Symantec™

ISTR

《互联网安全威胁报告》

第 24 期 | 2019 年 2 月

本文档按“现状”提供，赛门铁克对此文档中所有明示或暗示的条件、声明和保证概不负责，包括有关适销性、特定目的适用性或不侵权的任何担保，除非此类免责声明被判无效。

对于与提供、执行或使用本文档相关的偶然或连带损失，赛门铁克不承担任何责任。本文档内容如有更改，恕不另行通知。

从第三方来源获得的信息被认为是可靠的，但并不保证百分之百正确。

本文档中所提及的安全产品、技术服务和任何其他技术数据（“管制产品”）均需遵循美国出口管制和管辖法律的规定与要求，同时还需遵循其他国家的出口或进口法规。

您同意严格遵守上述法律、法规和要求，并承认需要获得授权许可、允许或其他批准，方可出口、再出口、国内转让或进口此类管制产品。

目录

BIG NUMBERS

数据统计

Symantec™

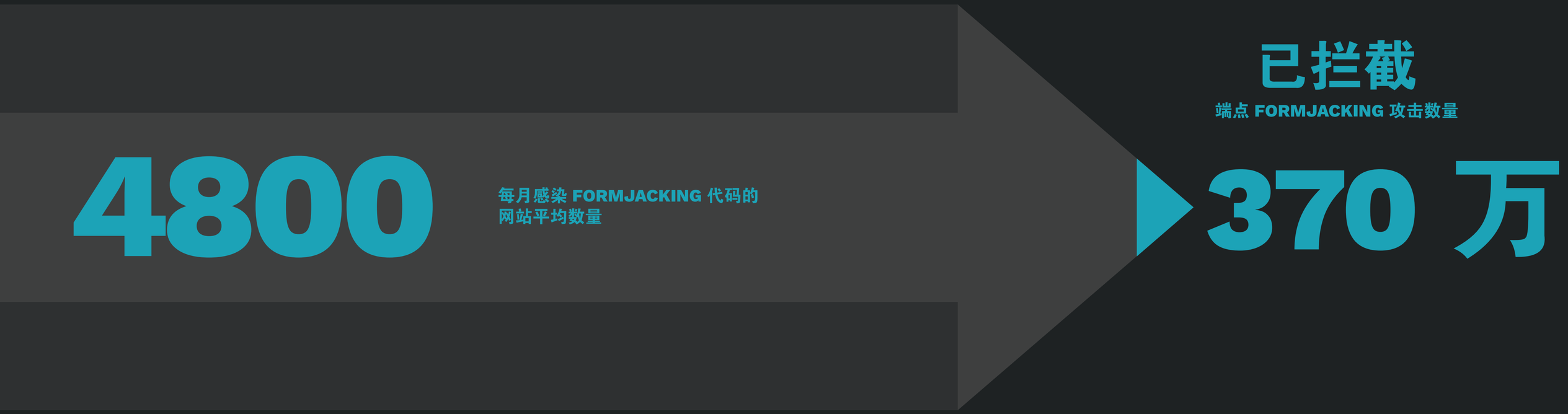
恶意 URL

1/10

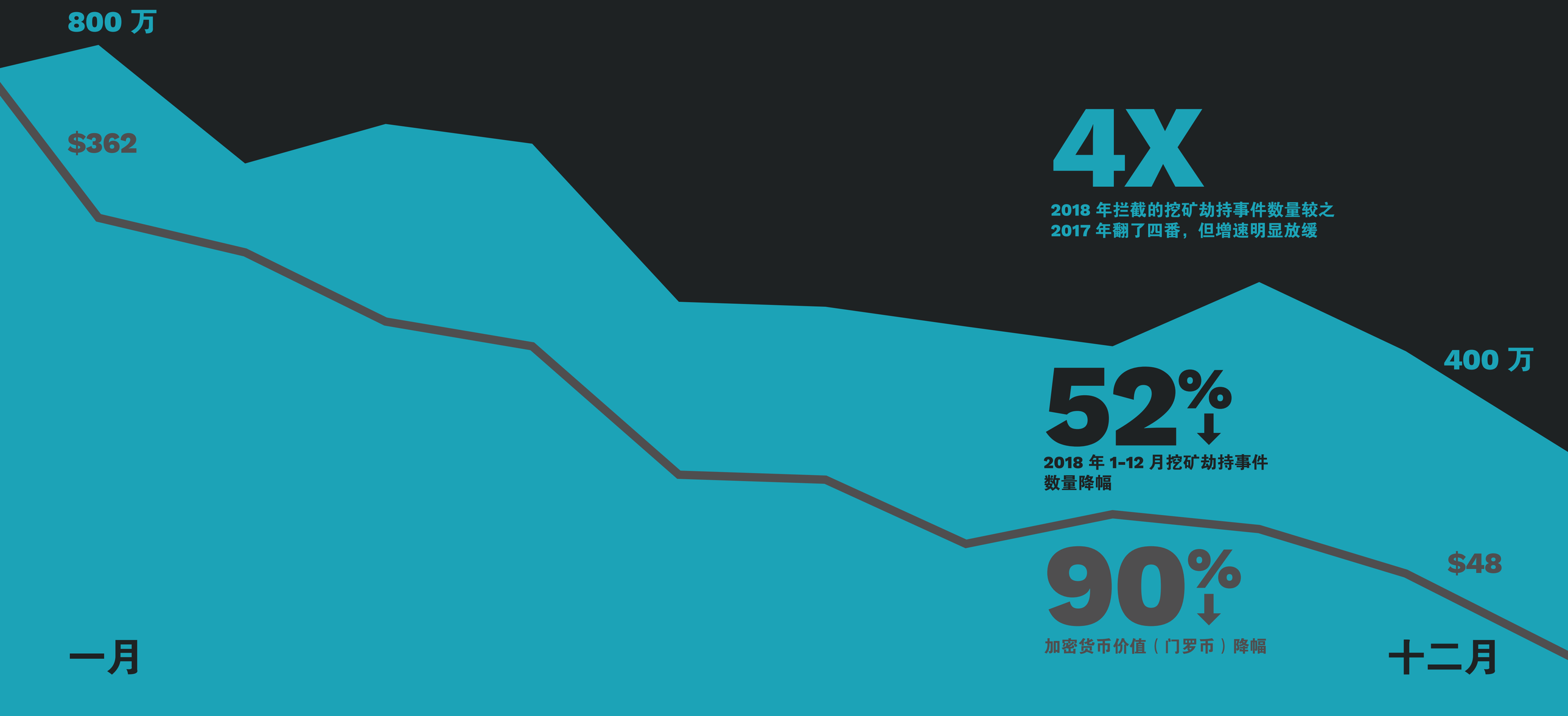
的 URL 为恶意链接

Web 攻击

FORMJACKING 攻击



挖矿劫持



4X

2018 年拦截的挖矿劫持事件数量较之 2017 年翻了四番，但增速明显放缓

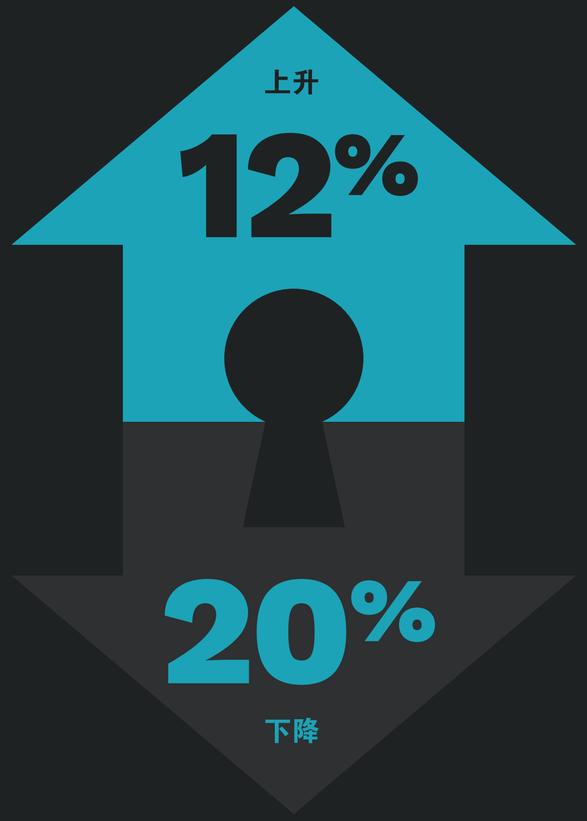
52%↓

2018 年 1-12 月挖矿劫持事件数量降幅

90%↓

加密货币价值（门罗币）降幅

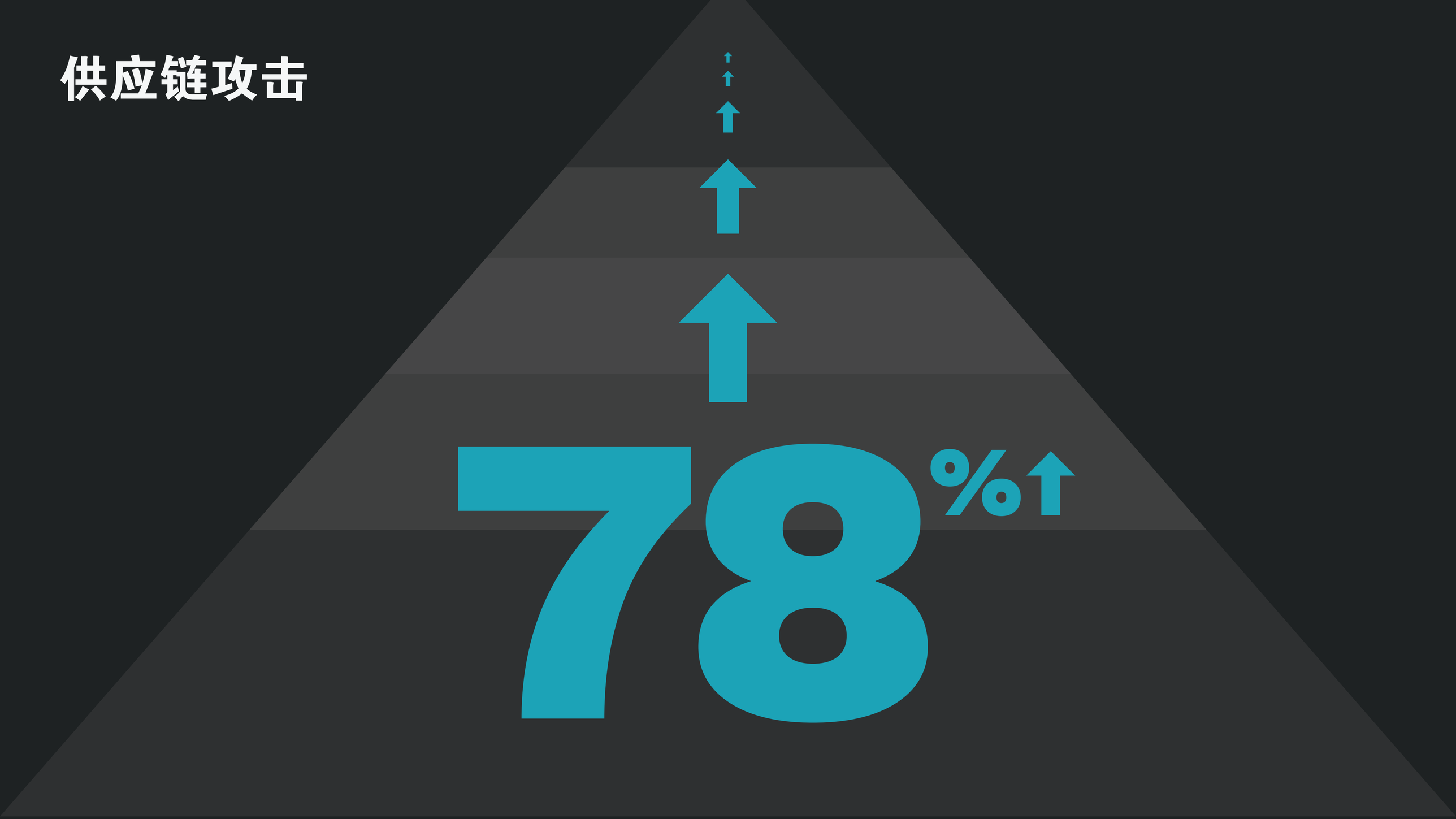
企业勒索软件



移动设备勒索软件

勒索软件总数

供应链攻击



恶意电子邮件

48%

的恶意电子邮件使用 OFFICE 文件作为附件，较 2017 年的 5% 有大幅上涨

POWERSHELL

> 1000%

恶意 POWERSHELL 脚本增幅

使用破坏性恶意软件的
攻击团伙数量

各攻击团伙的攻击目标
组织平均数量

YEAR IN REVIEW 2

年度回顾

Symantec™

{FORMJACKING}

网络犯罪分子以支付卡数据为目标。

Formjacking 事件—使用恶意 JavaScript 代码窃取电商网站结账页面的付款表中的信用卡详细信息和其他信息，这一攻击在 2018 年呈增多趋势。

赛门铁克的数据表明，2018 年每个月都有 4818 个网站感染 Formjacking 代码。在黑市上，单张信用卡的数据只售 45 美元，不过，网络犯罪分子每个月只需用 10 张从受感染网站盗取的信用卡，就能谋取高达 220 万美元的暴利。对于网络犯罪分子而言，Formjacking 攻击的吸引力显而易见。

2018 年，赛门铁克共阻止了超过 370 万次 Formjacking 攻击，其中超过 100 万次是在当年最后两个月发生的。2018 年全年均有 Formjacking 攻击发生，其中 5 月攻击次数反常激增（当月共有 55.6 万次攻击），且后半年的攻击次数总体呈上升趋势。

大部分此类 Formjacking 攻击都被归咎于称为 Magecart 的发起者，有人认为，Magecart 有诸多团伙，其中至少有一些团伙属于竞争关系。公众普遍认为 Magecart 策划了好几次知名攻击事件，包括对英国航空、Ticketmaster、英国电子产品零售商 Kitronik 和隐形眼镜公司 VisionDirect 的攻击。

Formjacking 攻击的上涨反映了我们在《互联网安全威胁报告》第 23 期中讨论的供应链攻击的整体上升趋势。在许多攻击案例中，Magecart 以第三方服务为突破口，将恶意代码植入目标网站。例如，在备受关注的 Ticketmaster 攻击事件中，Magecart 攻击了第三方聊天机器人，从而将恶意代码加载到 Ticketmaster 网站访问者的网页浏览器中，秘密窃取客户的支付数据。

虽然只有针对知名品牌的攻击会成为头条新闻，但赛门铁克的遥测数据显示，销售服装、园艺设备和医疗用品等产品的中小型零售商网站才是 Formjacking 代码的主要攻击目标。这是一个全球性问题，有可能对所有接受客户在线付款的企业造成不利影响。

2018 年加密货币贬值可能是 Formjacking 攻击增多的原因之一：原先使用网站进行挖矿劫持的网络犯罪分子如今可能选择发起 Formjacking 攻击。在当前的环境下，网络黑市中被盗信用卡信息的价值可能比加密货币的价值更有保障。

