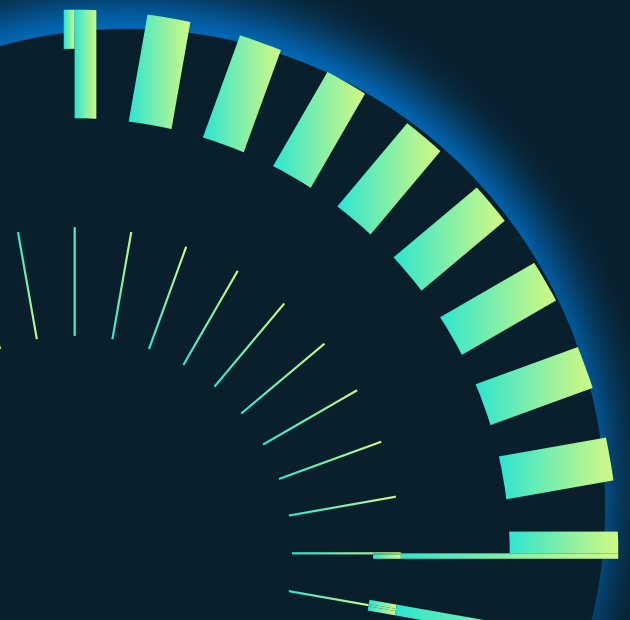
详情请参见第 49 页

网络雇佣军威胁网络空间的稳定性，因为这个由私营公司组成的蓬勃发展的行业正在开发和销售先进的工具、技术和服务，以使其客户（通常是政府）能够侵入网络和设备。

详情请参见第 52 页

引言

在 2020 年和 2021 年备受关注的攻击之后，国家层面威胁行为者花费了大量资源来应对组织为抵御复杂威胁实施的各种新安全保护措施。



与企业组织非常相似，攻击者开始利用自动化、云基础结构和远程访问技术方面的进步，将攻击范围扩大到一组更广泛的目标。这些战术调整促使攻击者采用新方法，针对企业供应链发起大规模攻击。随着行为者研究出新方法来迅速利用未修补的漏洞，发展技术来入侵公司网络，并使用开源或合法软件混淆其行动，IT 安全机制变得更加重要。新的攻击技术提供了更难检测的新媒介来获取目标网络的访问权限。最后，随着战时物理攻击的升级，我们看到网络攻击在军事活动中发挥着重要作用。

乌克兰冲突的例子不免过于尖锐，但它很好地说明了网络攻击如何演变为与地面军事冲突一起影响着世界格局。电力系统、电信系统、媒体和其他关键基础设施均已成为物理攻击和网络攻击的目标。网络入侵攻击通常被视为间谍活动和信息窃取活动的一部分，已在针对关键基础设施系统进行的破坏性 Wiper 恶意软件攻击中成为混合战争的重点。如果将这些系统的安全性连接到云，可以及早检测和瓦解潜在的破坏性攻击。[1]

在一次重大网络事件中，利用机器学习的行为检测技术首次使用已知的攻击模式成功发现并阻止了进一步的攻击，而无需事先了解底层恶意软件；它甚至在人类意识到威胁之前，已探测到威胁。我们还证实了与保护这些系统的防御者实时共享威胁情报的价值，并为他们提供了重要信息，从而成功预测和防御主动攻击。

世界各地的国家层面威胁行为者不断以新旧方式扩大行动规模。China, North Korea, Iran, and Russia all carried out attacks on Microsoft customers.IT 服务供应链已是一个共同目标，因为行为者将关注重点转移到可作为入侵多个组织的接入点的上游服务。我们预计行为者会继续利用企业供应链中的信任关系，因此应重视全面执行身份验证规则、经常修补、对远程访问基础结构进行帐户配置以及经常审核合作关系以验证真实性的重要性。

国家层面行为者与勒索软件和犯罪行动者一样，通过将攻击目标转向配置不当或未经修补的企业系统（VPN/VPS 基础结构、本地服务器、第三方软件）来执行离地攻击，以应对日益增加的暴露风险。许多攻击者越来越多地使用商业恶意软件和开源红队 (red team) 工具来混淆其恶意活动。

因此，通过优先进行修补、启用防篡改功能、使用像 RiskIQ 这样的攻击面管理工具从外向内查看攻击面，以及在整个企业中启用多重身份验证，从而维持强大的 IT 安全机制基线，这已成为主动防御许多复杂行为者的基础准则。

国家层面行为者也越来越多地使用勒索软件作为攻击策略，经常在攻击中重复使用犯罪生态系统创建的勒索恶意软件。我们已经看到，伊朗和朝鲜的攻击者会利用商业勒索软件工具破坏地区敌对方的目标系统，其中通常包括关键基础设施。最后，我们看到网络雇佣兵正在开发和销售工具、技术和服务，以扩大对易受攻击的第三方解决方案的攻击，所造成的威胁日益严峻。国家层面行为者在攻击方面的复杂性和敏捷性将逐年提高。组织必须深入了解行为者的这些变化，以进行响应并同时发展防御措施。

John Lambert
Microsoft 威胁情报中心公司副总裁兼杰出工程师

民族国家数据的背景

国家层面威胁是指在特定国家 / 地区发起，以促进国家利益为明确目的的网络威胁活动。国家层面行为者发起了我们客户面临的一些最先进、最持久的威胁，包括知识产权盗窃、间谍活动、监视、凭据盗取和破坏性攻击等等。

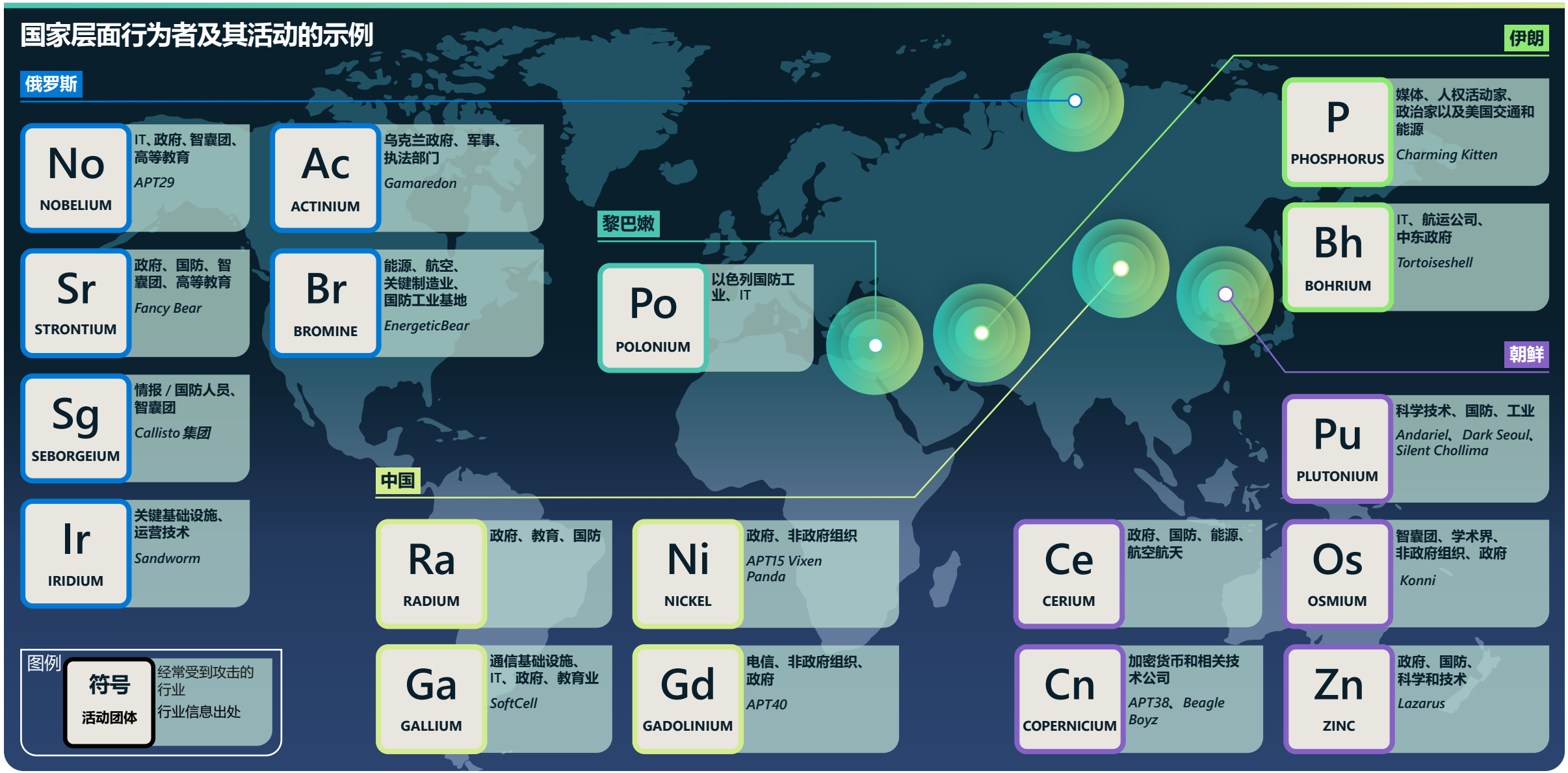
我们投入大量资源来发现、了解和应对这些威胁。当组织或个人帐户持有者被观察到的国家层面活动作为攻击目标或遭到其入侵时，Microsoft 会以国家层面通知 (NSN) 的形式直接向客户发送警报，其中包括他们调查该活动所需的信息。自 2018 年开始以来，截至 2022 年 6 月，我们已经提供了超过 67,000 个 NSN。

本章呈现了 Microsoft NSN 警报数据，以提供可衡量活动的情况。图表中显示的国家层面活动的级别基于 Microsoft 向客户发出的 NSN 数量，这些通知用于响应检测到的国家层面行为者将客户组织中的至少一个帐户作为攻击目标或发起入侵的行为。

我们在本报告中纳入其国家层面威胁团体的四个主要国家是俄罗斯、中国、伊朗和朝鲜。这些国家代表过去一年中将 Microsoft 客户作为攻击目标的最常见行为者的来源国 / 地区。此外，该报告还包括我们对来自黎巴嫩和网络雇佣兵的威胁团体或雇佣的私营部门攻击行为者的观察。

Microsoft 使用化学元素名称（例如 NOBELIUM）来标识国家层面团体，下一页显示了其中的一些名称。我们使用 DEV-#### 指称作为未知、新兴或发展中的一组威胁活动的临时名称，从而在确定该活动背后的行为者的来源或身份之前，将其作为一组独特的信息进行跟踪。

一旦符合标准，DEV 将转换为指定的行为者或与现有行为者合并。在本章中，我们引用国家层面和 DEV 团体的示例，来更深入地说明攻击目标、技术和动机分析。尽管其中许多组织使用与网络犯罪分子相同的工具，但他们能够定制恶意软件、发现和利用零日漏洞并逃脱法律制裁，从而带来了特殊的威胁。


国家层面行为者及其活动的示例
俄罗斯
No
NOBELIUM
IT、政府、智囊团、高等教育
APT29
Ac
ACTINIUM
乌克兰政府、军事、执法部门
Gamaredon
Sr
STRONTIUM
政府、国防、智囊团、高等教育
Fancy Bear
Br
BROMINE
能源、航空、关键制造业、国防工业基地
EnergeticBear
Sg
SEBORGEIUM
情报 / 国防人员、智囊团
Callisto 集团
Ir
IRIDIUM
关键基础设施、运营技术
Sandworm
黎巴嫩
Po
POLONIUM
以色列国防工业、IT
伊朗
P
PHOSPHORUS
媒体、人权活动家、政治家以及美国交通和能源
Charming Kitten
Bh
BOHRIUM
IT、航运公司、中东政府
Tortoiseshell
朝鲜
Pu
PLUTONIUM
科学技术、国防、工业
Andariel、Dark Seoul、Silent Chollima
中国
Ra
RADIUM
政府、教育、国防
Ni
NICKEL
政府、非政府组织
APT15 Vixen Panda
Ce
CERIUM
政府、国防、能源、航空航天
Os
OSMIUM
智囊团、学术界、非政府组织、政府
Konni
Ga
GALLIUM
通信基础设施、IT、政府、教育业
SoftCell
Gd
GADOLINIUM
电信、非政府组织、政府
APT40
Cn
COPERNICIUM
加密货币和相关技术公司
APT38、Beagle Boyz
Zn
ZINC
政府、国防、科学和技术
Lazarus
图例
符号
活动团体
经常受到攻击的行业
行业信息出处

不断演变的威胁格局

Microsoft 的任务是跟踪国家层面行为者的活动，并在发现客户成为其攻击目标或遭到入侵时向其发出通知，这深深植根于我们致力于保护客户免受攻击的使命。

此通知是我们承诺的重要组成部分，我们会告知客户观察到的攻击是否已由我们的安全产品保护措施成功阻拦，或者攻击是否因未知的安全漏洞而成功奏效。随着时间的推移跟踪这些通知有助于 Microsoft 发现行为者不断变化的威胁趋势，并将产品保护重点放在主动减轻对我们云服务中的客户造成的威胁。

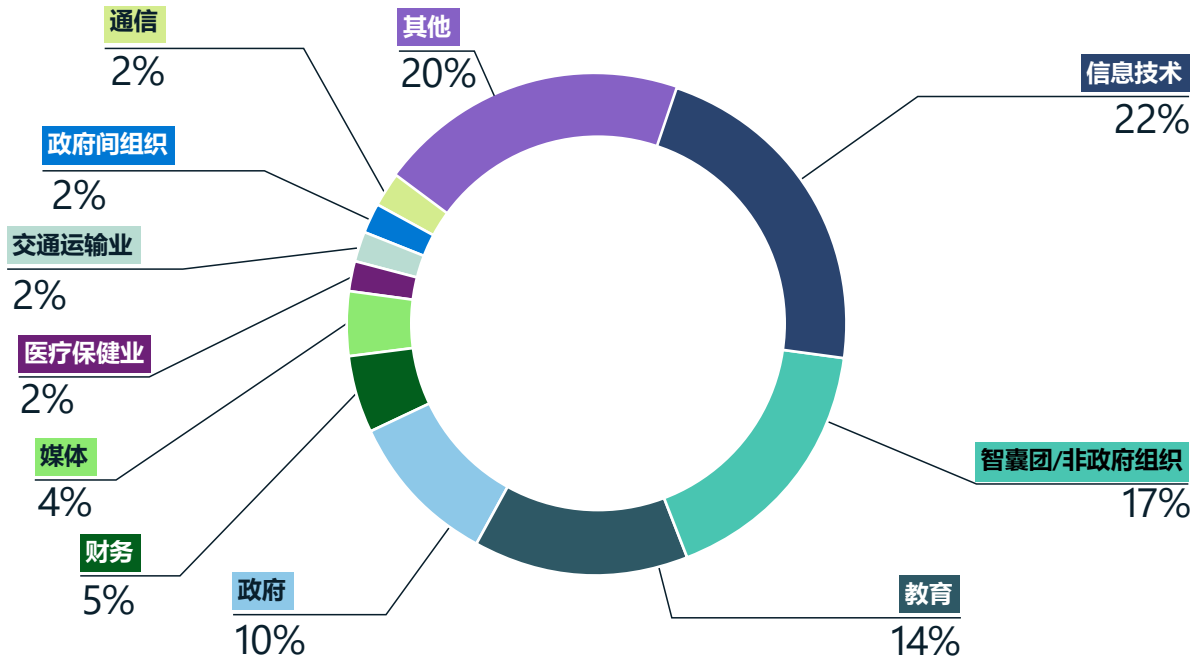
通过跟踪，我们还可以分享关于我们所见情况的数据和见解。在跟踪这些行为者及其攻击时，分析师会结合使用技术指标和地缘政治专业知识来了解行为者的动机，从而融合技术和全局背景以形成新的见解。这种规划让我们能够通过独特的视角来了解国家层面网络行为者的优先事项，以及他们的动机如何反映出雇用他们的国家的政治、军事和经济优先事项。

全球由国家支持的威胁团体的优先事项和风险承受能力受到过去一年政治发展状况的影响。随着地缘政治关系瓦解和鹰派人士在一些国家 / 地区获得更多控制权，网络行为者变得更加肆无忌惮，行为更加激进。例如：

- 俄罗斯始终坚持将乌克兰政府和该国的关键基础设施作为攻击目标，以辅助其实地军事行动。[2]
- 伊朗积极寻求入侵美国的关键基础设施，例如港口当局。
- 朝鲜继续从事窃取金融和技术公司加密货币的活动。
- 中国扩大了其全球网络间谍活动。

虽然国家层面行为者采用的技术可能十分复杂，并会采用各种策略，但通常可以通过良好的网络安全机制来减少其发起的攻击。其中许多行为者依靠技术含量相对较低的手段（例如鱼叉式网络钓鱼电子邮件）来传递复杂的恶意软件，而不是投资开发定制的攻击手段或使用有针对性的社会工程来实现其目标。

国家层面行为者视为攻击目标的行业领域



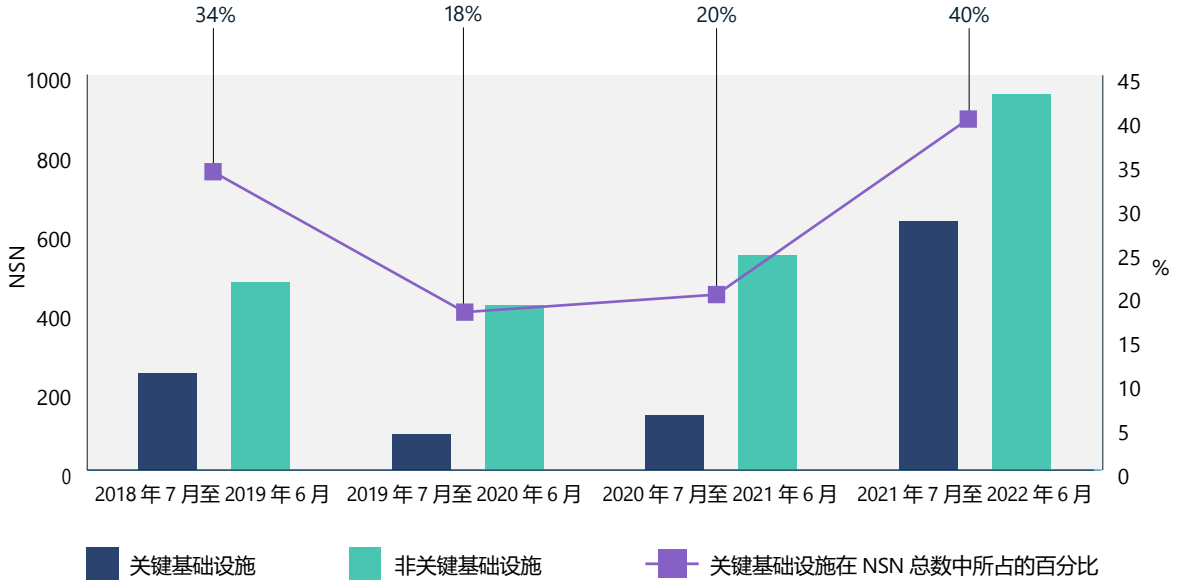
国家层面团体以多个领域为攻击目标。俄罗斯和伊朗国家层面行为者将 IT 行业作为攻击目标，并通过这种手段来访问 IT 公司的客户信息。国家层面行为者其他的共同目标仍为智囊团、非政府组织 (NGO)、大学和政府机构。

国家层面行为者有各种不同目标，为此，他们可能会以特定的组织或个人团体为攻击目标。去年，供应链攻击有所增加，特别是针对 IT 公司。通过入侵 IT 服务提供商，威胁行为者通常能够利用与管理连接系统的公司的信赖关系达到其初始目标，或者有可能通过在一次攻击中入侵数百个下游客户来发起更大规模的攻击。紧随 IT 领域之后，受攻击最频繁的实体为智囊团、大学附属学者和政府官员。这些都是间谍收集地缘政治问题情报的理想“软目标”。

不断演变的威胁格局

接上页

关键基础设施攻击趋势

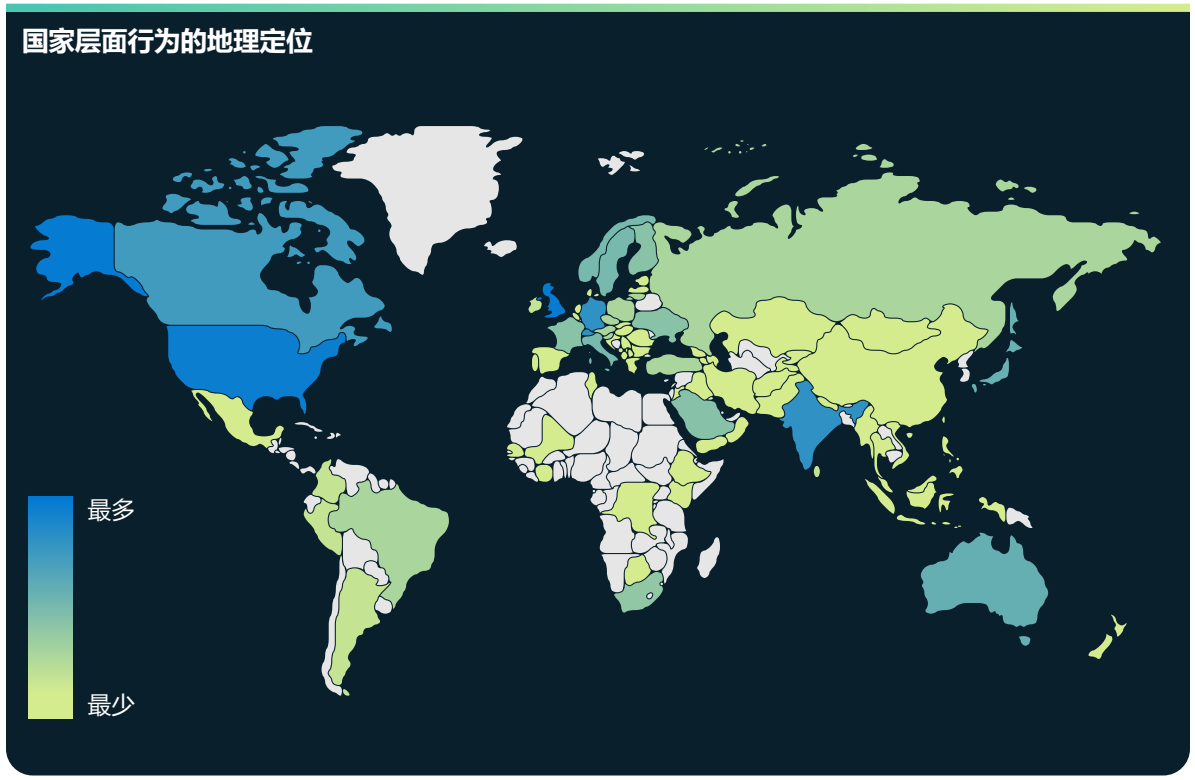


在过去的一年中，国家层面团体以关键基础设施[3]为目标的活动有所增加，行为者重点攻击的是 IT 领域、金融服务、交通系统和通信基础设施公司。

“在乌克兰遭到入侵之前，各国政府认为数据需要留在国内才能保证安全。在乌克兰遭到入侵之后，将数据迁移到云并移到境外现已成为复原计划和良好治理的一部分。”

Cristin Flynn Goodwin，
客户安全和信任部门副总法律顾问

国家层面行为的地理定位



去年，国家层面团体的网络攻击遍及全球，针对美国和英国企业的攻击尤其多。根据我们的 NSN 数据，以色列、阿联酋、加拿大、德国、印度、瑞士和日本的组织也是受攻击最频繁击的一些组织。

切实可行的见解

1. 确定并保护可能与国家层面团体的战略优先事项相符的潜在高价值数据目标、有风险的技术、信息和业务运营。
2. 启用云保护，以便大规模识别和减轻对网络的已知和新型威胁。

IT 供应链作为数字生态系统的门户

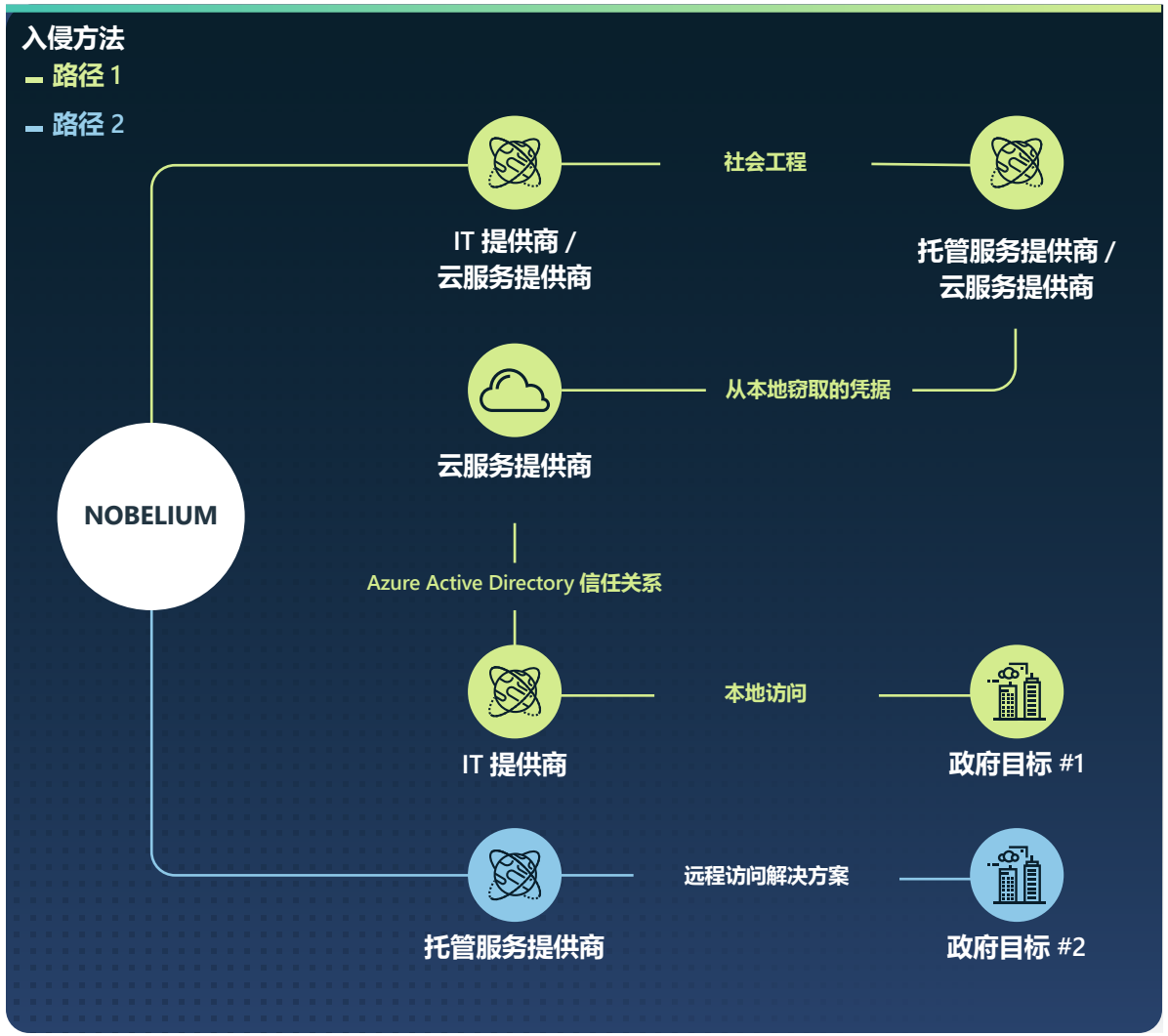
国家层面对 IT 服务提供商的攻击，可能会使威胁行为者利用授予这些供应链提供商的信任和访问权限，对其他感兴趣的组织加以利用。在过去的一年中，国家层面网络威胁团体将 IT 服务提供商作为攻击目标来攻击第三方目标并获取对政府部门、政策和关键基础设施领域下游客户的访问权限。

IT 服务提供商是富有吸引力的中间目标，因为他们为外国情报服务组织感兴趣的数百个直接客户和数千个间接客户提供服务。如果被利用，这些公司的日常业务实践和享有的委托管理特权可能会致使恶意行为者访问和操作 IT 服务提供商客户网络，而不会立即触发警报。

在过去的一年中，NOBELIUM 试图入侵和利用云解决方案和其他托管服务提供商的特权帐户，设法主要针对美国和欧洲政府和政策客户获取下游访问权限。

NOBELIUM 展示了如何采用“入侵一方来入侵多方”的方法来针对视为地缘政治对手的目标发起攻击。在过去的一年中，威胁行为者对总部位于北大西洋公约组织 (NATO) 成员国的敏感组织展开了第三方和直接入侵，俄罗斯政府认为北约对其生存构成了威胁。2021 年 7 月至 2022 年 6 月初期间，Microsoft 有关俄罗斯针对在线服务客户展开威胁活动的客户通知有 48% 发往了总部位于北约成员国的 IT 领域公司，这些公司可能充当了中间访问点。总体而言，同一时期有关俄罗斯威胁活动的通知有 90% 发往了总部位于北约成员国的客户，主要涉及 IT 领域、智囊团和非政府组织 (NGO) 以及政府部门，这表明威胁行为者采用的策略是通过多种手段来获取对这些目标的初始访问权限。

行为者已从利用软件供应链转变为利用 IT 服务供应链，将云解决方案和托管服务提供商作为攻击目标来入侵下游客户。



此图描述了 NOBELIUM 采用多媒介方法来入侵其最终目标以及在整个过程中对其他受害者造成的附带伤害。除了上述行动之外，NOBELIUM 还对相关实体发起了密码喷射和网络钓鱼攻击，甚至至少以一名政府员工的个人帐户为攻击目标来作为另一种潜在的入侵途径。

IT 供应链作为数字生态系统的门户

接上页

全年，Microsoft 威胁情报中心 (MSTIC) 检测到有越来越多的伊朗国家层面和与伊朗关联的行为者在入侵 IT 公司。在许多情况下，MSTIC 检测到行为者窃取登录凭据来获取对下游客户的访问权限，以实现从收集情报到实行具有破坏性的报复性攻击的一系列目标。

- 2021 年 7 月和 8 月，DEV-0228 入侵了一家以色列商业软件提供商，后来又入侵了以色列国防、能源和法律部门的下游客户。[4]
- 从 2021 年 8 月至 9 月，Microsoft 检测到以总部位于印度的 IT 公司为攻击目标的伊朗国家层面行为者数量激增。缺乏促使发生这种转变的紧迫地缘政治问题表明，以这些公司为攻击目标是为了间接访问印度境外子公司和客户。
- 2022 年 1 月，我们评估的一个与伊朗政府关联的团体 DEV-0198 入侵了一家以色列云解决方案提供商。经 Microsoft 评估，此行为者可能使用了提供商遭到泄露的凭据来进行身份验证，以侵入一家以色列物流公司。当月晚些时候，MSTIC 观察到同一行为者试图对这家物流公司发起破坏性网络攻击。
- 2022 年 4 月，我们评估的一个黎巴嫩团体 POLONIUM 与伊朗国家层面团体联手破解 IT 供应链技术，入侵了另一家以色列 IT 公司来获取对以色列国防和法律组织的访问权限。[5]

过去一年的活动表明，NOBELIUM 和 DEV-0228 等威胁行为者比组织本身更了解组织的可信赖关系。这种日益严重的威胁态势突出表明，组织需要了解和强化其数字资产的边界和入口点。这还凸显了 IT 服务提供商严格监控自身网络安全健康状况的重要性。例如，组织应该实施多重身份验证和条件访问策略，使恶意行为者难以捕获特权帐户或侵入整个网络。

对合作伙伴关系进行全面审查和审核有助于最大限度地减少组织与上游提供商之间具有的任何不必要的权限，并立即删除任何看似陌生的关系的访问权限。通过增加对活动日志的了解并审查可用活动，可以更轻松地发现可能会引发进一步调查的异常情况。

通过以第三方为目标的国家层面的活动，他们可以利用供应链中具有的信任和访问权限来攻击敏感组织。

切实可行的见解

1. 审查和审核上游与下游服务提供商关系及委托特权访问，以最大限度地减少不必要的权限。删除任何看似陌生或尚未审核的合作伙伴关系的访问权限。[6]
2. 启用日志记录并审查远程访问基础结构和虚拟专用网络 (VPN) 的所有身份验证活动，重点关注配置有单重身份验证的帐户来确认真实性并调查异常活动。
3. 为所有帐户（包括服务帐户）启用 MFA，并确保对所有远程连接强制执行 MFA。
4. 使用无密码解决方案来保护帐户。[7]

更多信息的链接

- NOBELIUM 针对委托管理特权发起攻击以实现更广泛的攻击 | Microsoft 威胁情报中心 (MSTIC)
- 伊朗以 IT 领域为目标的活动呈上升趋势 | Microsoft 威胁情报中心 (MSTIC)、Microsoft 数字安全部门
- 揭露以以色列组织为目标的 POLONIUM 活动和基础结构攻击 | Microsoft 威胁情报中心 (MSTIC)

快速漏洞利用

随着组织改善其网络安全状况，国家层面行为者的应对措施是采用独特的新型策略来发起攻击和逃避检测。发现和利用以前未知的漏洞（称为零日漏洞）是其中的关键策略。

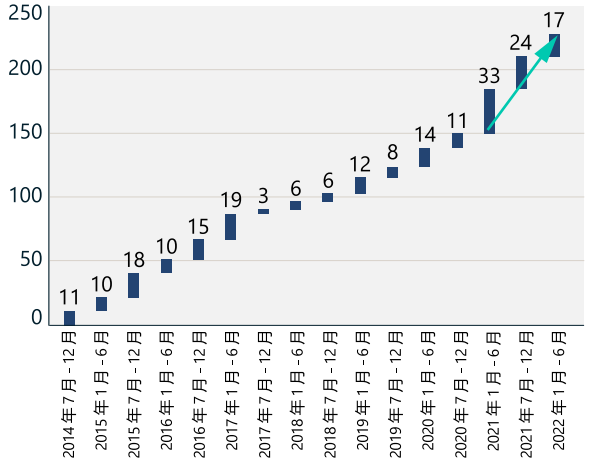
零日漏洞是一种特别有效的初始攻击手段，一旦公开，其他国家层面行为者和犯罪分子可能会迅速重复利用这些漏洞。过去一年公开披露的零日漏洞数与上一年持平，达到历史最高水平。

随着网络威胁行为者（包括国家层面行为者和犯罪分子）越来越善于利用这些漏洞，我们观察到从漏洞公开到漏洞商品化之间的时间缩短了。这使得组织必须立即修补漏洞。同样，发现新漏洞的组织或个人必须按照协调一致的漏洞披露程序，以负责任的态度尽快向受影响的供应商进行披露或报告，这一点至关重要。