CRYPTOJACKING

挖矿劫持

虽有减缓，但从未停止。

挖矿劫持指的是网络犯罪分子在受害者不知情的情况下，利用受害者的设备秘密运行挖矿软件，并使用其中央处理器 (CPU) 挖掘加密货币。该攻击于 2017 年最后一季度风行，并成为 2018 年网络安全领域的主要特征之一。

挖矿劫持活动在 2017 年 12 月至 2018 年 2 月达到顶峰，在此期间，赛门铁克每月拦截约 800 万次挖矿劫持攻击。2018 年，我们拦截的挖矿劫持攻击相当于 2017 年的四倍多。在 12 个月内，我们共拦截了近 6900 万次挖矿劫持攻击，而 2017 年这一数字才刚刚超过 1600 万次。然而，2018 年的挖矿劫持攻击呈下降趋势，从 1 月到 12 月下降了 52%。尽管攻击次数呈下降趋势，但我们在 2018 年 12 月仍拦截了超过 350 万次挖矿劫持攻击。

虽然 2018 年加密货币的价值大幅下降，但挖矿劫持攻击仍然不容忽视。加密货币的价值在 2017 年底达到了历史最高值，这是挖矿劫持攻击最初风行的主要原因之一。

虽然部分最初进行挖矿劫持攻击的犯罪分子转而选择 Formjacking 等其他牟利方式，但相当一部分网络犯罪分子认为挖矿劫持仍有潜力。2018 年，部分挖矿劫持犯罪分子利用挖矿劫持脚本 WannaMine (MSH.Bluwimps)，通过因 WannaCry 而声名大噪的永恒之蓝漏洞利用程序在企业网络间扩散，导致部分设备因 CPU 使用率过高而无法使用。

2018 年，大部分挖矿劫持活动仍然源自基于浏览器的挖矿软件。基于浏览器的挖矿行为在网页浏览器内部进行，并使用脚本语言执行。如果某网页中包含挖矿脚本，只要打开该网页，网页访问者计算机的计算能力就会被用于挖掘加密货币。网络犯罪分子可以利用基于浏览器的挖矿软件入侵设备，甚至是完全修补过的设备，在受害者毫无察觉的情况下隐秘操作。

我们曾预测，网络犯罪分子是否进行挖矿劫持活动在很大程度上取决于加密货币的价值是否居高不下。随着加密货币价值的下滑，挖矿劫持活动的次数也有所下降。然而，挖矿劫持活动的减少幅度远远不及加密货币价值的下跌幅度：2018 年，门罗币的价值下降近 90%，而挖矿劫持活动仅减少了约 52%。这意味着部分网络犯罪分子仍然认为挖矿劫持有利可图，或者在等待加密货币的价值再次飙升。这还表明挖矿劫持具有其他吸引网络犯罪分子的特质，例如匿名性和低门槛。因此，网络犯罪分子很有可能继续将挖矿劫持作为攻击手段之一。

攻击活动有所消停，但对企业而言仍是一项严峻的挑战。

2018 年，勒索软件活动自 2013 年以来首次减少，各端点的勒索软件总感染数下降 20%。其中，WannaCry 及其山寨版以及 Petya 造成的感染大大抬高了总感染数。如果从统计数据中删除这些蠕虫病毒，感染数的下降就更为明显：52%。

然而，总体数据中呈现出一个戏剧性变化。2017 年之前，个人用户更易受到勒索软件的攻击，在总感染中占据绝大多数。2017 年，天平已然倾向企业用户，大部分勒索软件感染是针对企业用户的。2018 年，这一趋势加快发展，企业用户在勒索软件总感染数中占据 81%。2018 年，虽然勒索软件总感染数有所下降，但企业用户感染数上升了 12%。

勒索软件受害者的变化可能是由于漏洞利用工具包活动有所减少，而这曾是勒索软件传播的重要渠道之一。2018 年，最主要的勒索软件传播方式是电子邮件。企业更容易受到基于电子邮件的攻击影响，因为电子邮件仍然是企业的主要通信工具。

与此同时，越来越多的个人用户只使用移动设备，他们的基本数据往往备份在云端。由于大多数主要的勒索软件系列仍然以 Windows 电脑为目标，个人用户遭到勒索软件攻击的几率逐渐下降。

勒索软件活动整体减少的另一个原因是赛门铁克在感染初期阻止勒索软件的效率进一步提升，无论是通过电子邮件防护还是使用行为分析或机器学习等技术。部分网络犯罪团伙逐渐失去了对勒索软件的兴趣，这也导致了勒索软件活动的减少。赛门铁克发现，众多曾参与传播勒索软件的团伙已转而传播其他恶意软件，如银行木马和信息窃取软件。

但是，部分勒索软件团伙仍然会带来严峻的威胁。对企业来说，更坏的消息是，2018 年，大量破坏性极强的目标性勒索软件攻击对众多企业造成重创，其中很多攻击是由 SamSam 团伙发起。2018 年，赛门铁克共检测到 67 次 SamSam 攻击，其中大部分是针对美国企业。在 SamSam 的推动下，其他目标性勒索软件团伙也更为活跃。

其他目标性威胁也不断涌现。涉及 Ryuk (Ransom.Hermes) 的攻击活动在 2018 年年末激增。该勒索软件是 12 月美国几家知名报纸的印刷和发行中断的罪魁祸首。

Dharma/Crysis (Ransom.Crysis) 也经常用于针对企业的目标性攻击。2018 年，赛门铁克检测到的 Dharma/Crysis 感染企图翻了三番，从 2017 年的平均每月 1473 例增至 2018 年的每月 4900 例。

11 月，两位伊朗公民在美国被指控参与了 SamSam 攻击。这一指控是否会对该团伙的活动产生任何影响还有待观察。

勒索软件

LIVING OFF THE LAND AND SUPPLY CHAIN ATTACKS

离地攻击和供应链攻击

仍是最新威胁态势的关键要素之一。

我们在以往的报告中强调了攻击者利用现成工具和操作系统功能发起攻击的趋势。2018 年，这一“离地”趋势并未显示出减弱迹象，事实上，部分活动呈现出明显上升态势。目前，使用 PowerShell 是网络犯罪和目标性攻击的主要手段。2018 年，端点上拦截的恶意 PowerShell 脚本数量激增 1000%，也从侧面证明了这一点。

2018 年，Microsoft Office 文件在所有恶意邮件附件中占近一半 (48%)，而 2017 年这一比例仅为 5%。Mealybug 和 Necurs 等网络犯罪团伙在 2018 年继续使用 Office 文件中的宏作为传播恶意负载的首选方法，同时也尝试使用 DDE 负载的恶意 XML 文件和 Office 文件。

2018 年，零日漏洞在目标性攻击团伙中的利用率呈持续下降趋势。据了解，2018 年仅有 23% 的攻击团伙仍在使用零日漏洞，较 2017 年 27% 下降三个百分点。同时，去年开始出现了仅仅依靠离地攻击技术而不使用任何恶意代码的攻击。目标性攻击团伙 Gallmaker 就是其中之一，他们专门借助常用现成工具来执行其恶意活动。

自我传播的威胁仍然是企业面临的一大难题，但与以往蠕虫不同的是，现代蠕虫不再使用可远程利用的漏洞来进行传播。相反，诸如 Emotet (Trojan.Emotet) 和 Qakbot (W32.Qakbot) 等蠕虫病毒会采用从内存转储密码或暴力访问网络共享等简单的技术在网络中横向移动。

供应链攻击仍然是威胁态势中的一大主角，2018 年的攻击数量增加了 78%。供应链攻击可通过多种形式利用第三方服务和软件来感染最终目标，包括劫持软件更新和将恶意代码植入合法软件等等。开发人员仍被用作供应链攻击的来源，途径就是攻击者要么盗取版本控制工具的凭据，要么感染集成到大型软件项目中的第三方库。

2018 年 Formjacking 攻击数量激增，进一步证明供应链仍然是电商网站和电商卖家的薄弱环节。许多此类攻击的入口都是攻击者破坏电商卖家常用的第三方服务，例如聊天机器人或客户评论小部件。

供应链攻击和离地攻击导致企业和个人面临越巨大挑战，因为攻击越来越多地通过可信渠道、采用无文件攻击方法或合法工具执行恶意操作。我们每个月阻止的恶意 PowerShell 脚本平均多达 11.5 万个，但这个数字在 PowerShell 总体使用量中却只占不到百分之一。只有借助分析技术和机器学习等先进的检测方法才能有效地识别和阻止这些攻击。

MORE AMBITIOUS
更加疯狂

AND STEALTHIER
更加隐秘

2018 年，由于大量新团伙不断涌现，现有团伙持续改进工具和策略，目标性攻击者仍然对企业构成重大威胁。规模大、活跃度高的攻击团伙在 2018 年的活动力度似乎有所加大。在过去三年中，赛门铁克跟踪的 20 个最活跃团伙平均攻击了 55 家企业，这一数字在 2015 至 2017 年之间为 42。

TARGETED ATTACKS.
目标性攻击

去年的一个显著趋势是攻击目标出现多样化，越来越多的攻击团伙对入侵可操作性计算机产生兴趣。只要他们愿意，可能就会获取相关权限，实施破坏性操作。

这种策略由 Dragonfly 间谍团伙所开创，该团伙因对能源公司发起的攻击而广为人知。2018 年，我们发现 Thrip 团伙入侵了一家卫星通信运营商并感染了正在运行卫星监测和控制软件的计算机。Thrip 完全可以借助这次攻击严重破坏该公司的运营。

我们还检测到 Chafer 团伙入侵了一家中东地区的通信服务提供商。该公司向该地区多家通信运营商销售解决方案，此次攻击的目的可能是为了方便监视这些运营商的最终用户客户。

这种对潜在破坏性攻击的浓厚兴趣也反映在已知使用破坏性恶意软件的团伙数量上，这些团伙在 2018 年上涨了 25%。

2018 年，赛门铁克揭露了四个前所未知的目标性攻击团伙。至此，赛门铁克自 2009 年以来首次曝光的目标性攻击团伙数量增加至 32 个。虽然赛门铁克在 2017 年和 2018 年分别曝光了四个新的攻击团伙，但发现这些团伙的方式却大有不同。在 2018 年揭露的四个新团伙中，有两个是因为他们使用了离地攻击工具而被发现。事实上，其中一个团伙 (Gallmaker) 在攻击中并未使用任何恶意软件，而是完全依赖于离地攻击工具和公开可售的黑客工具。

近年来，离地攻击愈加受到目标性攻击团伙的青睐，原因在于它能够将攻击活动隐藏在大量合法的进程中而更具隐秘性。这种趋势也是赛门铁克在 2018 年创建目标性攻击分析 (TAA) 解决方案的主要动机之一。该方案利用高级人工智能技术，可及时发现与目标性攻击相关的恶意活动模式。2018 年，我们两次在离地攻击工具触发的调查中使用目标性攻击分析发现了此前未知的目标性攻击团伙。离地攻击工具使用量的上涨也可以从其他老派攻击技术的衰落中反映出来。去年，已知的目标性攻击团伙中使用零日漏洞的百分比为 23%，较 2017 年底的 27% 有所下降。

2018 年最引人注目的事件之一莫过于美国大力控诉有政府背景的间谍活动，被起诉的涉嫌参与人员数量大幅增加。2018 年有 49 名个人或组织遭到起诉，而 2017 和 2016 年这一数字分别为 4 和 5。尽管大多数新闻头条都在集中报道对 18 名俄罗斯特工的控诉，其中大多数人被指控参与了 2016 年美国总统大选有关的袭击事件，但实际上这些控诉的范围要广得多。除俄罗斯公民之外，还有 19 名中国个人或组织、11 名伊朗人和 1 名朝鲜人遭到指控。

这种突发的公开控诉有可能会给部分涉事组织带来不少麻烦。被起诉之后，涉事个人的国际通行会受到高度限制，也就无法顺利针对其他国家的目标开展行动。

安全挑战
从多个方位汹汹袭来。

2018 年，从简单的配置不当问题到硬件芯片中的漏洞，我们发现云端同样面临着各种安全挑战。

安全性不高的云端数据库仍然是企业的短板。2018 年，S3 存储桶成为了企业的致命弱点，由于配置不当，超过 7000 万条记录被盗或泄露。在此之前，攻击者还对 MongoDB 等公开数据库发起一系列勒索软件攻击，他们擦除数据库内容并以恢复数据为由勒索钱财。然而攻击者并未就此罢手。他们还将目标转向容器部署系统（如 Kubernetes）、无服务器应用程序和其他公开的 API 服务。这些事件中的一个共同主题就是配置不当。

网络上有众多现成工具可让潜在攻击者识别出配置不当的云资源。企业必须主动采取防护措施，妥善保护云资源，例如听从亚马逊的建议来保障 S3 存储桶安全，才能避免遭受攻击。

2018 年，随着硬件芯片的几个漏洞被曝光，云计算面临的一个更危险的威胁浮出水面。Meltdown 和 Spectter 在名为推测执行的过程中利用其中漏洞。如果漏洞被成功利用，攻击者就可以堂而皇之地访问通常被禁止的存储位置。这样会对云服务造成很大困扰，因为云实例虽然各有其自身的虚拟处理器，但却共享内存池，这就意味着对单个物理系统的成功攻击极可能导致多个云实例的数据泄漏。

Meltdown 和 Spectre 并非孤立的存在，它们的变体在随后的一年中逐渐浮出水面。紧接着又出现了类似的芯片级漏洞利用，例如 Speculative Store Bypass 和 Foreshadow 或 L1 Terminal Fault。这可能还只是开端，因为目前研究人员和攻击者都将目光集中到芯片级漏洞上，这表明未来云端会继续面临挑战。

成为攻击目标
逃离不了网络犯罪分子和目标性攻击团伙的魔爪

尽管蠕虫和僵尸程序仍是物联网 (IoT) 攻击的主要作案伎俩，但在 2018 年，我们发现了一种新的威胁形式，目标性攻击者似乎有意将物联网用作一种感染载体。

2018 年物联网攻击的总数居高不下，与 2017 年基本持平（仅下降 0.2%）。路由器和联网摄像机最易受到感染，它们的感染比例分别占到 75% 和 15%。毫无疑问，路由器是最容易遭到攻击的设备，因为它们可从互联网轻易访问。它们受攻击者青睐的另一个原因在于，它们是高效的起跳点。

臭名昭著的 Mirai 分布式拒绝服务 (DDoS) 蠕虫仍然十分活跃，在所有攻击中占比 16%，是 2018 年第三大常见的物联网威胁。Mirai 不断演变，其变体可利用多达 16 种不同的漏洞。它们还在不断添加新的漏洞利用来提高感染几率，因为设备的漏洞通常并不能及时得到修补。这种蠕虫还通过追踪未修补的 Linux 服务器来扩大目标范围。另一个明显的趋势是工业控制系统 (ICS) 遭到的攻击逐渐上涨。Thrip 团伙感染了卫星运行系统，而 Triton 则侵入工业安全系统。这些系统被置于险地，随时可能遭受破坏性攻击或勒索攻击。任何计算设备都有可能成为攻击目标。