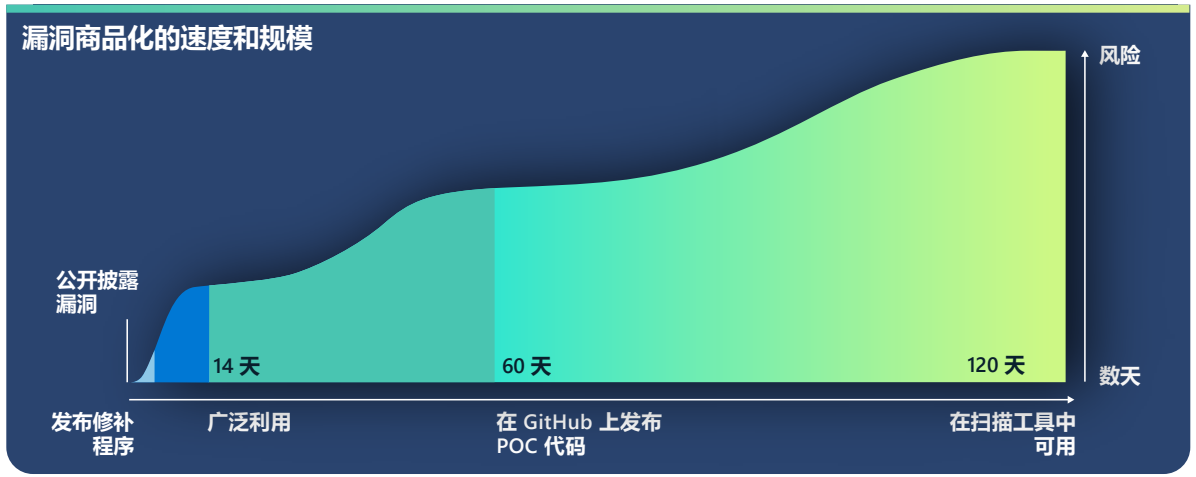
这可确发现别漏洞并及时开发修补程序，保护客户免遭以前未知的威胁。

许多组织认为，如果漏洞管理是其网络安全不可或缺的一部分，则他们不太可能成为零日漏洞攻击的受害者。但是，漏洞商品化会使他们更快地遭受攻击。零日漏洞经常被其他行为者发现并在短时间内被广泛地重复利用，使未修补的系统面临风险。尽管可能很难检测到零日漏洞，但检测行为者在攻击后采取的行动通常会更加容易，并且如果漏洞来自完全修补的软件，则可以作为入侵的警告信号。

针对零日漏洞发布的修补程序



常见漏洞和披露 (CVE) 列表中公开披露的零日漏洞数。



漏洞公开披露后，平均只需 14 天就会被广泛利用。此视图分析了利用零日漏洞的时间线，以及自首次公开披露以来易受到特定攻击并在 Internet 上处于活动状态的系统数量。

虽然零日漏洞攻击最初往往以数量有限的组织为攻击目标，但这种攻击方式很快就会在更大的威胁行为者生态系统中被采用。这使威胁行为者竞相在潜在目标安装修补程序之前尽可能广泛地利用此漏洞。

虽然我们观察到许多国家层面行为者利用未知漏洞开发漏洞，但基于中国的国家层面的威胁行为者特别擅长发现和开发零日漏洞。中国的漏洞报告条例于 2021 年 9 月生效，这是世界上首例政府要求在与产品或服务所有者共享漏洞之前，向政府机构报告漏洞，以供审查。 这项新规定可能会使中国政府中的一些人员能够储存报告的漏洞，以便将其武器化。去年，来自中国的行为者使用零日漏洞的情况有所增加，这可能反映了中国对中国安全社区的漏洞披露要求的第一个完整年度，以及将零日漏洞利用作为国家优先事项的重要一步。下面描述的漏洞首先是由基于中国的国家层面行为者在攻击中开发和部署的，然后才被发现并在更大的威胁生态系统中的其他行为者之间传播。

快速漏洞利用

接上页

即使组织并非国家层面攻击的目标，在这些漏洞被更广泛的行为者生态系统利用之前，可用于修补零日漏洞的时间也有限。

这些新发现的漏洞示例表明，距离修补漏洞并在线提供概念证明 (POC) 代码及其经常被其他行为者获取来重复利用之时，组织平均有 60 天的时间。同样，漏洞在 Metasploit 等自动漏洞扫描和利用工具中可用（这通常会导致漏洞被大规模利用）之前，组织平均有 120 天的时间。这突出表明，即使组织并非国家层面威胁行为者的目标，在这些漏洞被更广泛的行为者生态系统利用之前，可用于修补零日漏洞的时间也有限。

CVE-2021-35211 SolarWinds Serv-U

2021 年 7 月，SolarWinds 发布了一项针对 CVE-2021-35211 的安全公告，表示 Microsoft 及时发布了相关通知。[8] 当时，我们发现国家层面威胁行为者 DEV-0322 正在积极利用 SolarWinds Serv-U 漏洞。6 月 15 日至 7 月 9 日期间，我们的 RiskIQ 团队观察到有 12,646 个 IP 地址在托管受影响设备的联网版本。

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

2021 年 9 月，我们的研究人员观察到与中国有关联的行为者在几个美国实体中利用 Zoho ManageEngine。此漏洞于 9 月 6 日公开报告为 CVE-2021-40539 Zoho ManageEngine ADSelfService Plus，组织通常使用此服务来处理密码重置。[9] DEV-0322 在 9 月晚些时候利用了此漏洞，将其用作初始媒介来在网络中站稳脚跟并执行其他操作，包括凭据转储、安装自定义二进制文件和投放恶意软件以维持攻击持久性。在披露时，RiskIQ 观察到有 4,011 个这些系统的实例在 Internet 上处于活动状态。

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

2021 年 10 月下旬，我们观察到 DEV-0322 正在利用另一个 Zoho ManageEngine 产品 ServiceDesk Plus 中的漏洞 (CVE-2021-44077)，ServiceDesk Plus 是一款具有资产管理功能的 IT 技术支持软件。DEV-0322 使用此漏洞来瞄准和入侵医疗保健、信息技术、高等教育和关键制造业领域的实体。12 月 2 日，联邦调查局 (FBI) 和网络安全和基础设施安全局 (CISA) 向公众发布了一项有关国家层面威胁行为者利用此漏洞的联合咨询警告。在披露时，RiskIQ 观察到有 7,956 个这些系统的实例在 Internet 上处于活动状态。

CVE-2021-42321 Microsoft Exchange

2021 年 10 月 16 日至 17 日在中国成都举行的国际网络安全峰会和黑客竞赛天府杯期间，Exchange 漏洞 CVE-2021-42321 的零日漏洞被披露。10 月 21 日，仅在漏洞被发现三天后，Microsoft 的安全研究人员观察到 Exchange 漏洞被广泛利用。在披露时，RiskIQ 观察到有 61,559 个这些系统的实例在 Internet 上处于活动状态。我们继续观察到漏洞利用活动持续到 2021 年 11 月。

CVE-2022-26134 Confluence

在 Confluence 漏洞 (CVE-2022-26134) 于 6 月 2 日公开披露前四天，一个与中国有关的行为者可能已经掌握了该漏洞的零日漏洞代码，并可能利用它来对付一个位于美国的实体。在披露时，RiskIQ 观察到有 53,621 个 Confluence 系统的实例在 Internet 上易受到攻击。

漏洞正在被大规模获取和利用，而且时间范围越来越短。

切实可行的见解

1. 零日漏洞一经发布就要优先修补，不要等待部署修补程序管理周期。
2. 记录和清点所有企业硬件和软件资产来确定风险，并快速确定何时采取行动来进行修补。

俄罗斯国家层面行为者的战时网络策略威胁着乌克兰及其他地区

今年，俄罗斯国家层面行为者发动了网络行动来辅助俄罗斯入侵乌克兰期间的军事行动，通常使用针对乌克兰境外目标部署的相同策略和技术。全球组织必须采取措施加强网络安全，以抵御与俄罗斯步调一致的威胁行为者造成的数字威胁。

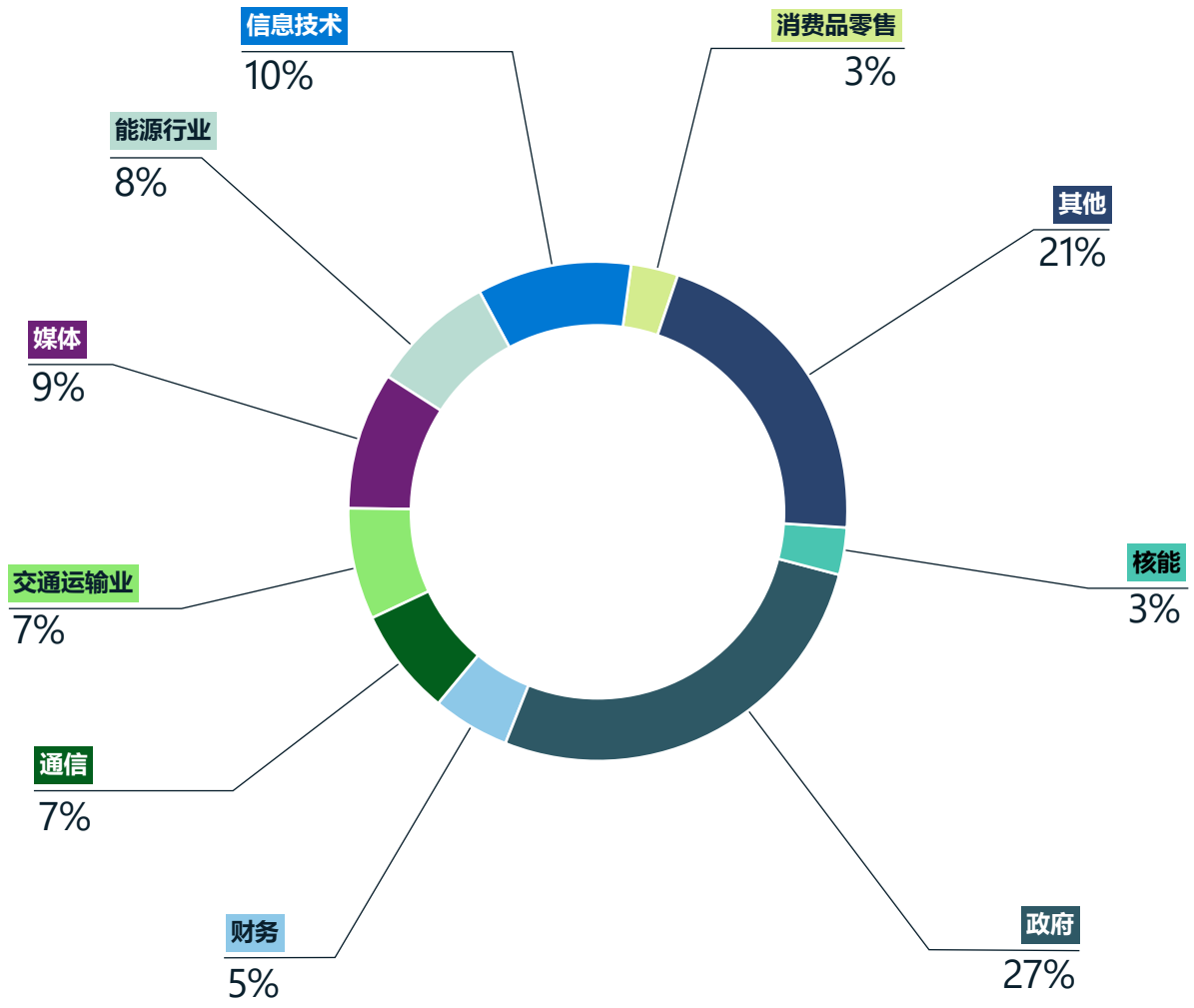
随着军事冲突的持续，当地局势依旧动荡不定，如果俄罗斯国家层面网络行动者依照军事目标增加入侵的频率或强度，乌克兰及其盟国应做好防御准备。在战争的前四个月，Microsoft 观察到与俄罗斯军方相关的威胁行为者对近 50 个不同的乌克兰机构和企业发起了数波破坏性网络攻击，并对许多其他组织发起了以间谍活动为主的入侵。2 月下旬至 6 月期间，除了针对在线服务客户发起的行动，俄罗斯针对已知目标开展的威胁活动有 64% 的攻击目标都是乌克兰的组织。

在每次行动中，俄罗斯威胁行为者采用了许多我们观察到在其入侵乌克兰境内外目标之前就已采用的策略、技术和程序 (TTP)。这些行为者企图破坏数据并使乌克兰政府机构在冲突初期陷入失衡的状态。此后，他们曾试图破坏向乌克兰运送军事和人道主义援助物资的交通运输系统、中断公众获取服务和媒体的通道，并窃取对俄罗斯而言具有长期情报或经济价值的信息。

以交通运输系统为攻击目标威胁到了对竭力在冲突中生存下来的乌克兰公民而言至关重要的一个领域。根据 5 月份由联合国儿童基金会赞助的一项调查，受冲突影响的城市地区受访者最担心交通运输和燃料、供应中断、安全以及获取食物、医疗服务和金融服务受限。[10] 6 月，联合国乌克兰危机协调员表示，乌克兰至少有 1,570 万人急需人道主义援助，而且随着战争的继续，这一数字还会增加。[11]

2 月下旬至 6 月期间，Microsoft 检测到俄罗斯在乌克兰境外对 42 个国家 / 地区的 128 个组织发起了网络入侵活动。美国是俄罗斯的头号目标。向乌克兰运送的大部分国际军事和人道主义援助物资都途径波兰，因此在此期间，波兰也成为其重要目标。此外，在 4 月和 5 月，与俄罗斯政府关联的威胁行为者也针对波罗的海国家 / 地区的组织以及丹麦、挪威、芬兰和瑞典的计算机网络展开行动。

自遭受入侵以来乌克兰受到攻击的主要行业领域



在整个冲突期间，乌克兰联邦、州和地方政府组织一直是俄罗斯国家层面和与国家关联的威胁团体的首要目标。重点攻击交通运输、能源、金融和媒体领域组织凸显了这些网络行动给乌克兰公民所依赖的服务带来的风险。

俄罗斯国家层面行为者的战时网络策略威胁着乌克兰及其他地区

续

我们发现以北约国家 / 地区外交部为攻击目标的类似活动有所增加。

去年，俄罗斯国家层面威胁团体仍有意于入侵乌克兰境内外的关键基础设施。IRIDIUM 部署了 Industroyer2 恶意软件，试图切断乌克兰数百万人的电源，但未能成功。在乌克兰境外，BROMINE 于 2022 年初入侵了使用制造和工业控制系统的组织。

今年，俄罗斯国家层面和与国家关联的行为者使用下面的许多 TTP 对乌克兰、其盟国及其他具有情报价值的目标开展了网络行动：

使用恶意附件或链接进行鱼叉式网络钓鱼

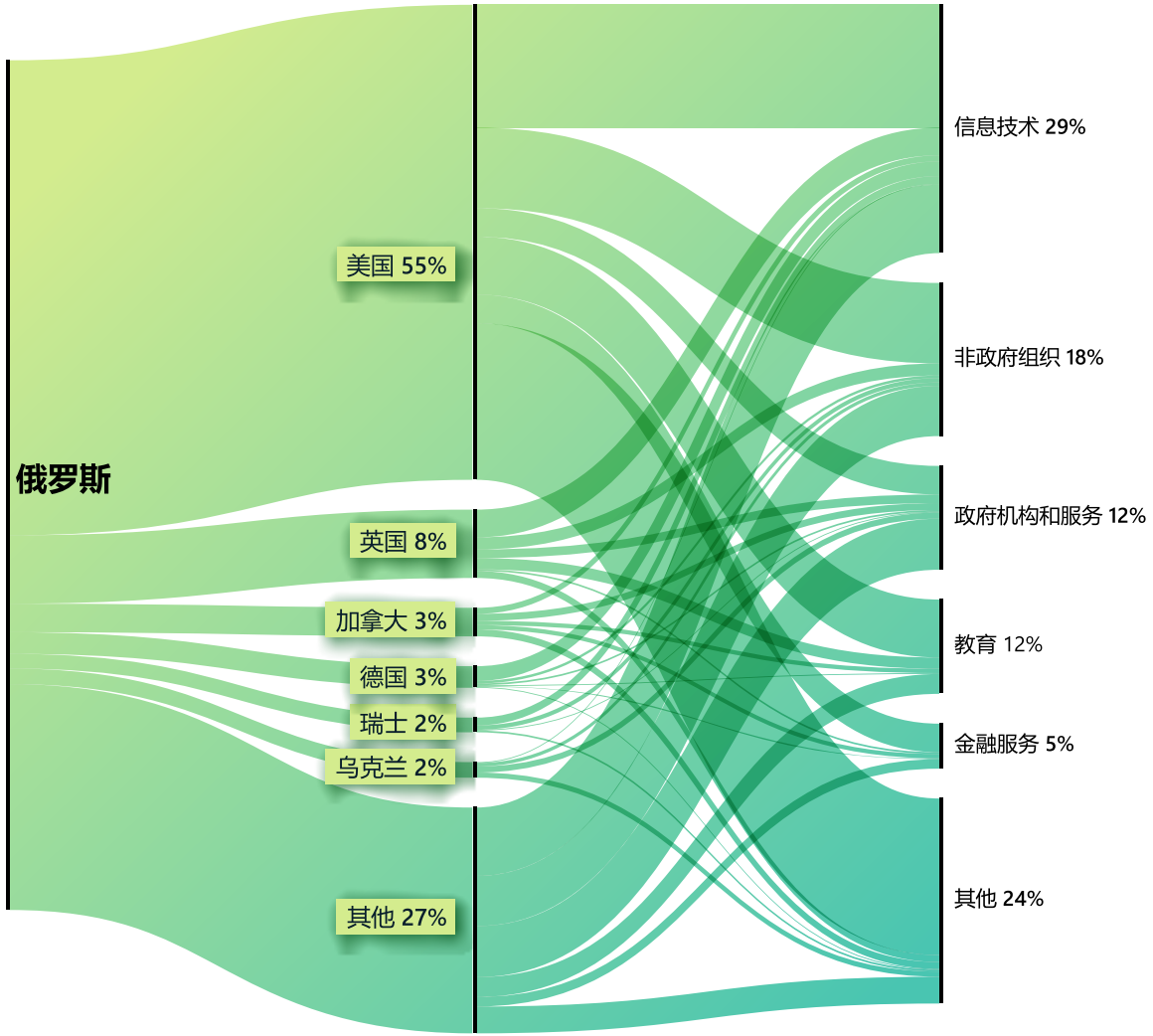
ACTINIUM、NOBELIUM、SRONTIUM、DEV-0257、SEABORGIUM 和 IRIDIUM 等俄罗斯国家层面和与俄罗斯关联的团体都利用网络钓鱼活动来获得对乌克兰境内外组织中所需帐户和网络的初始访问权限。许多活动均利用目标组织或同一行业内被盗用的帐户或虚假帐户以及引人注目的主题来引诱受害者。NOBELIUM 使用被盗用的外交账户向全球外交部员工发送伪装成外交通信的网络钓鱼邮件。STRONTIUM 根据美国智囊团公开发布的帐户持有人姓名创建了虚假帐户，并发送网络钓鱼邮件来获取对这些智囊团帐户的访问权限。SEABORGIUM 使用与报道乌克兰冲突相关的诱饵进行网络钓鱼，以获取对北欧国家 / 地区国际事务智囊团帐户的初步访问权限。

利用 IT 服务供应链对下游客户造成影响

2021 年底，俄罗斯国家层面行为者入侵了 IT 服务提供商，并利用此访问权限帮助 DEV-0586 于 1 月开展网站破坏行动和部署 Whispergate 破坏性恶意软件。[12] DEV-0586 还入侵了一家 IT 公司的网络，该公司为乌克兰国防部以及通信和交通运输领域的其他组织构建了资源管理系统，这表明该团体也在探索这些领域的第三方攻击选项。

2021-2022 年期间，在全球范围内，尤其是在美国和西欧，NOBELIUM 以 IT 服务提供商为攻击目标来获取对政府和其他敏感网络的访问权限（请参阅本章前面有关供应链漏洞的讨论）。

俄罗斯：攻击针对的主要国家 / 地区和行业领域



尽管自 2022 年初以来对乌克兰组织的攻击力度增强，但总部位于北美和西欧的企业仍是受俄罗斯行为者主要攻击的在线服务客户。NOBELIUM 针对 IT 领域开展的活动使其成为过去一年中受攻击最多的领域。

俄罗斯国家层面行为者的战时网络策略威胁着乌克兰及其他地区

续

利用面向公众的应用程序获取对网络的初始访问权限

至少自 2021 年末以来，STRONTIUM 一直致力于培养和提升其利用面向公众的服务（如 Microsoft Exchange Server）窃取信息的能力。STRONTIUM 利用未修补的 Exchange Server 访问乌克兰政府账户以及美国、黎巴嫩、秘鲁和罗马尼亚的军事和国防工业相关组织及总部位于亚美尼亚、波斯尼亚、科索沃和马来西亚的其他政府机构。DEV-0586 也与俄罗斯军方有关联，它利用 Confluence 服务器漏洞获取了对乌克兰和其他东欧国家 / 地区政府和 IT 领域组织的初始访问权限。

在战争及和平时期，俄罗斯国家层面和与国家关联的威胁行为者使用许多相同的 TTP 来入侵其感兴趣的组织。

使用管理帐户和协议及原生实用程序进行网络发现和横向移动

Microsoft 观察到，在获取对网络的初始访问权限后，俄罗斯国家层面行为者利用用于执行基本维护任务的合法帐户和软件实用程序尽可能长时间地逃避检测。他们依靠具有管理功能及有效管理协议、工具和方法的被盗用身份在网络中横向移动，而不会立即引起自动监视器和网络防御者的注意。

建立基本网络安全机制并采用终结点检测和响应工具有助于减轻这些类型的行动在和平及战争时期带来的负面影响。

持续冲突具有不可预测性，这要求全球组织采取措施加强网络安全，抵御俄罗斯国家层面和与俄罗斯关联的威胁行为者造成的数字威胁。

切实可行的见解

1. 通过实施 MFA 身份保护工具并强制执行最小特权访问来保护最敏感的特权帐户和系统，从而保护用户身份，最大限度地减少凭据盗窃和帐户滥用。
2. 应用更新以确保所有系统尽快获得最高级别的保护并保持最新状态。
3. 在整个组织中部署反恶意软件、终结点检测和身份保护解决方案。通过结合使用深度防御安全解决方案并配备训练有素的得力员工，你的组织能够识别、检测和预防对业务有影响的入侵。
4. 通过备份关键系统并启用日志记录，在检测到或收到环境威胁通知时启用调查和恢复。强烈建议制定事件响应计划。

更多信息的链接

- 保卫乌克兰：网络战争早期阶段的经验教训 | Microsoft 对这些问题的看法
- 乌克兰混合战争 | Microsoft On the Issues
- 在乌克兰开展的网络威胁活动：分析和资源 | Microsoft 安全响应中心 (MSRC)
- 破坏针对乌克兰的网络攻击 | Microsoft On the Issues
- 针对乌克兰政府的恶意软件攻击 | Microsoft On the Issues
- MagicWeb：NOBELIUM 入侵后以任何人的身份进行身份验证的招术 | Microsoft 威胁情报中心 (MSTIC)、检测和响应团队 (DART)、Microsoft 365 Defender 研究团队

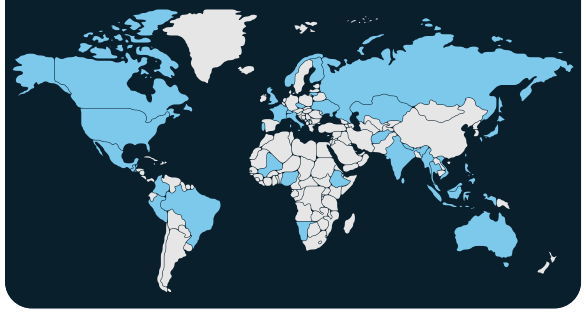
中国扩大全球目标以获得竞争优势

在当今复杂的地缘政治环境中，中国国家和国家附属的威胁行为者开展网络行动的目的通常是为了推进国家的军事、经济和外交关系战略目标，这是中国获得竞争优势目标的一部分。去年，Microsoft 观察到中国针对世界各国的广泛威胁活动。

自 2021 年中期以来，在 2019 冠状病毒病 (COVID-19) 疫情两年来最严重的情况下，中国一直在采取措施确保经济和金融稳定。[13] 中国继续在地缘政治事件上调整自己的立场，例如努力平衡与俄罗斯的“无限”伙伴关系，[14] 并保持其在世界舞台上的地位。[15] 此外，中国在台湾 [16] 和南海问题上反对美国及其盟友的立场继续导致与许多国家的外交关系紧张。[17]

中国国家和国家附属的威胁组织增加了针对全球较小国家的目标，并以东南亚为重点，以在各个方面获得竞争优势。

中国国家和国家附属团体针对的国家

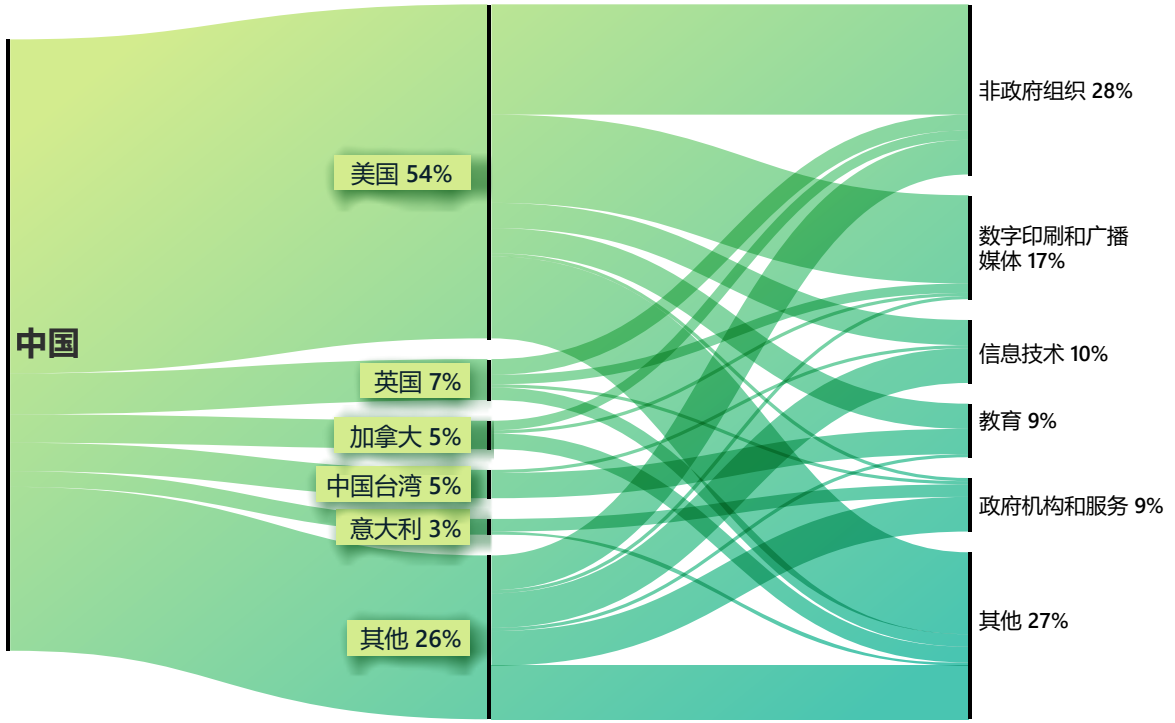


中国还通过之前提出的“一带一路”倡议 (BRI) 继续扩大其在全球的经济影响力，试图恢复与欧盟的全面投资框架，[18] 并与亚太地区 15 个国家谈判一项新的区域贸易协定，即“区域全面经济伙伴关系协定”。[19] 由于观察到的网络行动和目标实体的广度，Microsoft 评估中国将继续利用网络收集作为一种工具，以帮助推进其政治、军事和经济的战略目标。

有针对性的网络行动可能有助于获得经济和军事利益。

Microsoft 观察到中国国家和国家附属的威胁组织普遍将世界各地的小国作为目标，这表明中国可能将网络间谍活动作为其全球经济和军事影响力的一个组成部分。

China: Top targeted countries and industry sectors



智库 / 非政府组织、媒体、IT、政府和教育部门是基于中国的威胁组织最有针对性的部门，可能是为了持续收集情报和侦察。

目标范围包括但不限于非洲、加勒比地区、中东、大洋洲和南亚国家 / 地区，其中对东南亚和太平洋群岛国家 / 地区的攻击尤为频繁。

根据中国的“一带一路”战略，以中国为基地的威胁组织将阿富汗、哈萨克斯坦、毛里求斯、纳米比亚以及特立尼达和多巴哥的实体作为目标。[20]

例如，特立尼达和多巴哥是 2018 年第一个支持中国“一带一路”战略的加勒比国家，中国视其为地区重要合作伙伴。自 2021 年以来，NICKEL 一直针对特立尼达和多巴哥开展持续的网络行动。例如，2022 年 3 月，NICKEL 对政府机构进行了侦察活动，可能是出于情报收集目的。

中国扩大全球目标以获得竞争优势

续

与此同时，Microsoft 观察到中国国家和国家附属的威胁组织将其网络行动集中在东南亚的实体上，并扩展到太平洋岛国，因为中国改变了其军事和经济重点以应对美国在该地区重新产生兴趣的挑战。2022 年 1 月，Microsoft 观察到 RADIUM 针对越南的一家能源公司和一家与能源相关的政府机构，以及一家印度尼西亚政府机构。RADIUM 的活动可能符合中国在南海的战略目标。[21]2 月下旬和 3 月初，GALLIUM 入侵了东南亚地区一个著名政府间组织（IGO）的 100 多个账户。GALLIUM 瞄准该地区 IGO 的时间恰逢美国和地区领导人宣布预定会晤。GALLIUM 参与者的任务可能是在事件发生前监控通信和收集情报。

随着中国扩大在太平洋岛国的影响力，中国威胁组织的活动也随之而来。4 月，中国和所罗门群岛签署了旨在“促进和平与安全”的安全协议。该协议可能允许中国向所罗门群岛部署武装警察和军队。[22]5 月，中国在斐济主办第二次中国 - 太平洋岛国（PICs）外长会，提出推进“全面战略伙伴关系”，促进政治、文化、社会、安全、气候变化等利益，以及共同应对心冠疫情大流行。[23] 大约在 5 月的同一时间，Microsoft 在所罗门群岛政府系统上发现了 GADOLINIUM 的恶意软件。RADIUM 还在巴布亚新几内亚一家电信公司的系统上运行了恶意代码。我们评估这些活动可能是为了收集情报，以支持中国的整体区域战略。

Microsoft 破坏了 NICKEL 的运作，但该威胁组织显示出其持久性。

2021 年 12 月，Microsoft 数字犯罪部门 (DCU) 向美国弗吉尼亚东区地方法院提交了诉状，请求授权没收由 NICKEL 控制的 42 个命令和控制 (C2) 域。自 2019 年 9 月以来，这些 C2 域被用于针对中南美洲、加勒比地区、欧洲和北美的政府、外交实体和非政府组织的行动。[24] 自 2019 年底以来，通过这些行动，NICKEL 实现了对多个实体的长期访问并持续泄露一些受害者的数据。

随着中国继续与更多国家 / 地区建立双边经济关系（通常通过达成与“一带一路”相关的协议），中国的全球影响力将继续增强。我们评估中国国家和国家附属的威胁行为者将在其政府、外交和非政府组织部门追捕目标以获得新的见解，可能是为了追求经济间谍活动或传统的情报收集目标。自 Microsoft 的干扰以来，NICKEL 已将多个政府机构作为目标，可能试图重新获得失去的访问权限。在 2022 年 3 月下旬到 2022 年 5 月期间，NICKEL 再次入侵了全球至少五个政府机构。这表明该组织拥有这些实体的其他入口点或通过新的 C2 域重新获取了访问权限。NICKEL 坚持在全球范围内反复侵入相同的政府机构，表明这项任务在高层的重要性。

中国在外交政策上的立场更加自信。我们评估网络经济间谍活动和情报收集可能会继续下去。

切实可行的见解

1. 加强网络防御，主动缓解网络威胁。中国威胁行为者的持续存在要求组织及时识别、保护、检测和响应可能的入侵。
2. 威胁行为者滥用计划任务[25] 作为持久性和防御规避的常用方法，确保您的环境采用额外的安全准则来防止这种常用技术。[26]
3. 我们继续观察使用 web shell 作为目标网络的初始向量。[27] 组织应该加强他们的系统以抵御网络外壳攻击，这些攻击可以为攻击者提供运行远程命令的访问权限。[28]

更多信息的链接

- NICKEL 瞄准拉丁美洲和欧洲的政府组织 | Microsoft 微软威胁情报中心（MSTIC），Microsoft 数字安全部门（DSU）
- 保护人们免受最近的网络攻击之害 | Microsoft On the Issues

伊朗在权力交接后行事愈发激进

Microsoft 观察到伊朗国家团体和联盟行动者增加了针对以色列的网络攻击的速度和范围，将勒索软件攻击范围从区域对手扩展到美国和欧盟的受害者，并将备受瞩目的美国关键基础设施作为目标，至少为潜在的破坏性网络攻击做好准备。

在伊朗总统权力交接之后，伊朗国家层面行为者的网络攻击愈演愈烈。2021 年夏天，强硬派总统易卜拉欣·莱希 (Ibrahim Raisi) 取代了温和派总统哈桑·鲁哈尼 (Hassan Rouhani)。与最高领袖门生、伊斯兰革命卫队 (IRGC) 的亲密盟友莱希形成鲜明对比的是，前总统鲁哈尼热衷于外交，经常与最高领袖和 IRGC 高级领导人发生矛盾。[29] 莱希政府的鹰派观点似乎提高了伊朗行为者对以色列和西方采取更大胆行动的意愿，尤其是针对美国，尽管美国恢复了与伊朗的外交接触以重启核协议。

伊朗对以色列网络攻击的速度和范围都在增加

在莱希完成其外交政策团队组建的几周内，[30] 伊朗国家层面行为者以比去年更快的速度恢复了对以色列的破坏性网络攻击。从 9 月开始，这些勒索软件和“入侵并泄露”攻击每隔几周就会进行一次，涉及至少三个与伊朗有关联的行为者，这表明这些攻击可能是针对以色列的全国性报复行动的一部分。至少在一个案例中，Microsoft 观察到，2021 年底针对以色列一家组织的勒索软件攻击意在掩盖潜在的数据删除攻击。Microsoft 恶意软件分析确定，传递给受害者的勒索软件被编程为在加密后执行 Wiper 恶意软件。

到 2022 年，伊朗的网络攻击在目标选择和攻击形式上都有所升级。2 月，DEV-0198 试图对以色列的关键基础设施进行破坏性攻击。Microsoft 还观察到，一个与伊朗有关联的行为者很可能为今年 6 月在以色列触发紧急火箭警报器的复杂网络攻击负责，该攻击很可能采用了可调整 Audio over IP 网络的软件。