2018 年出现的 VPNFilter 代表了物联网威胁的一大演变。VPNFilter 是首个广泛存在的持久性物联网威胁，它能够在设备重启后继续存在，因而极难删除。VPNFilter 不同于 DDoS 和挖矿攻击等传统物联网威胁活动，它拥有一系列可用的攻击负载，例如中间人 (MitM) 攻击、泄露数据、盗取凭据以及拦截 SCADA 通信。它还可以按照攻击者的命令“毁掉”设备或擦除设备数据来摧毁一切攻击证据。VPNFilter 是一名技术娴熟、资源丰富的攻击者的成果，它表明当前物联网设备正面临来自多方位的攻击。

ELECTION INTERFERENCE 2018

2018 年选举干扰事件

由于 2016 年的美国总统选举遭受了多次网络攻击，例如民主党全国委员会 (DNC) 遭到的袭击，2018 年的中期选举可谓万众瞩目。就在选举过去一个月后，共和党众议院全国委员会 (NRCC) 证实其电子邮件系统在中期选举准备期间遭受了未知第三方的攻击。据报道，黑客窃取了四名 NRCC 高级助手的电子邮件帐户访问权限，可能在几个月的时间内收集了数千封电子邮件。

2019 年 1 月，DNC 透露在中期选举结束后不久就被鱼叉式钓鱼攻击盯上，但所幸的是该次攻击未得逞。由美国国土安全部 (DHS) 和联邦调查局定性为俄罗斯组织的网络间谍团伙 APT29 被认定是该事件的主谋。

2018 年 7 月和 8 月，Microsoft 发现并关闭多个仿冒政治机构网站的恶意域。由国土安全部和联邦调查局定性为俄罗斯组织的网络间谍团伙 APT28 被认定是这些网站的创建人。这些网站是鱼叉式钓鱼攻击的重要组成部分，目标直指 2018 年中期选举的候选人。为抵抗此类网站欺骗攻击，赛门铁克面向网站所有者推出一款免费的安全工具 Dolphin 计划。

2018 年，攻击者仍然借助社交媒体平台对选民施加影响。虽然这已不是什么新鲜花招，但他们使用的策略却更为狡猾。例如，众多与俄罗斯相关的帐户通过第三方为这些域购买了社交媒体广告，但他们并没有使用俄罗斯 IP 地址或俄罗斯货币。诸多虚假帐户也开始关注宣传活动和集会，这类事件不像政治目标广告那样受到严密监控。

2018 年社交媒体公司和政府机构在打击选举干扰方面发挥了更积极的作用。Facebook 专门成立了“作战室”来应对选举干扰，并拦截了大量疑似与试图影响美国、英国、中东和拉丁美洲等地政治的国外实体相关联的帐户和页面。

Twitter 则删除了 10,000 个劝说人们不参加投票的僵尸程序并更新了相关细则，引导民众识别虚假帐户，保证选举顺利进行。Twitter 还发布了与两场有政府参与的宣传活动相关的推文档案，这两次宣传活动曾滥用该平台传播影响公众舆论的虚假信息。

除此之外，2018 年美国各方也为对抗选举干扰做了积极努力，例如，美国网络司令部直接联系俄罗斯黑客，告诉他们美国特工已经确认了他们的身份并正在追踪他们；美国国土安全部对州选举机器和流程进行免费安全评估；以及广泛使用一种名为 Albert 传感器的硬件来帮助联邦政府监测选举用计算机是否受到干扰。

3 FACTS AND FIGURES

事实与数据

Symantec™

消息传送

相比而言，2018 年小企业员工要比大企业员工更易受到垃圾邮件、网络钓鱼及电子邮件恶意软件等电子邮件威胁的攻击。我们还发现，自 2015 年以来垃圾邮件数量一直呈增长趋势，2018 年 55% 的电子邮件归类为垃圾邮件，这个上涨趋势并没减缓的迹象。此外，电子邮件恶意软件数量变化不大，但网络钓鱼比例从 2017 年的 1/2995 降至 2018 年的 1/3207。网络钓鱼比例在过去四年呈持续下降趋势。

我们还发现恶意电子邮件中 URL 的使用率有所下降，原因在于攻击者已经将恶意电子邮件附件作为主要感染载体。2017 年恶意 URL 在电子邮件中使用比例已达到 12.3%，但这一数字在 2018 年回落至 7.8%。赛门铁克遥测数据显示，Microsoft Office 用户最容易成为基于电子邮件的恶意软件的受害者，Office 文件在所有恶意邮件附件中的占比从 2017 年的 5% 跃升至 48%。

48%↑

的恶意电子邮件使用 OFFICE 文件作为附件，较 2017 年的 5% 有大幅上涨

伪装成通知（例如发票或收据）的恶意电子邮件

1

附件中的 OFFICE 文件包含恶意脚本

2

打开附件执行脚本下载恶意软件

3

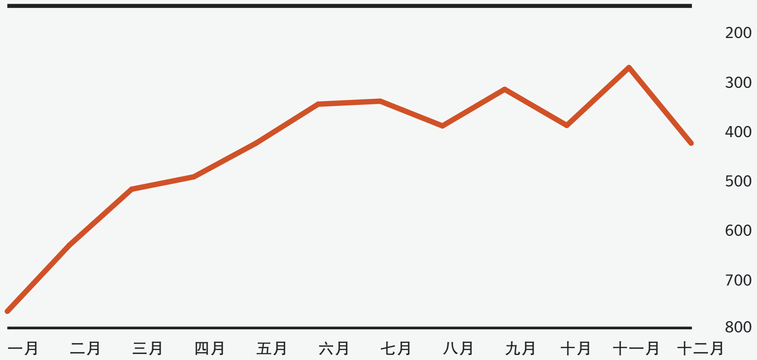
恶意电子邮件比例（年份）

2018
1/412

恶意电子邮件 URL 比例（年份）

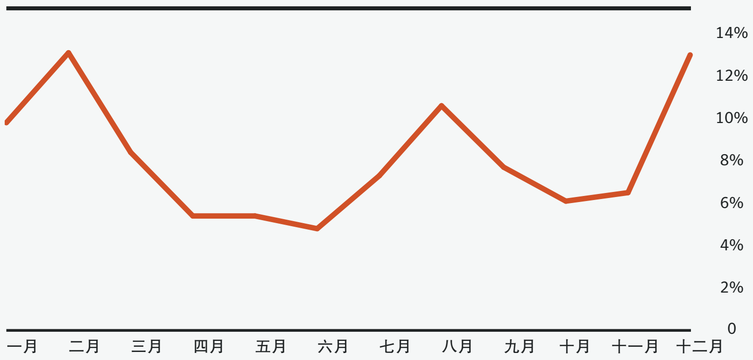
2018
7.8%

恶意电子邮件比例（月份）

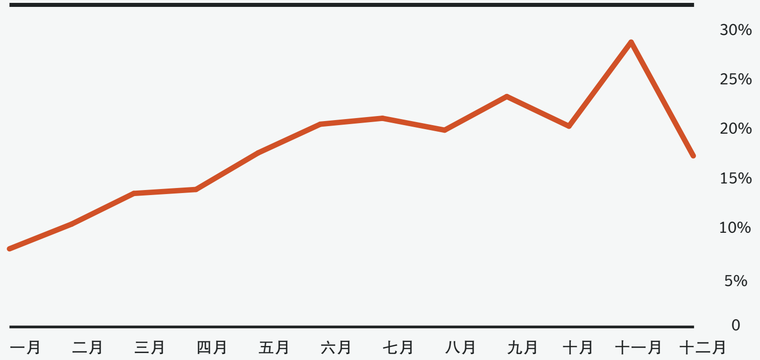


2018 年，受到恶意电子邮件攻击的用户比例呈上升趋势

恶意电子邮件 URL 比例（月份）



每位用户收到的恶意电子邮件数量（月份）



各行各业的恶意电子邮件比例（年份）

行业	恶意电子邮件比例（1/XX）
采矿业	258
农林渔业	302
公共管理	302
制造业	369
批发业	372
建筑业	382
无法归类机构	450
运输和公共事业	452
金融、保险和房地产业	491
服务	493
零售业	516

各行各业的恶意电子邮件 URL 比例（年份）

行业	电子邮件恶意软件 (%)
农林渔业	11.2
零售业	10.9
采矿业	8.9
服务	8.2
建筑业	7.9
公共管理	7.8
金融、保险和房地产业	7.7
制造业	7.2
无法归类机构	7.2
批发业	6.5
运输和公共事业	6.3

相比而言，小企业员工要比大企业员工更易受到垃圾邮件、网络钓鱼及电子邮件恶意软件等电子邮件威胁的攻击。

各行各业每位用户收到的恶意电子邮件数量（年份）

行业	针对的用户 (%)
采矿业	38.4
批发业	36.6
建筑业	26.6
无法归类机构	21.2
零售业	21.2
农林渔业	21.1
制造业	20.6
公共管理	20.2
运输和公共事业	20.0
服务	11.7
金融、保险和房地产业	11.6

恶意电子邮件比例（按企业规模）（年份）

企业规模	恶意电子邮件比例（1/XX）
1-250	323
251-500	356
501-1000	391
1001-1500	823
1501-2500	440
2501+	556

恶意电子邮件 URL 比例（按企业规模）（年份）

企业规模	恶意电子邮件 (%)
1-250	6.6
251-500	8.3
501-1000	6.6
1001-1500	8.3
1501-2500	7.3
2501+	8.6

每位用户收到的恶意电子邮件数量（按企业规模）（年份）

企业规模	针对的用户（1/XX）
1-250	6
251-500	6
501-1000	4
1001-1500	7
1501-2500	4
2501+	11

各个国家/地区的恶意电子邮件比例（年份）

国家/地区	恶意电子邮件比例（1/XX）
沙特阿拉伯	118
以色列	122
奥地利	128
南非	131
塞尔维亚	137
希腊	142
阿曼	160
中国台湾	163
斯里兰卡	169
阿联酋	183
泰国	183
波兰	185
挪威	190
匈牙利	213
卡塔尔	226
新加坡	228
意大利	232
荷兰	241
英国	255
爱尔兰	263
卢森堡	272
中国香港	294
中国	309
丹麦	311
马来西亚	311
哥伦比亚	328
瑞士	334
巴布亚新几内亚	350
德国	352
菲律宾	406
比利时	406
巴西	415
韩国	418
葡萄牙	447
西班牙	510
芬兰	525
加拿大	525
瑞典	570
新西兰	660
美国	674
法国	725
澳大利亚	728
印度	772
墨西哥	850
日本	905

各个国家/地区的恶意电子邮件 URL 比例（年份）

国家/地区	恶意电子邮件 (%)
巴西	35.7
墨西哥	29.7
挪威	12.8
瑞典	12.4
加拿大	11.5
新西兰	11.3
哥伦比亚	11.0
澳大利亚	10.9
法国	10.5
芬兰	9.7
瑞士	9.5
西班牙	9.4
卡塔尔	8.9
美国	8.9
葡萄牙	8.4
印度	8.3
菲律宾	8.1
新加坡	7.7
卢森堡	7.3
意大利	7.1
奥地利	6.7
南非	6.7
巴布亚新几内亚	6.5
韩国	6.5
德国	6.3
日本	6.3
比利时	6.1
英国	6.1
匈牙利	5.9
沙特阿拉伯	5.2
丹麦	5.1
中国香港	5.1
马来西亚	5.1
中国	4.9
荷兰	4.9
塞尔维亚	4.4
中国台湾	4.4
阿联酋	4.2
斯里兰卡	4.1
爱尔兰	3.9
阿曼	3.6
泰国	3.4
希腊	3.3
波兰	2.8
以色列	1.9

最常用的电子邮件主题（年份）

主题话题	百分比
账单	15.7
邮件投递失败	13.3
软件包投递	2.4
法律/执法	1.1
扫描的文档	0.3

最常用的电子邮件关键字（年份）

词汇	百分比
发票	13.2
邮件	10.2
发件人	9.2
付款	8.9
重要	8.5
信息	7.7
全新	7.2
退回	6.9
:	6.9
发送	6.6

最常用的恶意电子邮件附件类型（年份）

文件类型	百分比
.doc、.dot	37.0
.exe	19.5
.rtf	14.0
.xls、.xlt 和 .xla	7.2
.jar	5.6
.html、htm	5.5
.docx	2.3
.vbs	1.8
.xlsx	1.5
.pdf	0.8

最常用的恶意电子邮件附件类别（年份）

文件类型	百分比
脚本	47.5
可执行文件	25.7
其他	25.1

每月受到 BEC 诈骗攻击的平均企业数量（年份）

平均值
5,803

每个企业平均收到的 BEC 电子邮件数量（年份）

平均值
4.5

最常用的 BEC 电子邮件关键字（年份）

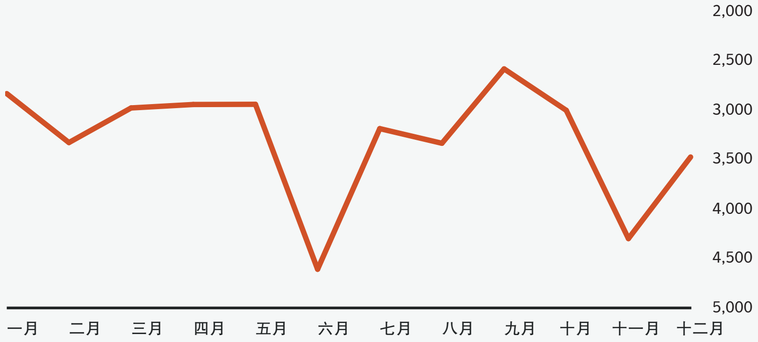
主题	百分比
紧急	8.0
请求	5.8
重要	5.4
付款	5.2
注意	4.4
欠款	4.1
信息	3.6
重大更新	3.1
收件人	2.3
交易	2.3

电子邮件网络钓鱼比例（年份）

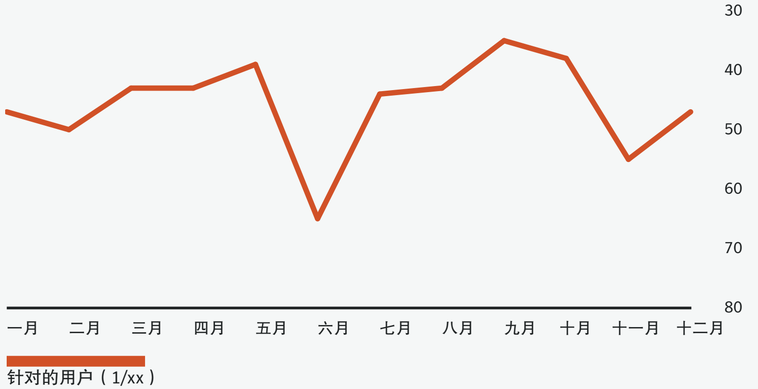
网络钓鱼比例（1/XX）
3,207

网络钓鱼比例从 2017 年的 1/2995 降至 2018 年的 1/3207。

电子邮件网络钓鱼比例（月份）



每位用户收到的电子邮件网络钓鱼比例（月份）



各行各业的电子邮件网络钓鱼比例（年份）

行业	网络钓鱼比例（1/XX）
农林渔业	1769
金融、保险和房地产业	2628
采矿业	2973
批发业	3042
公共管理	3473
服务	3679
建筑业	3960
零售业	3971
制造业	3986
无法归类机构	5047
运输和公共事业	5590

各行各业每位用户收到的电子邮件网络钓鱼比例（年份）

行业	针对的用户（1/XX）
批发业	22
农林渔业	28
采矿业	30
零售业	36
建筑业	39
金融、保险和房地产业	46
制造业	52
无法归类机构	53
公共管理	57
运输和公共事业	62
服务	64

电子邮件网络钓鱼比例（按企业规模）（年份）

企业规模	网络钓鱼比例（1/XX）
1-250	2696
251-500	3193
501-1000	3203
1001-1500	6543
1501-2500	3835
2501+	4286

每位用户收到的电子邮件网络钓鱼比例（按企业规模）（年份）

企业规模	针对的用户（1/XX）
1-250	52
251-500	57
501-1000	30
1001-1500	56
1501-2500	36
2501+	82

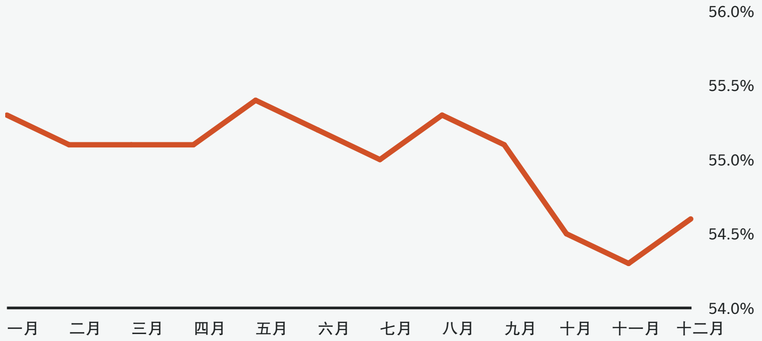
各个国家/地区的电子邮件网络钓鱼比例（年份）

国家/地区	网络钓鱼比例（1/XX）
沙特阿拉伯	675
挪威	860
荷兰	877
奥地利	1,306
南非	1,318
匈牙利	1,339
泰国	1,381
中国台湾	1,712
巴西	1,873
阿联酋	2,312
新西兰	2,446
中国香港	2,549
新加坡	2,857
卢森堡	2,860
意大利	3,048
卡塔尔	3,170
中国	3,208
美国	3,231
爱尔兰	3,321
比利时	3,322
瑞典	3,417
澳大利亚	3,471
瑞士	3,627
西班牙	3,680
英国	3,722
阿曼	3,963
巴布亚新几内亚	4,011
斯里兰卡	4,062
葡萄牙	4,091
菲律宾	4,241
加拿大	4,308
希腊	4,311
以色列	4,472
哥伦比亚	4,619
马来西亚	4,687
德国	5,223
丹麦	5,312
墨西哥	5,389
法国	5,598
印度	5,707
塞尔维亚	6,376
芬兰	6,617
日本	7,652
韩国	8,523
波兰	9,653

垃圾邮件比例（年份）

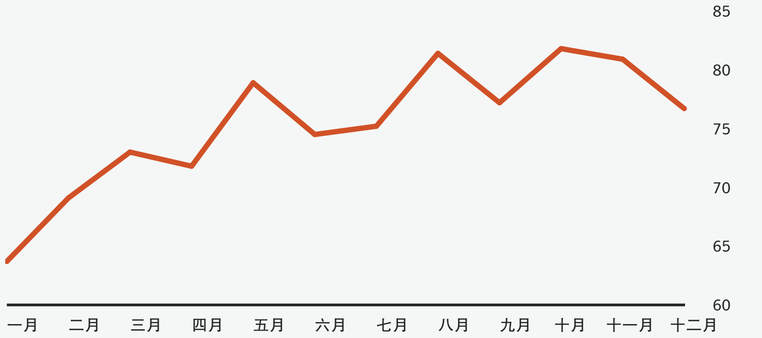
垃圾邮件比例 (%)
55

垃圾邮件比例（月份）



垃圾邮件比例 (%)

每位用户收到的垃圾邮件数量（月份）



每位用户收到的垃圾邮件数量

各行各业的垃圾邮件比例（年份）

行业	垃圾邮件比例 (%)
采矿业	58.3
金融、保险和房地产业	56.7
制造业	55.1
公共管理	54.9
农林渔业	54.6
运输和公共事业	54.6
无法归类机构	54.2
服务	54.1
零售业	53.7
建筑业	53.6
批发业	52.6

各行各业每位用户收到的垃圾邮件数量（年份）

行业	每位用户收到的垃圾邮件数量
批发业	135
零售业	111
采矿业	109
建筑业	103
无法归类机构	97
运输和公共事业	93
制造业	79
农林渔业	66
公共管理	63
金融、保险和房地产业	61
服务	59

垃圾邮件比例（按企业规模）（年份）

企业规模	垃圾邮件比例 (%)
1-250	55.9
251-500	53.6
501-1000	54.5
1001-1500	56.9
1501-2500	53.7
2501+	54.9

每位用户收到的垃圾邮件数量（按企业规模）（年份）

企业规模	每位用户收到的垃圾邮件数量
1-250	55
251-500	57
501-1000	109
1001-1500	125
1501-2500	107
2501+	55

各个国家/地区的垃圾邮件比例（年份）

国家/地区	垃圾邮件比例 (%)
沙特阿拉伯	66.8
中国	62.2
巴西	60.8
斯里兰卡	60.6
挪威	59.1
阿曼	58.6
瑞典	58.3
墨西哥	58.1
阿联酋	58.1
美国	57.5
哥伦比亚	56.8
比利时	56.2
塞尔维亚	55.8
新加坡	55.4
英国	54.8
德国	54.8
中国台湾	54.5
奥地利	54.4
芬兰	54.4
匈牙利	54.4
希腊	54.2
以色列	54.1
丹麦	54.1
法国	54
荷兰	53.9
澳大利亚	53.9
新西兰	53.4
加拿大	53.4
意大利	53.4
波兰	53.2
西班牙	52.9
卡塔尔	52.6
韩国	52.4
葡萄牙	52.1
卢森堡	51.4
马来西亚	51.4
泰国	51.1
爱尔兰	51
印度	50.9
南非	50.8
瑞士	50.8
中国香港	50.5
巴布亚新几内亚	50
菲律宾	49.5
日本	48.7

恶意软件

2018 年，Emotet 继续积极扩大其势力范围，在金融木马中的占比从 2017 年的 4% 上升至 16%。Emotet 同时也被用来传播 Qakbot，在金融木马列表中排名第 7，占总检测量的 1.8%。这两种威胁都能够进行自我传播，致使企业面临的挑战更加严峻。

由于攻击者更加青睐离地攻击技术，2018 年恶意 PowerShell 脚本的使用数量暴涨 1000%。常见的攻击场景则是使用 Office 宏调用 PowerShell 脚本，之后再由 PowerShell 脚本下载恶意负载。在被检测到的下载程序中，Office 宏下载程序占了大头，而 VBS.Downloader 和 JS.Downloader 威胁数量均在下降。

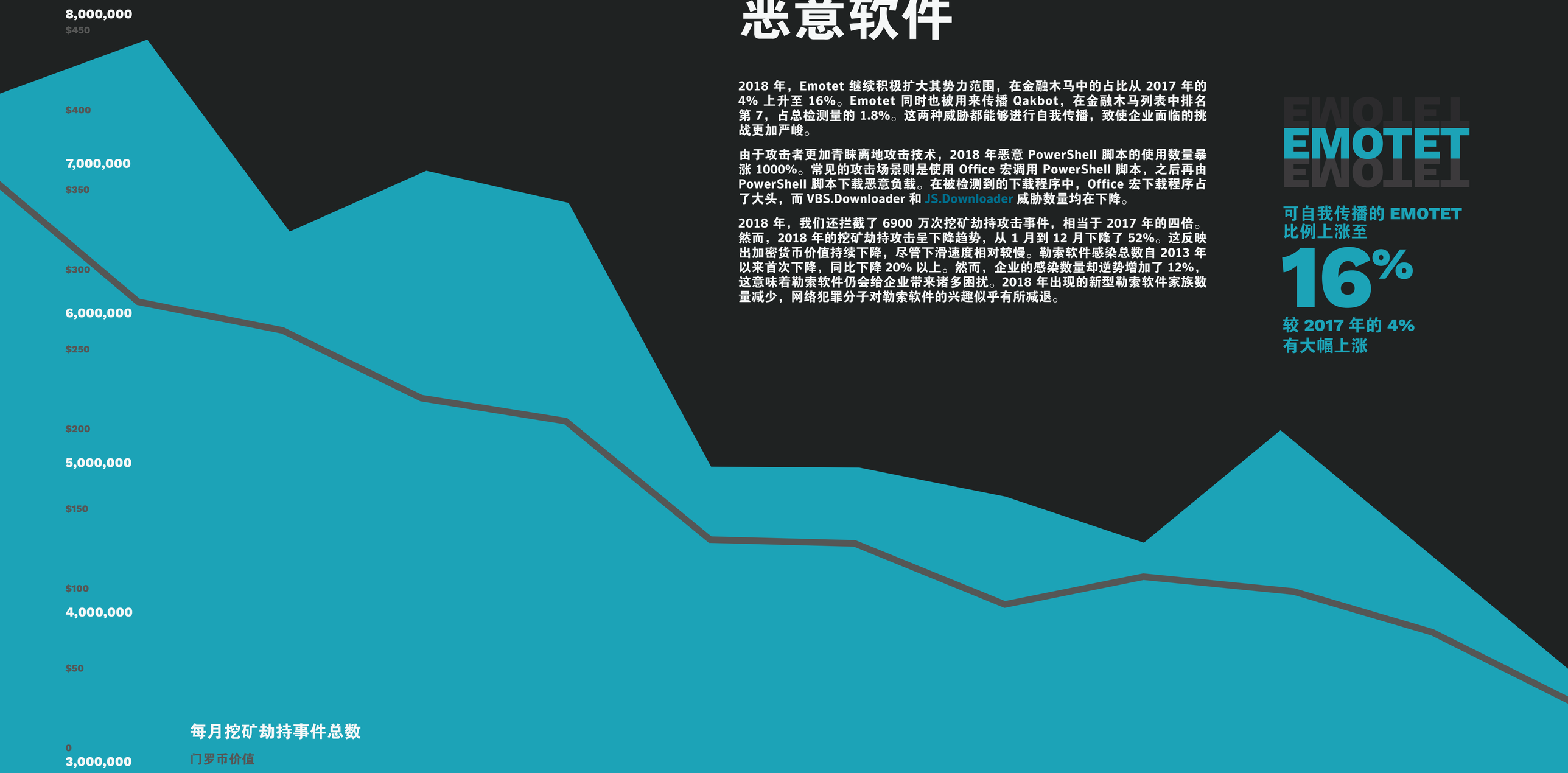
2018 年，我们还拦截了 6900 万次挖矿劫持攻击事件，相当于 2017 年的四倍。然而，2018 年的挖矿劫持攻击呈下降趋势，从 1 月到 12 月下降了 52%。这反映出加密货币价值持续下降，尽管下滑速度相对较慢。勒索软件感染总数自 2013 年以来首次下降，同比下降 20% 以上。然而，企业的感染数量却逆势增加了 12%，这意味着勒索软件仍会给企业带来诸多困扰。2018 年出现的新型勒索软件家族数量减少，网络犯罪分子对勒索软件的兴趣似乎有所减退。