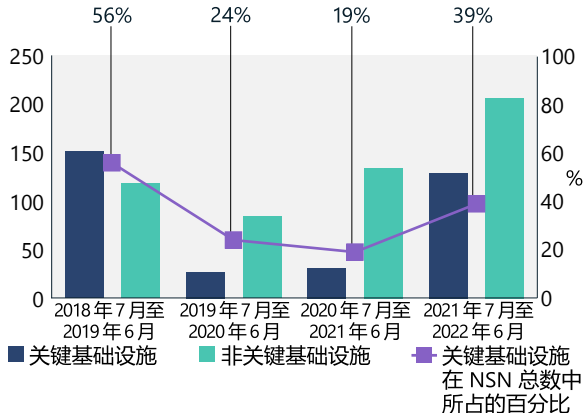
伊朗对美国和以色列关键基础设施的威胁全年不断增加

Microsoft 评估认为，伊朗国家层面行为者隶属于 IRGC（PHOSPHORUS 和 DEV-0198），在 2021 年末到 2022 年中期间以美国和以色列的关键基础设施作为攻击目标。IRGC 高级官员曾指责美国和以色列扰乱了伊朗的一些领域，而伊朗进行此攻击的目的可能是为德黑兰提供针对这些领域的报复方案。[31] 我们估计，这一活动与 2021 年 10 月下旬伊朗被动防御组织负责人 IRGC 将军 Gholamreza Jalali 的声明有关，他在声明中回应了政权中其他有影响力人物针对美国和以色列对伊朗的港口、铁路和加油站进行的网络攻击的指责。[32] Jalali 在一个有导弹击中“美国”字样的讲台上进行周五祷告时，在事先准备好的讲话中第二次提出了这一指控，暗示他的前辈也持同样的观点。[33]

PHOSPHORUS 于 2021 年 10 月开始对美国组织进行广泛扫描，查找未修补的 Fortinet 和 ProxyShell 漏洞。一旦遭到入侵，这些未修补的系统就会被用来执行勒索软件攻击，在某些情况下，还会攻击美国和其他西方国家的关键基础设施。这些标志着在中东以外地区发生的伊朗国家附属勒索软件攻击的首批确认事件。Microsoft 发现，继 10 月底针对伊朗加油站发起网络攻击之后，伊朗针对美国公司的勒索软件攻击激增，表明可能存在相关性。

与此同时，PHOSPHORUS 开始直接攻击美国重要的基础设施公司（通常通过鱼叉式网络钓鱼），包括主要海港和入境机场、运输系统、公用事业公司以及石油和天然气公司。这种攻击通常通过鱼叉式网络钓鱼进行，持续到了 2022 年中期。这些目标与德黑兰指责美国和以色列在伊朗发动攻击的领域直接一致，并可能为伊朗提供报复方案。对接近相同的目标发起攻击有可能会阻止未来的此类攻击，同时通过暗示攻击的原因而不承认罪行来避免事态升级。

伊朗基础设施攻击的再次兴起



伊朗对关键基础结构的攻击增加到 2018 年底至 2019 年初以来的最高水平。我们使用美国《第 21 号总统政策指令》(PPD-21) 来确定一家公司是否符合关键基础结构的标准。(2021 年 7 月 - 2022 年 6 月)。

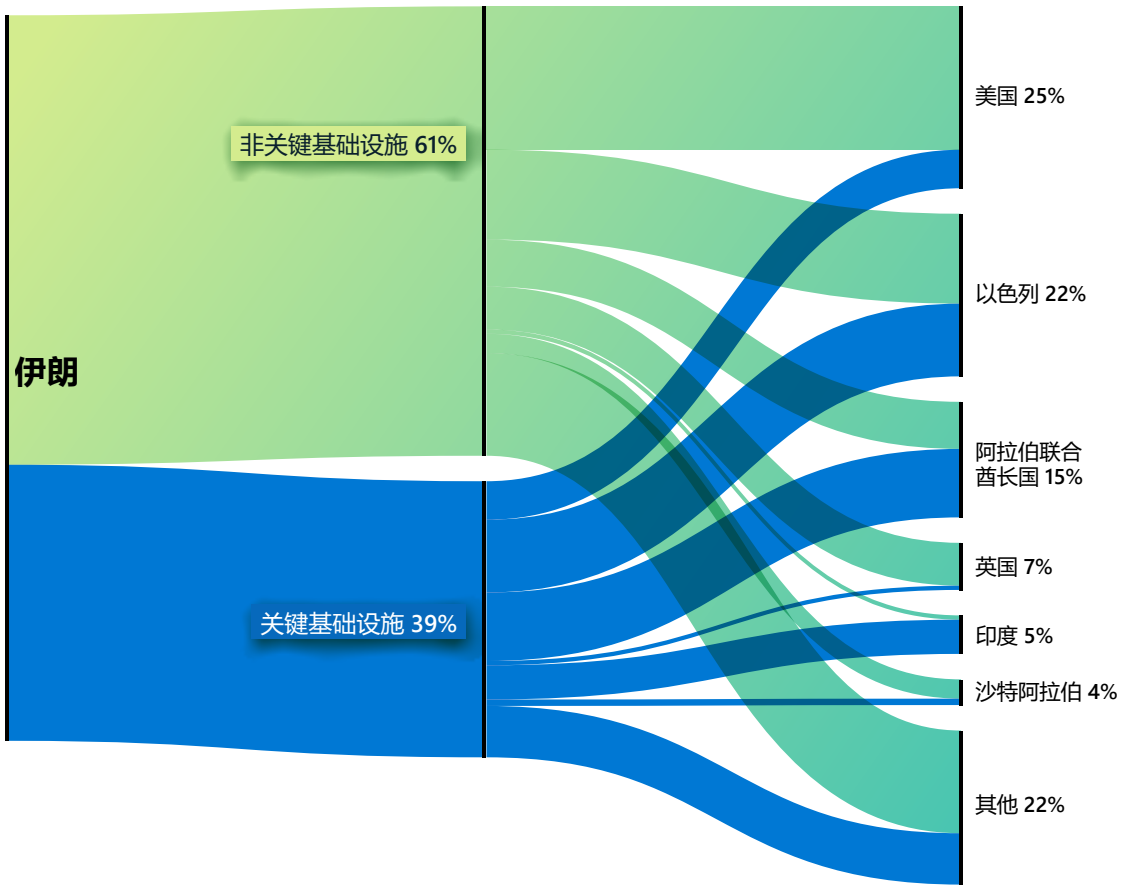
伊朗在权力交接后行事愈发激进

续

在以色列，DEV-0198 以以色列的铁路、物流公司、物流公司的软件提供商以及燃料公司为攻击目标，重点目标为加油站。2022 年初，该团体对以色列一家大型物流公司的网络进行了破坏性攻击，迫使该公司关闭了其计算机和部分业务以遏制攻击。在另一起案件中，我们观察到该团体试图通过被盗或重复使用的凭据访问以色列一家主要运输提供商的网络。与此同时，另一个伊朗行为者 DEV-0343 在 2021 年初入侵了以色列运输和港口相关实体的帐户，该团体针对国防、海上运输和卫星图像公司的攻击表明与 IRGC 存在关联。

伊朗的威胁团体可能仍会对美国和以色列的运输和能源公司构成威胁，尤其是在重启伊朗核协议的外交努力减弱，华盛顿、特拉维夫和德黑兰寻求其他胁迫手段以迫使对方让步的情况下。

按国家 / 地区划分的伊朗关键基础设施攻击活动



伊朗对关键基础设施的攻击主要针对以色列、阿联酋和美国的组织。

未来一年，伊朗行为者可能仍然会对美国和以色列的运输和能源公司构成威胁。

伊朗团体扩大了勒索软件攻击的范围，不仅继续针对区域敌对者，还将目标对准了美国和以色列的关键基础设施。

切实可行的见解

1. 通过启用无密码解决方案（如 MFA）并强制将其用于所有远程连接，减少任何可能遭到泄露的凭据，从而改善组织的整体网络卫生状况。
2. 评估所有入站电子邮件流量的真实性，以确保发件人地址是合法的。
3. 尽早并经常修补漏洞。[34]
4. 评估和审核与服务提供商的每个合作伙伴关系，以最大限度地减少组织与上游提供商之间的任何不必要的权限。Microsoft 建议立即删除任何看似陌生或尚未审核的合作伙伴关系的访问权限。[35]

更多信息的链接

- 伊针对 IT 领域的攻击呈上升趋势 | Microsoft 威胁情报中心 (MSTIC)、Microsoft 数字安全部门 (DSU)
- 与伊朗相关的 DEV-0343 针对国防、GIS 和海事部门发起攻击 | Microsoft 威胁情报中心 (MSTIC)、Microsoft 数字安全部门 (DSU)

总部位于黎巴嫩、与伊朗有关的团体对以色列发起攻击

Microsoft 密切监视网络威胁活动，无论平台、目标受害者或地理区域如何。我们在全球范围内保持可见性并积极搜寻威胁，为客户开发更好的检测方法。

尽管来自俄罗斯、中国、伊朗和朝鲜的威胁占我们观察到的国家层面行为体活动的大部分，但我们也跟踪和交流来自北约成员国和民主国家的威胁。去年，我们重点研究了一个位于土耳其的行为者 (SILICON) 和一个位于越南的行为者 (BISMUTH) 的攻击活动。今年，我们将深入研究之前公开披露的一个黎巴嫩团体的细节。[36]

Microsoft 发现了一个以前没有记录的黎巴嫩团体，且比较确信该团体与隶属于伊朗情报与国家安全部 (MOIS) 的行为者合作开展行动。德黑兰的这种合作或指示将与自 2020 年底以来伊朗政府利用第三方开展网络行动的披露相一致，这可能会增强伊朗貌似合理的推诿。

在观察到的活动中，POLONIUM 在 2022 年 2 月至 5 月期间，在 Microsoft 中断并公开披露其活动之前，攻击或入侵了位于以色列的 20 多个组织和一个在黎巴嫩开展业务的政府间组织。近一半的以色列组织是以色列国防工业的一部分，或与以色列国防公司有联系，这表明该团体在收集关于以色列的情报和 / 或直接打击以色列方面与伊朗有着类似的利益。[37]

之所以认为 POLONIUM 与 MOIS 团体存在关联，是因为我们观察到了二者的受害者重叠以及所用工具和技术的共同性。

- 受害者重叠：一个与伊朗 MOIS 有关联的伊朗国家层面团体（Microsoft 跟踪为 MERCURY）以前曾入侵多名 POLONIUM 的受害者，这表明二者的任务要求趋于一致，或者各团体之间可能存在受害者“交接”。
- 常用工具和技术：与 POLONIUM 类似，MSTIC 观察到 DEV-0588（也称为 CopyKittens）通常使用 AirVPN 开展行动，DEV-0133（也称为 Lyceum[38]）使用 OneDrive 进行 C2 和渗透。与伊朗国家层面行为者类似，POLONIUM 使用云服务提供商入侵以色列航空公司和律师事务所。[39]

POLONIUM 使用用于 C2 和数据泄露的云服务（特别是 OneDrive 和 DropBox）部署了一系列自定义植入程序。POLONIUM 经常为目标创建独特的 OneDrive 应用程序，可能会逃避检测。

截至 2022 年 6 月，Microsoft 暂停了 20 多个 POLONIUM 创建的 OneDrive 应用程序，通知了受影响的组织，并部署了一系列安全情报更新来隔离 POLONIUM 开发的工具。

Microsoft 成功检测并禁用了 POLONIUM 滥用 OneDrive 作为 C2 的行为。

切实可行的见解

1. 更新防病毒工具[40]并确保已开启云保护[41]以检测相关指标。
2. 对于具有服务提供商关系的客户，请确保评估和审核所有合作伙伴关系，以最大限度地减少组织与上游提供商之间的不必要的权限。[4] 2 立即删除任何看似陌生或尚未审核的合作伙伴关系的访问权限。

更多信息的链接

- 揭露以以色列组织为目标的 POLONIUM 活动和基础结构攻击 | Microsoft 威胁情报中心 (MSTIC)、Microsoft 数字安全部门 (DSU)
- MERCURY 利用未修补系统中的 Log4j 2 漏洞攻击以色列组织 | Microsoft 威胁情报中心 (MSTIC)、Microsoft 365 Defender 研究团队、Microsoft Defender 威胁智能

朝鲜利用网络功能实现政权的三个主要目标

朝鲜过去一年的网络优先事项反映了该政府声明的全球优先事项。金正恩在几次重要讲话中强调了建设国防能力、支持国家艰难的经济和确保国内稳定这三个优先事项。[43] 朝鲜国家层面行为者采取的行动清楚地表明，网络正在被用来实现这三个目标。

朝鲜国家行为者使用各种策略试图渗透到全球的航空航天公司。

朝鲜国家威胁团体，主要是 CERIUM 和 ZINC，使用各种策略试图渗透全球国防和航空航天公司的网络。2022 年上半年，朝鲜开始了有史以来最激进的导弹试验，它利用网络间谍活动帮助朝鲜研究人员在两方面取得优势：开发本土防御系统，针对其敌对者所取得的进步制定应对对策。

我们观察到 COPERNICIUM 攻击了世界各地与加密货币相关的各种公司，通常都取得了成功，以帮助支持朝鲜艰难的经济。虽然我们无法确认该团体能否在入侵后窃取资金，但我们观察到 COPERNICIUM 通过发送伪装成其他加密货币公司提案的恶意文件感染了数十台机器。

最后，Microsoft 还发现，其跟踪为 DEV-0215 的一个团体通过攻击报道朝鲜问题的新闻机构来致力于维护朝鲜的稳定和对朝鲜的忠诚。这些媒体在朝鲜和脱北者群体中都有消息来源，因此平壤认为这是一种生存威胁。此外，该团体还努力进入讲韩语的基督教团体网络，这些团体往往直言不讳地反对朝鲜并积极与脱北者合作。

针对国防和航空航天公司发起攻击

以 CERIUM 和 ZINC 为首的朝鲜国家层面行为者投入了大量精力来制定旨在渗透国防和航空航天公司的策略。CERIUM 通过下载客户端和寻找弱点来反复探测韩国虚拟专用网络 (VPN)。它还下载了韩国军方和政府客户常用的应用程序，可能意欲寻找漏洞。该团体密切关注时事并编写了新的诱饵文档，这些文档使用备受瞩目的主题作为诱饵，以诱使目标点击他们的恶意软件可执行程序和链接。

ZINC 和 CERIUM 在活动中都使用了社交媒体和社会工程。ZINC 尤其擅长在 LinkedIn 和其他专业社交媒体网站上创建虚假个人资料，其运营商在这些网站上冒充大型国防和航空航天公司的招聘人员。利用这些个人资料，他们通过社交媒体或电子邮件向潜在受害者直接发送链接或恶意文件附件。

除了企业员工之外，CERIUM 还广泛针对韩国军方成员，对韩国军事院校和在学术界工作的军事人员表现出特别的兴趣。

窃取加密货币以平衡损失

自 2016 年联合国制裁实施以来，朝鲜经济持续萎缩，洪水[44] 和干旱[45] 等自然灾害，以及自 2020 年初 COVID-19 疫情开始以来进口边境几乎完全封锁，又加剧了这一状况。[46] 尽管朝鲜在 2022 年初短暂开放了与中国的贸易边界，但很快又再次关闭。[47] 5 月中旬，朝鲜报告了国内首例 COVID-19 病例。[48] 自那以后，朝鲜采取了中国式的“动态清零”大规模封锁战略以对抗病毒，这对朝鲜本就脆弱的经济造成了很大的负面影响。

朝鲜国家团体 COPERNICIUM 试图通过从其可以渗透网络的任何公司窃取资金（通常以加密货币的形式）来弥补部分收入损失。我们发现，数十台属于美国、加拿大、欧洲和整个亚洲的加密货币相关公司的机器遭到入侵。COPERNICIUM 甚至还入侵了朝鲜最强大的盟友中国大陆和香港特别行政区的加密货币相关公司的机器。该团体在早期侦察和接近目标方面严重依赖社交媒体。行为者会建立个人资料，伪装成加密货币相关业务的开发人员或高级管理者。然后，他们将与业内人士建立关系，一旦建立融洽关系，就会向后者发送恶意链接或文件。

朝鲜利用网络功能实现政权的三个主要目标

续

一个与 PLUTONIUM 相关的团体开发并部署勒索软件

Microsoft 跟踪发现，一个来自朝鲜的行为者团体 DEV-0530 于 2021 年 6 月开始开发和使用勒索软件进行攻击。这个自称为 H0lyGh0st 的团体在其活动中使用了同名的勒索软件有效负载，早在 2021 年 9 月就成功入侵了多个国家 / 地区的小型企业。

Microsoft 观察到，DEV-0530 与另一个被跟踪为 PLUTONIUM（也称为 DarkSeoul 或 Andariel）的朝鲜团体存在关联。虽然在活动中使用 H0lyGh0st 勒索软件是 DEV-0530 独有的，但 MSTIC 观察到了两个团体之间的通信，以及 DEV-0530 使用由 PLUTONIUM 专门创建的工具。

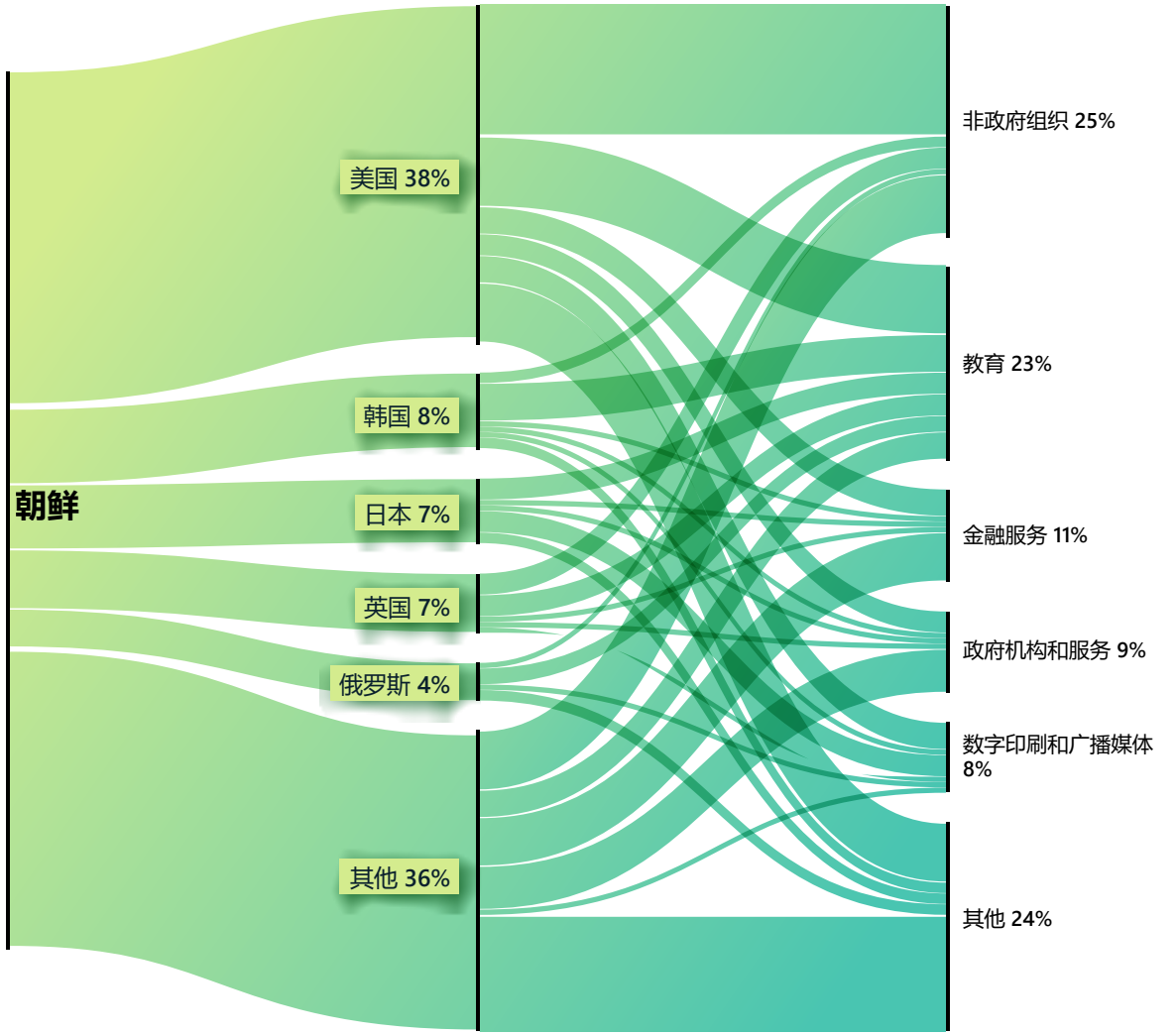
目前尚不确定 DEV-0530 活动是否由政府赞助。尽管政府下令进行勒索软件攻击的原因可能与其赞助从加密货币公司盗窃资金的原因相同，但 DEV-0530 背后的行为者也有可能独立行动以为自己谋利。如果是朝鲜黑客独立行动，那就可以解释为什么与政府赞助的针对加密货币公司的盗窃行动相比，这种活动并不普遍。

针对朝鲜新闻媒体、脱北者、宗教团体和援助组织发起攻击

去年，朝鲜最高领导人金正恩公开表示，与导弹和核武器相比，他更关注内部安全和忠诚。至少有两个朝鲜国家层面团体将注意力集中在政府认为是国内威胁的方面，这反映出朝鲜对国内问题的关注。

第一个是 Microsoft 跟踪为 DEV-0215 的团体，其目标是密切关注朝鲜新闻的媒体组织。造成这一目标的一个可能原因是，这些媒体机构通过各种方式与外界交流，从脱北者、与朝鲜密切合作的中国公民，甚至一些居住在国内的朝鲜公民那里获取信息。朝鲜政府将这些团体视为生存威胁，尤其是朝鲜境内被视为叛徒和间谍的公民。DEV-0215 可能试图确定这些媒体的消息来源，以便他们可以消除潜在的信息泄露。

朝鲜：攻击针对的主要国家 / 地区和行业领域



朝鲜将美国、韩国和日本视为其主要敌人。虽然俄罗斯是长期盟友，但朝鲜威胁行为者以俄罗斯智囊团、学者和外交官员为目标，以获取有关俄罗斯对全球事务看法的情报。

朝鲜利用网络功能实现政权的三个主要目标

续

Microsoft 还发现了 DEV-0215 针对说韩语的基督教社区发起攻击的证据。韩国福音基督教教会往往对支持与朝鲜接触的朝鲜和韩国政府都持批评态度。这些教会可能会向脱北者伸出援手，有些还会参与涉及朝鲜的人道主义工作。朝鲜将他们视为威胁，因为虽然来自朝鲜的脱北者在疫情期间几乎绝迹，[49] 但这些基督教团体通常在帮助脱北者逃离方面发挥关键作用。DEV-0215 为讲韩语的人制作了有关基督教会议的假文件，以此作为诱饵来针对此团体发起攻击并发现叛逃的协助组织者。

最后，国家层面团体 OSMIUM 在这一年中对国际援助组织表现出了稳定的兴趣，包括过去援助过朝鲜的组织。虽然朝鲜通常拒绝来自国外的帮助，尤其是自 COVID-19 爆发以来，[50] 但目前朝鲜可能正考虑接受帮助，只不过对允许外国援助人员进入其国内的安全后果持谨慎态度。朝鲜可能正在渗透全球援助组织网络，以确定是否允许此类援助进入其本国。

切实可行的见解

1. 朝鲜国家层面行为者技术娴熟、残酷无情且极富创造力，但组织可以抵御他们。
2. 大多数成功的攻击都可以通过基本的网络卫生来阻止，比如双重身份验证或在虚拟环境中不打开来自未知个人的附件。

更多信息的链接

- 朝鲜威胁行为者利用 H0lyGh0st 勒索软件攻击中小型企业 | Microsoft 威胁情报中心 (MSTIC)、Microsoft 数字安全部门 (DSU)

朝鲜专家长期以来一直在争论，朝鲜政府的公开声明是认真的，还是只是装腔作势。网络攻击与朝鲜宣布的优先事项保持一致，证实了专家们认为朝鲜在公开谈论其目标时言行一致的观点。

网络雇佣兵威胁网络空间的稳定性

越来越多的私营公司开发和销售工具、技术和服务，使他们的客户（通常是政府）能够侵入网络、计算机、电话和联网设备。作为国家层面行为者的资产，这些实体经常危及持不同政见者、人权维护者、记者、民间社会倡导者和其他私人公民。我们称他们为网络雇佣兵或私营部门的攻击性行为者。

一个私营企业制造和销售网络武器的世界对消费者、各种规模的企业和政府来说都更为危险。这些攻击性工具的使用方式可能不符合善治和民主的规范和价值观。Microsoft 认为，保护人权是一项基本义务，我们通过在全球范围内减少“监控即服务”来认真对待这一义务。

Microsoft 发现，民主和专制政权的某些国家层面行为者外包了“监控即服务”技术的开发或使用。这就是他们避免责任和监督，并获得在本土难以培养的能力的方式。

这些网络武器为民族国家提供了他们无法单独培养的监控能力。

网络雇佣兵开展行动的市场是不透明的。尽管如此，我们继续观察到这些团体使用零日攻击甚至零点击攻击，这些攻击根本不需要受害者交互，从而实现了监控即服务。

Microsoft 最近宣布了一个欧洲私营部门攻击性行为者，我们称之为 KNOTWED，这是一家总部位于奥地利的 PSOA，名为 DSIRF。多个新闻报道将该公司与开发和尝试销售名为 Subzero 的恶意软件工具集联系起来。[51] 受害者包括奥地利、英国和巴拿马等国家的律师事务所、银行和战略咨询公司。[52]

由于这些攻击性监控功能不再是国防和情报机构创造的高度机密功能，而是现在提供给公司和个人的商业产品，因此任何网络武器的监管制度都不应仅限于出口管制。这些网络武器的影响可能是毁灭性的。

当网络雇佣兵利用产品或服务中的漏洞时，会给整个计算生态系统带来风险。当漏洞被公开确定时，公司就会在时间紧迫的情况下，在广泛的攻击发生之前发布保护措施（请参阅我们之前关于漏洞利用的讨论）。对于软件供应商（他们必须方便地开发修补程序）和产品消费者（他们必须立即实施修补程序）来说，这是一个危险且艰难的循环。

作为网络安全技术协议[53]（一个集合了 150 多家科技公司的领先联盟）的创始成员，Microsoft 承诺不参与网络攻击行动。我们信守这一承诺，履行我们在这一领域的人权责任。我们着手解决技术中断和法律挑战，以突出网络雇佣兵提供的服务造成的负面影响，并将在发现滥用情况时继续保护我们的客户。

网络雇佣兵创建并提供“监控即服务”功能，这些功能在技术上很复杂且广泛可用，包括高级恶意软件和一系列技术。

针对政府的切实可行的见解

1. 实施监控即服务的透明度和监督要求，尤其是在采购方面，包括禁止这些攻击性行为者，就像美国商务部将一些公司列入实体清单所做的一样。
2. 为该部门的前雇员制定离职限制措施。
3. 履行“了解客户”的义务，并鼓励公司履行其人权承诺。

更多信息的链接

- KNOTWEED 解读：利用零日漏洞的欧洲私营部门攻击性行为者 | Microsoft 威胁情报中心 (MSTIC)、Microsoft 安全响应中心 (MSRC)、RiskIQ（Microsoft Defender 威胁智能）
- 继续打击私营部门的网络武器 | Microsoft On the Issues

实施网络安全规范，确保网络空间和平与安全

我们迫切需要一个一致的全球性框架，优先考虑人权，保护人们免受网上鲁莽行为的伤害。这一点在正在进行的乌克兰战争中表现得最为明显。除了全球战略努力之外，各政府还可以立即采取行动，以产生即时的积极影响。

五年前，Microsoft 呼吁签署《数字日内瓦公约》，以推进各部门捍卫网络和平与安全的责任和义务。网络空间正在成为国家 / 地区间冲突和竞争的一个独特而动荡的领域，攻击变得越来越常见，甚至在和平时期也是如此。

今天，很明显这样一个框架仍然是有必要的 - 俄罗斯入侵乌克兰时对乌克兰的网络攻击就是明证。这场战争创造了一个新的前线，这与我们以前所知的任何前线都大不相同。

要实现网络空间的稳定性，就需要加强和重新构想全球治理机构，使其能够符合我们的目标。网络空间与其他领域有着根本性的不同 - 它是无边界的、合成的，主要由私营企业维护。这意味着技术行业需要对产品和服务的安全以及更广泛的数字生态系统承担更大的责任。虽然各方面都取得了显著进展，但挑战也急剧增加。

我们必须加倍付出集体努力，维护网络空间的安全。我们不能将我们在网上期望的权利和自由视为理所当然。在我们努力应对挑战的同时，恶意行为者正在计划如何以及在哪里通过 AI 利用虚假信息进行下一次攻击，并寻找方法来破坏刚刚起步的元宇宙。人权维护者、技术行业和尊重人权的政府必须共同努力，实现建立安全可靠的网络世界的坚定愿景。未来的路还很漫长，但政府现在可以做一些事情来立即改善网络安全生态系统：

- 在归因中引用规范、法律和后果。过去五年的一个重大进步是政府对网络攻击归因的速度和协调。这些声明不仅需要对网络攻击进行点名批评，还需要强调违反了哪些国际法律或规范，将造成何种后果，以帮助加强对国际期望的认识。
- 澄清国际法在网上的适用情况。尽管各政府都同意国际法在网上适用，但人们仍对其在具体情况下如何适用存在疑问。这在俄罗斯入侵乌克兰后尤为重要。各政府可以通过说明他们如何理解自己在国际法下的义务，在树立期望、避免误解和建立信任方面大有作为。
- 咨询其他利益相关者。随着国际论坛继续寻找促进强有力的多方利益相关者包容性的理想途径，各政府可以通过与多方利益相关者社区（尤其是技术行业）进行咨询来支持知情对话，确保具有不可或缺专业知识的人能够推进对话。
- 成立一个常设机构，支持网络空间中负责任的国家 / 地区行为。国际外交论坛在网络上推进负责任的国家 / 地区行为的工作从未像现在这样重要。显然，有必要建立一个联合国常设机制，将网络空间作为一个冲突领域进行处理。
- 针对不断变化的威胁定义新规范。网络空间威胁伴随着技术创新不断演变。虽然国际规范应该是技术中立的，但需要根据威胁格局的变化和我们使用技术的方式更新和削弱这些规范。即使在今天，我们仍然看到现有国际框架中的漏洞被滥用。各国 / 地区应承诺明确保护当前未受保护的支撑数字生态系统的核心流程，如软件更新流程。此外，某些特定领域也应得到额外的保护。例如，正如我们在疫情中了解到的那样，保护医疗保健的规范至关重要。

国家层面行为者和攻击的数量和复杂性都在增加，造成了一种无法维持的局面。

立即采取行动是必要的 - 政府现在可以采取一些措施来立即改善网络安全生态系统，包括实施商定的网络空间国家行为准则和规则，并与更广泛的多方利益相关者群体合作，弥补新出现的差距。

必须重新构想多边机构，以应对国家层面网络攻击的紧迫挑战。

更多信息的链接

- 复盘时刻：强有力的全球网络安全应对措施的必要性 | Microsoft On the Issues
- 针对医疗保健的网络攻击必须停止 | Microsoft On the Issues
- 联合国网络外交的下一篇章即将开启 | Microsoft On the Issues

尾注

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. 本章中关键基础结构的定义参见《第 21 号总统政策指令》(PPD-21)“关键基础结构安全和复原能力”(2013 年 2 月)。
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

尾注（续）

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. 特别是针对 ProxyShell 漏洞（CVE-2021-26855、CVE-2021-26857、CVE-2021-26858 和 CVE-2021-27065、CVE-2021-34473）修补 Exchange 服务器。此外，请务必修补 Fortinet FortiOS SSL VPN 设备的漏洞。
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：“在令人毛骨悚然的间谍软件之谜中，这条线索通过 Wirecard 通往克里姆林宫”，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：“我们揭开了来自奥地利的国家木马‘Subzero’的面纱”，Europe-cities（2021）https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/；Andre Meister：“我们揭开了来自奥地利的国家木马‘Subzero’的面纱”，Netzpolitik.org (2022)https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich。
52. 正如我们的技术博客所指出的，在一个国家 / 地区确定目标并不一定意味着 DSIRF 客户居住在同一个国家 / 地区，因为国际攻击是很常见的。
53. 主页 | 网络安全技术协议 (cybertechaccord.org)

设备与基础结构

随着数字化转型的加速，数字基础结构的安全比以往任何时候都更加重要。

设备与基础结构概述 57

引言 58

政府纷纷采取行动提升关键基础设施安全性和复原能力 59

IoT 和 OT 设备暴露：趋势和攻击 62

供应链和固件黑客攻击 65

聚焦固件漏洞 66

基于侦察的 OT 攻击 68

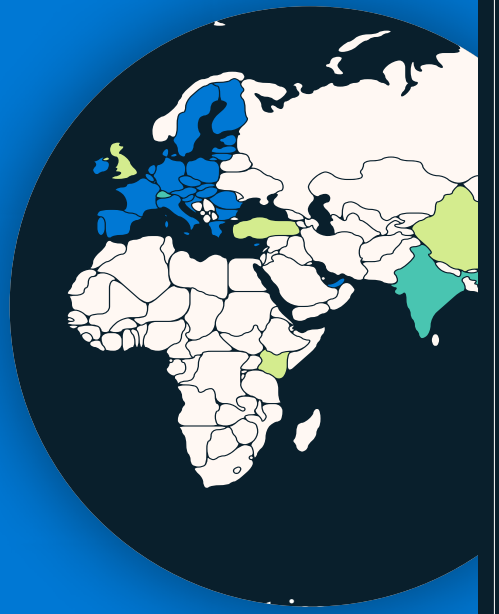
设备与基础结构

概述

这场疫情的原因，再加上各类面向 Internet 的设备作为加速数字化转型的组成部分被迅速采用，大大增加了数字世界的攻击面。

网络犯罪分子和民族国家迅速乘机而入。虽然近年来 IT 硬件和软件的安全性得到了加强，但物联网 (IoT) 和运营技术 (OT) 设备的安全性却没有跟上。威胁行为者正在利用这些设备在网络上建立访问并实现横向移动，在供应链中建立立足点，或破坏目标组织的 OT 运营。

世界各地政府正在通过提高 IoT 和 OT 安全性来保护关键基础设施。

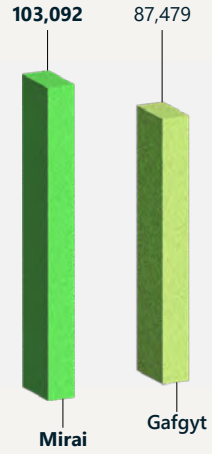


详情请参见第 59 页

安全政策需要在全球范围内保持一致并可互操作以确保广泛采用。

详情请参见第 59 页

恶意软件即服务已开始针对基础设施和公用事业以及企业网络中暴露的 IoT 和 OT 采取大规模行动。



详情请参见第 63 页

针对远程管理设备的攻击呈上升趋势。2022 年 5 月，我们观察到发起的攻击超过 1 亿次，在过去的一年中增加了五倍。

详情请参见第 62 页

攻击者越来越多地利用 IoT 设备固件中的漏洞来渗透到公司网络并发起毁灭性攻击。

详情请参见第 65 页

分析的固件映像有 32% 至少包含 10 个已知的严重漏洞。

详情请参见第 66 页

引言

加快数字化转型增加了关键基础设施和网络物理系统面临的网络安全风险。

在过去几年中，数字世界发生了前所未有的变化。组织正在逐步开始利用智能云和智能边缘中计算功能方面的进步。在疫情的影响下，实体不得不实现数字化以谋求生存，加之全球各个行业都在争相采用面向 Internet 的设备，数字世界的攻击面呈指数级增长。