EMOTET

可自我传播的 EMOTET 比例上涨至

16%

较 2017 年的 4% 有大幅上涨

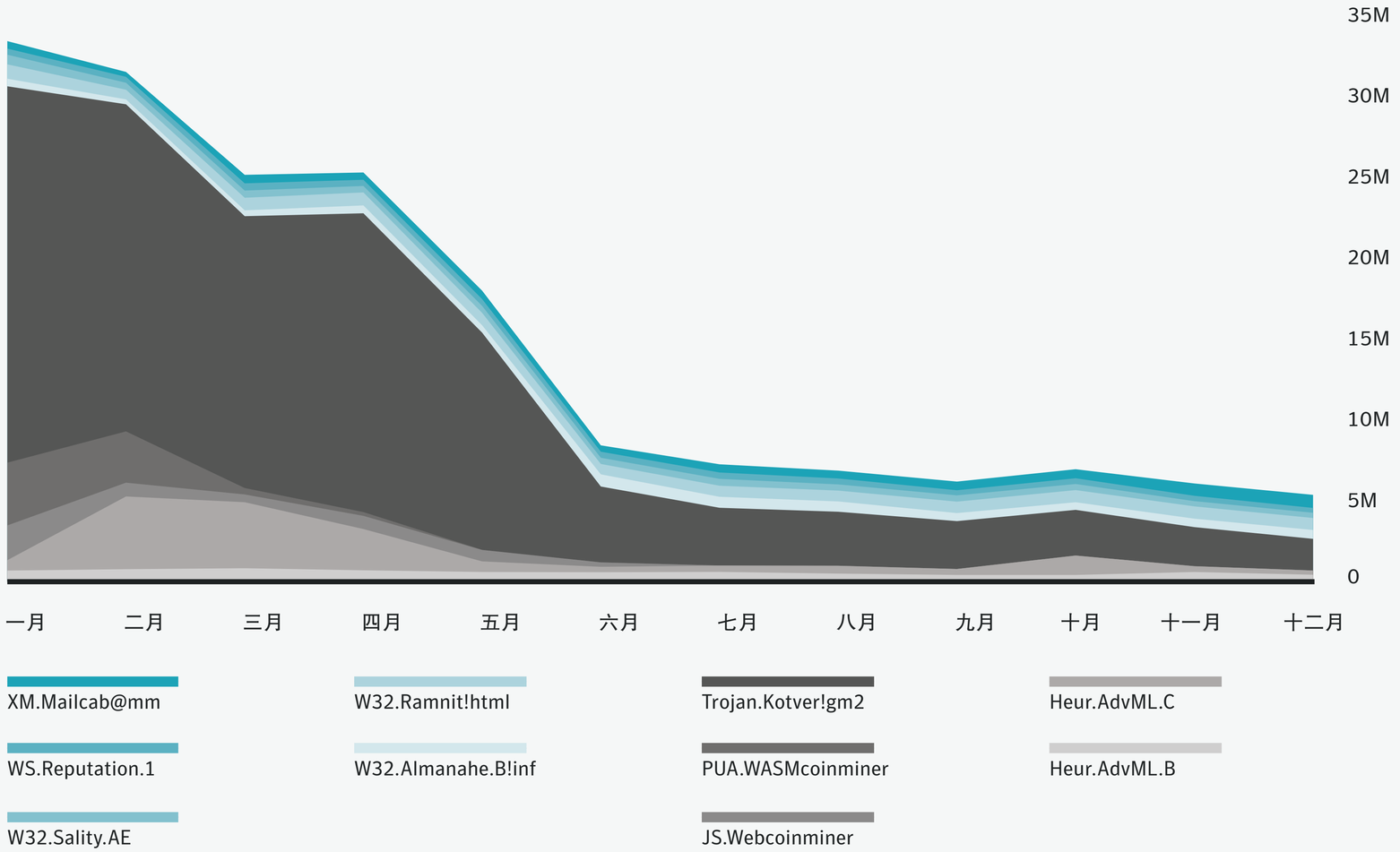


新型恶意软件变体（年份）

年份	新型变体	变动百分比
2016	357,019,453	0.5
2017	669,947,865	87.7
2018	246,002,762	-63.3

2018 年，Emotet 继续积极扩大其势力范围，在金融木马中的占比从 2017 年的 4% 上升至 16%。

最常见的新型恶意软件变体（月份）

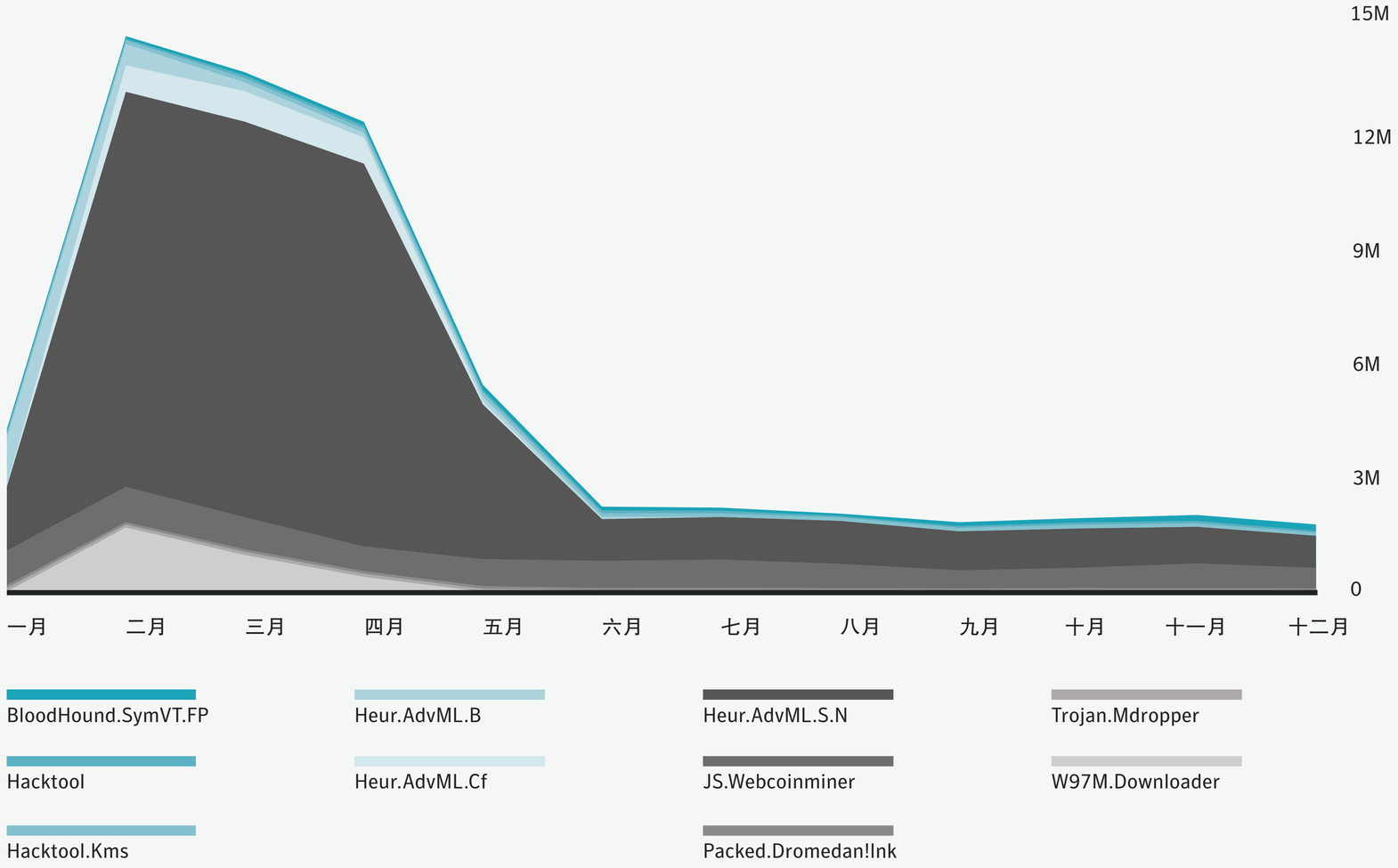


最常见的恶意软件（年份）

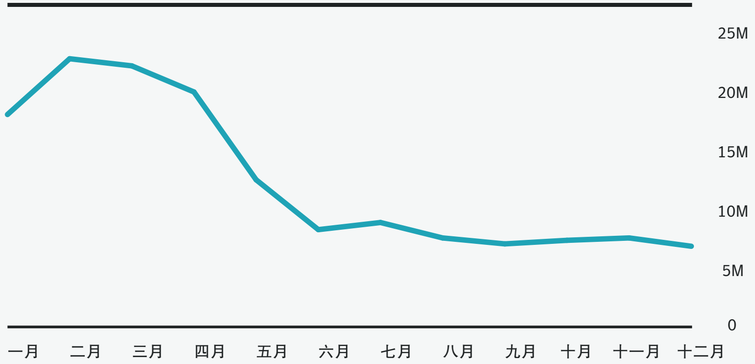
威胁名称	拦截的攻击	百分比
Heur.AdvML.C	43,999,373	52.1
Heur.AdvML.B	8,373,445	9.9
BloodHound.SymVT.FP	3,193,779	3.8
JS.Webcoinminer	2,380,725	2.8
Heur.AdvML.S.N	2,300,919	2.7
W97M.Downloader	1,233,551	1.5
Packed.Dromedan!Ink	1,215,196	1.4
Hacktool	846,292	1.0
Hacktool.Kms	763,557	0.9
Trojan.Mdropper	679,248	0.8

Mealybug 和 Necurs 等网络犯罪团伙在 2018 年继续使用 Office 文件中的宏作为传播恶意负载的首选方法。

最常见的恶意软件（月份）

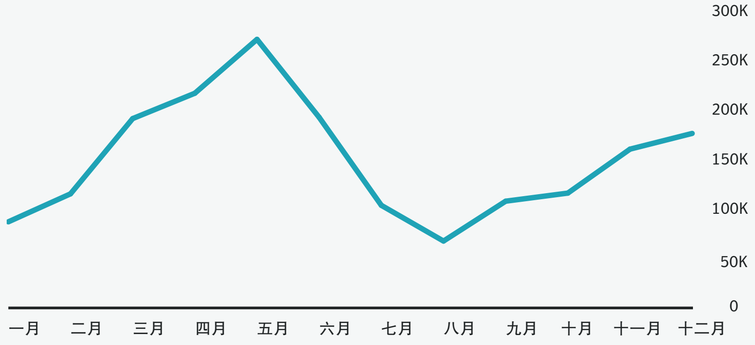


所有恶意软件（月份）



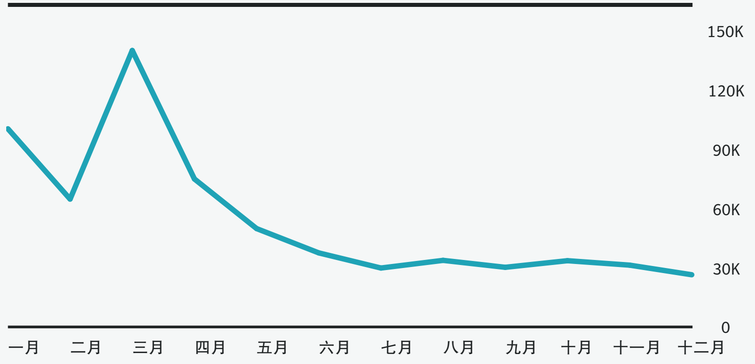
拦截的攻击

OFFICE 宏下载程序（月份）



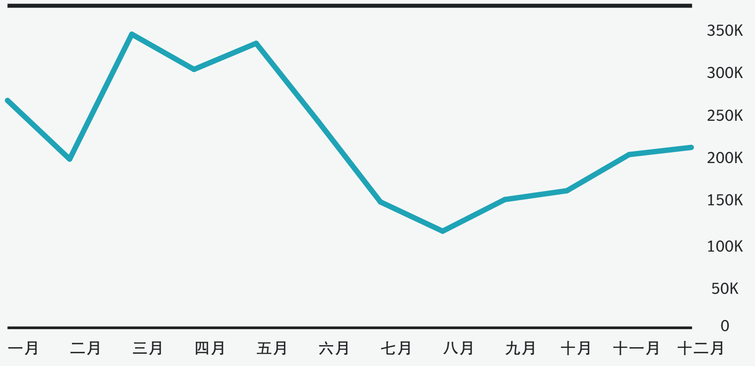
被阻止的下载程序

JAVASCRIPT 下载程序（月份）



被阻止的下载程序

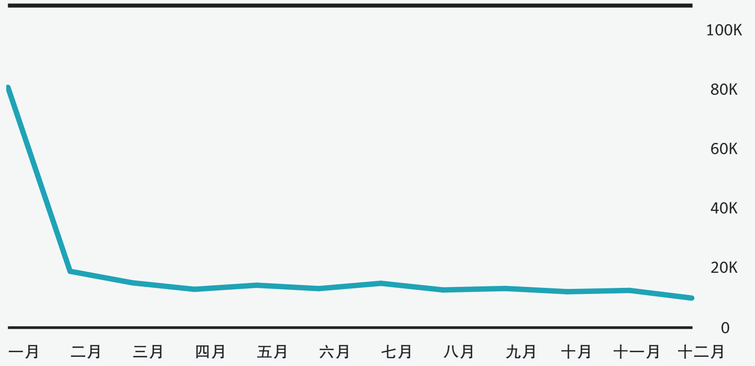
所有下载程序（月份）



被阻止的下载程序

虽然 VBS.Downloader 和 JS.Downloader 威胁在 2018 年呈下降趋势，但 Office 宏下载程序在年底前却趋于上升。

VBSCRIPT 下载程序（月份）

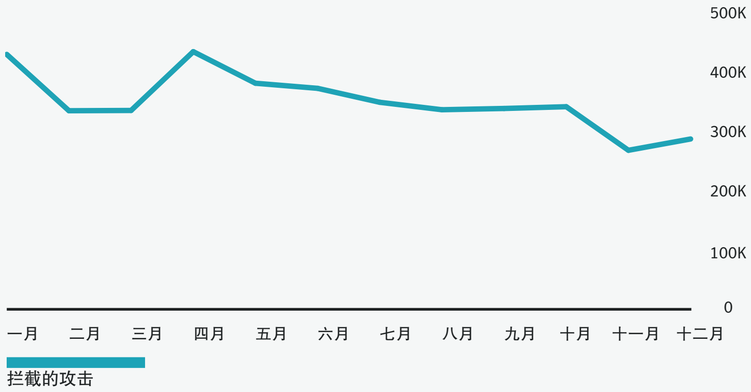


被阻止的下载程序

恶意软件总数（按操作系统）（年份）

年份	操作系统	拦截的攻击	百分比
2016	Windows	161,708,289	98.5
	Mac	2,445,414	1.5
2017	Windows	165,639,264	97.6
	Mac	4,011,252	2.4
2018	Windows	144,338,341	97.2
	Mac	4,206,986	2.8

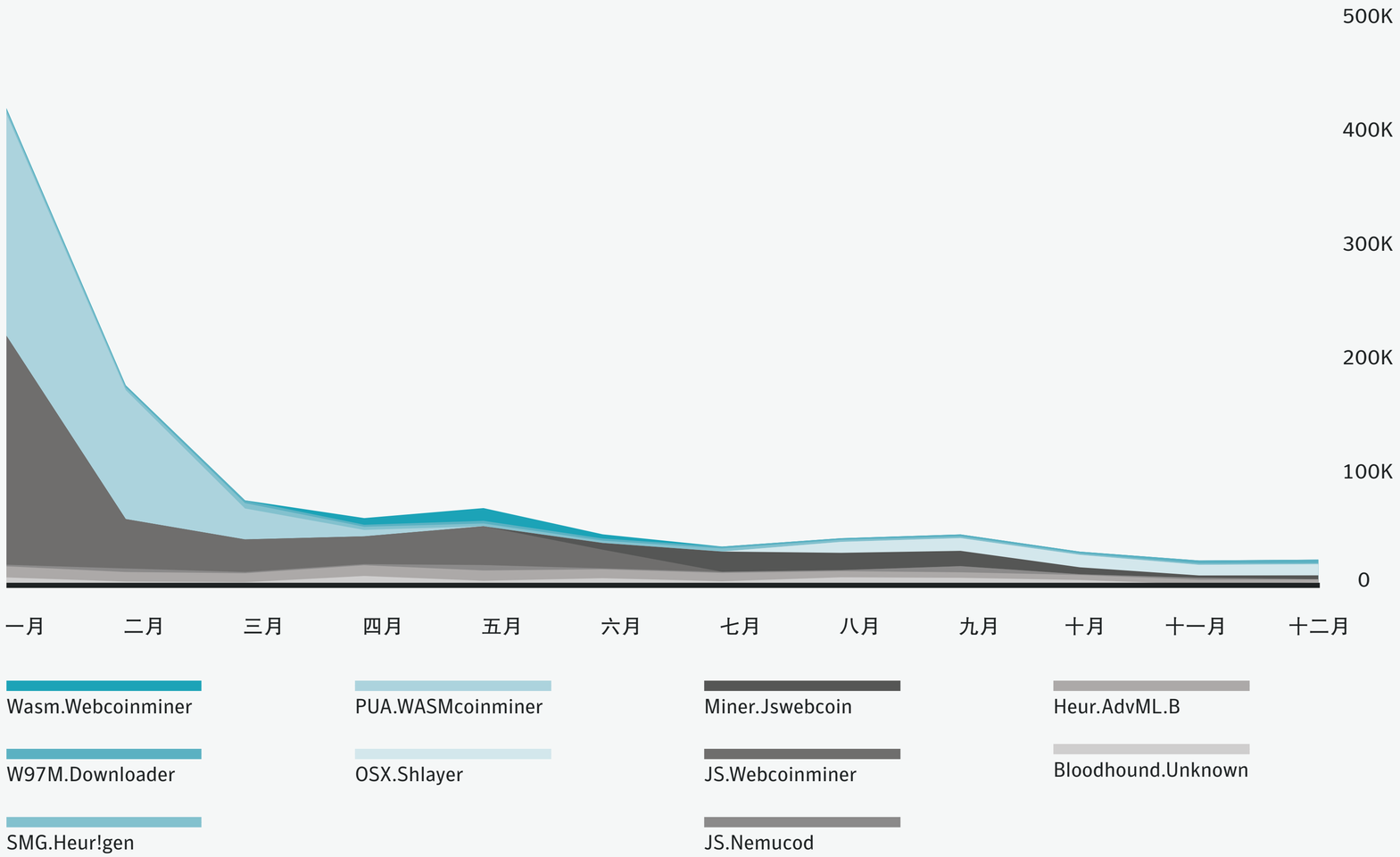
MAC 恶意软件总数（月份）



新型 MAC 恶意软件变体（年份）

年份	变体	变动百分比
2016	772,018	
2017	1,390,261	80.1
2018	1,398,419	0.6

最常见的新型 MAC 恶意软件变体（月份）

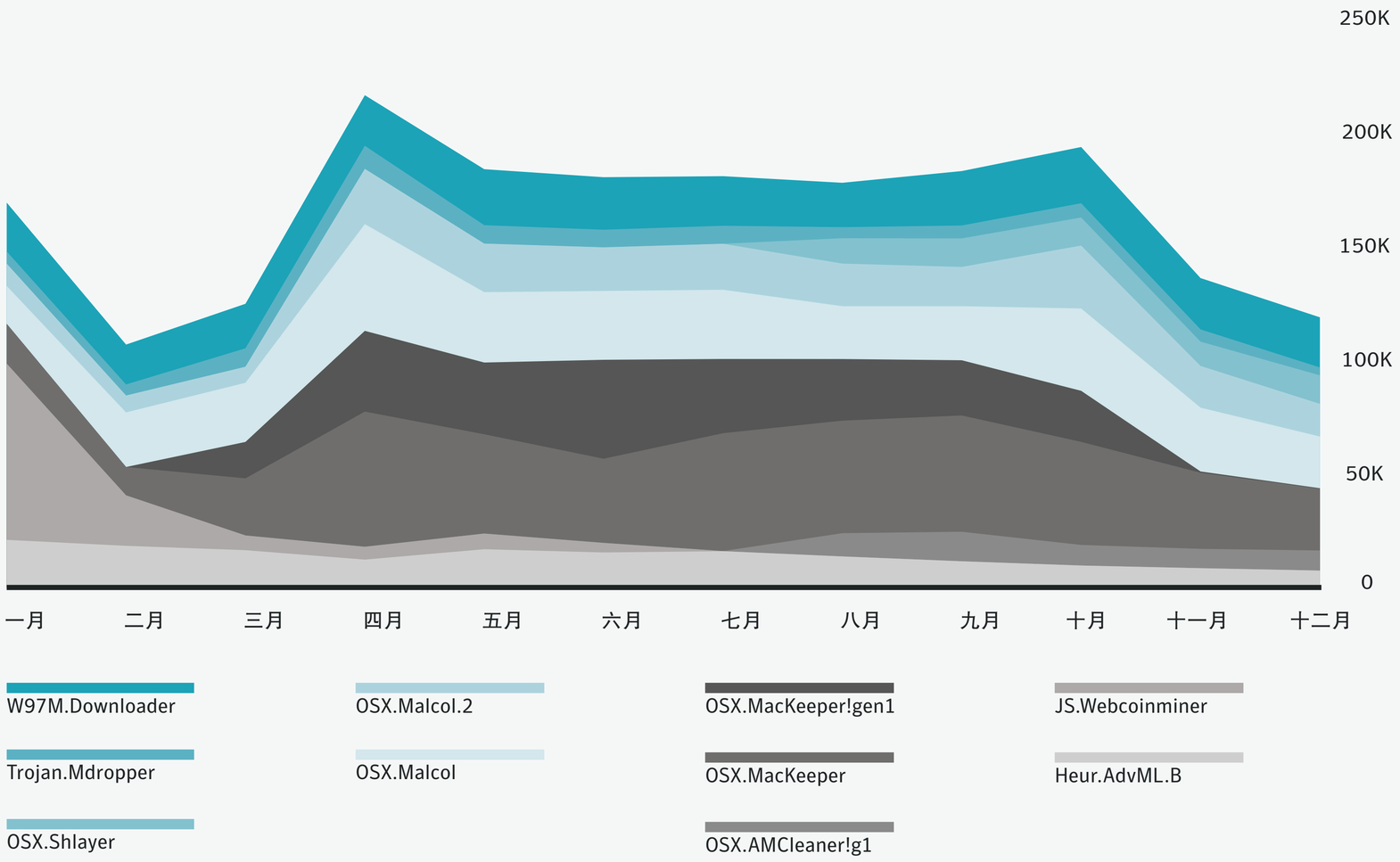


最常见的 MAC 恶意软件（年份）

威胁名称	拦截的攻击	百分比
OSX.MacKeeper	452,858	19.6
OSX.Malcol	338,806	14.7
W97M.Downloader	262,704	11.4
OSX.Malcol.2	205,378	8.9
Heur.AdvML.B	166,572	7.2
JS.Webcoinminer	122,870	5.3
Trojan.Mdropper	77,800	3.4
OSX.Shlayer	59,197	2.6
OSX.AMCleaner!g1	49,517	2.1
JS.Downloader	40,543	1.8

2018 年，赛门铁克拦截了 6900 万次挖矿劫持攻击事件，相当于 2017 年的四倍。

最常见的 MAC 恶意软件（月份）



启用 SSL 的恶意软件百分比（年份）

年份	使用 SSL 的恶意软件的百分比
2017	4.5
2018	3.9

勒索软件总数（年份）

年份	合计
2018	545,231

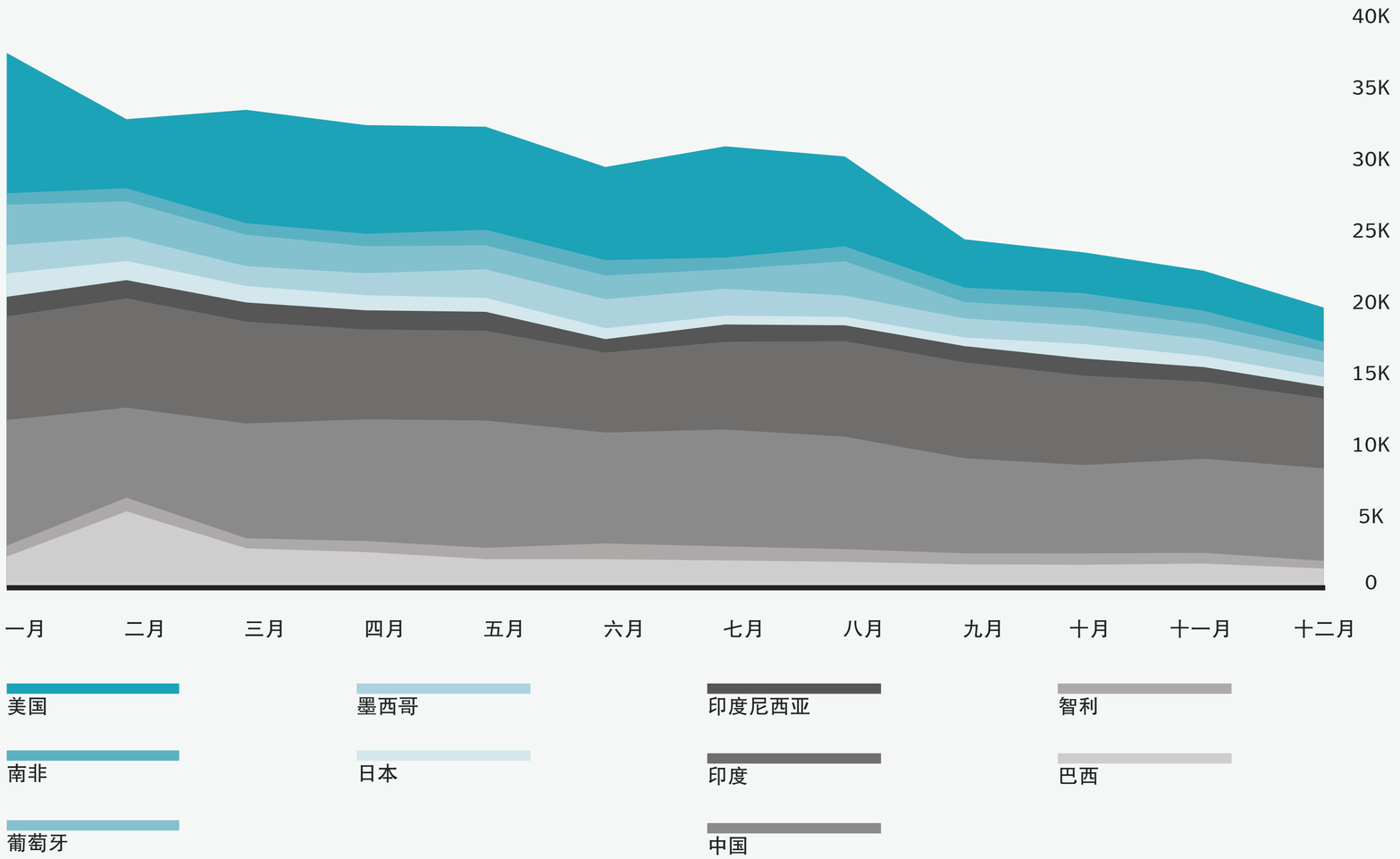
各大市场的勒索软件数量（年份）

市场	合计
个人用户	100,907
企业	444,259

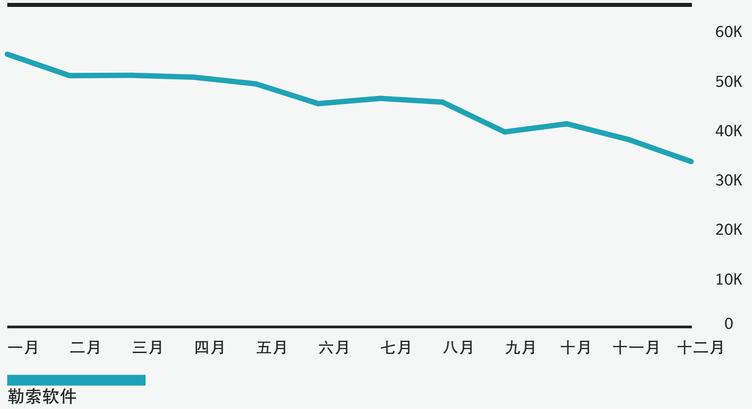
各个国家/地区最常见的勒索软件（年份）

国家/地区	百分比
中国	16.9
印度	14.3
美国	13.0
巴西	5.0
葡萄牙	3.9
墨西哥	3.5
印度尼西亚	2.6
日本	2.1
南非	2.1
智利	1.8