迁移速度过快，安全社区已无法跟上其步伐。在过去的一年中，我们观察到威胁行为者正在利用组织各部门的设备，从传统的 IT 设备到运营技术 (OT) 控制器乃至简单的物联网 (IoT) 传感器。尽管近年来 IT 设备的安全性得到了加强，但 IoT 和 OT 设备的安全性却没有跟上。威胁行为者正在利用这些设备在网络上建立访问并实现横向移动或中断组织的 OT 运营。我们发现他们对电网进行攻击、通过勒索软件攻击中断 OT 运营、利用 IoT 路由器提高攻击持久性并针对固件漏洞发起攻击。

虽然 IoT 和 OT 漏洞普遍存在对于所有组织来说都是一个挑战，但关键基础设施面临的风险也在增加，因为威胁行为者已了解到禁用关键服务可发挥强大的作用。2021 年，针对 Colonial Pipeline Company 的勒索软件攻击展示了犯罪分子如何通过中断关键服务来增加支付赎金的可能性。而俄罗斯针对乌克兰的网络攻击则表明，一些国家 / 地区将针对关键基础设施的网络攻击视为实现其军事目标的可接受的破坏行为。

但希望就在眼前。决策者和网络防御者正在采取行动来改善关键基础设施的网络安全，包括他们所依赖的 IoT 和 OT 设备。决策者正在加快制定法律法规来建立公众对关键基础设施和设备网络安全的信任。

Microsoft 正在与世界各国政府合作以借机增强网络安全，欢迎更多人参与其中。但是，我们担心不一致、定制或复杂的要求可能会造成不良影响，包括在某些情况下将稀缺的安全资源转向遵守多个重复的认证要求，从而降低了安全性。

从安全运营的角度来看，网络防御者采用多种方法来改善其组织的 IoT/OT 安全态势。一种方法是对 IoT 和 OT 设备实施持续监控。另一种方法是“左移”，这意味着要求针对 IoT 和 OT 设备采用更好的网络安全实践并实施这种实践。第三种方法是实施跨 IT 和 OT 网络的安全监控解决方案。这种整体方法可推动关键组织流程，带来显著的额外好处，例如“打破 OT 与 IT 之间的孤岛”，进而帮助组织在实现业务目标的同时改善安全状况。

Michal Braverman-Blumenstyk
云和 AI 安全部门公司副总裁兼首席技术官

政府纷纷采取行动提升关键基础设施安全性和复原能力

世界各国政府正在制定和完善管理关键基础设施网络安全风险的政策。许多政府还在制定政策来提升 IoT 和 OT 设备安全性。日益增长的全球政策举措浪潮为加强网络安全创造了巨大机遇，但也给整个生态系统的利益相关者带来了挑战。

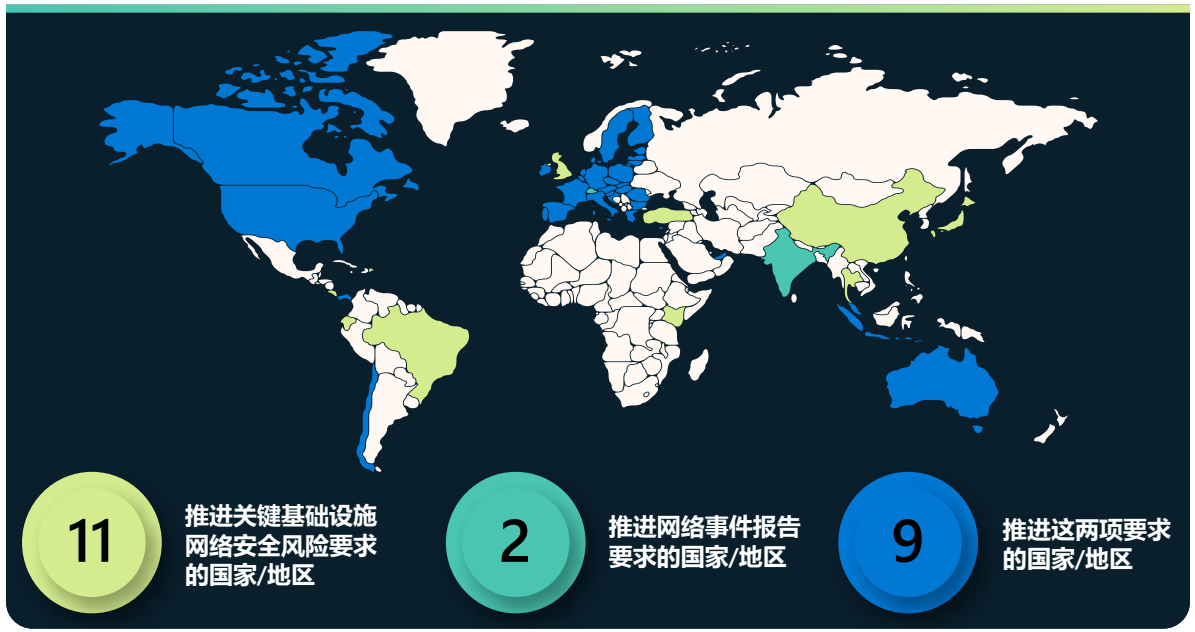
制定管理关键基础设施网络风险的整体愿景至关重要，但也十分复杂，特别是考虑到各个技术和全球供应商之间存在密切联系、技术使用和相关风险的范围，以及短期和长期战略投资需求。可推动反复学习和改进并支持全球跨领域互操作性的有效范围政策有助于降低复杂性并在实现数字化转型时提高安全意识。但是，零散的立法方式可能导致法规要求重叠并出现不一致。这可能会对资源产生影响，最终将不利于实现安全目标。例如，组织可能会将资源从致力于创新和安全性转向形式化的合规活动。

Microsoft 寻求与世界各国政府合作，制定有效的关键基础设施网络安全政策、加深对挑战和机会的了解，并支持共同致力于改善风险状况。

制定关键基础设施网络安全风险管理政策

去年，包括澳大利亚、智利、欧盟 (EU)、日本、新加坡、英国 (UK) 和美国在内的多个司法管辖区制定、更新或实施了跨领域或领域特定的网络安全要求。[1] 其中许多政府以及印度[2] 和瑞士[3] 等其他国家 / 地区政府已发布针对关键基础设施和重要服务提供商的网络安全事件报告要求或正在制定相关要求。[4]

去年，澳大利亚、欧盟、印度尼西亚和美国制定了一些值得关注的政策。澳大利亚制定了两项法律来帮助管理跨领域关键基础设施网络安全风险。这些法律以及一些其他法律指定了新的关键基础设施领域、要求制定风险管理计划、规定进行网络安全事件报告，并授权政府在确定关键基础设施运营商不愿意或无法充分响应事件时进行干预。



欧盟致力于更新其 2016 年颁布的《NIS 指令》，该指令为欧盟成员国提供了一个框架来监管被视为对其经济和社会运转至关重要的技术服务和产品。提出的 NIS 2 包括一些修订，用于创建新的关键数字基础结构类别、增加网络事件报告要求，并施加额外的网络安全风险管理要求。欧盟还提出对其《数字运营弹性法案》(DORA) 进行更新，针对金融服务领域使用的信息通信技术制定新的要求。

5 月，印度尼西亚发布了有关保护重要信息基础结构的总统令（“IIV”），这项总统令将于 2024 年 5 月生效，涵盖能源、交通运输、金融和医疗保健等领域。印度尼西亚的这项总统令旨在确保 IIV 实施的连续性、防范网络攻击，并更好地为处理网络事件做好准备。IIV 提供商将负责提供安全可靠的保护、实施有效的网络风险管理，并向相应政府机构报告网络风险结果。这项总统令还要求在 24 小时内报告网络事件。

政府纷纷采取行动提升关键基础设施安全性和复原能力

续

美国国会通过了一项法律，授权网络安全和基础设施安全局 (CISA) 发布要求关键基础设施运营商报告网络事件的法规，并授权美国运输安全管理局 (TSA) 在交通运输领域发布新的领域特定网络安全要求。2021 年，为了应对 Colonial Pipeline Company 遭受的勒索软件攻击，TSA 向危险液体和天然气管道运营商发布了两项安全指令：

- 第一项指令要求运营商指定一名网络安全协调员、在 12 小时内报告网络事件，并对其系统进行漏洞评估。
- 第二项指令（TSA 在 2022 年进行了修订）要求他们实施特定的缓解措施来防范针对 IT 和 OT 系统的勒索软件攻击和其他已知威胁、在 30 天内制定和实施网络安全应急和响应计划，并接受年度网络安全体系结构设计审查。

在管道相关法规的基础上，TSA 于 2021 年晚些时候发布了另外两项安全指令，要求货运铁路、客运铁路公司或铁路运输系统增强网络安全。这些指令要求相关运营商指定网络安全协调员、在 24 小时内报告网络安全事件、制定和实施网络安全事件响应计划，并完成网络安全漏洞评估。同时，TSA 还宣布更新了其航空安全计划，要求机场和航空运营商执行前两项规定，即指定协调员并在 24 小时内报告事件。

制定 IoT 和 OT 设备的安全政策

数十个国家 / 地区的政府正在积极制定相关要求来提高信息和通信技术 (ICT) 产品和服务（包括 IoT 和 OT 设备）的网络安全。就 ICT 产品和服务而言，最受关注的是软件供应链安全和 IoT 安全。

- 欧盟委员会提出了《网络弹性法案》，该法案将针对独立软件和互联设备及辅助性服务制定网络安全要求。[5] 软件供应商的相关做法包括利用安全的软件开发生命周期 [6] 并提供软件物料清单。[7] 新的安全要求适用于互联设备，所有制造商都需要管理已发布产品的协同漏洞披露 [8] 流程。

决策者还将着重关注 IoT 设备和网络 OT 设备的持续扩散上。

- 在英国，《产品安全和电信基础设施法案》草案要求智能电视等消费类可连接产品的制造商停止使用容易成为网络犯罪分子目标的默认密码、制定漏洞披露策略（例如如何接收安全漏洞通知），并就提供安全更新的最短最长保持透明。[9]
- 欧盟正在通过多个立法文件实施新的安全标准或要求，其中包括针对《无线电设备指令》的授权法案，该指令适用于无线设备，旨在提高网络复原能力、保护消费者隐私并降低货币欺诈风险。[10] 此外，由于 2019 年颁布了《欧盟网络安全法案》[12]，可能还需要使用当前正在制定的云认证计划 [11]。

保持一致的必要性

在许多情况下，会同时跨区域、领域、技术和运营风险管理领域在广阔的范围内开展活动，对于力图利用指导或证明合规性的组织而言，这可能会在范围、要求和复杂性方面造成重叠或不一致。如果没有普遍接受的 IoT 定义，则对于 IoT 和 OT 设备法规，确定范围尤其具有挑战性。以上示例可能适用于“互联产品和辅助性服务”、“消费类可连接产品”和“无线设备”。同时，许多政府致力于实施更强大的评估制度，从而更好地了解组织和产品是否以及如何满足当前、新兴和不断变化的要求。随着这些趋势的融合，复杂性将会增加。令人鼓舞的是，在《欧盟网络弹性法案》咨询期间提出的问题探讨了新法规可能如何与现有网络安全法规相互影响，这表明力图避免存在冲突的网络安全要求。

基于风险以及以结果或流程为导向的（而不是特定于实施）的迭代方法有助于增强网络安全和持续改进。同样，专注于跨领域、区域和政策领域实现互操作性可跨全球互联的供应链持续提高网络安全。

政府纷纷采取行动提升关键基础设施安全性和复原能力

续

跨区域、领域和主题领域制定的关键基础设施网络安全政策越来越复杂。此项活动带来了巨大的机会和挑战。政府之后如何采取行动对于未来的数字化转型和整个生态系统的安全至关重要。

加快整个生态系统在软件供应链安全和零信任架构的投资

关于改善网络安全的美国行政令 (EO) 14028 有助于推动 Microsoft 持续进行投资来实现自身和整个生态系统供应链安全的计划，并支持我们的客户实现零信任目标。

我们一直认为，强化软件供应链需要分享经验教训和最佳实践，这始于大约 15 年前我们公开发布的 Microsoft 安全开发生命周期。

此外，我们正在与国家网络安全卓越中心密切合作，展示适用于本地和云技术的零信任架构的方法并打造新的产品功能，包括针对混合和多云环境强制执行防网络钓鱼身份验证的功能。

如今，我们将超越 EO 要求，证明我们符合软件供应链安全要求，并以两种方式提供软件物料清单 (SBOM) 信息：

1. 首先，我们正在共享 SBOM 生成器工具的开源版本，我们构建该工具是为了轻松地与 CI/CD 管道集成，支持在 Windows、Linux、Mac、iOS 和 Android 平台上的构建。[13]
2. 其次，我们将参与制定供应链完整性、透明度和信任 (SCITT) 的行业标准。这样就可以自动交换可验证的供应链信息，包括证明符合要求（例如 EO 软件供应链指导中提出的要求）的工件。

切实可行的见解

1. 必须重新构想多边机构，以应对国家层面网络攻击的紧迫挑战。
2. 制定跨区域、领域和主题领域保持一致且可互操作的网络安全政策。

更多信息的链接

- 持续投资于供应链安全以支持网络安全行政令 | Microsoft Tech Community
- 美国政府制定零信任体系结构战略和要求 | Microsoft 安全博客
- 网络 EO | Microsoft Federal
- 供应链的完整性、透明度和信任 | github.com
- 实施零信任架构 | NCCoE (nist.gov)

IoT 和 OT 设备暴露：趋势和攻击

在日益互联的数字世界中，设备联机速度很快，它们将与大型系统通信、收集数据，并在之前模糊的领域中实现可见性。这为组织和威胁行为者均带来了机会，网络犯罪业务成为一个价值数十亿美元的行业，相应地也会带来巨大风险。

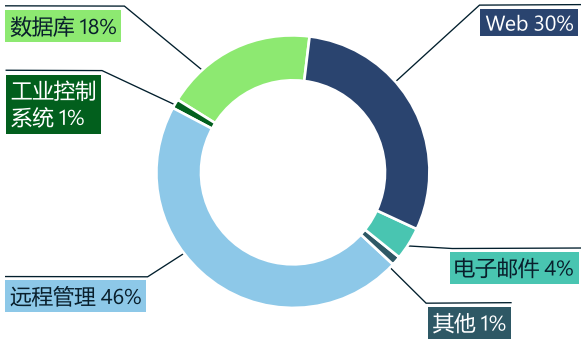
IoT 设备（包括从打印机到 Web 摄像头、气候控制设备和建筑准入控件在内的各种设备）给个人、组织和网络带来了独特的安全风险。虽然它们对许多组织的运营至关重要，但可能很快就会带来麻烦和安全风险。几乎每个行业都在迅速采用 IoT 解决方案，这增加了攻击媒介数量和组织的暴露风险。

恶意软件即服务已转为针对民用基础设施和公用事业（包括医院、石油和天然气、电网、交通运输服务和其他关键基础设施）以及公司网络发起大规模行动。威胁行为者需要开展大量研究工作来发现和利用操作环境及嵌入式 IoT 和 OT 设备的配置。

作为网络中的入口和枢纽点，IoT 设备带来了独特的安全风险。数百万台 IoT 设备未修补或遭到暴露。

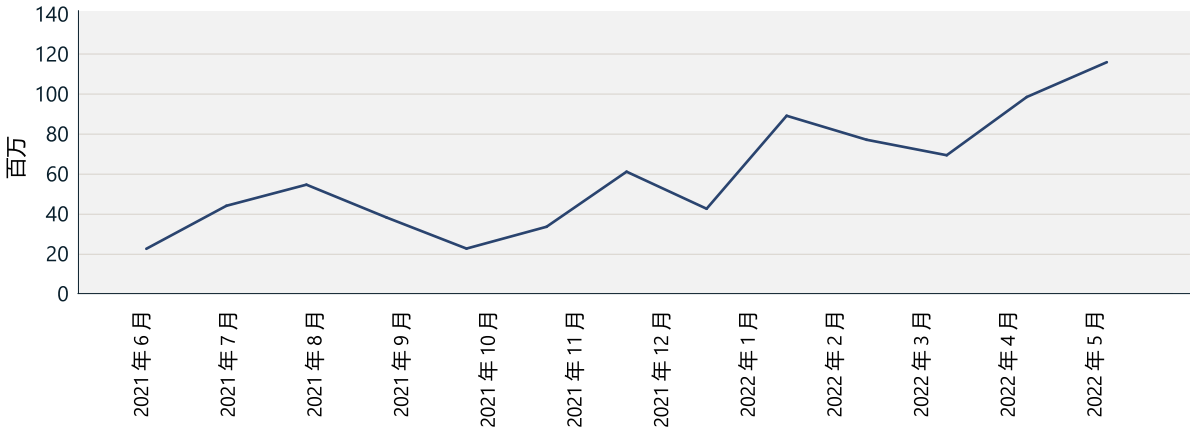
可以通过 Internet 搜索工具识别开放网络端口上的服务侦听行为来发现暴露的设备。这些端口通常用于对设备进行远程管理。如果没有得到适当保护，暴露的 IoT 设备可能会被用作进入企业网络另一层的枢纽点，因为未经授权的用户可能会远程访问端口。我们观察到许多威胁行为者都试图利用暴露于 Internet 的设备（从摄像头到路由器再到恒温器）中的漏洞。但是，尽管存在风险，仍有数百万台设备未修补或遭到暴露。

IoT/OT 攻击类型汇总



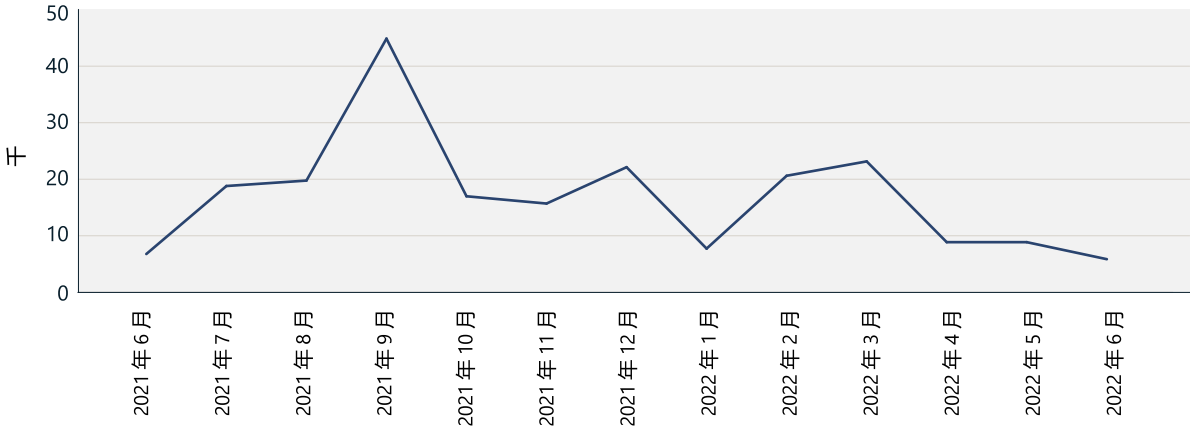
通过 MSTIC 传感器网络观察到的攻击类型。最常见的类型是针对远程管理设备的攻击、通过 Web 进行的攻击和针对数据库的攻击（暴力攻击或漏洞利用）。

针对远程管理设备的攻击



通过 MSTIC 传感器网络可以了解到，随着时间的推移，针对远程管理端口的攻击有所增加。

针对 IoT 和 OT 的 Web 攻击



通过 MSTIC 传感器网络可以了解一段时间内的 Web 攻击量。随着直接连接到 Web 的设备数量持续下降，最终攻击者探测这些设备的几率可能会降低。

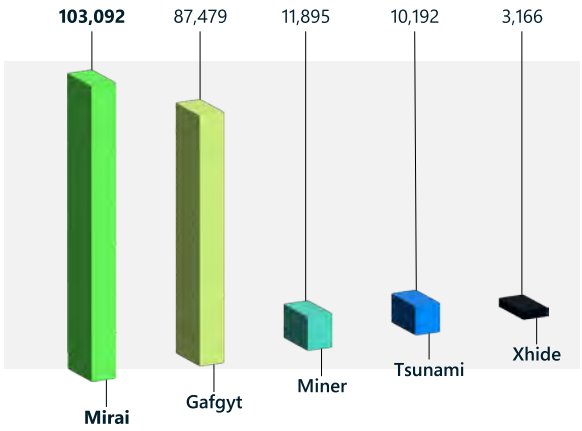
IoT 和 OT 设备暴露：趋势和攻击

续

经过改进的恶意软件实用程序

随着网络犯罪集团不断发展，其部署的恶意软件和选择的目标也在发生变化。在过去的一年中，我们观察到针对 Telnet 等常用 IoT 协议的攻击显著减少，在某些情况下降幅多达 60%。同时，僵尸网络被网络犯罪集团和国家层面行为者重新利用。Mirai 等恶意软件持续存在凸显了这些攻击的模块化特性和现有威胁的适应能力。

在环境中检测到的几大 IoT 恶意软件



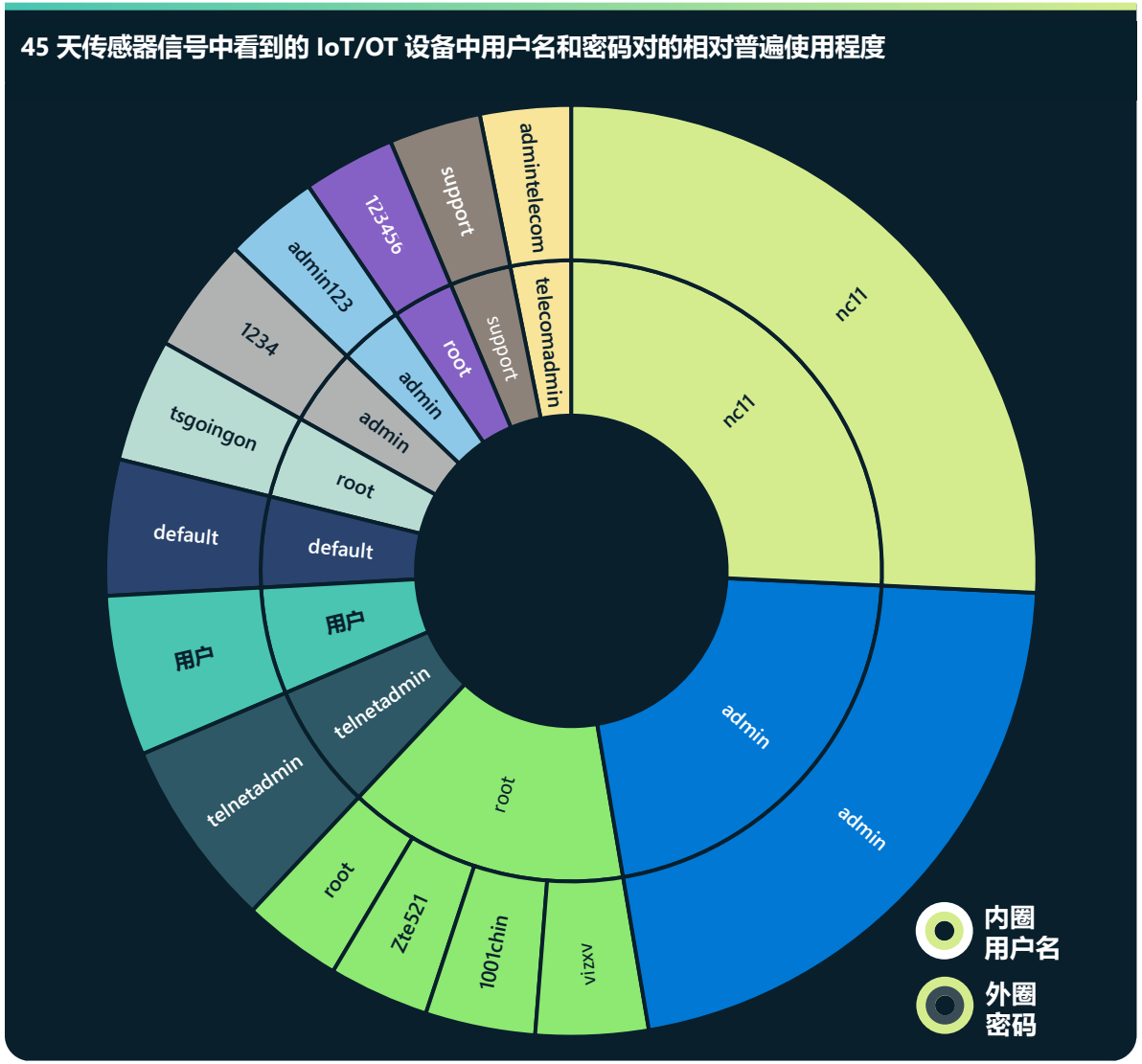
Mirai 演变为感染包括 Internet 协议摄像头、安全摄像头数字视频录像机和路由器在内的各种 IoT 设备。攻击媒介通过利用其他漏洞和横向移动绕过了旧式安全控件并给网络中的终结点带来风险。Mirai 已经过多次重新设计，其变体适应不同的体系结构，并利用已知和零日漏洞来使用新的攻击媒介进行入侵。

在过去的一年中，Mirai 在 32 位和 64 位 x86 CPU 体系结构中的使用量有所增加，这个恶意软件还具备了一些新功能，这些功能迅速被国家层面团体和犯罪集团采用。国家层面攻击现在会利用现有僵尸网络的新变体对外国敌对者进行分布式拒绝服务 (DDoS) 攻击。

随着 2022 年针对 IoT 设备的攻击带来的收入有所下降，我们观察到有多个威胁攻击者团体滥用 Log4j 和 Spring4Shell 等漏洞向服务器等设备提供恶意有效负载，从而感染这些设备并将其纳入执行 DDoS 攻击的大型僵尸网络中。针对易受攻击的 IoT 设备而设计的经过改进的恶意软件实用程序对组织和国家 / 地区都有严重影响，因为横向移动可能会暴露网络上其他有效负载和设备的后门。

许多工业控制系统协议不受监控，因此容易受到特定于 OT 的攻击。这可能意味着关键基础设施面临的风险增加。

45 天传感器信号中看到的 IoT/OT 设备中用户名和密码对的相对普遍使用程度



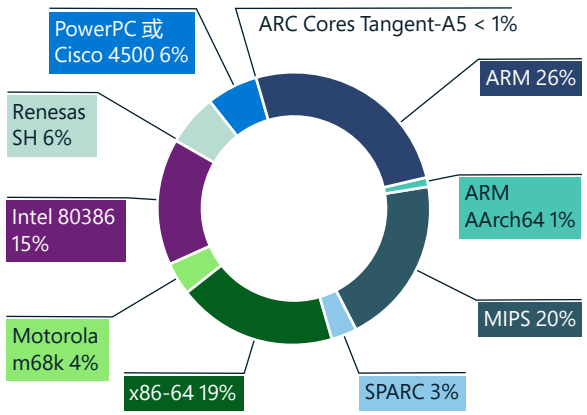
使用常见用户名和密码对会增加泄露风险。基于超过 3,900 万台 IoT 和 OT 设备的样本量，使用相同用户名和密码的设备约占 20%。

IoT 和 OT 设备暴露：趋势和攻击

接上页

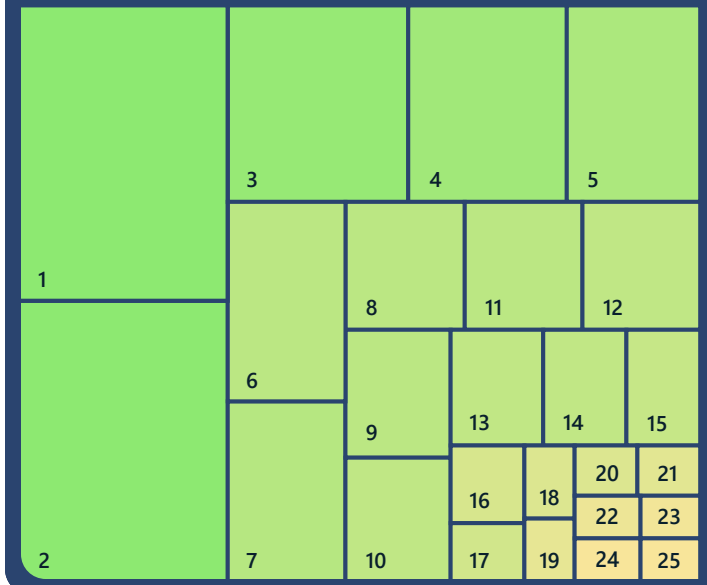
尽管弱配置和默认凭据仍会给网络带来风险，但 Microsoft 观察到许多基于 Web 的攻击是利用 HTTP 展开的。我们观察到使用旧式僵尸网络针对基于 Web 的服务发起的攻击有所增加。同时，Internet 上的开放 Telnet 端口数有所减少，这是网络安全的积极信号，因为过去给设备带来风险的僵尸网络已开始变得不合时宜。尽管开放的 Telnet 端口数有所减少，但我们仍观察到僵尸网络在传感器网络中持续存在。

按 CPU 架构列出的 IoT 恶意软件分布情况



Microsoft 观察到，在 ARM 上运行的 IoT 设备是恶意软件的主要攻击目标，其次是 MIPS、X86-64 和 Intel 80386 CPU。

工业控制系统协议普及度



1. 以太网/IP
2. MODBUS
3. BACNet
4. Siemens S7
5. Profinet 实时
6. Profinet DCP
7. Siemens S7 Plus
8. CodeSys
9. Siemens WinCC 代理
10. 以太网/IP O/O
11. Honeywell 控制数据访问
12. MMS
13. IEC-60870
14. Honeywell FDA 诊断
15. Suitelink
16. DeltaV
17. GSM
18. DNP3
19. AMS
20. SRTP
21. TwinCat
22. Emerson Roc
23. Bently Nevada
24. Mitsubishi MELSEC
25. TriStation Tricon

工业控制系统协议漏洞

我们研究了来自云连接传感器的 OT 数据，从中了解了常用的工业控制系统 (ICS) 协议。这些协议有助于深入了解这些设备的性质及其攻击面。这对于确保关键基础设施安全尤其重要。以下是一些重要的经验教训：

1. 所代表的大多数协议都是专有协议，因此标准的 IT 监控工具无法跨这些设备和协议提供足够的安全可见性。这导致网络不受监控，从而更易受到 OT 特定的攻击。
2. 有各种供应商特定的协议。这意味着供应商特定的安全解决方案无法充分覆盖整个网络。Microsoft 优先考虑与供应商无关的方法，为各种不同的设备提供安全保障。
3. 组织应确保这些协议不会通过其网络直接暴露在 Internet 上。由于这些协议存在漏洞且在本质上不安全，这种暴露情形可能会带来重大安全风险。

像 Mirai 这样的恶意软件通过开发新功能而持续存在，并被网络犯罪组织和国家层面行为者采用，利用现有僵尸网络的新变体对外国敌对者进行 DDoS 攻击。

切实可行的见解

1. 通过应用修补程序、更改默认密码和默认 SSH 端口，确保设备稳健可靠。
2. 消除不必要的 Internet 连接和开放端口、通过阻止端口限制远程访问、拒绝远程访问并使用 VPN 服务，从而减少攻击面。
3. 使用 IoT/OT 感知网络检测和响应 (NDR) 解决方案以及安全信息和事件管理 (SIEM)/ 安全编排和响应 (SOAR) 解决方案，监控设备是否存在异常或未经授权的行为，例如与陌生主机通信。
4. 对网络分段来限制攻击者在初始入侵后横向移动和破坏资产的能力。我们应通过防火墙将 IoT 设备和 OT 网络与公司 IT 网络隔离。
5. 确保 ICS 协议不直接暴露在 Internet 上。

供应链和固件黑客攻击

几乎每台联网设备都有固件，这是嵌入到设备硬件或电路板中的软件。在过去几年中，我们发现针对固件发动破坏性攻击的活动有所增加。由于固件可能会继续成为威胁行为者的重要目标，因此组织必须防范固件黑客攻击。

固件负责执行设备的主要功能，例如连接到网络或存储数据。固件存在于企业使用的路由器、摄像头、电视和其他设备 (IoT) 以及关键基础设施中所用的工业控制设备 (OT) 中。过去，固件是用不安全的代码编写的，这就产生了一些可被用来接管设备或将恶意代码注入固件的重大漏洞。

当涉及到供应链时，这种风险会加剧。大多数设备都是使用来自众多制造商以及开源库的软件和硬件组件构建的。在许多情况下，设备运营商无法查看硬件和软件物料清单 (H/SBOM) 来评估其网络上设备的供应链风险。2020 年 6 月，披露了许多不同制造商使用的一个网络堆栈中存在的漏洞，这对消费类和工业设备领域的数亿台 IoT 设备产生了影响。[14] 在某些情况下，其他供应商对这个网络堆栈进行了重新调整，并且没有迹象表明设备易受到攻击。我们发现越来越多的恶意行为者以 IoT/OT 设备的这一软件和硬件供应链为攻击目标来入侵组织，造成的威胁日益严峻。

固件更新过程在不同设备中存在很大差异，执行更新的复杂性及后勤方面的挑战会影响更新频率。我们并非总能确定设备是否在运行最新固件，这使得安全专家难以监控和确保其 IoT 和 OT 设备的安全状况。此外，某些设备具有未经过加密签名的固件，这样无需用户验证即可对其进行更新。这些漏洞使设备在整个生产和分销链中更易受到供应链攻击。

为了应对这些威胁，Microsoft 投入了大量资金来确保固件在供应链各个阶段的安全性和完整性，并随时证明其在引入期间或整个过程中未被篡改。这样，我们就能验证每个管道段之间的信任度，并为我们交付给客户的每个组件提供经过认证和可证明的端到端监管链。我们正在与合作伙伴合作，携手将这种芯片到云的安全性引入企业和 OT 网络上的所有设备。

“由于可针对 ICT 基础结构供应商广泛复制单次攻击，因此针对他们的攻击日益增多。同时，针对供应链安全性和复原能力的全球立法、法规和客户需求日益增加，相关要求往往存在差异。

解决方案是建立合作关系。Microsoft 与供应商和全球政府携手，共同致力于解决整个供应链生态系统中存在的安全问题，超越客户和监管机构的需求。为此，我们正在推行一种全面的方法来实现安全性和运营复原能力，此方法可在整个供应链中灵活部署。

推动实现从设计一直到设备运营的固件完整性是我们这种共同合作方法的关键。我们如何“实现”供应链完整性的示例包括确保执行供应商的 SDL 流程以及部署硬件信任根创新成果。

我们的社区正在利用包括新的防篡改技术和加密机制在内的共同研发成果，并将其与持续监控和异常检测相结合。我们正在一起努力，最大限度地减少供应链作为攻击面的吸引力。”

Edna Conway，
云基础结构部门副总裁兼安全与风险官

聚焦固件漏洞

攻击者越来越多地利用 IoT 设备固件中的漏洞来渗透到公司网络中。与使用 XDR 代理识别漏洞的传统 IT 端点不同，识别 IoT/OT 设备中的漏洞要困难得多。

Microsoft 和 Ponemon Institute 最近开展的一项调查凸显了企业在 IoT/OT 设备方面面临的机会和安全挑战。[15] 虽然 68% 的受访者认为采用 IoT/OT 对其战略性数字化转型至关重要，但 60% 的受访者认为 IoT/OT 安全性是 IT/OT 基础结构安全性最低的一个方面。