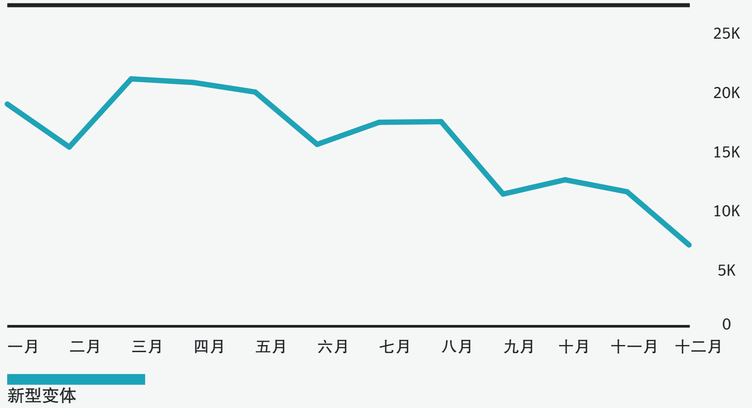
各个国家/地区的勒索软件数量（年份）



勒索软件总数（月份）



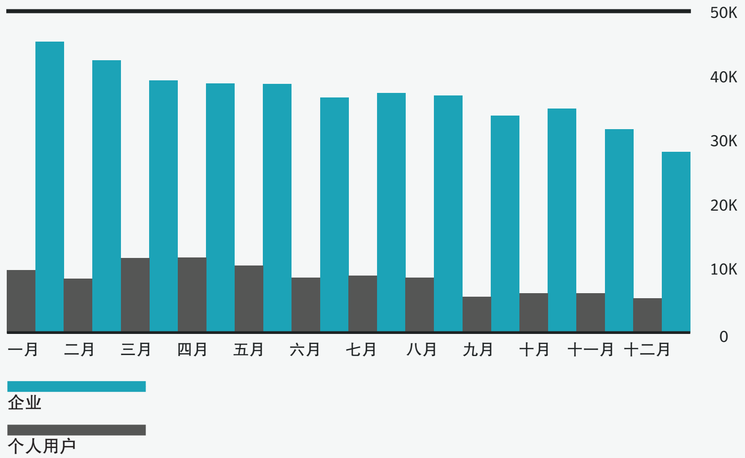
新型勒索软件变体（月份）



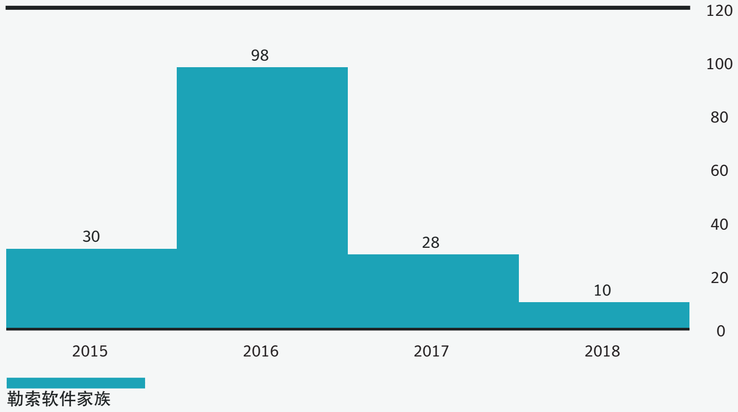
新型勒索软件变体（年份）

年份	合计
2018	186,972

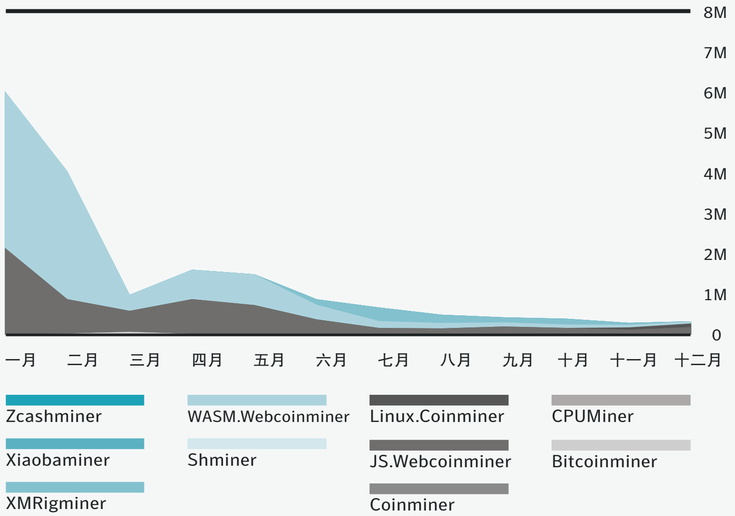
各大市场的勒索软件数量（月份）



新型勒索软件家族（年份）

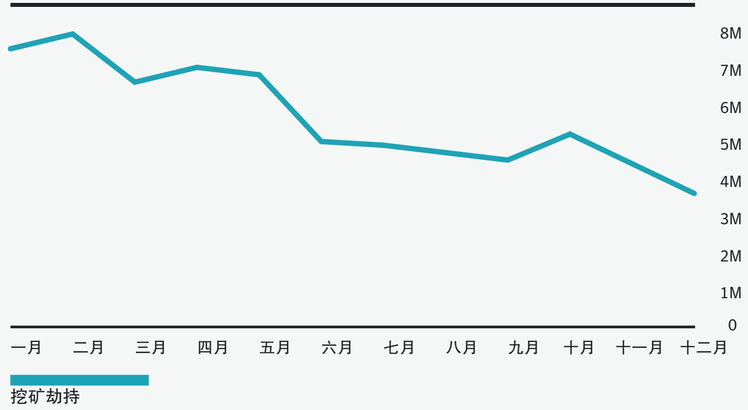


恶意软件：最常见的挖矿软件变体（月份）



勒索软件感染的总体数量下降，同比下降 20% 以上。然而，企业的感染数量却逆势增加了 12%，这意味着勒索软件仍会给企业带来诸多困扰。

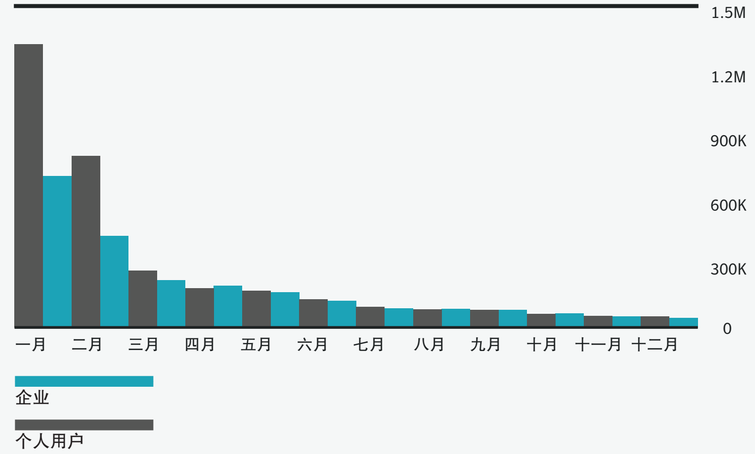
挖矿劫持总数（月份）



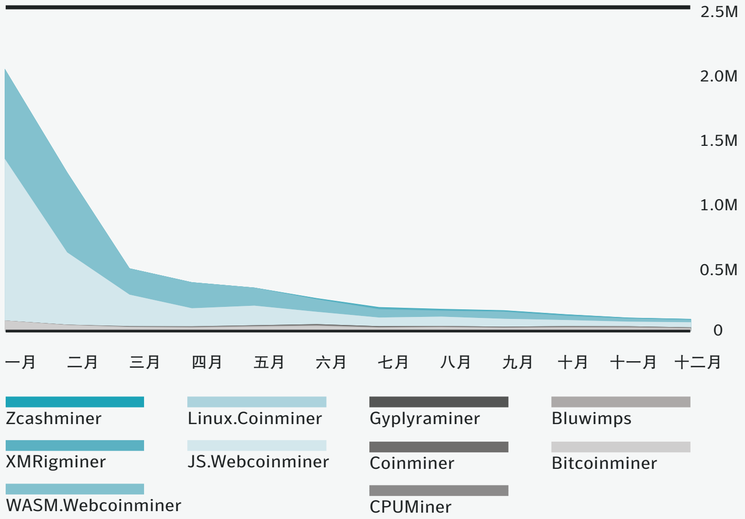
最常见的挖矿软件（年份）

威胁名称	拦截的攻击	百分比
JS.Webcoinminer	2,768,721	49.7
WASM.Webcoinminer	2,201,789	39.5
Bitcoinminer	414,297	7.4
Bluwimps	58,601	1.1
XMRigminer	58,301	1.0
Coinminer	38,655	0.7
Zcashminer	13,389	0.2
Gyplyraminer	5221	0.1
CPUMiner	3807	0.1
Linux.Coinminer	3324	0.1

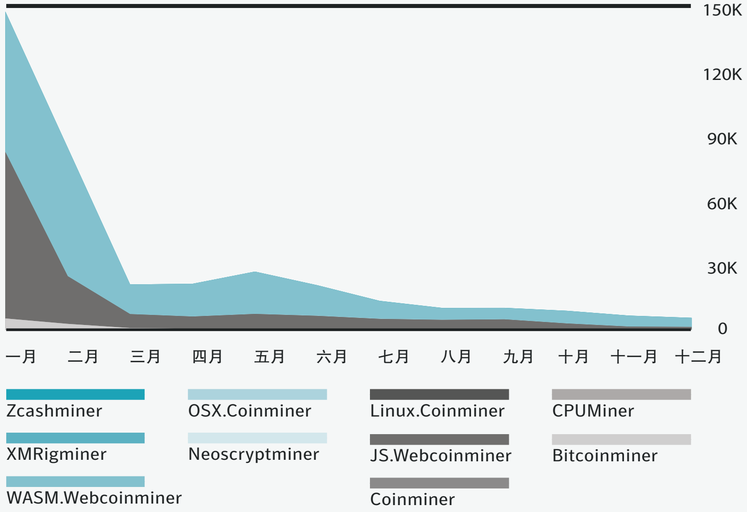
各大市场的挖矿软件数量（月份）



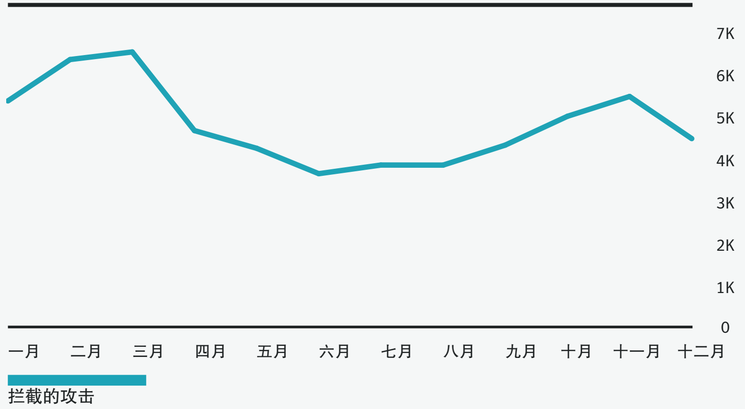
最常见的挖矿软件（月份）



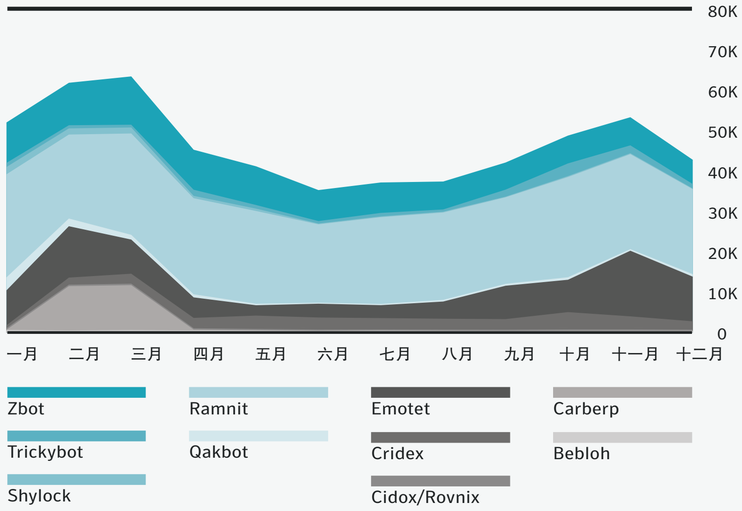
最常见的 MAC 挖矿软件（月份）



金融木马总数（月份）



最常见的金融木马（月份）

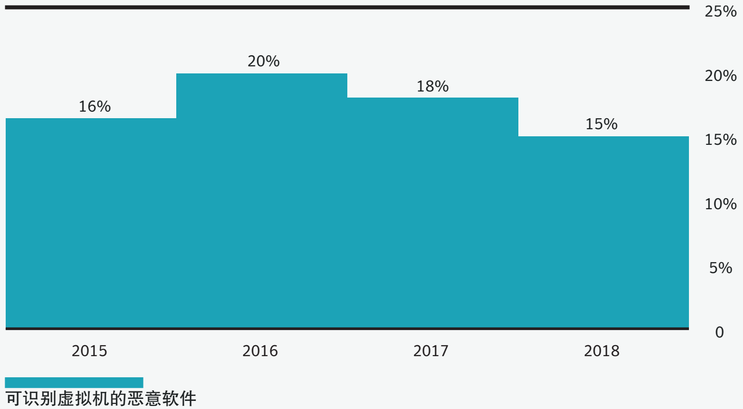


最常见的金融木马（年份）

金融木马	拦截的攻击	百分比
Ramnit	271,930	47.4
Zbot	100,821	17.6
Emotet	92,039	16.0
Cridex	31,539	5.5
Carberp	22,690	4.0
Trickybot	14,887	2.6
Qakbot	10,592	1.8
Shylock	7,354	1.3
Bebloh	5,592	1.0
Cidox/Rovnix	3,889	0.7

由于攻击者更加青睐离地攻击技术，2018 年恶意 PowerShell 脚本的使用数量暴涨 1000%。

可识别虚拟机的恶意软件（年份）



POWERSHELL 检出量（月份）

日期	恶意 POWERSHELL 脚本的百分比	比率
一月	0.1	1/1,000
二月	0.5	1/200
三月	2.5	1/40
四月	0.4	1/250
五月	1.3	1/77
六月	0.9	1/111
七月	1.4	1/71
八月	0.8	1/125
九月	1.0	1/100
十月	1.0	1/100
十一月	0.7	1/143
十二月	0.7	1/143

POWERSHELL 检出量（年份）

年份	恶意脚本占总数的百分比	比率	恶意脚本增加百分比
2017	0.9	1/111	
2018	0.9	1/111	998.9

移动设备

虽然移动恶意软件感染总数在 2018 年有所下降，但移动设备上的勒索软件感染数量与 2017 年相比却迅速增加了三分之一。美国是移动恶意软件攻击的重灾区，占总量的 63%。紧随其后的分别是中国 (13%) 和德国 (10%)。

移动设备安全管理仍是企业面临的一项挑战。2018 年，在企业使用的 36 台设备中就有 1 台为高风险设备。这些设备包括已破解或越狱的设备，以及很可能已被安装恶意软件的设备。

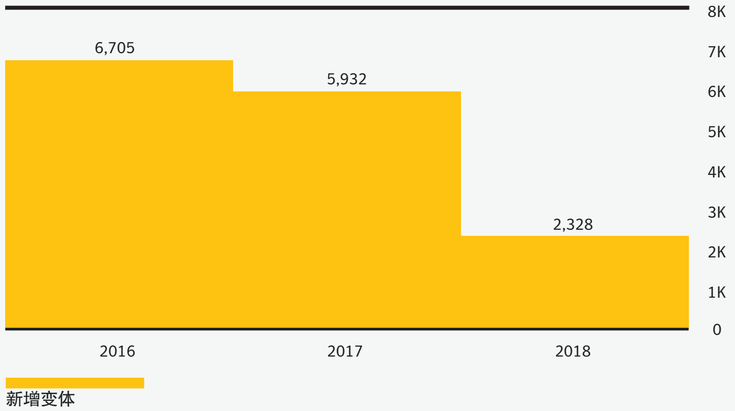
1/ 36

移动设备
安装了
高风险
应用程序

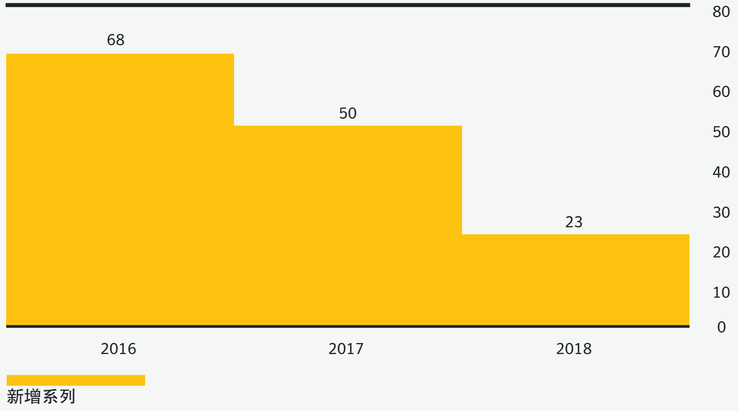
33%

移动勒索软件
感染上涨比例
同比 2017 年

新型移动恶意软件变体（年份）



新型移动恶意软件家族（年份）



2018 年，赛门铁克平均每天拦截 10,573 个恶意移动应用程序。工具 (39%)、生活类 (15%) 和娱乐 (7%) 是三大最常见的恶意应用程序类别。

被拦截的移动应用程序数量（年份）

每天
10,573

每月移动勒索软件平均数量（年份）

每月
4,675

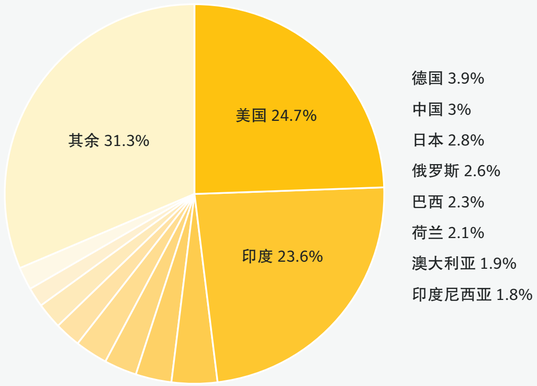
最常见的恶意移动应用程序类别（年份）

类别	百分比
工具	39.1
生活类	14.9
娱乐	7.3
社交与通信	6.2
音乐与音频	4.3
益智游戏	4.2
照片和视频	4.2
街机和动作游戏	4.1
书籍与参考资料	3.2
教育	2.6

最常见的移动恶意软件（年份）

威胁名称	百分比
Malapp	29.7
Fakeapp	9.1
MalDownloader	8.9
FakeInst	6.6
Mobilespy	6.3
HiddenAds	4.7
Premiumtext	4.4
Mobilespy	2.8
HiddenApp	2.5
Opfake	2.0

遭受移动恶意软件攻击最多的国家/地区（年份）



德国 3.9%
中国 3%
日本 2.8%
俄罗斯 2.6%
巴西 2.3%
荷兰 2.1%
澳大利亚 1.9%
印度尼西亚 1.8%

越狱版或破解版移动设备比例（年份）

分类	比率
Android 个人用户版	1/23
Android 企业版	1/3,890
iOS 个人用户版	1/828
iOS 企业版	1/4,951

各大市场有密码保护的移动设备（年份）

分类	百分比
个人用户	97.9
企业	98.4

移动设备面临网络威胁的时限（年份）

面临网络攻击风险的设备	百分比
1 个月后 （1-4 个月前创建的设备）	15.1
2 个月后 （2-5 个月前创建的设备）	21.8
3 个月后 （3-6 个月前创建的设备）	27.4
4 个月后 （4-7 个月前创建的设备）	32.2