攻击者使用 IoT 设备固件中的漏洞渗透网络的一个示例是 Trickbot 特洛伊木马，它利用 Mikrotik 路由器中的默认密码和漏洞 [16] 绕过了企业防御系统。就 IoT 设备固件而言，面临的根本性挑战是对设备安全状况和漏洞缺乏了解。

虽然有可用于构建安全设备的解决方案，但市面上已有数十亿台在企业中部署的设备。这些被称为棕色地带设备。2021 年，Microsoft 收购了 ReFirm Labs 来了解棕色地带设备的安全性，并帮助设备构建商提高产品安全性。ReFirm Labs 分析设备的二进制固件映像，并生成有关潜在安全漏洞的详细报告。[17] 这项技术将纳入 Microsoft Defender for IoT 的未来版本。

在过去的一年中，我们检查了客户扫描的唯一固件的聚合结果。虽然并非发现的每个漏洞都可能被利用，但它们凸显了在设备固件安全方面面临的根本性挑战。

请注意，IoT/OT 设备中存在的漏洞类型在传统的 Windows 或 Linux 终结点上是绝对无法接受的。

- 弱密码：扫描的固件映像中有 27% 包含使用弱算法 (MD5/DES) 编码的密码的帐户，这些密码很容易被攻击者破解。

分析的固件映像中的安全漏洞

- 已知漏洞：与其他的系统一样，IoT/OT 设备固件广泛利用了开源库。但是，设备在交付时经常包含这些组件的过时版本。在我们的分析中，32% 的映像至少包含 10 个被评为严重（9.0 或更高得分）的已知漏洞 (CVE)。有 4% 的映像至少包含 10 个存在超过六年的严重漏洞。
- 过期证书：证书用于对连接和身份进行身份验证以及保护敏感数据，但分析的映像中有 13% 至少包含 10 个已过期超过三年的证书。
- 软件组件：36% 的映像包含 Microsoft 建议在 IoT 设备中排除的软件组件（例如 tcpdump、libpcap 等数据包捕获工具），这些组件可能会作为攻击链的一部分用于网络侦察。

现实中的固件攻击

Viasat：使用固件漏洞定位卫星通信

2022 年 2 月，卫星网络事件导致战略通信网络断连，影响波及整个欧洲。Viasat 的 KA-SAT 系统接收了大量流量，使许多调制解调器断连，并针对网络发起了拒绝服务攻击。随着固定宽带中断，运营商无法对数千台风力涡轮机进行远程访问，同时 Wiper 恶意软件被部署到受影响的调制解调器。这次中断影响到了公司和组织用于通信的 30,000 多个卫星终端。

Cyclops Blink：使用固件供应链攻击来攻击防火墙网关

对于威胁行为者来说，开发和扩展命令与控制 (C2) 和攻击基础结构是成功的关键一环。随着对稳定 C2 基础结构的需求不断增长，路由器因修补不频繁和缺乏全面的安全解决方案而成为理想的攻击媒介。

Microsoft 正在与政府和行业组织合作开发固件分析技术，以便更深入地了解设备安全，并为设备构建商和运营商提供完整的生命周期安全性。

自 2019 年 6 月以来，一个与国家关联的高级持续性威胁 (APT) 团体使用模块化恶意软件 Cyclops Blink 执行恶意固件更新并将其纳入大型僵尸网络，以此针对易受攻击的 WatchGuard 防火墙设备和 ASUS 路由器发起攻击。这个恶意软件利用允许特权升级的已知漏洞成功感染设备，使威胁行为者能够管理设备。感染设备后，行为者可利用恶意软件安装更多模块并逃避固件更新。连接到其他 WatchGuard 设备上托管的 C2 服务器时，发现设备遭到入侵。Cyclops Blink 运营商通过执行恶意固件更新和逃避扫描等传统安全方法，获取了对网络的特权远程访问，在各种 TCP 端口上为其 C2 颁发了许多 SSL 证书。

Microsoft 如何提高供应链安全性

Microsoft 正在与政府和行业组织合作，共同应对这些 IoT 和 OT 设备安全挑战（请参阅第 66 页上的讨论）。我们参与的工作包括利用固件分析技术帮助设备运营商了解网络上设备的安全状况。这将帮助客户识别需要额外保护、升级或更换的设备以及确定其优先级，并拉动对设备构建商投资提高设备安全性的需求。同时，我们为构建商提供构建安全设备和采用安全开发生命周期的全面解决方案，从而为其提供支持。

另一个关键要素是为构建者和运营商提供强大的基础结构，以便在发现和解决安全问题时更新设备固件。Microsoft 将 Defender for IoT 的固件分析与 Device Update for IoT Hub 整合在一起，以提供在整个生命周期内保证 IoT 和 OT 设备安全的解决方案。这些都是实现我们对客户的愿景的重要步骤，即让客户可以通过在其 IoT 和 OT 解决方案中采用支持零信任方法的设备来保护基础结构。[18]

攻击者越来越多地将 IoT 设备固件中的漏洞作为攻击目标，渗透到企业网络中。

切实可行的见解

1. 更深入地了解网络上的 IoT/OT 设备，并根据企业（如果已遭入侵）面临的风险确定设备的优先级。
2. 使用固件扫描工具了解潜在安全漏洞，并与供应商合作，确定如何降低高风险设备的风险。
3. 要求供应商采用安全开发生命周期最佳实践，从而对提高 IoT/OT 设备安全性产生积极影响。

更多信息的链接

- 评估支持美国信息和通信技术行业的关键供应链

基于侦察的 OT 攻击

复杂的供应链使用特定设计信息来规划实际系统。在构成这些设计信息的各种资产中，最敏感的是项目文件，它定义环境及其资产。对于试图获得访问权限并成功部署完全针对环境定制的攻击的威胁行为者来说，此文件是至关重要的战略目标。

将工业系统作为目标来破坏操作流程涉及两个步骤。

1. 第一步，攻击者必须访问 OT 网络。这可以通过以下方式来实现：通过网络上企业端的 IoT 设备（普渡模型第 4 层）进入，以及跨越 IT-OT 边界（通常由防火墙和网络设备分隔）进入操作和控制层。
2. 第二步，必须识别网络设备。工业系统在专门为其环境设计的定制体系结构中使用标准设备和组件。这些标准设备之一是可编程逻辑控制器 (PLC)。每个制造商都为其 PLC 开发独特的接口和功能，PLC 是工业系统的重要组成部分，这些设备还进一步配置有专为客户环境设计的定制架构。

每种 PLC 的独特配置均在项目文件中得到了描述，项目文件中还包含环境及其资产的定义、梯形逻辑等。

在出现攻击迹象的大多数环境中，分析表明攻击前的时间线远远超过了攻击本身的时长。威胁行为者通常会花费几个月的时间来远程模拟环境及其资产，多次尝试构建模型并准备有针对性的攻击。随着环境不断变化和加入新设备，漏洞开始专门围绕项目和配置文件中的数据产生。项目文件盗窃可能会先于攻击数周或数月出现，它使攻击者能够快速、准确地对目标环境进行建模，从而增加了检测恶意活动的难度。

Industroyer 和 Incontroller

我们观察到，由国家支持的行为者使用模块化恶意软件和攻击框架对组织、关键基础结构和政府目标发起的攻击有所增加。乌克兰境内干预关键操作的全新尝试揭示了基于侦察且根据目标环境进行高度定制的 OT 攻击日益增长。国家层面网络行为者执行的侦察和调查阶段延长，这表明出现了利用网络战争远程破坏基础结构的战略，目的是通过以网络为动力的混合运作和政治战略实现特定的战略或运作目的。

我们观察到，基于侦察的 OT 攻击会根据目标环境进行高度定制，它们带来的威胁日益严峻。

基于侦察的 OT 攻击

接上页

2022 年初发现了两种适应性强的关键 OT 攻击。对乌克兰境内的变电站和保护继电器发起的网络物理攻击是通过定制的恶意软件进行的，包括 Industroyer 的变体。Industroyer 是一款恶意软件，2016 年在乌克兰境内部署后造成了停电。

Industroyer2 是恶意 OT 攻击恶意软件首次重新部署到新目标上。它利用了为 Industroyer 开发的 IEC104 协议（用于电力系统监控和控制的标准协议）插件，主要针对型号为 ABB RTU540/560 的 PLC 类远程终端设备。这款恶意软件的编写者利用对于受害者环境的了解来反复向预先确定的输出发出命令，以确保它们无法手动打开。这确保了更长时间的停电和更具破坏性的影响。

Incontroller 是同一时期发现的模块化攻击框架，它是模块化工具包，可显著缩短绕过传统的安全解决方案而渗透并攻击 OT 设备的提前期。该通用工具包具有可针对不同环境进行高度定制的数据收集、侦察和攻击功能，可以极大地影响 OT 攻击的调查阶段，从而减少执行侦察所需的时间，并通过提取有关设备及其配置的信息来支持环境模拟信息。

Incontroller 框架支持适用于 Schneider Electric 和 Omron PLC 的协议，并收集固件版本、模型类型和连接的设备等信息。该工具包可以发出命令以更改配置并打开和关闭输出。可以访问环境后，该框架支持在设备中植入后门以交付更多有效负载，从而创造漏洞以增加访问点、上传梯形逻辑并能够发起 DoS 攻击。该工具包的通用性质使威胁行为者能够快速攻击环境，而无需为每个 PLC 或位置编写新的攻击。这使得行为者可以轻松与可能属于多个行业的不同类型计算机进行交互。

切实可行的见解

1. 避免通过不安全的通道传输包含系统定义的文件，或避免传输给非必要人员。
2. 当不可避免地传输此类文件时，请务必监控网络上的活动并确保资产安全。
3. 通过使用 EDR 解决方案进行监控来保护工程站。
4. 主动对 OT 网络执行事件响应。
5. 部署持续的监控，如 Defender for IoT。

尾注

1. 参考资料：Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe’ s digital future (europa.eu)：https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1；Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (homeaffairs.gov.au)；Chile: Bill for cybersecurity and critical information infrastructure introduced in Senate | News post | DataGuidance；Japan passes economic security bill to guard sensitive technology | The Japan Times；Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs (csa.gov.sg)；Proposal for legislation to improve the UK’ s cyber resilience - GOV.UK (www.gov.uk)；Telecommunications (Security) Act 2021 (legislation.gov.uk)；Updating the NIST Cybersecurity Framework - Journey To CSF 2.0 | NIST
2. Cert-In - 主页
3. Initiation of consultation on introduction of cyberattack reporting obligation (admin.ch)
4. 参考资料：无标题 (house.gov)
5. Cyber Resilience Act | Shaping Europe’ s digital future (europa.eu)
6. 参考资料：Microsoft 安全开发生命周期
7. 参考资料：Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft - Engineering@Microsoft；还可参见 The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. 参考资料：https://www.microsoft.com/en-us/msrc/cvd
9. The Product Security and Telecommunications Infrastructure (PSTI) Bill - product security factsheet - GOV.UK (www.gov.uk)
10. Commission strengthens cybersecurity of wireless devices and products (europa.eu)
11. Cloud Certification Scheme: Building Trusted Cloud Services Across Europe - ENISA (europa.eu)
12. Certification - ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool “GitHub-microsoft / sbom-tool：SBOM 工具是一种高度可扩展且企业就绪工具，可为各种工件创建兼容 SPDX 2.2 的 SBOM。
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years- to-come
15. IoT/OT 创新至关重要但伴随重大风险（2021 年 12 月）：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. 了解 Trickbot 如何利用 C2 基础结构中的 IoT 设备（2022 年 3 月）：https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. 第 9 频道上有关 IoT 固件扫描的一期 “IoT Show” 节目（2022 年 5 月）：https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. 如何对 IoT 解决方案应用零信任方法（2021 年 5 月）：https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

网络影响行动

如今的国外影响力行动利用新的方法和技术，使旨在削弱信任的活动更加高效且有效。

网络影响力行动概述 72

引言 73

网络影响力行动的趋势 74

聚焦 COVID-19 和俄罗斯入侵乌克兰期间的影响力行动 76

跟踪俄罗斯宣传指数 78

合成媒体 80

防范网络影响力行动的整体方法 83

网络影响力行动

概述

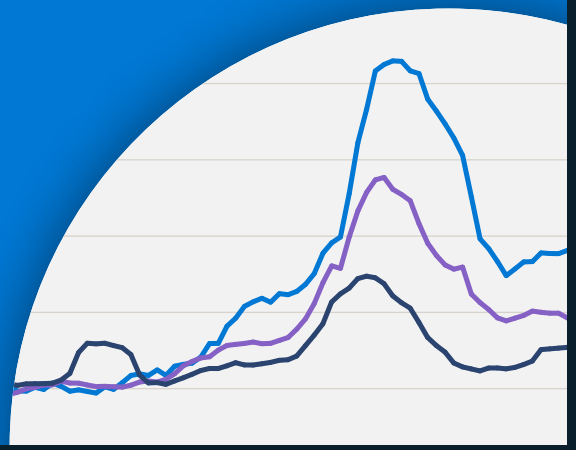
如今的国外影响力行动利用新的方法和技术，使旨在削弱信任的活动更加高效且有效。

国家层面越来越多地利用复杂的影响行动进行宣传，影响国内和国际的公众舆论。这些活动会削弱人民的信任感，加剧两极分化，并阻碍民主进程。熟练的 Advanced Persistent Manipulator 行为者正在使用传统媒体以及 Internet 和社交媒体来大幅增加其活动的范围、规模和效率，以及他们在全球信息生态系统中产生的巨大影响。在过去的一年里，我们看到这些行动被用作俄罗斯在乌克兰的混合战争的一部分，但也看到俄罗斯和包括中国和伊朗在内的其他国家，越来越多地转向以社交媒体为动力的宣传行动，以扩大其全球影响力。

随着越来越多的政府和国家开始利用网络影响力行动来塑造舆论、抹黑对手和推动不和，这类行动变得越来越复杂。

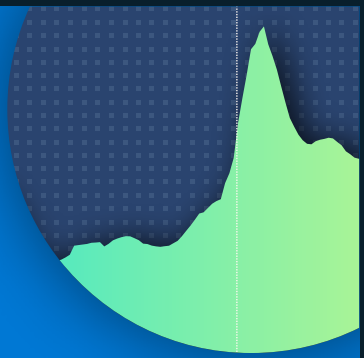
详情请参见第 74 页

俄罗斯入侵乌克兰证明了，网络影响力行动与更传统的网络攻击和动态军事行动相结合，可以最大限度地发挥影响力。



详情请参见第 76 页

俄罗斯、伊朗和中国在整个 2019 冠状病毒病（COVID-19）大流行期间开展了宣传和影响力活动，这往往是实现更广泛政治目标的战略手段。



详情请参见第 76 页

由于可以轻松创建和传播高度逼真的人工图像、视频和音频的工具激增，合成媒体正变得越来越普遍。用于认证媒体资产来源的数字溯源技术有望打击滥用现象。

详情请参见第 80 页

防范网络影响力行动的整体方法

Microsoft 正在利用已经成熟的网络威胁情报基础结构来打击网络影响力行动。我们的战略是发现、干扰、防御和阻止国外攻击者的宣传活动。

详情请参见第 83 页

引言

民主需要值得信赖的信息才能蓬勃发展。Microsoft 的一个重点关注领域是国家层面正在制定和延续的影响力行动。这些活动会削弱人民的信任感，加剧两极分化，并阻碍民主进程。

国外影响力行动一直都是信息生态系统面临的威胁。然而，Internet 和社交媒体时代的不同之处在于，此类活动的范围、规模和效率得到了大大提升，并且它们可能会对全球信息生态系统的健康发展产生巨大影响。

过去有句名言："谎言环游全球的时候，真相还没穿好鞋子"，现在这一点正在被数据证实。麻省理工学院 (MIT) 的一项研究[1] 发现，谎言被转发的可能性比真相高 70%，并且其传播范围首次达到 1,500 人的速度是后者的六倍。随着宣传活动在 Internet 和社交媒体上迅猛发展并削弱人们对传统新闻的信任，信息生态系统变得越来越不可信。2021 年的一项研究[2] 指出，在美国，只有 7% 的成年人表示，他们对报纸、电视和广播新闻报道拥有"极大的"信任和信心，而 34% 的成年人表示"完全没有"。

Microsoft 一直在努力确定国外网络影响领域的主要行为者、威胁和策略，并分享获得的经验教训。今年 6 月，我们发布了一份全面的报告来介绍从乌克兰获得的经验教训，其中详细分析了俄罗斯的网络影响力行动。[3]

我们还研究了先进技术（例如深度伪造）如何被用作武器，破坏新闻工作者的可信度。我们正在与行业、政府和学术界合作，研究更好的方法来检测合成媒体并恢复信任，例如可以发现伪造的人工智能 (AI) 系统。

信息生态系统和国家在线宣传（包括传统网络攻击与影响力行动的结合以及对民主选举的干预）的快速变化特性对通过一种社会整体方法来减轻对民主的在线和离线威胁提出了要求。

Microsoft 致力于为信息生态系统的健康发展提供支持，让可信的新闻和信息焕发勃勃生机。我们正在开发工具和威胁检测功能，以应对国家发起的影响力行动带来的不断演变和扩大的风险。为了实现这一目标，我们最近收购了 Miburo Solutions，我们与 Global Disinformation Index 和 NewsGuard 等第三方验证机构合作，我们参与并多次主导了涉及多方利益相关者（包括内容溯源和真实性联盟 (C2PA)）的合作。只有携手合作，我们才能成功对抗那些试图破坏民主进程和机构的人。

Teresa Hutson

技术与企业责任部门副总裁

网络影响力行动的趋势

随着技术的稳步发展，网络影响力行动变得越来越复杂。我们发现，用于执行传统网络攻击的工具，有很大一部分也用于网络影响力行动，而且这类工具的数量还在增多。此外，我们看到国家之间的协调配合和大肆传播活动有所增加。

今年，Microsoft 在应对国外影响力行动方面进行了投资，收购了 Miburo Solutions，这是一家专门分析国外影响力行动的公司。Microsoft 将这家公司的分析师与 Microsoft 的威胁上下文分析师聚集在一起，成立了数字威胁分析中心 (DTAC)。DTAC 分析并报告国家层面威胁（包括网络攻击和影响力行动），以将信息和威胁情报与地缘政治分析相结合来提供见解并告知有效的响应和保护措施。

全球超过四分之三的人表示，他们担心信息被用作武器，[4] 我们的数据也能证实这些担忧。Microsoft 及其合作伙伴一直在跟踪国家层面的行为者如何利用影响力行动实现其战略目标和政治目标。除了破坏性的网络攻击和网络间谍工作，专制政权越来越多地利用网络影响力行动来塑造舆论、抹黑对手、激起恐惧、推动不和以及扭曲现实。

这些国外网络影响力行动通常分为三个阶段：

预先铺陈

与在组织计算机网络中预先置入恶意软件一样，国外网络影响力行动会在 Internet 的公共域中预先铺陈虚假言论。预先铺陈策略长期以来对更传统的网络活动起到了推波助澜的作用，特别是如果 IT 管理员扫描最近的网络活动。网络上长时间处于休眠状态的恶意软件，后续得到使用时可能会变得更加有效；而在 Internet 上未得到关注的虚假言论，后续得到引用时则可能会看起来更加可信。

启动

通常，行为者会在最利于实现目标的时候启动协调一致的活动，以通过受到政府支持和影响的新闻媒体和社交媒体渠道来传播言论。

大肆传播

最后，国家控制的媒体和代理会在目标受众中大肆传播言论。通常，技术促成方会在不知情的情况下扩大言论的影响范围。例如，在线广告可以帮助筹措资金，而协调一致的内容交付系统则会让相关内容遍布搜索引擎。

这种三步方法在 2021 年末被用于支持俄罗斯围绕乌克兰所谓的生物武器和生物实验室编织虚假言论。这段言论在 2021 年 11 月 29 日首次上传到 YouTube，它包含在来自莫斯科的美国侨民定期更新的英语节目中，此人声称美国在乌克兰资助的生物实验室与生物武器有关。这个报道沉寂了好几个月。2022 年 2 月 24 日，当俄罗斯坦克越过边界时，这段言论也卷入到了战争当中。Microsoft 的一个数据分析团队发现，10 个由俄罗斯控制或影响的新闻网站在 2 月 24 日同时发布了报道，并指出这是“去年的报告”，试图证明它的可信度。此外，俄罗斯外交部官员举行了新闻发布会，在信息环境中进一步散播了有关美国生物实验室的虚假声明。然后，俄罗斯支持的团队想方设法在社交媒体和 Internet 网站上更广泛地大肆传播这一言论。

我们看到，世界各地的专制政权正在联手污染信息生态系统，以便他们可以相互受益。例如，在整个 2019 冠状病毒病（COVID-19）大流行期间，俄罗斯、伊朗和中国采用公开、半隐蔽和隐蔽的混合传播方法进行宣传和影响力行动，以针对民主国家和更多的地缘政治目标（第 76 页有进一步讨论）。这三种体系相互作用于彼此的消息传递和信息生态系统，以宣传其偏好的言论。大部分这类报道宣传有关美国及其盟友的批判言论或阴谋论，这些报道由政府官员在官方声明中宣扬，同时宣传自己的疫苗和 COVID-19 应对措施优于美国和其他民主国家。通过相互放大，国有媒体创造了一个生态系统，在这个系统中，一家国有媒体对民主国家的负面报道或对俄罗斯、伊朗和中国的正面报道将被其他媒体所强化。

示意图显示了有关美国生物实验室和生物武器的言论如何通过许多国外影响力行动分三个主要阶段（预先铺陈、启动和大肆传播）进行传播。

网络影响力行动的趋势

接上页

私营部门技术实体可能会在不知情的情况下促成这些活动，进一步加剧了挑战。促成方可能包括注册 Internet 域名、托管网站、在社交媒体和搜索网站上推广材料、引导流量以及通过数字广告帮助支付这些活动费用的公司。组织必须了解专制政权用于网络影响力行动的工具和方法，以便能够检测并阻止这些活动传播。此外，组织也越来越需要帮助消费者提高熟练识别国外影响力行动并限制与其言论或内容互动的能力。

网络影响力行动（包括对专制主义的宣传）是全球民主制度面临的威胁，因为它们会削弱信任、加剧两极分化并威胁民主进程。

在政府、私营部门和民间团体之间需要加强协调配合和信息共享，以提高透明度并揭露和干扰这些影响力活动。

在全球范围内，超过四分之三的人对信息被用作武器的现象表示担心。

聚焦 COVID-19 和俄罗斯入侵乌克兰期间的影响力行动

试图在整个疫情期间以及在俄罗斯入侵乌克兰期间控制信息环境的国家提供了鲜明的例子，说明了专制政权如何将网络和信息行动相结合。

COVID-19 宣传

俄罗斯、伊朗和中国在整个 COVID-19 大流行期间开展了宣传和影响活动。COVID-19 在这些活动中发挥了突出作用，主要体现在两个方面：

1. 对疫情本身的宣传。
2. 部分活动将 COVID-19 作为战略工具来实现更远大政治目标。

从广义上讲，这些类型的活动有双重目的：第一，破坏民主制度和民主机构，以及美国及其盟友在全球的形象；第二，在国内和国际上巩固自己的地位。

知名俄罗斯帐户和媒体组织面向英语读者传达的消息，以及俄罗斯政府如何就疫苗和 2019 冠状病毒病（COVID-19）的严重性与本国公民进行沟通，这两方面产生的对比就是一个典型示例。

RT.com 上 10 个观看次数最多的冠状病毒报道涵盖的主题（2021 年 10 月至 2022 年 4 月）

针对非俄罗斯读者进行了反疫苗宣传

俄语（以下已翻译为英语）	英语
“封闭和加强针可以阻断传播”	“疫苗不能遏制传播，对新的毒株也无效”
“俄罗斯官员正在积极测试”	“Pfizer 疫苗有严重的副作用”
“俄罗斯的感染和死亡人数正在增加”	“大规模疫苗接种有政治目的”
“Sputnik V 疫苗非常有效”	“Pfizer 和 Moderna 的试验是在不受监管的情况下进行的”
“乘坐公共交通需要接种疫苗的证明”	

俄罗斯的 COVID-19 宣传内容因语言而异。

试图掩盖 COVID-19 病毒起源的活动是另一个示例。自疫情爆发以来，俄罗斯、伊朗和中国的 COVID-19 宣传促进了其他国家的报道力度，以放大这些中心主题。这些报道的大部分内容是宣传对美国的批评或阴谋论。官方媒体经常相互放大，形成了一个生态系统。在这个生态系统中，一个官方媒体对民主国家的负面报道或对俄罗斯、伊朗和中国的正面报道，一次又一次地被其他媒体强化。

这方面的一个示例是，俄罗斯和伊朗官方媒体早些时候暗示 2019 冠状病毒病（COVID-19）可能是美国制造的生物武器。疫情早期一位法学教授接受了采访，他声称他认为 COVID-19 是作为一种武器制造的，之后几个非主流的阴谋论网站散布了这一说法。[6] 采访在覆盖人群有限的几个网站上发布后，这个报道被官方媒体选中。由伊朗政府[7] 赞助的伊朗英语和法语媒体 PressTV 于 2020 年 2 月发表了一篇英文报道，题为“冠状病毒是否如 Francis Boyle 所相信的那样是美国的生物战武器？”文章暗示美国是 2019 冠状病毒病（COVID-19）爆发的幕后黑手，并写道：“在所有美国战争中，都使用了放射性、化学、生物和其他被禁止的武器，给目标地区的人们造成毁灭性的伤亡。”[8] 俄罗斯官方媒体和中国政府的报道也表达了同样的看法。《今日俄罗斯》（RT）是一家以传播克里姆林宫宣传而闻名的国有媒体[9]。它至少发表了一篇报道宣传伊朗官员的声明，声称新冠肺炎可能是“美国针对伊朗和中国的‘生物攻击’的产物”，[10] 并在社交媒体上发布相同暗示的帖子。例如，RT 于 2020 年 2 月 27 日在推特上发文，其中写道：“举手表态，如果揭露出 #coronaviru 就是生物武器，谁会感到惊讶？”[11]

乌克兰战争 - 将宣传作为战争武器

俄罗斯入侵乌克兰提供了鲜明的示例，说明了如何将网络影响行动力与更传统的网络攻击和地面军事行动相结合，以最大限度地发挥其影响力。

在入侵乌克兰之前，Microsoft 威胁情报分析师看到，至少 6 个与俄罗斯结盟的不同行为者针对乌克兰发起了超过 237 次网络攻击。这些活动旨在降低服务和机构的等级，破坏乌克兰人获取可靠信息的途径，并散播对该国领导层的怀疑。

聚焦 COVID-19 和俄罗斯入侵乌克兰期间的影响力行动

接上页

在 Microsoft 于 2022 年 4 月发布的报告中，我们展示了俄罗斯如何在针对一家主流乌克兰媒体公司发起恶意软件攻击的当天，针对基辅的一座电视塔发动导弹攻击，这些行为的意图非常明显，就是控制基辅的信息环境。[12]

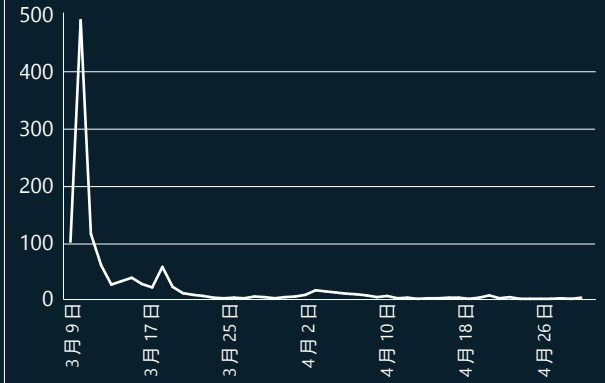
在说明网络攻击如何与影响力行动相结合的另一个示例中，一名俄罗斯威胁行为者向乌克兰市民发送了声称来自马里乌波尔居民的电子邮件，指责乌克兰政府对战争的升级，并呼吁他们的同胞反击政府。这些电子邮件专门（按姓名）发送给了接收电子邮件的人，并指出在之前的间谍活动相关网络攻击中他们的信息可能被盗了。但是没有提供恶意链接，这表明他们的意图就是纯粹的影响力行动。

展示声称已遭黑客入侵 / 已遭泄露内容或其他敏感材料是在影响力行动中俄罗斯行为者使用的常见策略。在整个乌克兰战争中，支持俄罗斯的社交媒体渠道一直宣传他们声称源自乌克兰的已遭泄露内容或其他敏感材料。支持俄罗斯的社交媒体渠道和媒体会在扩大影响力的战略中会使用已遭泄露内容或敏感材料，目的是降低对政府机构的信任，并引起对主流媒体言论的怀疑。这些信息可能会被操纵以针对乌克兰和西方发起宣传，降低对数字安全的信任，并削弱对西方援助乌克兰的支持声音。

俄罗斯利用其他信息攻击在现场事件发生后塑造公众舆论，以掩盖或颠倒事实。例如，3 月 7 日，俄罗斯通过向联合国 (UN) 提交的一份文件，事先申明了乌克兰马里乌波尔的一家妇产医院被清空并被用作军事基地。3 月 9 日，俄罗斯轰炸了这家医院。在爆炸事件的消息传出后，俄罗斯驻联合国代表 Dmitry Polyanskiy 在推特上发文称，对爆炸事件的报道是“假新闻”，并援引了俄罗斯早些时候有关医院已涉嫌用作军事基地的说法。随后，俄罗斯在自己控制的网站上大肆推送这一言论，并且在医院遭到袭击后持续了两周。

域及其流量

(2022 年 3 月 9 日至 2022 年 4 月 30 日)



宣传网站发布了关于妇产医院的故事，持续了大约两周，并于 2022 年 4 月 1 日开始短暂复苏。资料来源：Microsoft AI for Good Lab。

2022 年 2 月和 3 月马里乌波尔妇产医院的卫星图像

Microsoft 自己的卫星图像分析显示妇产医院遭到轰炸。第一张照片是 2022 年 2 月 24 日拍摄的，第二张照片是 2022 年 3 月 24 日拍摄的。照片来源：Planet Labs。

随着战争的进行，俄罗斯继续粉饰其暴行。例如，在 2022 年 6 月下旬，俄罗斯媒体和有影响力的人物发表言论，轰炸购物中心是正义行径并且是不得已而为之，谎称它不是用作购物中心，而是用作乌克兰领土边防军的军械库。[13] Telegram 上几个支持克里姆林宫的博主发布并大肆宣传这些内容以助推“虚假”言论，这些博主指出了涉嫌捏造的几点迹象，包括监控录像中有人穿着军装[14]以及录像中没有女性。[15] 俄罗斯依靠在外建立的宣传水军和媒体系统启动了这些活动。在网上大肆宣传这些报道使俄罗斯能够在国际舞台上推卸责任，并避免被问责。

像俄罗斯这样的国家明白以下这些做法的价值：利用从封闭来源获得的信息来影响公众看法，利用“黑客入侵和泄露”活动来传播对抗性言论和播撒不信任种子。

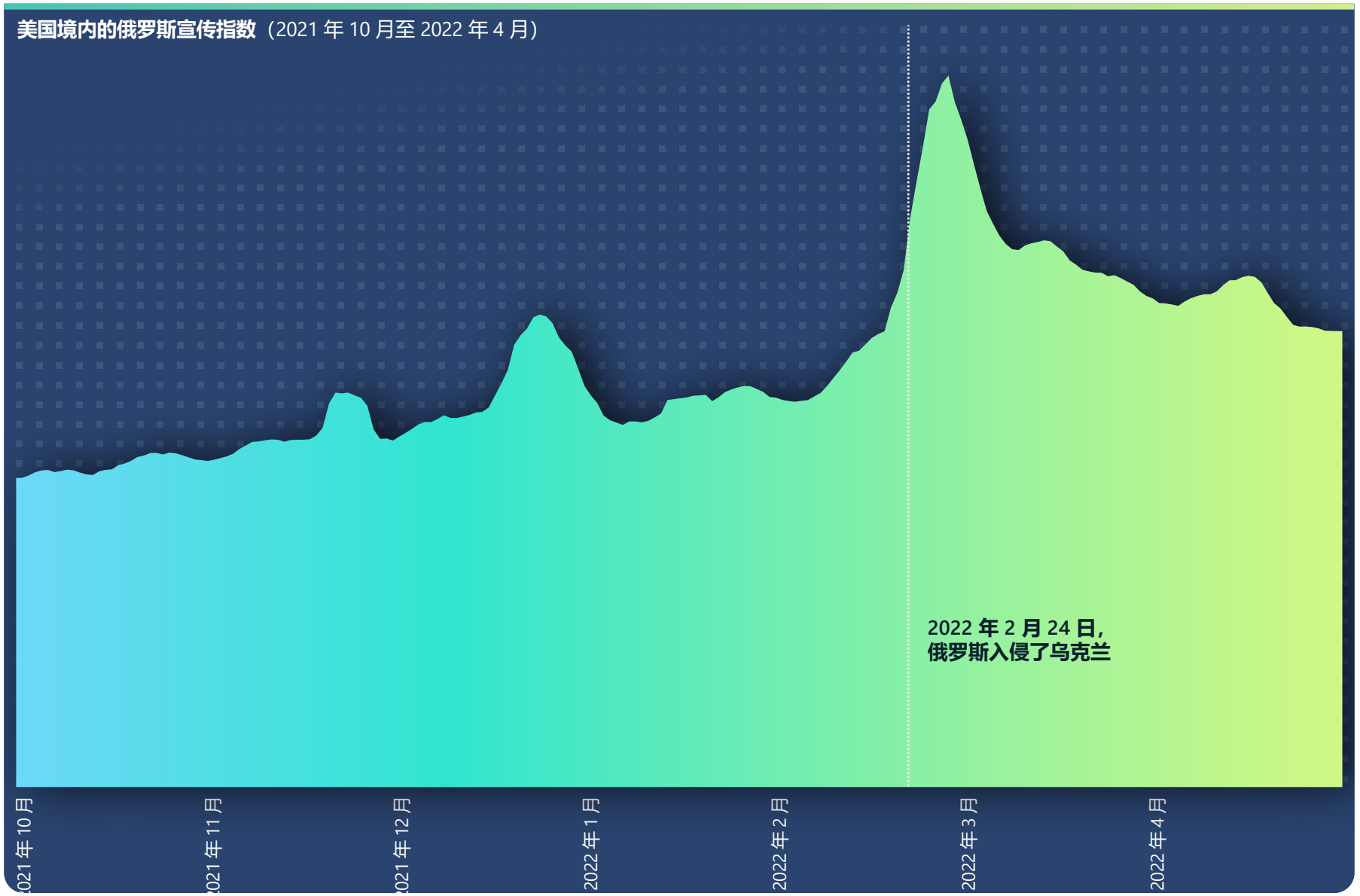
更多信息的链接

- 保卫乌克兰：网络战争早期阶段的经验教训 | Microsoft 对这些问题的看法
- 俄罗斯在乌克兰的网络攻击活动概述 | Microsoft 特别报告
- 破坏针对乌克兰的网络攻击 | Microsoft On the Issues

跟踪俄罗斯宣传指数

2022 年 1 月，近 1,000 个美国网站将流量引向了俄罗斯宣传网站。俄罗斯宣传网站上针对美国受众的最常见主题是乌克兰战争、美国国内政治（支持特朗普或支持拜登）和 COVID-19 及疫苗相关言论。

俄罗斯宣传指数 (RPI) 监控来自俄罗斯官方控制和支持的新闻媒体和大肆宣传媒介的新闻的传播情况，以在 Internet 上的全部新闻流量中所占的比例表示。RPI 可用于在准确的时间线上绘制俄罗斯宣传在 Internet 上和不同地理区域中的被关注情况图表。然而，Microsoft 注意到，我们只能观察俄罗斯发布到我们之前已发现的网站上的宣传。我们无法深入了解其他类型的网站上的宣传，包括权威新闻网站、未发现的网站和社交网络群组。



跟踪俄罗斯宣传指数

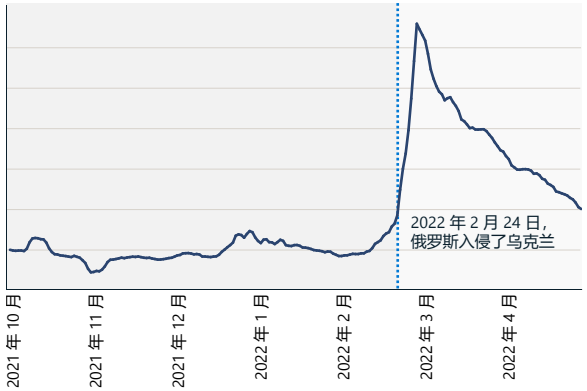
接上页

俄罗斯宣传指数：乌克兰

当乌克兰战争开始时，我们看到俄罗斯的宣传增加了 216%，在 3 月 2 日达到顶峰。下图显示了这种突增是如何与入侵同时发生的。两个图显示了入侵开始后，俄罗斯的宣传迅速激增。

RPI，乌克兰

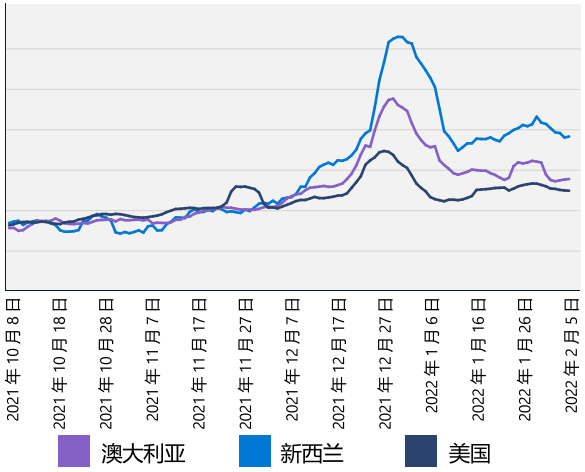
(2021 年 10 月 7 日至 2022 年 4 月 30 日)



俄罗斯宣传指数：新西兰与澳大利亚和美国

新西兰境内的 RPI 评估显示，2021 年末出现了与 COVID-19 宣传相关的峰值。俄罗斯宣传在新西兰境内被关注的峰值出现在 2022 年初惠灵顿公众抗议活动增加之前。第二次峰值显然与俄罗斯入侵乌克兰有关，超过了澳大利亚和美国的 RPI。

RPI，新西兰对澳大利亚和美国



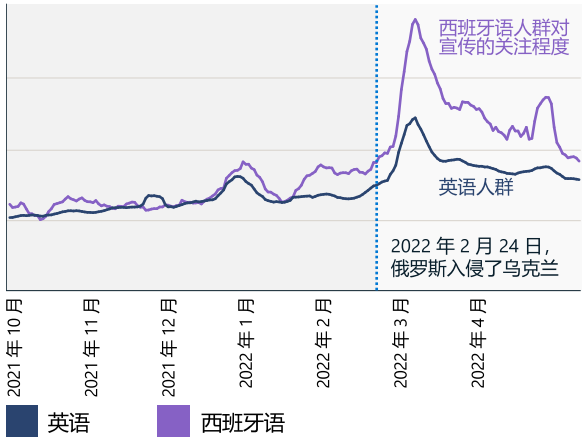
俄罗斯宣传在新西兰境内被关注的情况与在澳大利亚境内类似，都是直到 2021 年 12 月的第一周才得到广泛关注。进入 12 月之后，相对于在澳大利亚和美国境内被关注的情况，俄罗斯宣传在新西兰境内被关注的情况增长了超过 30%。

美国境内的俄罗斯宣传指数：英语和西班牙语

RPI 还跟踪以不同语言进行的宣传。多个媒体（包括 RT 和 Sputnik News）支持超过 20 种语言。其中包括英语、西班牙语、德语、法语、希腊语、意大利语、捷克语、波兰语、塞尔维亚语、拉脱维亚语、立陶宛语、摩尔达维亚语、白俄罗斯语、亚美尼亚语、奥塞梯语、格鲁吉亚语、阿塞拜疆语、阿拉伯语、土耳其语、波斯语和达里语。

下图显示，在美国境内西班牙语新闻的 RPI 比英语新闻高得多。

俄罗斯宣传在西班牙语人群中的被关注程度是英语人群的 2 倍



在美国境内，俄罗斯宣传在西班牙语人群中的被关注程度是英语人群的 2 倍。

俄罗斯在拉丁美洲的宣传力度很大

西班牙语 RT 是页面浏览量和 Facebook 粉丝数最多的国际新闻媒体。

来源：Microsoft AI for Good Research Lab

合成媒体

我们正在进入支持 AI 的媒体创建和操纵的黄金时代。Microsoft 分析师指出，这是由两个关键趋势推动的：用于人工创建高度逼真的合成图像、视频、音频和文本的易于使用的工具和服务的激增，以及快速传播针对特定受众优化的内容的能力。

这些发展本身本质上是没有问题的。基于 AI 的技术可用于创建趣味无穷且激动人心的数字内容，无论是创建纯粹的合成材料还是增强现有的材料。这些工具被企业广泛用于广告和传播材料，并被个人用于为其关注者创建引人入胜的内容。然而，合成媒体出于危害目的而创建和分发，可能会给个人、公司、机构和社会造成严重损害。Microsoft 一直积极推动在内部甚至范围更广的整个媒体生态系统中开发技术和实践来限制这种危害。

本节探讨了 Microsoft 通过对当前用于创建破坏性合成内容的先进技术、如果广泛传播此内容可能产生的危害以及可以防御基于合成媒体的网络威胁的技术缓解措施的分析所获得的见解。

创建合成媒体

合成文本和媒体领域正在迅速发展，因为以前只有依靠大型电影工作室的丰富计算资源才能实现的技术现在已经集成到手机应用中。同时，工具变得更加简单易用，并且可以生成逼真度甚至可以欺骗取证媒体专家的内容。我们快要达到这样的水平了，即不管是谁，都能够创建模仿任何人说话做事的合成视频。有人认为我们正在进入这样一个时代，即我们在网上看到的大量内容都是使用 AI 技术完全或部分合成的，这并非毫无道理。

> 随着更加先进、易于使用且应用广泛的工具的推出，合成内容的创建呈现出了上升趋势，并且很快就能达到以假乱真的程度。

高质量的免费和商业图像、视频和音频编辑工具有很多。这些工具可用于对数字内容进行简单但可能有损害性的更改，例如添加误导性文本、换脸以及删除或篡改上下文。这类“低级伪造”被广泛用于传播恶意内容、宣传政治思想和损害声誉。一个著名的例子是 2019 年[16] 众议院议长 Nancy Pelosi 的视频，视频中她口齿不清并且看起来醉醺醺的。虽然很快确定视频放慢了速度，但是在原始视频和情境浮出水面之前，“低级伪造”的视频已经四处传播。

更复杂的媒体内容篡改方法包括应用高级 AI 技术 (a) 创建纯粹的合成媒体，以及 (b) 对现有媒体进行更复杂的编辑。使用先进 AI 技术创建的合成媒体中通常会用到术语“深度伪造”，这个名字来源于有时使用的深度神经网络。这类技术正在作为独立应用、工具和服务被开发和集成到成熟的商业和开源编辑工具中。

此类技术被恶意行为者用作武器，目的是给个人和机构造成损坏。深度伪造技术的示例包括：

- **换脸（视频、图像）** - 将视频中的一张人脸换成另外一张人脸。此技术可能被用于尝试勒索个人、公司或机构，或者使个人陷入尴尬的境地或状况。
- **木偶操纵（视频、图像）** - 使用视频对静态图像或瞬时视频进行动画处理。这可以使其看起来像是一个人说了令人尴尬或容易造成误解的话。
- **生成式对抗网络（视频、图像）** - 一组用于生成逼真图像的技术。
- **变形器模型（视频、图像、文本）** - 基于文本描述中创建丰富的图像。

这类基于 AI 的先进技术在如今的网络影响力活动中尚未得到广泛应用，但是随着这些工具易用性的提升和普及程度的提高，我们预计这类问题会增加。

操纵合成媒体的影响

利用信息行动造成危害或扩大影响力并不新鲜。然而，信息传播的速度非常快，并且我们无法快速分辨事实和虚假信息，这意味着伪造和其他以合成手段生成的恶意媒体会造成更大的影响和危害，Pelosi 的例子就说明了这一点。

我们考虑了几类危害：操纵市场、支付欺诈、电话钓鱼、假冒、损害品牌、损害声誉和僵尸网络。上述许多类别都报告了大量真实示例，这可能会削弱我们分辨事实与虚假信息的能力。

如果我们不能再信任我们所看到和听到的，我们辨别是非的能力则会面临更加隐蔽的长期威胁。因此，公众人物或普通大众的任何质量有损的图像、音频或视频都可以被视为伪造，这一行为带来的后果称为“说谎者红利”。[17] 最近的研究[18] 表明，这一技术滥用行为已被用于攻击金融系统，尽管很多其他滥用场景是合理的。

合成媒体

接上页

检测合成媒体

各行各业、政府和学术界正在努力研究更好的方法来检测和减少合成媒体，并恢复信任。要实现这一目的，有几条很有前景的道路，此外还有需要考虑的障碍。

一种方法是构建能够发现伪造的基于 AI 的系统 - 本质上是用于对抗攻击性 AI 系统的防御性 AI 系统。这是一个十分活跃的研究领域，当前用于创建合成音频和视频的系统会留下明显的人工处理痕迹，它们可被训练有素的媒体取证分析师和自动化工具发现。

遗憾的是，虽然当前的赝品有可被发现的缺陷，但不易察觉的人工处理痕迹往往由特定工具或算法专门检测。这意味着有关已知伪造的训练通常不会推广到其他算法，在 2020 年公开赛中构建深度伪造图像检测器可以证明这一点。[19] 人们往往会加大投资来开发更先进的检测器，但 Microsoft 高度怀疑这能否带来有意义的改进，原因有两个：

首先，我们拥有反映真实世界的出色物理模型。当前的伪造内容创建者会走捷径，从而导致出现了可检测的人工处理痕迹，但是模型越新，逼真度越高。摄像机拍摄的真实世界的场景并没有什么内在的特别之处，计算机无法对此进行建模。

其次，高级伪造内容创建算法会在创建过程中使用一种称为生成性对抗网络 (GAN) 的技术。GAN 运行两个相互对抗的 AI 系统，它们使用生成器创建伪造内容并使用鉴别器检测伪造图像并训练生成器。投资开发更好的检测器只会导致生成器提高伪造质量。

合成媒体

接上页

数字资产溯源

如果检测伪造不可靠，可以做些什么来防范将合成媒体用于有危害性的用途？一种重要的新兴技术是数字溯源 - 这种机制使数字媒体创建者能够对资产进行认证，并帮助消费者识别数字资产是否遭到篡改。在当今社交媒体网络环境中，数字溯源特别重要，因为内容在 Internet 上的传播速度极快，而恶意行为者有机会轻而易举地操纵内容。

数字溯源技术是加密文档签名的现代版本，设计用于在对象于如今的 Web 中传输时捕获对象的来源、编辑历史记录和元数据。用于实现这种端到端媒体防篡改认证的愿景和技术方法是跨团队的 Microsoft 研究人员和科学家研究出来的。我们在项目来源（由 Microsoft、BBC、CBC/Radio-Canada 和 New York Times 创立）中共同领导了跨行业的合作，目的是将媒体溯源技术变成现实，并且参与了内容真实性计划（由 Adobe 创立）。Microsoft 还与技术和媒体服务领域的合作伙伴共同建立了内容溯源和真实性联盟 (C2PA)。C2PA 是一个标准组织，最近发布了最先进的数字溯源规范，可用于图像、视频、音频和文本等媒体资产。

支持 C2PA 的对象具有一个清单，用于保护对象和元数据免遭篡改，并且附带的证书用于标识发布者。

合成媒体最初的设计目的不是制造危害，但是恶意行为者却使用它来削弱对个人和机构的信任。

数字溯源是有前景的新兴技术，它有可能通过认证媒体资产的来源来帮助恢复人们对在线媒体内容的信任。

基于 C2PA 规范的公开发布解决方案正在涌现，可能是以现有产品的新功能形式，也可能是以新的独立应用和服务形式。我们预计大多数常用的捕获、编辑和创作工具在几年后都将支持 C2PA。这使企业有机会确定他们如今对于数字溯源的需求和使用情况，并要求在现有工作流所用的工具中额外增加这层保护。

切实可行的见解

1. 采取主动措施，通过主动考虑 PR 和通讯回应，保护组织免受虚假信息威胁。
2. 使用溯源技术来保护官方通讯内容。

更多信息的链接

- 在虚假信息方面迈出有前景的一步 | Microsoft On the Issues
- 里程碑的到来，2022 年 1 月 31 日
- 项目来源 | Microsoft ALT 创新
- 内容来源和真实性联盟 (C2PA)
- 探索有关将系统“项目来源”用于媒体身份验证的技术详细信息 | Microsoft ALT 创新

900%

自 2019 年以来，深度伪造现象逐年增加。[20]

防范网络影响力行动的整体方法

Microsoft 正在其已经成熟的网络威胁情报基础结构的基础上，开发更广泛、更具包容性的网络影响力行动的视图。

我们借助于提供建议的响应和缓解策略框架来应对这类行动带来的威胁，该框架可分为四个关键支柱：检测、干扰、防御和阻止。

此外，为了划定我们在这一领域的工作，Microsoft 采取了四项原则。第一，承诺尊重言论自由，并维护客户通过我们的平台、产品和服务创建、发布和搜索信息的权利。第二，我们积极主动地防止我们的平台和产品被用于大肆宣传国外网络影响力网站和内容。第三，我们不会在知情的情况下通过国外网络影响力内容或行为者获利。最后，我们会在我们的产品中利用内部数据和可信的第三方数据来确定显示内容的优先顺序，对抗国外网络影响力行动。

检测

与网络防御一样，对抗国外网络影响力行动的第一步是提高检测能力。任何一家公司或组织都不要指望依靠单打独斗就能取得所需的进展。跨技术部门开展更广泛的新型协作至关重要，因为分析和报告网络影响力行动的进展在很大程度上依赖于民间团体（包括学术机构和非营利组织）的作用。

认识到它们的作用后，普林斯顿大学的研究人员 Jake Shapiro 和 Alicia Wanless 以及卡内基国际和平基金会分别制定了相应计划以启动新的“信息环境研究机构”(IRIE)。在 Microsoft、奈特基金会和克雷格·纽马克慈善基金会的支持下，IRIE 将建立一个以欧洲核研究组织 (CERN) 为蓝本的包容性多方利益相关者研究机构。它将数据处理和分析方面的专业知识相结合，以加快和扩展这一领域的新发现。它会分享研究结果，为决策者、科技公司和消费者提供更加广泛的信息支持。

防御

第二个战略支柱是加强民主防御，这是一项长期的重点工作，需要投入资金和进行创新。它应该考虑技术给民主带来的挑战，以及技术为更有效地捍卫民主社会创造的机会。

Microsoft 的战略框架旨在帮助跨部门的利益相关者检测、干扰、防御和阻止宣传，尤其是国外侵略者的活动。

我们应该首先了解一下我们这个时代面临的一项重大技术挑战 - Internet 和数字广告对传统新闻业造成的影响。自 18 世纪以来，自由和独立媒体在为全球各个民主国家提供支持方面发挥了特殊的作用 - 揭露腐败、记录战争和阐明当代和其他时代面临的最大社会挑战。然而，Internet 吞噬了广告收入并抢走了付费用户，从而给当地新闻造成了致命打击。许多当地报纸倒闭了。从我们近期的工作成果中得出的众多见解之一是，缺少报纸的城镇会在不知不觉中不可避免地接触国外宣传，而且接触程度高于平均水平。出于这些原因，关于民主的一项重要防御举措是必须加强传统新闻业和自由媒体，特别是在地方上。这需要持续投资和创新，创新必须反映不同国家 / 地区和大陆的当地需求。这些问题并不容易解决，需要采用涉及多方利益相关者的方法，Microsoft 和其他科技公司越来越支持这种方法。

我们还需要在公共政策方面引入新的创新，这需要成为公共领域的一项重点工作。这可能包括使出版商能够与技术公司共同洽谈广告收入的法律，以及为当地新闻室免除其所雇新闻工作者的部分工资税的税收抵免立法。新闻工作者需要许多其他工具以提升他们的技能，包括能够区分来自合法来源和欺诈来源的内容。

还有一项快速变化的需求，即帮助消费者培养更高能力以识别国家推动的信息行动。虽然这可能看起来非常棘手，但是它与技术部门为了应对其他网络威胁长期以来所追求的工作目标类似。可以考虑指导消费者更仔细地查看电子邮件地址，以帮助发现垃圾邮件或其他欺诈性通讯。美国推出的一些计划（例如新闻素养项目和可信新闻计划）

如果我们不能再信任我们所看到和听到的，我们辨别是非的能力则会面临更加隐蔽的长期威胁。

防范网络影响力行动的整体方法

接上页

将帮助培养更有判断力的新闻和信息消费者。在全球范围内，来自 NewsGuard 的浏览器插件等新技术可以帮助更快地推动这项工作。

这也提醒我们，民主的基础涉及公民教育。这项工作一如既往需要从学校抓起。但是我们生活的世界要求我们在一生当中不断接受公民教育。全新的“工作中的公民素养”(Civics at Work) 承诺书由战略与国际研究中心主导，Microsoft 是首个签署方和合作伙伴，它的目的是在企业社区内重新唤醒公民素养。这是一个很好的示例，说明了广泛存在的加强民主防御的机会。

干扰

近年来，Microsoft 的数字犯罪部门 (DCU) 改进了策略并开发了工具以干扰网络威胁，从勒索软件到僵尸网络和国家层面的攻击都涵盖在内。我们获得了许多重要的经验教训，首先是在对抗广泛的网络攻击中积极干扰所起的作用。

当我们考虑对抗网络影响力行动时，干扰可能会发挥着更重要的作用，而干扰的最佳方法越来越明朗。各种欺骗的最有效解决方法是实现公开透明。这就是为什么 Microsoft 通过收购 Miburo Solutions 来提高其检测和干扰国家影响力行动的能力，Miburo Solutions 是一家专门检测和响应国外网络影响力行动的领先网络威胁分析和研究公司。

我们的经验表明，政府、科技公司和非政府组织应在有充分证据的情况下慎重对网络攻击进行归因。了解干扰攻击的影响至关重要，并且在干扰网络影响力方面可能更有帮助。我们目睹了美国政府在俄罗斯入侵乌克兰前夕分享信息，这将实现公开透明纳入了有效行动 - 例如公开俄罗斯计划，包括密谋使用伪造图形视频等具体活动。

去年夏季日内瓦网络和平研究院发布了关于乌克兰内外持续遭受的网络攻击的出版物，根据其中所述，各种民间团体和私营组织有机会提高与网络影响力行动有关的公开透明度。关于新发现和有据可查的行动的可靠报告可以帮助公众更好地评估所读、所看和所听的内容，尤其是在 Internet 上。为此，Microsoft 将改进并扩展现有网络报告，并将发布与网络影响力行动研究成果有关的全新报告、数据和更新，包括归因陈述（如果适用）。

我们将发布年度报告，这份报告使用数据驱动的方法来了解整个公司内普遍存在的国外信息行动以及确保逐步改进的后续步骤。我们还将考虑在保证公开透明的基础上采取的其他步骤。

例如，数字广告的作用尤其重要，因为广告可以帮助为国外行动筹措资金，同时使国外支持的宣传网站看起来合法。我们需要尽更大努力来破坏这些资金流动。

阻止

最后，如果不用为违反国际规则负责，我们不能指望国家改变行为。强制执行这种问责制是政府的专属责任。然而，多方利益相关者行动在加强和扩展国际规范方面发挥着越来越重要的作用。包括 Microsoft 在内的 30 多个在线平台、广告商和出版商签署了最近更新的“欧洲委员会虚假信息行为守则”，同意进一步承诺以应对这一日益严峻的挑战。与最近的“巴黎倡议”(Paris Call)、“基督城倡议”(Christchurch Call) 和“未来 Internet 宣言”(Declaration on the Future of the Internet) 一样，多边和多方利益相关者行动可以将民主国家的政府和公众团结在一起。然后，政府可以在这些规范和法律的基础上，推进全球民主国家需要和值得推行的问责制。

通过从根本上快速实现公开透明，民主政府和社会可通过对国家层面的攻击来源进行归因，告知公众和建立对机构的信任，有效地削弱影响力行动。

我们提高了检测和干扰国外影响力行动的技术能力，并致力于透明地报告这些行动，就像我们报告网络攻击一样。

切实可行的见解

1. 在整个组织中实施强有力的数字安全机制。
2. 考虑如何减少员工或业务实践在无意中支持网络影响力活动的情况。这包括减少给已知国外宣传网站的供给。
3. 支持信息素养提升和公民参与活动，这是帮助社会抵御宣传和国外影响力的关键举措。
4. 直接与所在行业的相关团体沟通，设法应对影响力行动。

尾注

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. 保卫乌克兰：网络战争早期阶段的经验教训（microsoft.com）
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. 俄罗斯外交部发言人 Maria Zakharova：https://tass.com/politics/1401777Lavrovhttps://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. Russia’ s Kremenchuk Claims Versus the Evidence - bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. 事实核查：“醉酒的”南希 · 佩洛西（Nancy Pelosi）的视频是被篡改的 | 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. 深度伪造检测挑战结果：促进 AI 发展的开放倡议（facebook.com）
20. Deepfakes 2020: The Tipping Point，Johannes Tammekänd、John Thomas 和 Kristjan Peterson，2020 年 10 月

网络复原能力

了解现代化的风险和回报对于通过整体方法实现复原能力至关重要。

网络复原能力概述 87
引言 88
网络复原能力：互联社会的关键基础 89
实现系统和架构现代化的重要性 90
基本安全状况是高级解决方案有效性的决定性因素 92
保持身份健康是组织健康运作的基础 93
操作系统默认安全设置 96
软件供应链的集中性 97
建立针对新兴 DDoS、Web 应用程序和网络攻击的复原能力 98
开发平衡的数据安全方法和网络复原能力 101
针对网络影响力行动的复原能力：人文层面 102
通过技能强化人为因素 103
来自我们的勒索软件消除计划的见解 104
立即就量子安全问题采取行动 105
整合业务、安全性和 IT 资源以提高复原能力 106
网络复原能力钟形曲线 108

网络复原能力

概述

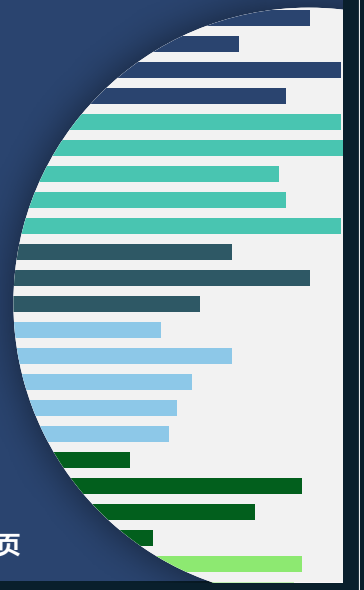
安全性是技术成功的关键推动因素。创新和提高工作效率只能通过引入使组织能够尽可能弹性抵御现代攻击的安全措施来实现。

疫情大流行迫使我们调整安全实践和技术，以保护 Microsoft 的员工，无论他们在哪里工作。去年，威胁行为者继续利用在疫情期间以及向混合工作环境转变期间暴露的漏洞。从那时起，我们面临的主要挑战便一直是应对各种普遍且复杂的攻击方法以及加剧的国家层面活动。

有效的网络复原能力需要通过一种适应性强的整体方法，来抵御核心服务和基础结构面临的不断演变的威胁。

详情请参见第 89 页

现代化的系统和架构对于应对超互联世界中的威胁至关重要。

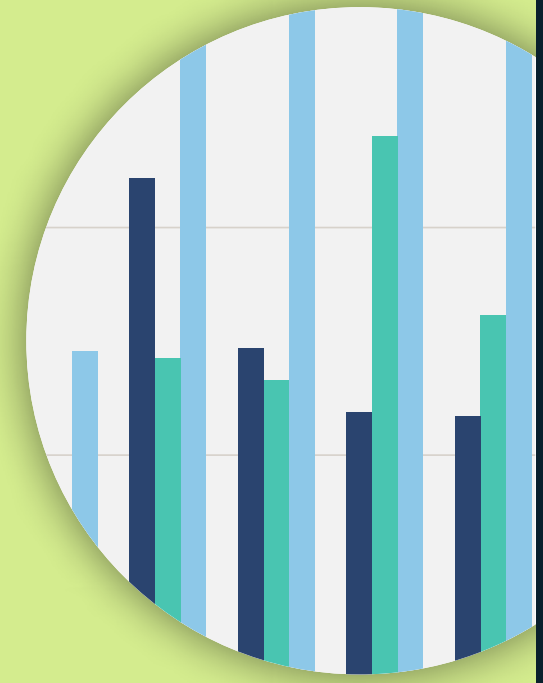


详情请参见第 90 页

基本安全状况是高级解决方案有效性的决定性因素

详情请参见第 92 页

虽然基于密码的攻击仍然是身份泄露的主要根源，但其他类型的攻击也在涌现。



详情请参见第 93 页

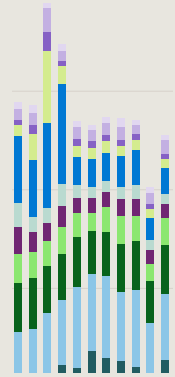
网络影响力行动的复原能力的人文层面是我们的协作和合作能力。

详情请参见第 102 页

绝大多数成功的网络攻击可以使用基本安全机制来防范。

详情请参见第 108 页

在过去的一年里，全球发生的 DDoS 活动在数量、复杂性和频率上都是前所未有的。



详情请参见第 98 页

引言

疫情大流行迫使我们调整安全实践和技术，以保护 Microsoft 的员工，无论他们在哪里工作。去年，威胁行为者继续利用在疫情期间以及向混合工作环境转变期间暴露的漏洞。从那时起，我们面临的主要挑战便一直是应对各种普遍且复杂的攻击方法以及加剧的国家层面活动。

数字威胁活动和网络攻击的复杂程度每天都在增加。如今许多复杂的攻击都侧重于入侵身份体系结构、供应链和第三方，虽然它们在不同程度上实施了安全控制措施。特别是，我们观察到身份网络钓鱼攻击是当下存在的一种显而易见的威胁。但是，如果身份管理、网络钓鱼控制和终结点管理实践得当，这类攻击通常不会成功。因此，我们必须牢记基本原则：通过实施基本安全控制措施，就可以阻止 98% 的攻击。在 Microsoft，我们将身份和设备作为零信任方法的一部分进行管理，这种方法包括最小特权访问和防网络钓鱼凭据，以有效阻止威胁行为者并保护我们的数据。

如今，即使是没有掌握先进技术技能的威胁行为者也可以发起难以置信的破坏性攻击，因为在网络犯罪经济中访问高级策略、技术和程序已得到广泛普及。乌克兰战争展示了国家层面的行为者如何通过更多地使用勒索软件来升级其攻击性网络行动。勒索软件现在是一个复杂的行业，威胁行为者使用双重或三重勒索策略来索取赎金，并且开发人员提供勒索软件即服务 (RaaS)。借助 RaaS，威胁行为者可以利用联盟网络进行攻击，从而降低了技术水平不高的网络犯罪分子的进入门槛，最终扩大了攻击者群体。

因此，Microsoft 设计了勒索软件消除计划。这个计划的目的是弥补控制措施和覆盖范围方面的不足，帮助增强服务的功能，并为安全运营中心和工程团队编写在发生勒索软件攻击时可以参考的恢复行动手册。

最近的供应链和第三方供应商攻击表明，这个行业出现了一个重要转折点。这些攻击对客户、合作伙伴、政府和 Microsoft 造成的破坏日益严重，这说明了重点关注网络复原能力和安全利益相关者之间开展协作的重要性。攻击者还将本地系统作为目标，这增强了组织的以下需求：通过对基础结构进行现代化改造并将其迁移到具备更强大安全功能的云中来管理旧系统带来的漏洞。

在我们生活的这个时代，安全性是技术成功的关键推动因素。创新和提高工作效率只能通过引入使组织能够尽可能弹性抵御现代攻击的安全措施来实现。随着数字威胁的增加和演变，在每个组织的结构中建立网络复原能力至关重要。

Bret Arsenault
首席信息安全官

网络复原能力：互联社会的关键基础

数字技术革命见证了组织的转型，他们在运营方式和提供的服务的方式上变得更加互联。随着网络环境中面临的威胁增加，在组织的结构中建立网络复原能力与建立财务和运营复原能力同样重要。

数字转型彻底改变了组织与客户、合作伙伴、员工和其他利益相关者互动的方式。新技术为人员互动、改造产品和优化运营带来了巨大的机会。疫情大流行通过推动使人们能够以全新方式在任何地方进行协作的创新技术，加速了数字转型。

随着网络威胁愈演愈烈，在“始终互联”的世界中阻止威胁入侵组织变得更加困难。网络复原能力是指组织即使遭受无休止的攻击，仍能继续正常运营并保持加速增长的能力。必须在防护与生存和恢复能力之间取得平衡，政府和企业正在开发能够延伸到安全和隐私之外的全面模型以作为网络复原能力的一部分，目的是保护资产、数据和其他资源。

开发用于实现网络复原能力的整体方法

网络复原能力需要一种适应性强的全局性整体方法，这种方法应该能够抵御核心服务和基础结构面临的不断演变的威胁，包括：

- 网络复原能力钟形曲线中描述的基本网络卫生
- 了解和管理数字转型风险 / 回报之间的权衡。
- 实时响应功能，可实现主动检测威胁和漏洞。
- 抵御已知攻击以及针对新型和预期攻击途径的预防性活动，包括自动补救能力。
- 通过故障隔离和细分降低攻击和灾难带来的影响。
- 发生中断时的自动恢复和冗余。
- 优先进行运营测试以发现不足，并了解共同责任和对于外部资源（如基于云的安全解决方案）的依赖。

有效的网络复原能力计划从获知资源基本信息开始，例如了解可用的服务并准备在发生中断时可调用的可靠资源目录。在此基础上，这项计划必须能够评估自身的有效性，衡量关键服务及其依赖项的性能，测试和验证本地和云服务的功能，并在整个组织的数字生命周期中为持续改进提供建议。

为了提供整体方法，我们与不同组织合作，以确定最关键的本地和在线服务、业务流程、依赖项、人员、供应商和提供商。我们还希望确定与客户和市场期望、法规和合同义务以及内部运营关联的资产和资源。在确定这些关键资源时，同时处理的工作应该包括检测和监控威胁、中断、潜在攻击途径以及系统和流程漏洞。要在当前技能不足的情况下做到这一点，需要根据对组织造成的总体风险来严格确定优先顺序。

在威胁形势不断演变的背景下，这种整体方法需要具备适应性，目标是提升可衡量的性能，缩短检测、响应和恢复时间，并在发生中断时缩小影响半径。这种方法还必须认识到威胁之间的联系日益紧密。例如，安全事件可能会导致数据泄露，从而影响隐私，这需要许多内部和外部团队通力合作以快速做出响应并最大限度地降低影响。

网络复原能力是指即使发生中断（包括遇到网络攻击），企业仍能继续正常运营并保持加速增长的能力。

切实可行的见解

1. 构建和管理用于限制入侵影响的技术系统，并使其在入侵成功时仍能继续安全有效地运行。关注常见的关键资产、支持敏捷性、构建适应性（例如，混合和多云、多平台）、减少攻击面（例如，删除未使用的应用程序和过度预配的访问权限）、假定资源遭到入侵，并预见攻击者的演变。
2. 在规划数字项目时，考虑潜在的威胁和机会，并共同承担跨数字技术供应链（包括基于云的安全解决方案）实现复原能力的责任。
3. 构建系统以嵌入安全设计，并采取相应步骤以预测、检测、抵御、适应和响应未来不断演变的威胁。
4. 确保企业领导者在必要时咨询安全团队，以了解与新开发内容关联的风险。同样地，安全团队应考虑业务目标，并就如何安全地实现目标为领导者提供建议。
5. 确保针对网络事件实施了明确的运营实践和程序以实现组织复原能力。

实现系统和架构现代化的重要性

为超互联世界开发新功能时，我们必须管理旧系统和软件带来的威胁。

旧系统是指在智能手机、平板电脑和云服务等现代连接工具成为常态之前开发的系统，对于仍在使用它们的组织来说，它们是一种风险。Microsoft 事件响应安全服务团队的调查结果强化了这种风险的暴露，该团队由一群安全专家组成，可帮助客户对攻击做出响应并从攻击中恢复。

在过去一年里，在从攻击中恢复的客户中间发现的问题与六个类别相关，如本页中的图表所示。下一页概述了为提高复原能力，可采取的可行步骤。

超过 80% 的安全事件可以追溯到几个缺失的要素，这些可以通过现代安全方法来解决。

影响网络复原能力的关键问题

这个图表显示了因缺少对于提高组织网络复原能力至关重要的基本安全控制措施而受影响的客户百分比。研究结果基于过去一年 Microsoft 参与的各项研究。

“领导者应将网络复原能力视为业务复原能力的关键方面。他们应该像对待自然灾害或其他不可预见的事件那样制定应对网络中断的计划，并将内部利益相关者（如运营、通讯、法律团队）聚集在一起以制定战略。这样做有助于确保组织尽快使其关键业务系统恢复联机状态，恢复正常的业务运营。

但仅仅这样是不够的。由于许多组织依赖于第三方供应商和服务提供商，因此领导者应将网络复原能力规划扩展到其端到端价值链，进一步确保业务连续性和复原能力。”

Ann Johnson
安全性、合规性、身份和管理业务发展部门
公司副总裁

实现系统和架构现代化的重要性

接上页

明确地说，组织可以解决以下几个方面的问题，以采用现代化方法并抵御威胁：

问题	可行步骤
标识提供者的配置不安全 配置错误和暴露的身份平台及其组件是未经授权获得高特权访问权限的常见途径。	在部署和维护身份系统（如 AD 和 Azure AD 基础结构）时，遵循安全配置基准和最佳实践。 通过强制执行特权分离、最小特权访问以及利用特权访问工作站（PAW）管理身份系统来实施访问限制。
特权访问和横向移动控制力度不足 管理员在整个数字环境中拥有过多的权限，并且经常在面临 Internet 和工作效率风险的工作站上公开管理凭据。	保护和限制管理访问权限，以使环境更具复原能力并限制攻击范围。采用特权访问管理控制机制，如实时访问和最低管理权限。
未启用多种身份验证 (MFA) 如今的攻击者不是强行闯入的，而是正常登录的。	MFA 是一项关键的基本用户访问控制措施，所有组织都应启用。MFA 与条件访问相结合，可以在抵御网络威胁方面发挥重大价值。
成熟度低的安全运营 受影响最严重的组织使用传统的威胁检测工具，并且没有及时做出响应和补救方面的相关见解。	全面的威胁检测战略要求在扩展检测和响应 (XDR) 以及使用机器学习分离噪声与信号的现代云原生工具方面进行投资。通过整合可以在整个数字环境中提供深入安全见解的 XDR，实现安全运营工具的现代化。
缺少信息保护控制措施 组织仍在继续努力整合全面的信息保护控制措施，这些控制措施全面覆盖所有数据位置，能够在整个信息生命周期中保持有效，并且契合数据的业务关键性。	确定关键业务数据及其位置。审查信息生命周期流程并强制实施数据保护，同时确保业务连续性。
采用的现代安全框架有限 身份是新的安全边界，允许访问不同的数字服务和计算环境。通过将零信任原则、应用程序安全措施和其他现代网络框架整合在一起，组织能够主动管理以其他方式难以设想的风险。	零信任框架强制实施最低特权、显式验证所有访问和始终假定入侵的概念。组织还应在开发运营（DevOps）和应用程序生命周期流程中实施安全控制措施和实践，以提高业务系统中的保证级别。

基本安全状况是高级解决方案有效性的决定性因素

通过分析，我们发现了组织防御中普遍存在的常见盲点，借助这些盲点，即使存在高级安全解决方案，攻击者也能获得初始访问权限、找到立足之地和实施攻击。

在许多情况下，网络攻击的结果在攻击开始早已确定。攻击者利用易受攻击的环境获取初始访问权限、进行监视，并通过横向移动和加密或外泄造成严重破坏。在早期阶段阻止攻击者大大增加了降低总体影响的机会。

Microsoft 研究了各种安全状况中的特定配置，以确定这些环境的实际实践中存在的最常见缺陷。这使我们能够发现在人工勒索软件攻击期间利用的最常见漏洞，这些漏洞使威胁行为者能够获取访问权限并在网络中四处探访而不被发现。

必须开启基本安全配置

对于攻击者来说，组织内未注册或已过时（与漏洞和安全代理状态相关）的设备是潜在入口点和用于建立访问的路线。我们发现，在确保在更新的端点检测和响应[1] (EDR) 和端点保护平台[2] (EPP) 解决方案注册设备是重要的一步，但是这并不能保证会阻止勒索软件。

高级解决方案（如 EDR 和 EPP）对于在攻击流中及早检测攻击者并实现自动补救和保护至关重要。但是，由于这些高级解决方案依赖于基本的攻击检测功能，因此需要开启基本安全配置。事实上，我们观察到以下情况普遍存在：虽然实施了高级解决方案，但由于缺少基本安全配置而导致功能大打折扣。

安全配置方面的最佳实践比安全运营中心 (SOC) 分析师响应时间更能体现复原能力

我们观察到，在我们的客户和合作伙伴群体中，六个月内，SOC 分析师查看并处理相关警报所需的时间缩短了 70%。认识有所提高是好的迹象。然而，虽然安全配置可见性提高了 SOC 分析师的绩效，但是通过注册和更新组织设备来实现产品可见性是成功防护的更准确预示因素。

未知设备带来的风险

在云网络中客户知道哪些资产在哪些操作系统上运行，而本地网络可能包含各种不受组织监控或管理的设备，如 IoT、桌面、服务器和网络设备。

企业网络中不受 EDR 代理保护且可以访问企业资源甚至高价值资产的互联设备平均超过 3,500 台。Microsoft Defender for Endpoint (MDE) 使用网络检查来发现设备，并提供这些联网设备的相关设备分类信息，如设备名称、操作系统分发版本和设备类型。

3,500

企业中不受终结点检测和响应代理保护的连接设备的平均数量。

对于不受 EDR 代理支持的设备，至少要知道它们的存在，并且通过评估漏洞和限制网络访问来设法保护它们。

切实可行的见解

1. 如果缺少基本安全配置，甚至可能导致高级解决方案的功能大打折扣。
2. 在安全状况配置的最佳实践方面进行投资，以抵御未来的攻击。这些基本设置可以在组织抵御攻击的能力方面产生巨大的投资回报。
3. 将所有适用的设备都注册到 EDR 解决方案中。
4. 确保更新安全代理并防止篡改，以更全面地了解产品并更充分地发挥产品的保护优势。

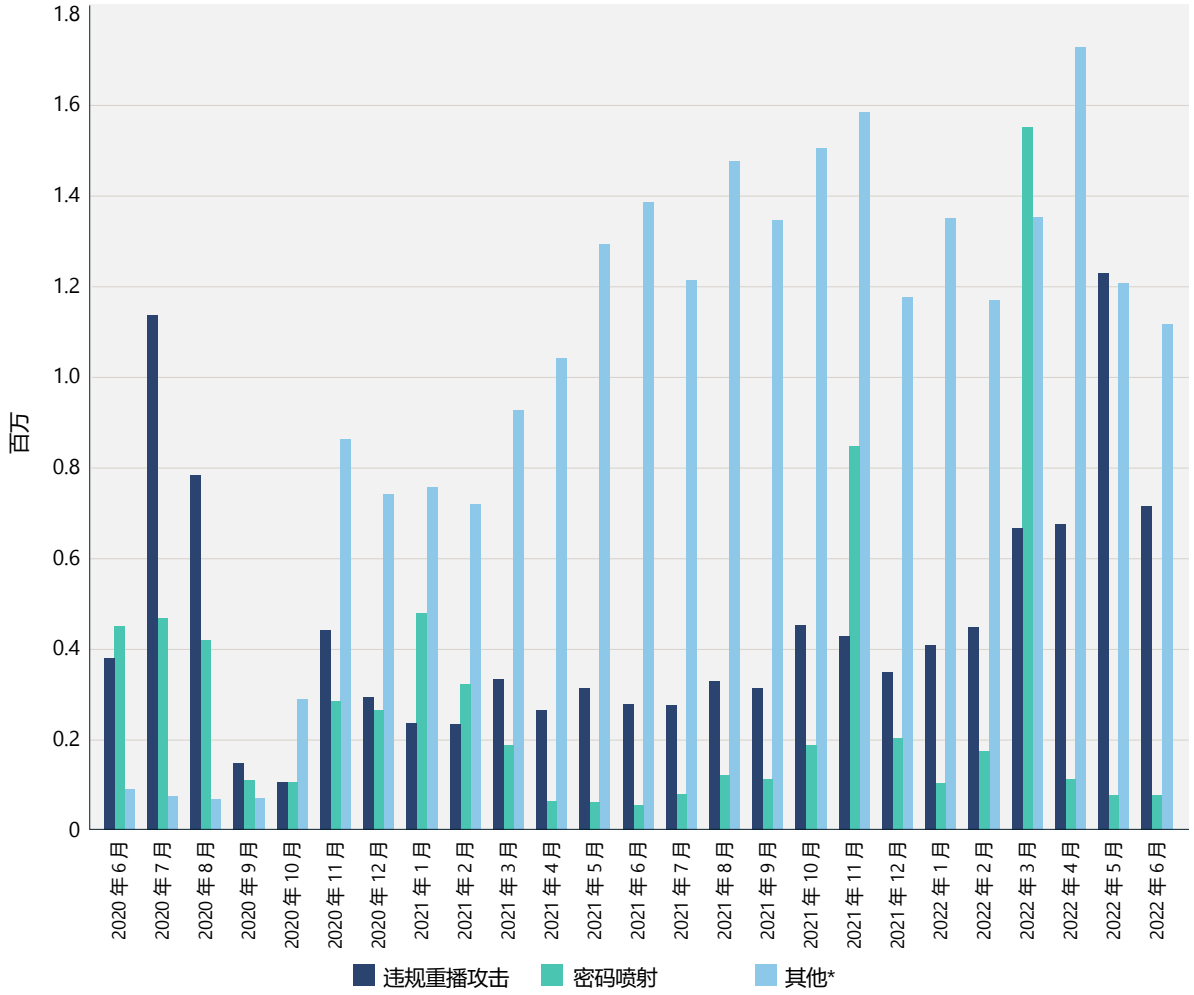
保持身份健康是组织健康运作的基础

保护身份比以往任何时候都更加重要。虽然基于密码的攻击仍然是身份泄露的主要根源，但其他类型的攻击也在涌现。相对于以前普遍存在的密码喷射和漏洞重放，复杂攻击的数量仍在增加。

基于密码的攻击仍很常见，在被攻击者通过这些方法入侵的帐户中，超过 90% 的帐户没有通过强身份验证进行保护。强身份验证使用多个身份验证因素，例如密码 + 短信和 FIDO2 安全密钥。

我们看到，有针对性的密码喷射攻击呈上升趋势，当攻击者流量达到巨大峰值时波及范围可达数千 IP 地址。

遭到入侵的用户（按攻击类别显示）



每个月遭到入侵的用户（按攻击类别显示）。密码喷射攻击量波动很大，如 2021 年 11 月和 2022 年 3 月的峰值所示。这些峰值表示数千用户和数千 IP 地址被攻击。*“其他”表示除密码喷射和违规重播之外的攻击，包括网络钓鱼、恶意软件、中间人攻击、本地令牌颁发者入侵和其他攻击。来源：Azure AD 标识保护。

4,500

在阅读本陈述的时间里，我们已经抵御了 4,500 次密码攻击。

保持身份健康是组织健康运作的基础

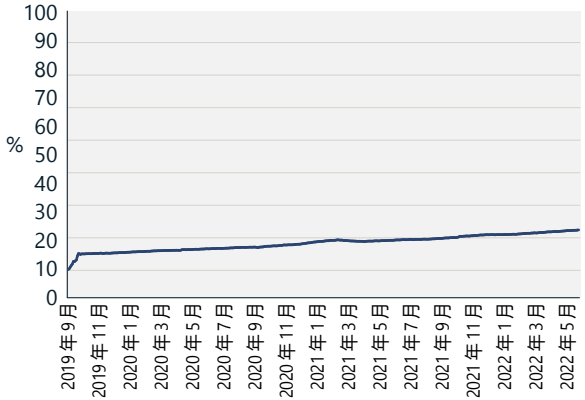
接上页

采用强身份验证

从积极的方面来看，我们看到在 Azure Active Directory (Azure AD) 企业客户群中，强身份验证的采用率稳步增长。对于 Azure AD，去年，强身份验证的月度活跃用户 (MAU) 从 19% 增长到了 26%，而管理帐户的强身份验证 MAU 从 30% 增长到了大约 33%。

这是良好发展趋势，但仍然需要显著增长，才能实现强身份验证覆盖大多数用户；尚未在环境中使用强身份验证的客户应开始规划和部署强身份验证，以保护其用户。[3] 在设计强身份验证部署时，应考虑无密码身份验证，因为它可以提供最安全的使用体验，消除了密码攻击风险。

强身份验证的使用情况
(2019 年 9 月至 2022 年 5 月)

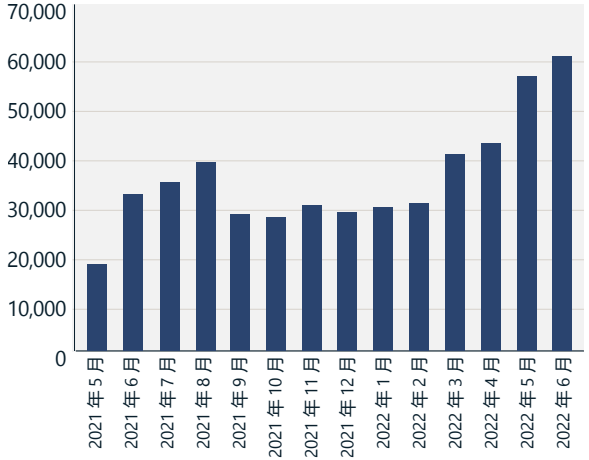


虽然自 2019 年以来，强身份验证的使用量增加了一倍，但只有 26% 的用户和 33% 的管理员在使用强身份验证。来源：Azure Active Directory。

令牌重播攻击稳步上升

2022 年，其他形式的攻击所占比例有所增加。我们看到有针对性的攻击有所增加，这些攻击会专门避开基于密码的身份验证，以降低被检测到的几率。这些攻击会利用通过恶意软件、网络钓鱼和其他方法获得的浏览器单一登录 (SSO) Cookie 或刷新令牌。在某些情况下，攻击者会选择目标用户所在地理位置附近的基础结构，以进一步降低被检测到的几率。我们看到令牌重播攻击稳步增长，Azure AD 标识保护每月检测到的攻击次数超过 40,000 次。令牌重播是指颁发给合法用户的令牌被拥有相应令牌的攻击者使用。令牌通常通过恶意软件获得，例如通过从用户浏览器中窃取 Cookie 或通过高级网络钓鱼方法。

检测到的令牌重播攻击数量



每月检测到的令牌重播攻击数量。来源：Azure AD 标识保护，由异常令牌检测标记的唯一会话。

保持身份健康是组织健康运作的基础

接上页

提取令牌

攻击者不仅需要恶意软件，还需要凭据来实现其目标。事实上，全部人为操作的勒索软件攻击都涉及被盗凭据。许多复杂的入侵都涉及从暗网购买的凭据，这些凭据最初是由并不复杂且广泛分发的凭据盗窃恶意软件盗取的。这类恶意软件已发展为窃取令牌，包括会话信息和 MFA 声明。这意味着，用户登录到公司资产时所用的家庭系统一旦受到感染，可能会导致公司网络上发生严重事件。

攻击者还可以通过中间人攻击从受害者的设备中提取令牌，在中间人攻击中受害者会单击网络钓鱼电子邮件或即时消息中的恶意链接，并被定向到一个看起来像是标识提供者合法登录页面的网站。实际上，它是由攻击者启动的 Web 服务，用于中继和拦截用户与标识提供者之间的所有流量。攻击者能够拦截用户名和密码，并中继 MFA 质询；因此，由标识提供者颁发并被攻击者拦截的最终令牌可能包含 MFA 声明，攻击者可以使用 MFA 声明来满足 MFA 要求。

Microsoft Defender for Cloud Apps 自 2022 年初以来，每月平均检测到 895 次这类攻击。通过使用 MFA 的防网络钓鱼因素（例如基于证书的身份验证、Windows Hello 企业版或 FIDO2 安全密钥），可以阻止这种形式的攻击。

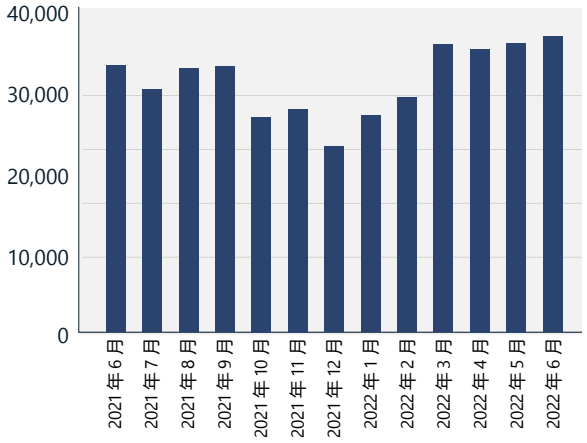
> 基于密码的攻击是入侵帐户的主要方法。

MFA 疲劳

攻击者利用“MFA 疲劳”的概念，向受害者的设备生成多个 MFA 请求，寄希望于受害者在无意中或因疲劳而接受请求。通过将 Microsoft Authenticator 等现代身份验证器应用与数字匹配[4]和启用其他上下文[5]等功能结合使用，可以阻止此攻击。据 Azure AD 标识保护估计，每月的 MFA 疲劳攻击可达 30,000 次。

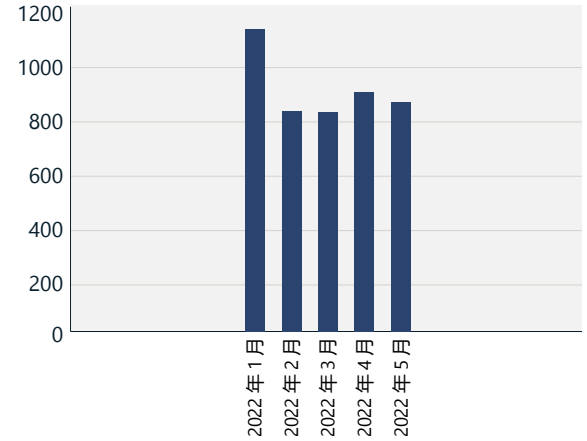
> 复杂攻击所占比例仍在上升，这突显了需要多重身份验证的防网络钓鱼因素。

预估的 MFA 疲劳攻击的发生次数



来源：Azure AD 标识保护。

检测到的网络钓鱼 + 中间人攻击的发生次数



来源：Microsoft Defender for Cloud Apps。

切实可行的见解

1. 确保实施强身份验证措施来保护整个组织中的所有帐户。
2. 无密码身份验证可提供最安全的用户友好体验，消除了密码攻击风险。
3. 在整个组织中禁用旧版身份验证。
4. 使用防网络钓鱼形式的强身份验证来保护高价值的管理帐户。
5. 从本地身份提供者迁移到云身份提供者以实现现代化，并将所有应用连接到基于云的身份提供者，以实现一致的用户体验和安全保护。

更多信息的链接

- 在这个世界密码日考虑完全放弃密码 | Microsoft 安全

操作系统默认安全设置

随着安全威胁格局的不断演变，我们看到对默认配置计算机安全性以提高网络复原能力的需求日益增长。虽然操作系统安全性比以往任何时候都更迫切需要得到保证、更复杂且更具业务关键性，但正确配置和管理可能具有挑战性。

过去，计算机和设备安全性包括内置的安全功能，客户或 IT 专业人员需要将其配置为自己所需的级别。现在仅依靠这种方法是不够的，因为攻击者在自动化、云基础结构和远程访问技术中使用更先进的工具来达到其目的。默认情况下，配置从芯片到云的所有安全层级变得至关重要。Microsoft 已发展为默认配置 Windows 操作系统安全性。[6]

采用了深度防御（包括分层安全状况、新的安全功能、定期和一致的修补和更新，以及报告网络钓鱼和其他欺诈的安全培训和意识）的客户，可以减少受到恶意软件攻击。

为了简化深度防御，Windows 11 默认情况下会开启紧密集成的硬件和软件保护，包括内存完整性、安全启动和受信任的平台模块 2.0。在硬件支持的情况下，Windows 10 用户还可以在“Windows 设置”应用或 BIOS 菜单中开启这些功能。

一般而言，旧的设备硬件安全和软件安全技术之间的协调一致性并非那么高。对于默认未启用安全性的设备，可以手动进行配置（如有可能）。[7]

对于默认未启用安全性的设备，Microsoft 建议在设置中手动进行配置（如有可能）。

主动应用不断发布的操作系统更新和安全修补程序，帮助在整个硬件和软件生命周期中提供保护。

切实可行的见解

1. 使用在受信任的平台模块中绑定登录凭据的无密码解决方案，特别要寻找符合 Faster Identity Online (FIDO) 联盟[8] 行业标准的无密码解决方案。
2. 及时清理组织设备上所有未使用和过时的可执行文件。
3. 启用内存完整性、安全启动和受信任的平台模块 2.0（如果默认情况下未启用），它们使用现代 CPU 中内置的功能增强启动安全性，从而抵御高级固件攻击。
4. 开启数据加密和凭据保护。
5. 启用应用程序和浏览器控制，以增强针对不受信任应用程序的防护和其他内置攻击防护。
6. 启用内存访问保护，以帮助抵御偶发性物理攻击，例如有人将恶意设备插入外部可访问的端口。

更多信息的链接

- Windows 安全手册 | 商业
- Windows 11 的新增安全功能可帮助为混合工作提供安全保护 | Microsoft 安全博客

软件供应链的集中性

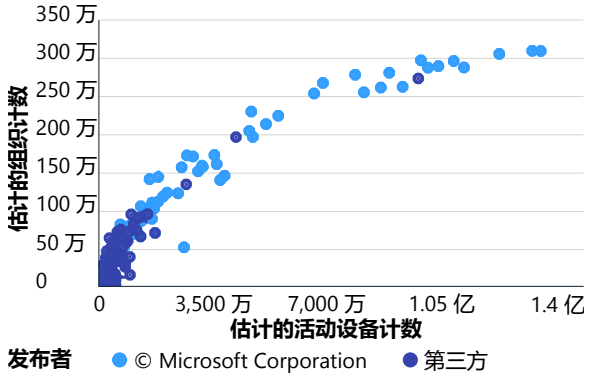
针对第三方应用、插件和扩展发起的攻击可能会削弱客户对在供应生态系统中发挥核心作用的供应商的信任。借助网络理论来审视软件的集中性有助于阐明修补的重要性，特别是对于核心应用而言。

包含 1,800 万个应用程序可执行文件的 Windows App Network 已在 500 万个组织中安装和使用，通过它可以简要了解我们的软件生态系统。在 100,000 个最常用的应用程序中，97% 由第三方组织开发，它们的更新和安全修补程序由这些组织维护。这说明了我们的商业应用生态系统的两个重要特征。

首先，Windows 商业应用程序生态系统具有集中性。在 1,800 万款应用程序中，只有前 100,000 款应用程序在 1,000 台或更多设备上使用。换而言之，在这些应用程序中，在设备生态系统中产生了这种广泛影响的应用程序刚刚超过 0.5%。

其次，这些应用程序的可管理性具有多样性，主要的 10,000 个应用程序提供商负责管理这些最常用的商业应用程序的更新和安全修补程序。这表明了一家公司在安全性、合规性和管理控制功能方面与各种软件供应商之间的相互依赖关系。

最常用应用程序的商业渗透



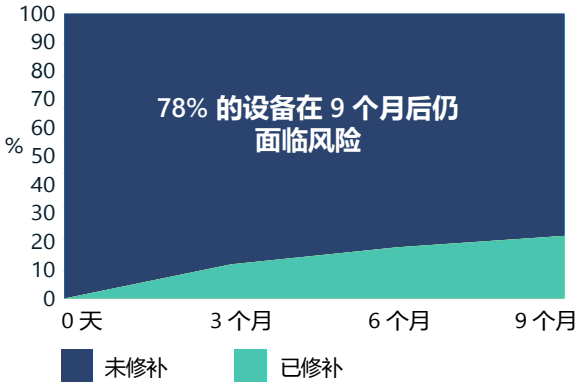
主要应用程序供数百万个组织和数千万台设备使用。由于它们几乎无处不在，因此攻击者会不断窥视以利用这些主要应用程序中的漏洞，这可能会影响用户群中的数百万台设备。

我们发现，数百万台商业设备在修补程序发布数月后甚至在产品支持结束数年后仍在使用易受攻击的应用程序版本。例如，超过 100 万台活跃的 Windows 商业设备使用的是自 2017 年便不再支持的 PDF 读取器版本。

数百万台商业设备仍在活跃使用不受支持的旧版本的应用程序。因此，组织面临具有不能修补漏洞的风险。

对于支持期内的应用程序版本，我们看到关键修补程序的采用速度处于停滞状态，这与提升复原能力的趋势相反。曲线应显示修补程序的采用逐月呈指数增长，才能实现所需的复原能力。

关键修补程序部署率



在分析了影响一组浏览器的 134 个版本的关键漏洞后，我们发现 78% 即数百万台设备在修补程序发布九个月后仍在使用受影响的版本之一。

我们使用 InterpretML[9] 工具包确定了与很有可能使用装有旧应用版本的设备的组织关联的特征。其中最重要的预示因素包括：设备使用时间较短；地理区域，如亚太和拉丁美洲；行业，如汽车、化学、电信，运输和物流、医疗付款机构（索赔处理机构）和保险。

软件复原能力的维护应包括定期禁用或卸载未使用的应用程序。

组织的安全性和合规性离不开组织自身与软件供应商的共同努力。

切实可行的见解

1. 及时更新组织内的所有应用程序和终结点。
2. 及时清理组织设备上所有未使用和过时的可执行文件

更多信息的链接

- Microsoft Intune 文档 | Microsoft Docs
- 管理应用 | Microsoft Docs
- Microsoft Defender for Endpoint | Microsoft 安全
- OSS 安全供应链框架 | Microsoft 安全工程
- Microsoft 开源软件安全供应链框架 | GitHub

建立针对新兴 DDoS、Web 应用程序和网络攻击的复原能力

加速的数字转型终结了传统网络和安全边界模型。迁移到云意味着企业必须采用云原生网络安全功能来保护数字资产。

攻击的复杂性、频率和数量不断增长，并且不再局限于节日假期，这表明正在向全年攻击转变。这突显了在传统的流量高峰季之外提供持续保护的重要性。

分布式拒绝服务（DDoS）攻击

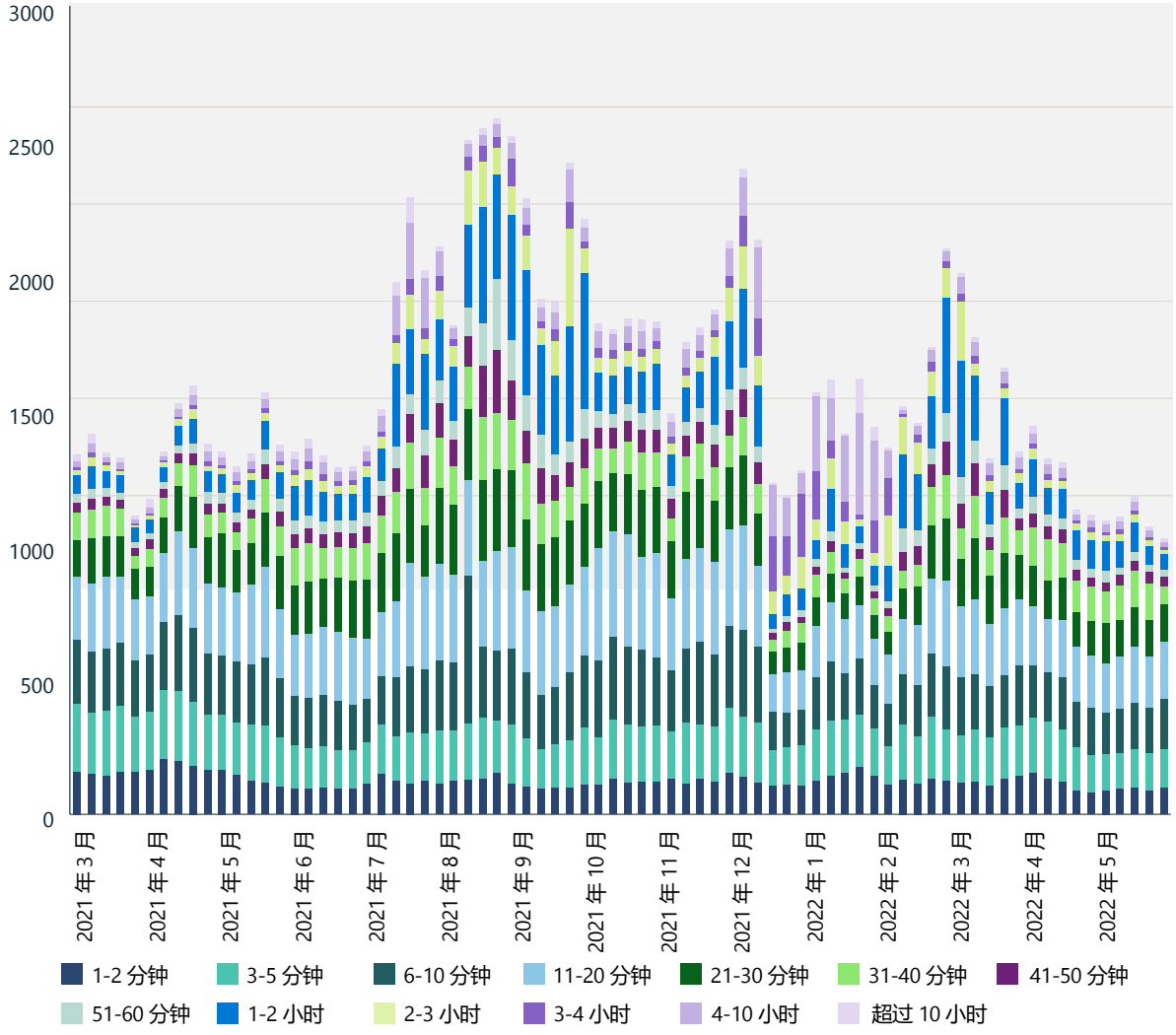
在过去的一年里，全球发生的 DDoS 活动在数量、复杂性和频率上都是前所未有的。国家层面的攻击大幅增加和低成本的受雇 DDoS 服务持续激增，这些推动了 DDoS 的爆炸性增长。Microsoft 平均每天缓解 1,955 次攻击，比上一年增加了 40%。以前，攻击次数的峰值通常发生年终节日季期间。然而，今年记录最多的一天是 2021 年 8 月 10 日。这可能表明正在向全年攻击转变，并且突显了在传统的流量高峰季之外提供持续保护的重要性。

2021 年 11 月，Microsoft 阻止了来自多个国家 / 地区的大约 10,000 个来源的容量 DDoS 攻击，攻击的吞吐量为每秒 3.4 TB (Tbps)。2022 年，得到缓解的是超过 2 Tbps 的类似大容量攻击，这突显了不仅攻击的复杂性和频率有所增加，攻击的容量（带宽）也有所增加。

攻击持续时间

过去一年中观察到的大多数攻击持续时间都不长。大约 28% 的攻击持续时间不到 10 分钟，26% 的攻击持续时间为 10-30 分钟，14% 的攻击持续时间为 31-60 分钟。32% 的攻击持续时间超过一小时。

DDoS 攻击次数和持续时间分布情况
(2021 年 3 月至 2022 年 5 月)



去年的大多数攻击持续时间都不长。大约 28% 的攻击持续时间不到 10 分钟。

构建对新兴 DDoS 的复原能力，Web 应用程序和网络攻击

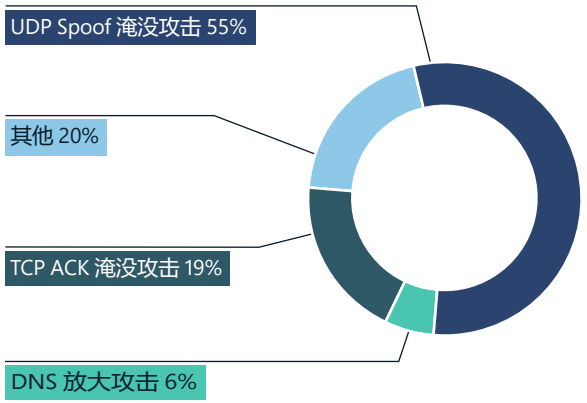
续

DDoS 攻击途径

在过去的一年里，常用攻击途径是使用简单服务发现协议 (SSDP)、无连接轻型目录访问协议 (CLDAP)、域名系统 (DNS) 和网络时间协议 (NTP) 在端口 80 上进行的包含一个峰值的用户数据报协议 (UDP) 反射。我们还看到，将网站作为目标的应用程序层 DDoS 攻击有所增加，峰值 RPS（每秒请求数）为 1,630 万次，峰值流量为 9.89 Tbps。

在 2022 年，Microsoft 每天缓解了近 2,000 次 DDoS 攻击，并阻止了有史以来最大的 DDoS 攻击。

DDoS 攻击途径



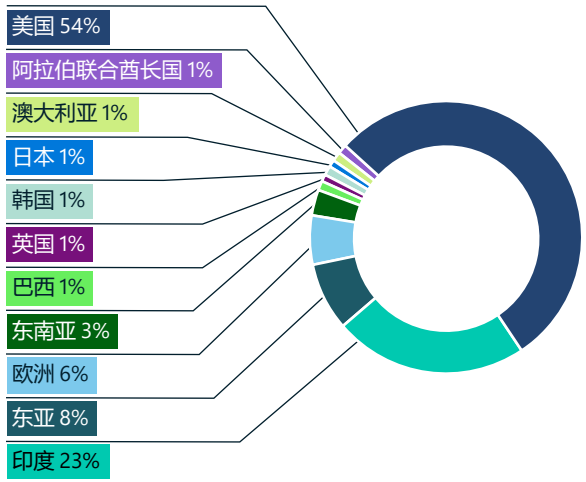
UDP Spoof 淹没攻击在 2022 年上半年上升到了最高水平，从 16% 上升到了 55%。TCP Ack 淹没攻击从 54% 降到了 19%。

游戏行业仍是 DDoS 攻击的主要目标，大多数攻击是 Mirai 僵尸网络的变异和低流量 UDP 协议攻击。由于 UDP 通常用于游戏和流式处理应用程序，因此绝大多数攻击途径是 UDP Spoof 淹没，而一小部分是 UDP 反射和放大攻击。

目标地理区域

在过去一年检测到的 DDoS 攻击中，54% 的攻击针对位于美国的目标发起，出现这一趋势的部分原因是大多数 Azure 和 Microsoft 客户都位于美国。我们还看到，针对印度的攻击急剧增加，从 2021 年下半年的 2% 上升到了 2022 年上半年的 23%。东亚 (尤其是香港) 仍是一个热门攻击目标，占 8%。在欧洲，我们看到攻击集中在阿姆斯特丹、维也纳、巴黎和法兰克福地区。

DDoS 攻击目标

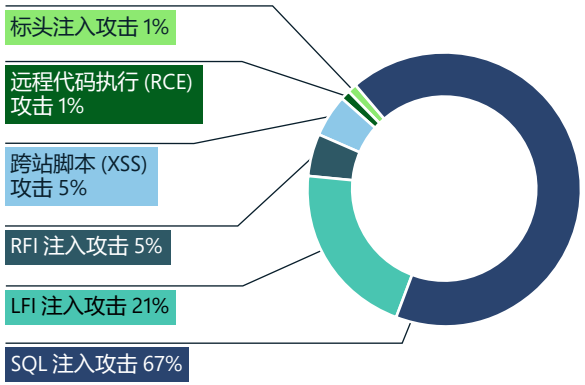


我们将亚洲的大量攻击归因于这个地区游戏体量庞大，尤其是在中国、日本、韩国和印度。智能手机渗透率的提升将推动移动游戏的普及，随着而来的是游戏体量的进一步扩大，这表明此地理目标受到的攻击只会继续增长。

Web 应用程序攻击

Web 应用程序防火墙 (WAF) 再加上 DDoS 防护，它们是保护 Web 和应用程序编程接口 (API) 资产的深度防御战略不可或缺的组成部分。Microsoft 观察到每月通过 Azure WAF 触发的 WAF 规则超过 3,000 亿。

最常见攻击类型的分布情况



Azure WAF 每天可以检测到数十亿次 Open Web Application Security Project (OWASP) 前 10 大[10] 攻击。根据我们的信号，攻击者大多数会先尝试 SQL 注入攻击，然后尝试本地文件注入和远程文件注入攻击。这与 OWASP 前 10 大攻击列表一致，此列表将注入攻击列为第三大最常见的 Web 攻击类型。

针对 Azure Web 应用程序的机器人攻击也有所增加，每月的机器人请求数量平均可达 17 亿，其中 4.6% 的流量涉及恶意机器人。

建立针对新兴 DDoS、Web 应用程序和网络攻击的复原能力

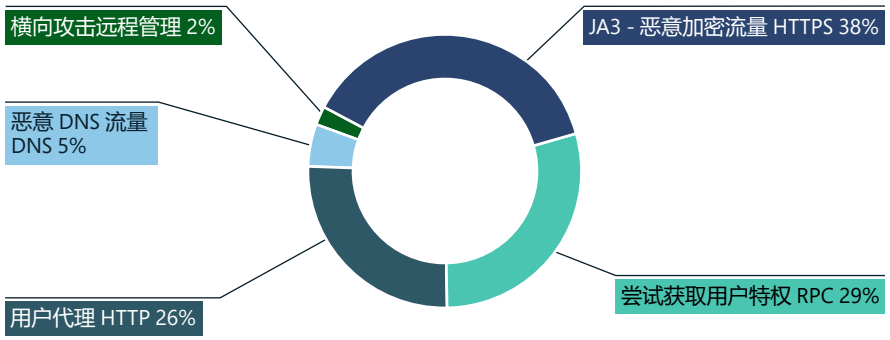
接上页

由于执行凭据填充攻击、信用卡欺诈、网络影响力活动和供应链攻击的机器人数量越来越多，我们预计针对 Web 应用程序的机器人攻击将稳步增长。

网络入侵：检测和防护

我们观察到，2022 年网络层攻击(尤其是恶意软件攻击)显著增加。仅 6 月份，Azure 防火墙入侵检测和防护系统 (IDPS) 就阻止了超过 1.5 亿次连接。

IDPS 拒绝流量的相关原因



IDPS 流量警报的相关原因

有关 IDPS 警报和拒绝流量的分析显示，攻击者使用了以下方法。在拒绝流量中，我们看到攻击者使用 SSL 隐藏其活动，远程执行攻击变得越来越常见。在警报流量中，我们看到使用 SMB/SMB2 协议来发起远程执行攻击。

切实可行的见解

1. 检查数据中心或云服务中系统之间的所有流量，以及试图访问它们的流量。
2. 制定稳健的全年网络安全响应战略。
3. 使用云原生安全服务实现稳健的零信任网络安全状况。

更多信息的链接

- 使用 Azure 防火墙改进针对勒索软件攻击的安全防御 | Azure 博客和更新 | Microsoft Azure
- DDoS 放大攻击的剖析 | Microsoft 安全博客
- 使用 Azure Web 应用程序防火墙实现从边缘到云的智能应用程序保护 | Azure 博客和更新 | Microsoft Azure

开发平衡的数据安全方法和网络复原能力

数字转型推动了数据资产的大幅扩展，并提高了安全性、合规性和隐私风险。具有网络复原能力的组织必须平衡在数据保护、合规性和恢复功能方面的投资，并将这些与专门的监管响应流程整合在一起，以解决不同类型的泄露。

数据泄露不是“是否泄露”的问题，而是“何时泄露”的问题。IBM 和 Ponemon Institute 开展的名为“2021 年数据泄露成本”的研究指出，全球的平均数据泄露成本为 424 万美元（比上年增长 10%），美国为 905 万美元。研究发现，不满足合规性是导致成本增加的主要因素。相反，泄露成本降低与以下最佳实践有关：事件响应 (IR) 规划、零信任部署成熟度、安全 AI 和自动化以及使用加密。

数据泄露不可避免。组织通过采取平衡的复原能力方法，可以降低泄露的频率、影响和成本。

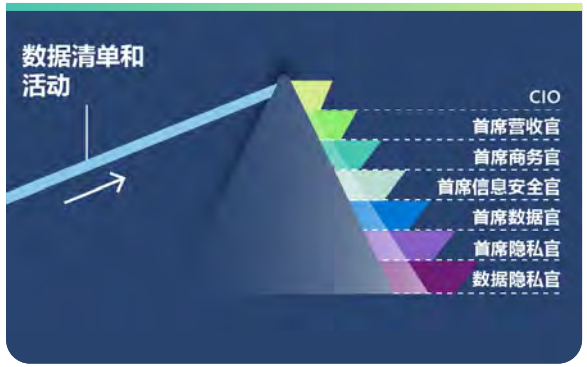
数据管理、安全性、合规性和隐私是相互依存的

我们看到，近年来数据作为组织的重要价值创造引擎而受到重视。与此同时，要求同时提供数据管理和安全保护的隐私法规的出现模糊了风险角色之间的界限。虽然首席数据官 (CDO) 或首席隐私官 (CPO) 等较新的高管角色可以从实现安全性和合规性中受益，但数据保护的实施和运作通常依赖于首席信息官 (CIO) 和 / 或首席信息安全官 (CISO) 领导的团队。它不是一条单行道，因为由 CDO 领导的数据管理计划对安全也有好处。由于存在相互关联，IT、数据管理、安全性、合规性和隐私团队需要更紧密地合作，以提高效率和管理风险。

针对整个组织数据资产建立统一的数据风险管理平台是未来发展方向

在各部门都有定制应用程序并且典型的组织混合、多云数据蔓延覆盖范围不一致的环境中，很难协调 IT、数据管理、安全性、合规性和隐私管理流程。我们认为，组织需要单一的管理平台，以便定位和了解其数据，保护其数据，管理数据的访问、使用和生命周期，并在整个数据资产中防止数据丢失。

使用相同的数据清单和活动信息可以帮助建立跨团队的流程，更全面地了解风险状况，使组织能够做好更充分的准备和简化数据泄露响应方法。



“单一管理平台”应该充当棱镜。如果数据安全性、合规性和隐私与团队息息相关，这些团队需要就相同的数据清单和活动获得不同但一致的视图，才能做到协调一致并开展协作。数据活动包括数据访问、修改和移动事件，它们是数据安全状况的一个重要组成部分。

有效的数据管理、安全性、合规性和隐私措施是相互依存的，并需要跨团队协作。

切实可行的见解

1. 通过在合规性、数据保护和响应功能方面进行投资，在防御与恢复之间实现平衡并最大限度地降低数据泄露产生的影响。
2. 开发和采用可以打破数据风险壁垒并覆盖整个数据资产的流程和工具。

更多信息的链接

- Microsoft Purview - 数据保护解决方案 | Microsoft 安全
- 合规性和数据管理已步入新时代：Microsoft Purview 简介 | Microsoft 安全博客

针对网络影响力行动的复原能力：人文层面

在过去的五年里，图形和机器学习的发展带来了简单易用的工具，它们能够快速生成高质量的逼真内容，这些内容在几秒钟内即可在 Internet 上广泛传播。

说到借助文本、音频和视觉内容报道事件，我们已经达到了人类和算法都难辨真假的水平。这些工具及其输出内容的激增使人们对所有数字媒体的可信度产生了怀疑，从而对我们了解当地和全球事件造成了干扰。技术发展催生了新形式的影响力行动，这对民主进程造成了严重影响。[11]

问题出现了：为了做好准备，打造更具复原能力的未来以应对这些网络影响力行动，我们可以做些什么。技术只是这个难题的一个方面。这需要多个方面的努力，包括以提高媒体素养、意识和警觉为目的的教育、高质量新闻方面的投资（在新闻现场、当地、国内和国际上拥有值得信赖的记者）、分享和提醒影响力行动的网络，以及对出于行骗目的而生成或操纵数字媒体的恶意行为者进行处罚的新型法规。

我们还认识到，恢复对数字内容的信任是一个远大的目标，需要贡献多元观点并积极参与。没有任何一家公司、一个机构或一个政府可以独自解决这些威胁。作为人类，我们拥有的超能力就是我们的协作和合作能力。如今，这种能力特别重要，因为需要各方（全球各国政府、各个行业、学术界，特别是新闻、社会和媒体组织）共同携手，促进社会的进步和健康发展。

更多信息的链接

- 人工智能在国防部网络任务中的应用 | Microsoft On the Issues
- 人工智能和网络安全：挑战和前景。人工智能在网络空间运营中的应用的听证会，参议院军事委员会网络安全小组委员会，第 117 届国会（2022 年 5 月 3 日；Eric Horvitz 的发言）

通过技能强化人为因素

解决人为因素是所有网络安全技能战略的关键组成部分。根据一项“Kaspersky IT 安全中的人为因素”的研究，[12]46% 的网络安全事件涉及疏忽大意或身穿制服的员工，他们在无意中为攻击创造了条件。

Microsoft 数字安全和复原能力组织中的教育与意识团队负责通过增强员工的能力来强化网络安全的人为因素，确保我们自己和客户的系统和数据安全无虞。我们的目标是：

- 通过在员工群体中集中培养企业级核心安全技能集，降低 Microsoft 和我们客户的风险。
- 通过多阶段培训强化方法深化员工安全知识，为达到预期的行为结果提供支持。
- 通过每年必须举办的安全培训和活动，使安全思维成为 Microsoft 文化的内在组成部分，从而促进文化变革。
- 推广集中的一站式 Web 资源，其中涵盖最佳实践、公司政策信息和事件报告，以提供所有网络安全相关内容。

每个 Microsoft 员工每年至少参加一次有针对性的集中式网络安全技能计划。培训课程经过优化，可以为当前的网络安全计划提供支持并提供可衡量的行为结果。Microsoft 的信息风险管理委员会 (IRMC) 在确定需要通过培训取得的重要网络安全行为改变结果方面发挥着关键作用。

对于我们所有的网络安全技能计划，我们会尽可能地衡量解决方案的效率、有效性和成效。例如，我们的内部威胁技能培训课程获得了高达 95% 的培训达标率和超高学员满意度，并且导致通过公司的“立即报告”工具报告潜在内部威胁案例的管理人员显著增加。这个计划包括：

安全基础知识：集中的企业级网络安全意识和合规性培训，介绍核心安全和隐私实践。这个备受期待的培训系列采用寓教于乐的模式，使网络安全学习变得引人入胜且趣味无穷。

STRIKE：必须完成的 Microsoft 技术培训，面向构建和维护业务线解决方案的工程师。这个只能受邀参加的培训介绍了网络安全机制最佳实践的有时效性的关键方面，并采用了根据受众需求量身定制的直播混合授课模式。

特定于计划的课程：有针对性的培训计划，为特定网络安全计划提供支持，包括影子 IT、内部威胁和 Microsoft Federal。这些课程已借助高管支持和记分卡报告紧密集成到各自网络安全计划的整体参与战略中，以防止采用“打勾式”的培训方法。

MSProtect：Microsoft 的集中式 Web 网络资源，涵盖最佳实践、公司政策信息和事件报告，以提供所有网络安全相关内容。此按需资源是正式培训课程之外员工的首选资源。

不得将安全技能培训视为达标所需的打勾式活动。相反，应该专注于改变行为，以便对确定的目标行为的结果进行监控，并建立倾听系统以确定产品的影响。

切实可行的见解

1. 随时随地为员工提供安全培训和资源。
2. 基于整个企业的利益相关者的意见制定集中的技能战略。
3. 确保跟踪和分析培训的影响，以了解效率（数量）、有效性（质量）和成效（业务影响）。

更多信息的链接

- Microsoft 在帮助了 3,000 万人后启动了下一阶段的技能计划

来自我们的勒索软件消除计划的见解

在过去五年里，Microsoft 一直在推进自己的零信任之旅[13]，以确保身份和设备得到稳健管理并保持正常运行。随着勒索软件风险的增加，我们进行了深入了解，以便为保护我们自身和我们客户的方法提供支持。

经过深入的内部评估，我们制定了勒索软件消除计划，以弥补控制措施和覆盖范围方面的不足，为增强 Defender for Endpoint、Azure 和 M365 等服务的功能做出贡献，并为我们的 SOC 和工程团队编写有关如何在发生勒索软件攻击时进行恢复的行动手册。

第一步是了解我们对将 Microsoft 作为目标的勒索软件攻击的防护程度。部署 Defender for Endpoint 并确保所有设备都得到管理且符合我们的零信任策略的相关工作进展顺利，但我们需要找到一种方法来了解更大的问题（即我们是否可以高效地从攻击中恢复）的方方面面。为了深入了解，我们评估了 NIST 8374：勒索软件风险管理：网络安全框架 (CSF) 概要文件，[14] 它与我们针对已知控制措施列表采取的整体企业政策一致。此分析很快确定了覆盖范围方面的不足。

接下来，我们就 CSF 的识别、检测、保护、响应和恢复功能存在的不足确定了优先顺序。我们发现了与零信任和其他计划的战略一致性，还发现了因缺少现有工作流而存在的不足。评估弥补这些不足所需完成的工作和付出的努力后，我们将它们分为两个支柱：

- **保护企业 (PtE)**：定义为了在攻击成功发起时能够保护自身并从攻击中恢复，作为企业我们需要完成的工作项。
- **保护客户 (PtC)**：在我们的产品 / 服务中构建相应功能以保护我们的客户和我们的业务。

将研究结果应用到我们自己的企业中

为了缓解主要风险并保护关键服务免受勒索软件攻击，我们计划未来 6 到 12 个月内在勒索软件专项计划中将投资重点放在实现以下五个场景上。一旦我们在每个场景中取得成功，我们将逐步扩大计划的范围，以覆盖企业的所有机构。

场景 1：安全团队成员了解与勒索软件攻击相关的总体风险，并建立流程以让高管了解控制措施方面的不足和风险状态。

场景 2：安全团队成员可以访问旨在帮助他们和 Microsoft 中的其他团队响应勒索软件攻击并从中恢复关键服务的行动手册。

场景 3：企业复原能力团队成员具有在备份关键系统时可遵循的标准。具有行动手册，并且完成了有关备份和恢复的常规练习，以确保在发生勒索软件攻击时可以恢复数据。

场景 4：服务负责人了解并实施所需的安全和运营控制措施和策略，以保护服务、客户数据、终结点和网络资产免受勒索软件攻击，并特别关注作为 Microsoft 关键服务优先考虑的服务。

场景 5：所有员工都可以访问教育和培训资源，这些资源介绍了如何识别勒索软件攻击，以及如何通知安全团队并做出响应。

切实可行的见解

1. 记录并验证与针对关键服务发起的勒索软件攻击相关的端到端恢复和补救活动。
2. 让利益相关者参与更新“企业危机管理”行动手册，以包括特定于勒索软件的活动以及确定是否 / 何时针对勒索软件支付赎金的决策过程和相关指导。
3. 通过启用已部署的安全产品中可用的功能（例如 Defender for Endpoint 攻击面减少规则）来改善检测和保护覆盖范围。
4. 与安全标准团队合作，为抵御勒索软件攻击定义基线，并向工程团队提供有关如何抵御勒索软件攻击的培训和文档。
5. 实施自动化以使 DevOps 团队可以更轻松地部署安全和运营策略，并确保如果系统变得不再合规，可以快速标记并做出补救。

更多信息的链接

- 分享 Microsoft 如何防范勒索软件 | Microsoft Inside Track

立即就量子安全问题采取行动

量子计算给如今的加密技术及其保护的一切构成了威胁，要管理这些威胁，压力自然就来了。最近发布的“关于加强国家安全、国防部和情报社区系统网络安全的备忘录”[15] 以有关“加强国家网络安全”的美国行政命令 10428[16] 为基础，它强调软件供应链安全性对于应对未来国家层面的攻击至关重要。

什么是量子计算机?

量子计算机是借助量子物理属性来存储数据并执行计算的机器。这对于某些任务来说可能非常有利，在这些任务中它们的性能甚至可能远远超过配置最高的超级计算机。量子计算已经为数据加密和处理开辟新的前景。研究预测，量子计算最早将在 2030 年成为价值数十亿美元（USD）的量子产业。[17] 事实上，量子计算和量子通信有望对医疗保健、能源、金融和安全等众多行业产生变革性的影响。

量子计算是如今的加密技术及其保护的一切所面临的威胁。

如今的加密技术面临的威胁

借助 Shor 1994 年提出的算法和超过数百万物理量子位的工业规模量子计算机，我们当前广泛部署的所有公钥加密算法都可能被破解。考虑、评估和标准化“量子安全”加密系统至关重要，这种加密系统可以高效、敏捷且安全地抵御基于量子的对抗性攻击。将软件迁移到“后量子加密技术”（即现有的传统算法和协议可以稳健地应对量子攻击）即使不需要十年甚至更久，也需要数年才能实现。[18]

这意味着需要管理如今的加密技术及其保护的一切所面临的威胁，因此压力自然就来了。攻击者现在可以记录加密的数据，并在量子计算机问世后再利用这些数据。如果什么都不做，等到量子计算在解决量子加密问题之前到来，那就晚了。

由于加密已在整个网络生态系统中使用，这意味着基于加密的安全服务可能会受到影响。例如，这包括用于通信（TLS、IPSec）、消息传递（电子邮件、Web 会议）、身份和访问管理、Web 浏览、代码签名、支付交易的服务以及依赖于加密提供保护的其他服务。

随着量子计算机成为现实，包含加密算法和功能实现的第三方软件组件也需要进行额外的审查。这要求价值链中的所有组织都履行各自的职责，以确保价值链安全无虞。行业机构和政府正在加大力度来定义软件供应链安全要求，在某些情况下，还出台了新的指令以保护供应链。“国家安全备忘录” NSM-8[19] 确立了在国家安全系统 (NSS) 中实施后量子加密的要求和时间表。它提出了时间预期，即在 180 天内“规划现代化，使用不受支持的加密、经过批准的任务专属协议、抗量子协议，以及在必要时规划使用抗量子加密”。

标准化是向量子安全加密过渡过程中的一项长期的准备活动。负责制定使用公钥加密技术相关标准的标准机构现在就必须开始尝试并适应后量子算法。

新的后量子加密 (PQC) 算法（被认为可以稳健应对量子攻击的传统算法）正在接受 NIST 后量子标准化计划的审查。[20] 这项工作将影响标准机构在全球开展的工作。虽然与美国政府做出的算法选择存在一些重叠，但是国家机构 / 监管机构针对合规算法做出的不同选择可能会带来国际挑战。这种分歧反过来会使产品和服务工程变得复杂化。

新的后量子加密算法正在接受 NIST 后量子加密标准化计划的审查。这项工作将影响标准机构在全球开展的工作。

切实可行的见解

除了 SAFECode 和合作成员，行业也应立即采取短期的活动，以便为 PQC 过渡做好准备。[21] 这包括：

1. 清点使用加密的产品 / 代码。
2. 在整个组织中实施加密敏捷性政策，包括最大限度地减少加密发生改变时所需的代码改动。
3. 在使用加密的产品或服务中试用候选量子安全算法。
4. 准备好使用不同的公钥算法进行加密、密钥交换和签名。
5. 测试应用程序以了解大型密钥、密码和签名的影响。

更多信息的链接

- Microsoft 演示了创建新型量子位所需的底层物理机制 | Microsoft 研究

整合业务、安全性和 IT 资源以提高复原能力

稳健的网络复原能力依赖于企业领导者与安全团队密切合作以实施安全措施。根据 Microsoft 的经验，安全领导是一项具有挑战性的领域，需要组织领导者的支持才能有效地保护组织。

安全领导者要应对一系列动态挑战，这涉及与风险、技术、经济、组织流程、业务模式、文化转型、地缘政治利益、间谍活动和国际制裁合规性相关的主题。每个方面都存在需要理解和严密管理的细微差别。

安全领导者还肩负着阻止狡猾、资金充足、积极性高的人类攻击者以及技能水平不高但高效的网络犯罪分子的任务。他们的团队必须保护复杂的技术资产，这些资产通常在 30 多年或更长时间内逐步建立，当时安全问题有限性不高或不存在。几年前做出的决策如今可能会带来风险，直到我们偿还技术债务并解决安全漏洞为止。

组织领导者和决策者可以通过积极支持安全领导者并帮助在综合安全管理和组织的其他部门之间建立桥梁，对安全产生巨大的积极影响。当 Microsoft 与具有这种一致看法的客户合作时，我们看到他们建立了更具复原能力的组织，并提高了敏捷性以快速适应并进行创新。

组织领导可以通过关注三个关键领域来支持安全领导者：

1. 构建安全设计

在业务流程中，安全性有时被视为障碍或事后考虑的问题，通常只有在为时已晚而无法避免风险或以较低成本轻松修复时，才会在决策中考虑。

组织领导者和决策者应确保他们：

尽早将安全性融入新计划之中。要推行新的数字计划和采用云，应优先考虑安全性，以确保组织风险不会随着每个新应用程序或数字功能的增加而增加。可靠地融入安全性之后，你可以使用这些流程对旧系统进行现代化改造，同时获得安全性和工作效率方面的好处。

规范化预防性维护以实现安全性。确保基本安全维护（如应用安全更新和修补程序以及安全配置）已得到组织的全面支持（包括预算、计划内停机时间、用于获得供应商产品支持的采购要求）。

遗憾的是，许多组织会延迟、推迟应用这些常见实践或者只应用一部分。这为攻击者带来了大量可利用的可乘之机。美国 NIST 800-40 说明了安全规范化方面的需求。[22]

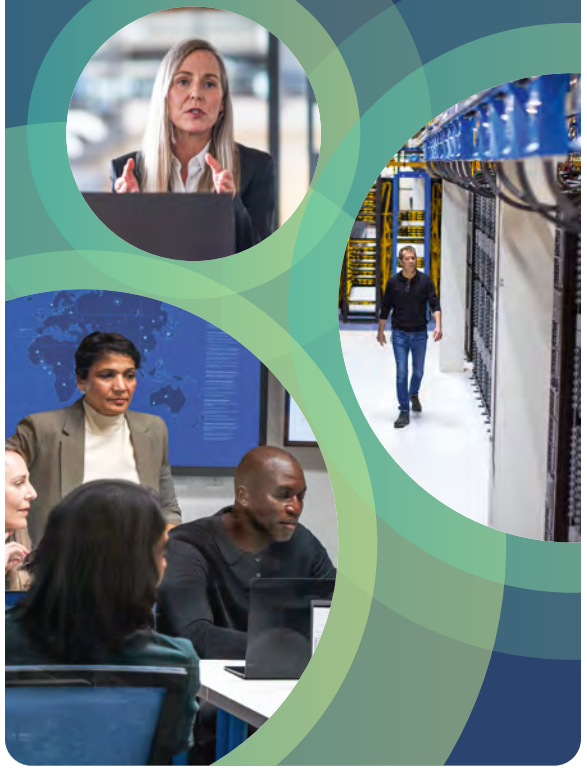
2. 参与安全方面的工作

组织领导者应积极参与和支持关键安全流程，以确保优先分配资源并做好应对安全灾难的准备。这包括参与：

确定关键业务资产。安全领导者和团队需要了解哪些资产属于关键业务资产，以便使安全资源专注于处理最重要的问题。这通常是新的实践，需要询问和回答以前没有解决过的新问题。

网络安全业务连续性和灾难恢复实践。网络攻击可能会成为使大多数或所有业务运营中断或停滞的重大事件。确保整个组织中的团队做好应对这些情况的准备，这样可以缩短恢复业务运营所需的时间，减少给组织带来的损害，并帮助保持客户、公民和选民的信任和信心。这应该集成到现有的业务连续性和灾难恢复流程中。

安全风险决策最好由全面了解所有风险和机会的业务或任务负责人做出。



整合业务、安全性和 IT 资源以提高复原能力

接上页

3. 将安全问题交给正确的人员处理

组织建立安全风险问责制的方式通常决定了，他们会做出不明智的安全风险决策。风险决策最好由全面了解所有风险和机会的业务或任务负责人做出，但是组织通常会（以含蓄或明确的方式）将安全风险责任分配给安全团队中的主题专家。这给安全团队带来了不必要的负担，同时剥夺了企业负责人对于业务关键风险的可见性和控制权。组织可以通过以下方式纠正这个问题：

帮助企业负责人做好准备：就整体安全风险以及这些威胁会对业务有何影响为企业负责人提供指导。让安全团队直接参与这项工作还可以增进在安全性和整体业务敏捷性方面的协作关系。

将安全风险分配给企业负责人：随着企业负责人掌握足够的信息以了解并接受安全风险，组织应明确将安全风险相关责任转给他们，同时仍让安全团队负责管理该风险并向负责人提供有根据的专业知识和指导。

“网络复原能力是不断发展的：从始于出色数据备份的传统业务连续性和灾难恢复；逐步发展为流程、技术及其依赖项（包括人员和第三方）的恢复能力；然后转变为始终正常运行的自我修复服务、关键角色的复原能力和关键第三方的故障转移。最具复原能力的组织会推动 IT、业务经理和安全专业人员之间的整合。强大的复原能力包括一开始便采用复原能力设计、安全的变更管理和精细的故障隔离。网络复原能力只是预先考虑了所有危险的出色规划计划中的一个场景。随着网络风险的增加以及网络安全和复原能力之间的交集变得越来越重要，首席信息安全官 (CISO) 与企业复原能力计划之间的联系会变得更加紧密。每年都会有越来越多的 CISO 负责在公司范围内建立复原能力。”

Lisa Reshaur
Microsoft 风险管理部门总经理

更多信息的链接

- 从复原能力到数字持久力：组织如何利用数字技术在前所未有的时代转危为安 | Microsoft 官方博客
- IT 和安全团队如何通力合作以提高终结点安全性 | Microsoft 安全

网络复原能力钟形曲线

每个组织都应采纳的复原能力成功因素

正如我们所看到的，许多网络攻击之所以成功，只是因为没有遵循基本安全机制。每个组织都应达到的最低标准如下：

- **启用多因素身份验证 (MFA)**：防止用户密码泄露，并且有助于针对身份提供额外的复原能力。
- **应用零信任原则**：所有复原能力计划的基石，用于限制对组织造成的影响。这些原则包括：

1 - 显式验证 - 在允许用户和设备访问资源之前确保它们状况良好。

2 - 使用最小权限访问 - 仅授予访问资源所需的特权，不会授予其他特权。

3 - 假定入侵 - 假定系统防御机制已被破坏并且系统可能已经遭到入侵。这意味着需要不断监控环境中是否发生了可能的攻击。

- **使用扩展检测和响应反恶意软件**：实施软件以检测和自动阻止攻击，并为安全运营提供见解。监控来自威胁检测系统的见解对于及时响应威胁至关重要。
- **保持最新状态**：未修补和过时的系统是许多组织受到攻击的关键原因。确保所有系统保持最新状态，包括固件、操作系统和应用程序。
- **保护数据**：了解重要数据、其存储位置以及是否实施了正确的系统对于实施适当的保护至关重要。

98%

基本的安全机制仍可抵御 98% 的攻击。

关键原则

- 启用多重身份验证
- 采用零信任原则
- 使用现代反恶意软件
- 保持最新状态
- 保护数据

尾注

1. 端点检测和响应 (EDR) 提供了一个企业级端点安全平台，旨在帮助企业网络防范、检测、调查和响应高级威胁。终结点检测和响应功能可提供接近实时的可操作性高级攻击检测。安全分析师可以有效地确定警报的优先级，深入了解整个入侵范围，并采取响应措施来减轻威胁。
2. 端点保护平台 (EPP) 是在终结点设备上部署的解决方案，用于阻止基于文件的恶意软件，检测和阻止来自受信任和不受信任应用程序的恶意活动，并提供动态响应安全事件和警报所需的调查和补救功能。
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. Windows 安全手册：商业
7. Windows 11 的新增安全功能可帮助为混合工作提供安全保护 | Microsoft 安全博客
8. FIDO Alliance: Open Authentication Standards More Secure than Passwords
9. https://interpret.ml/
10. OWASP Top Ten | OWASP Foundation
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. 行政命令 14028“改善国家网络安全”
17. https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth
18. “The Long Road Ahead to Transition to Post-Quantum Cryptography”，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

参与团队

参与团队

本报告中的数据和见解由一个专注于安全问题的多元化群体提供，他们在许多不同的 Microsoft 团队中工作。他们的共同目标是保护 Microsoft 及其客户和整个世界免遭网络攻击的威胁。我们很自豪能开诚布公分享这些见解，我们的共同目标是将世界打造成人人向往的安全环境。

AI for Good 研究实验室：利用数据和人工智能的强大功能来应对全球的许多挑战。这个实验室与 Microsoft 以外的组织协作，应用 AI 来改善生活和环境。重点关注领域包括在线安全（虚假信息、网络安全、儿童安全）、灾难响应、可持续性和 AI for Health。

Azure 边缘与平台、企业与操作系统安全：负责跨 Windows、Azure 和其他 Microsoft 产品保证核心操作系统和平台的安全。这个团队将行业领先的安全和硬件解决方案构建到 Microsoft 平台中，以减少攻击、身份泄露和恶意软件入侵，提供从芯片到云的保护。这个团队负责跨 PC、边缘和服务器以及 Microsoft Pluton 安全处理器等创建 Microsoft 安全核心平台。

Azure 网络、核心：一个云网络团队，专注于 Microsoft WAN、数据中心网络和 Azure 的软件定义的网络基础结构，包括 DDoS 平台、网络边缘平台和网络安全产品，如 Azure WAF、Azure 防火墙和 Azure DDoS 保护标准。

云安全研究团队：这个团队负责通过保护 Microsoft 云、构建创新的安全功能和产品以及开展研究，保护和赋能 Microsoft 客户安全地实现组织转型。

客户安全和信任 (CST)：这个团队可不断提升客户使用 Microsoft 产品和在线服务时的安全性。CST 与公司的工程和安全团队合作，确保合规性、增强安全性并提升透明度，以保护客户并增强全球客户对 Microsoft 的信任。

客户成功：客户成功部门中的安全团队直接与客户合作，分享最佳实践、获得的经验教训和指导，以加速实现安全转型和现代化。这个团队将从 Microsoft 旅程以及客户旅程中了解到的最佳实践和经验教训汇总并整理到参考战略、参考体系结构、参考计划等内容中。

网络防御运营中心 (CDOC)：Microsoft 的网络安全和防御机构，汇集了来自整个公司的安全专业人员，目标是保护我们的企业基础结构和客户可以访问的云基础结构。事件响应者与来自 Microsoft 服务、产品和设备团队的数据科学家和安全工程师携手，共同帮助全天候保护、检测和响应威胁。

民主推进计划：这个 Microsoft 团队致力于通过打造健康的信息生态系统、维护开放且安全的民主进程以及倡导企业公民责任，来维护、保护和推进民主的基础。

数字犯罪部门 (DCU)：一个由律师、调查人员、数据科学家、工程师、分析师和商务专业人士组成的团队，致力于借助技术、取证、民事诉讼、刑事移交以及公共和私人合作关系在全球范围内打击网络犯罪。

数字外交：一个由前外交官、政策制定者和法律专家组成的国际团队，致力于在面对不断升级的国家冲突时，推进和平、稳定、安全的网络空间。

数字安全与复原能力 (DSR)：这个组织致力于使 Microsoft 能够构建受信任的设备和服务，同时保证公司的安全并保护公司和客户的数据。

数字安全部门 (DSU)：一个由网络安全律师和分析师组成的团队，负责提供法律、地缘政治和技术专业知识，为 Microsoft 和客户提供保护。DSU 负责建立对 Microsoft 企业安全功能的信任，并抵御全球范围内的高级网络攻击。

数字威胁分析中心 (DTAC)：一个由专家组成的团队，负责分析和报告国家面临的威胁，包括网络攻击和影响力行动。这个团队将信息和网络威胁情报与地缘政治分析相结合，为客户和 Microsoft 提供见解，并告知有效的响应和保护措施。

企业和安全：这个团队专注于为智能云和智能边缘提供现代、安全和可管理的平台。

企业移动性：这个团队帮助交付现代工作场所和现代管理，以确保数据在云端和本地的安全。Endpoint Manager 包括 Microsoft 和客户用于管理和监控移动设备、台式计算机、虚拟机、嵌入式设备和服务器的服务和工具。

参与团队

接上页

企业风险管理：一个跨业务部门开展工作的团队，负责与 Microsoft 高层领导确定进行风险讨论的优先顺序。ERM 与多个运营风险团队沟通，管理 Microsoft 的企业风险框架，并使用 NIST 网络安全框架推动公司的内部安全评估。

全球网络安全政策：这个团队与政府、非政府组织和行业合作伙伴合作以促进网络安全公共政策的出台，使客户能够在采用 Microsoft 技术的同时增强其安全性和复原能力。

身份和网络访问 (IDNA) 安全：这个团队致力于保护所有 Microsoft 客户免遭未经授权的访问和欺诈。IDNA 安全是一个由工程师、产品经理、数据科学家和安全调查人员组成的跨学科团队。

M365 安全：这个组织负责开发安全解决方案（包括 Microsoft Defender for Endpoint (MDE)、Microsoft Defender for Identity (MDI) 等），以保护企业客户的安全。

Microsoft 工程和研究方面的 AI、伦理和效果 (AETHER)：Microsoft 的一个咨询委员会，它的使命是确保以负责任的方式开发和部署新技术。

Microsoft 必应搜索和分发：这个团队致力于提供一流的 Internet 搜索引擎，使世界各地的用户能够快速找到可信的搜索结果和信息，包括跟踪对他们重要的主题和热门报道，同时让用户能够掌控自己的隐私。

Microsoft 客户和合作伙伴解决方案：Microsoft 的统一商业上市组织，负责安全和技术销售专家和顾问等现场职责。

Microsoft Defender 专家：Microsoft 最大的全球组织，由专注于产品的安全研究人员、应用科学家和威胁情报分析师组成。Defender 专家在 Microsoft 365 安全产品和 Microsoft Defender 专家管理的服务中提供创新的检测和响应功能。

Microsoft Defender for IoT：一个由领域专家研究人员组成的团队，专门研究 IoT/OT 恶意软件、协议和固件的反向工程。这个团队搜寻 IoT/OT 威胁，以发现恶意趋势和活动。

Microsoft Defender 威胁智能 (RiskIQ)：这个团队通过分析 Microsoft 丰富的外部遥测数据集合来生成战术情报，从而随着威胁形势的不断演变绘制图表以发现之前未知的威胁基础结构，并添加威胁行为者和活动的上下文。这个团队定期发布及时且独特的研究，以向防御者提供重要战术情报。

Microsoft 安全业务发展团队：这个团队主导 Microsoft 网络安全增长战略、合作伙伴关系和战略投资。

Microsoft 安全响应中心 (MSRC)：这个团队与安全研究人员合作，致力于保护 Microsoft 客户和合作伙伴生态系统。MSRC 是 Microsoft 网络防御运营中心 (CDOC) 不可或缺的一部分，汇集了安全响应专家，以实时检测和响应威胁。

Microsoft 事件响应安全服务团队：一个由网络安全专家组成的团队，帮助客户完成抵御网络攻击的整个过程，从调查到与成功遏制和恢复相关的活动，都可以提供帮助。服务由两个高度融合的团队提供：检测和响应团队 (DART)，专注于调查和恢复的基础工作；入侵恢复安全实践 (CRSP)，专注于遏制和恢复方面。

Microsoft 威胁情报中心 (MSTIC)：这个团队致力于识别、跟踪和收集有关给 Microsoft 客户带来影响的最狡诈攻击者的情报，其中包括国家层面威胁、恶意软件、网络钓鱼。

One Engineering System (1ES)：这个团队的使命是提供一流的工具，以帮助尽可能保证 Microsoft 开发人员的效率和安全。这个团队负责领导制定用于保护 Microsoft 端到端软件供应链的核心战略。

运营威胁情报中心（OpTIC）：这个团队负责管理和传播网络威胁情报，以支持 Microsoft 网络防御运营中心（CDOC）履行保护 Microsoft 和客户的使命。

Microsoft

阐明威胁格局，加强数字防御。

了解更多: https://microsoft.com/mddr

深入了解: https://blogs.microsoft.com/on-the-issues/

保持联系: @msftissues and @msftsecurity