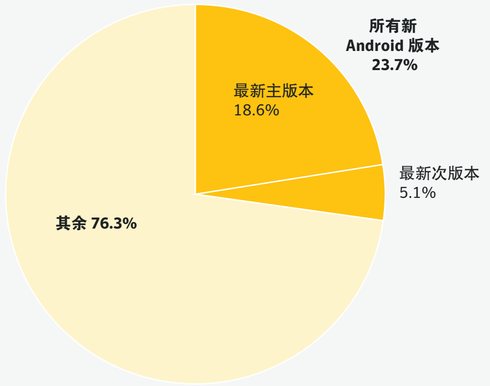
未启用加密的设备（年份）

分类	百分比
个人用户	13.4
企业	10.5

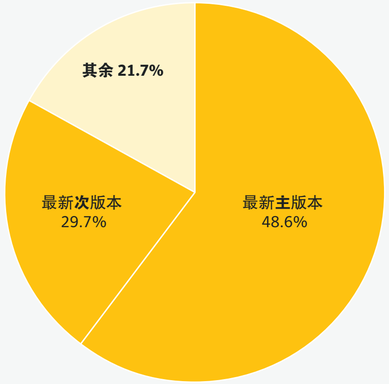
设备风险等级（年份）

设备风险级别	比率
最低	1/2
低	1/4
中	1/4
高（包括破解/越狱/很可能 已被安装恶意软件应用程序）	1/36

运行最新 ANDROID 版本的设备（年份）



运行最新 IOS 版本的设备（年份）



所有新 iOS 版本 78.3%

使用侵入式广告技术的移动应用程序数量有所下降，占比从 2017 年的 30% 下降到了 2018 年的 26%。

访问高风险数据的应用程序比例（年份）

年份	访问高风险数据的应用程序 (%)	比率	变动百分比 (PP)
2016	7.2	1/13.9	
2017	8.9	1/11.3	1.7
2018	6.9	1/14.5	-2

包含硬编码凭据的应用程序比率（年份）

年份	包含硬编码凭据的用程序 (%)	比率	变动百分比 (PP)
2016	0.8	1/124.5	
2017	1.1	1/91.0	0.3
2018	1.0	1/99.1	-0.1

使用热修补的应用程序比例（年份）

年份	使用热修补风险的应用程序 (%)	比率	变动百分比 (PP)
2016	0.7	1/142.1	
2017	0.35	1/285.1	-0.35
2018	0.01	1/7,146.0	-0.34

访问健康状况数据的应用程序比例（年份）

年份	访问健康状况数据的应用程序 (%)	比率	变动百分比 (PP)
2016	0.2	1/427.3	
2017	1.7	1/57.6	1.5
2018	2.2	1/46.3	0.5

使用侵入式广告的应用程序比例（年份）

年份	使用侵入式广告的应用程序百分比	比率	变动百分比 (PP)
2016	19.4	1/5.2	
2017	30.5	1/3.3	11.1
2018	26.4	1/3.8	-4.1

受访问健康状况数据的应用程序影响的企业百分比（年份）

年份	拥有 1 个以上应用程序可访问健康状况数据的企业 (%)	比率	变动百分比 (PP)
2016	27.6	1/3.6	
2017	44.9	1/2.2	17.3
2018	39.0	1/2.6	-5.9

受访问高风险数据的应用程序影响的企业百分比（年份）

年份	使用访问高风险数据的应用程序的企业百分比	比率	变动百分比 (PP)
2016	63	1/1.6	
2017	54.6	1/1.8	-8.4
2018	46	1/2.2	-8.6

受包含硬编码凭据的应用程序影响的企业百分比（年份）

年份	应用程序拥有硬编码凭据的企业百分比	比率	变动百分比 (PP)
2016	47.3	1/2.1	
2017	42.9	1/2.3	-4.4
2018	34.3	1/2.9	-8.6

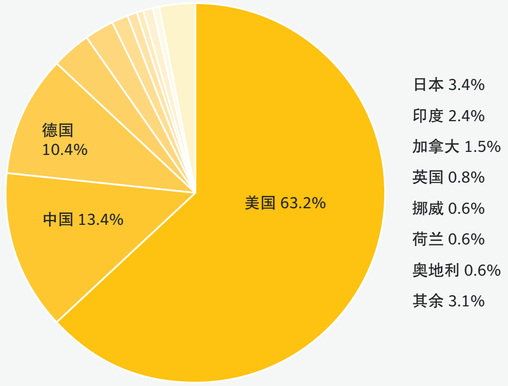
受使用热修补的应用程序影响的企业百分比（年份）

年份	应用程序使用热修补的企业百分比	比率	变动百分比 (PP)
2016	31.3	1/3.2	
2017	11.7	1/8.5	-19.6
2018	6.8	1/14.7	-4.9

受使用入侵广告的应用程序影响的企业百分比（年份）

年份	应用程序使用侵入式广告的企业百分比	比率	变动百分比 (PP)
2016	19.4	1/5.2	
2017	30.5	1/3.3	11.1
2018	26.4	1/3.8	-4.1

遭受移动勒索软件攻击最多的国家/地区（年份）

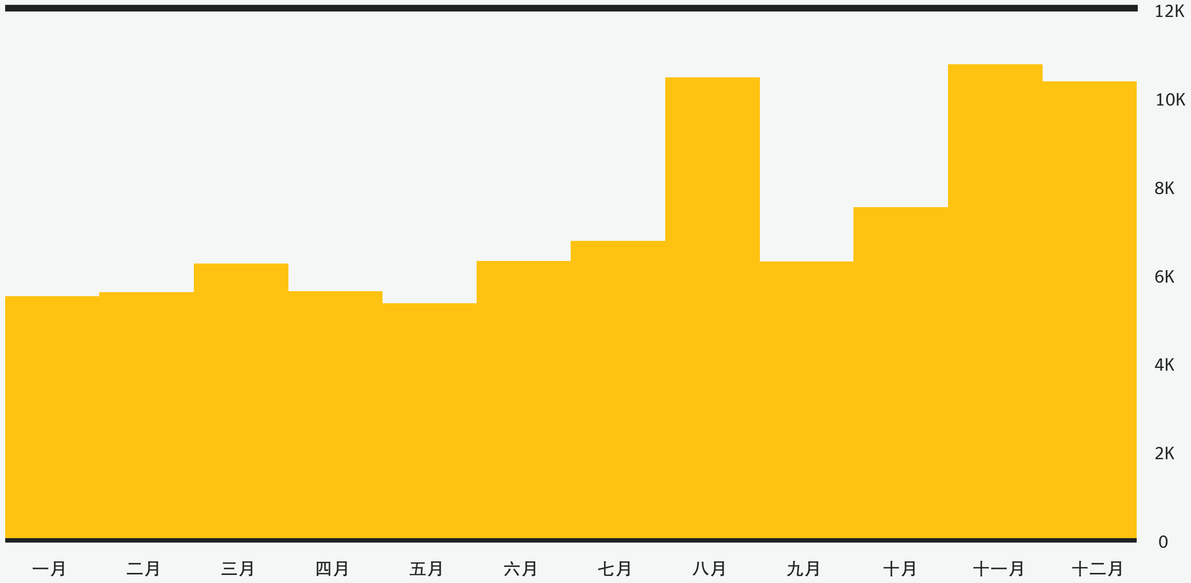


2018 年移动设备上的勒索软件感染数量明显增加，与 2017 年相比上涨了三分之一。

最常见的移动勒索软件（年份）

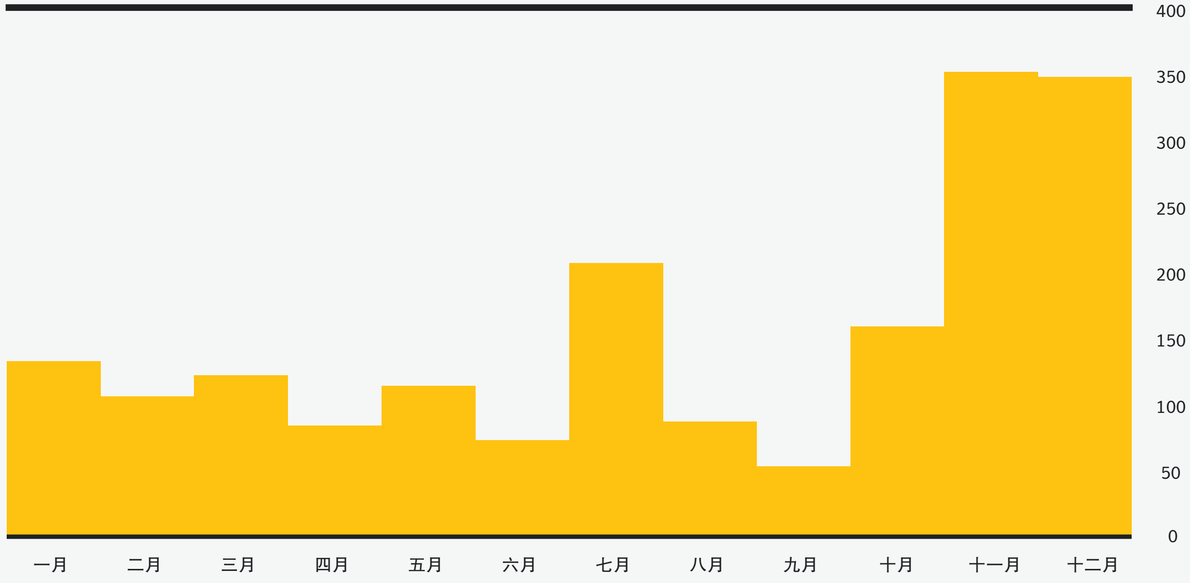
威胁名称	百分比
Simplocker	59.3
Lockdroid.E	26.2
LockScreen	7.1
Simplocker.B	2.8
Ransomware	2.7
Ransomeware	1.0
Lockdroid.F	0.7
Android.WannaLocker	<0.1
WannaLocker	<0.1
Lockdroid.G	<0.1

拦截的移动恶意软件数量（月份）



每月的恶意软件数量

拦截的移动勒索软件数量（月份）



每天的勒索软件数量

虽然移动恶意软件年度感染总数在 2018 年有所减少，但感染数量在去年第四季度开始再次上升。

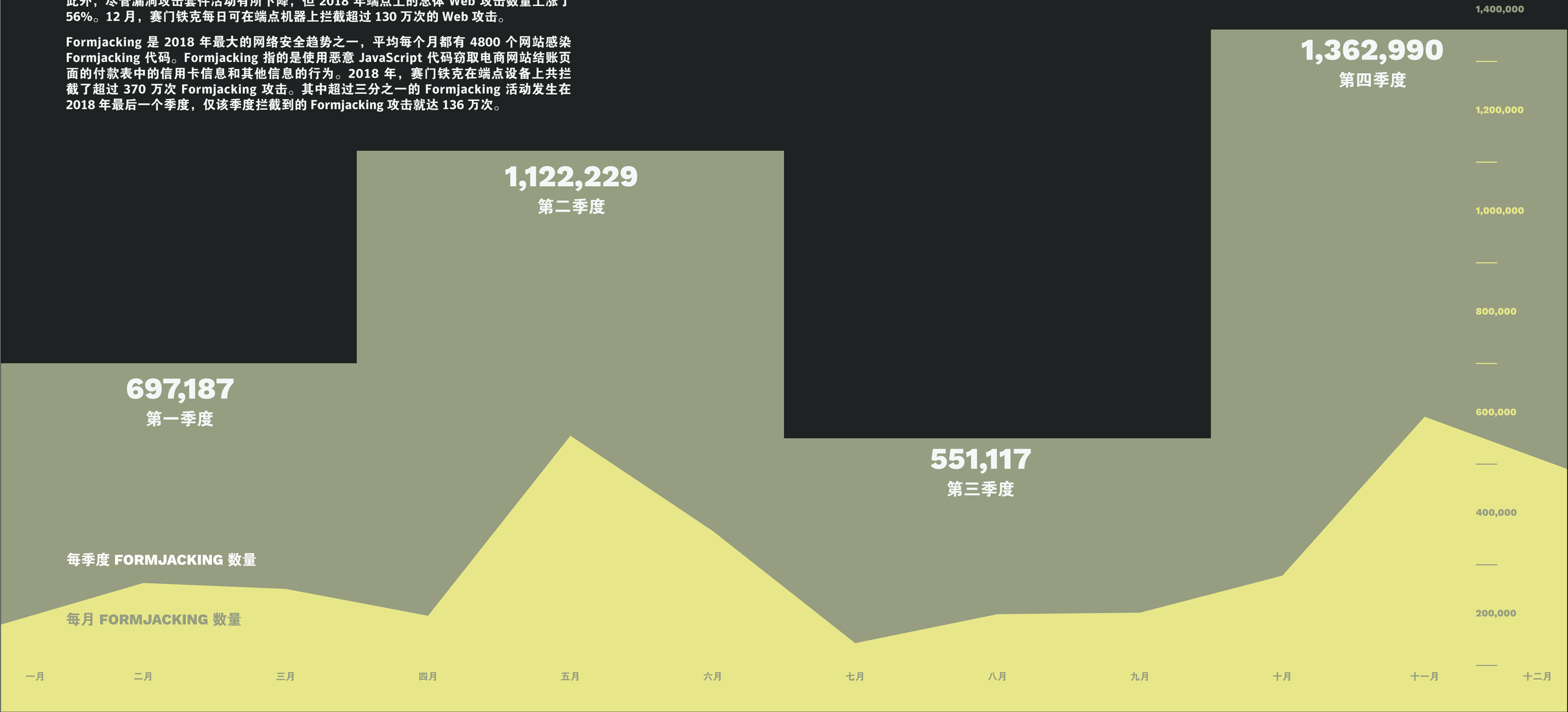
Web 攻击

2018 年，分析的 10 个 URL 中就有 1 个是恶意链接，而在 2017 年，这一比例为 1/16。此外，尽管漏洞攻击套件活动有所下降，但 2018 年端点上的总体 Web 攻击数量上涨了 56%。12 月，赛门铁克每日可在端点机器上拦截超过 130 万次的 Web 攻击。

Formjacking 是 2018 年最大的网络安全趋势之一，平均每个月都有 4800 个网站感染 Formjacking 代码。Formjacking 指的是使用恶意 JavaScript 代码窃取电商网站结账页面的付款表中的信用卡信息和其他信息的行为。2018 年，赛门铁克在端点设备上共拦截了超过 370 万次 Formjacking 攻击。其中超过三分之一的 Formjacking 活动发生在 2018 年最后一个季度，仅该季度拦截到的 Formjacking 攻击就达 136 万次。

FORMJACKING 活动

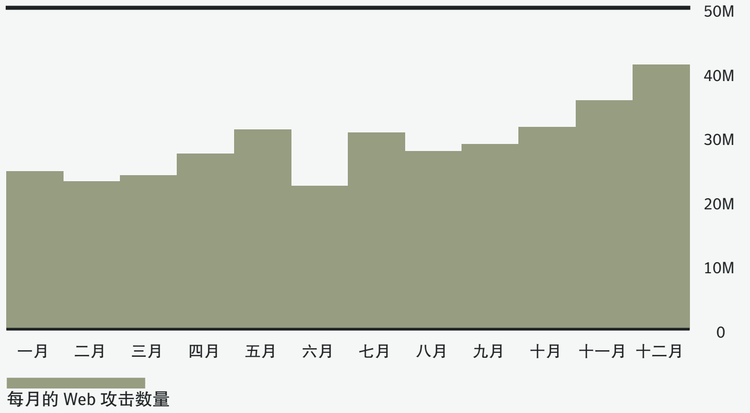
超过三分之一的 Formjacking 活动发生在 2018 年最后一个季度。



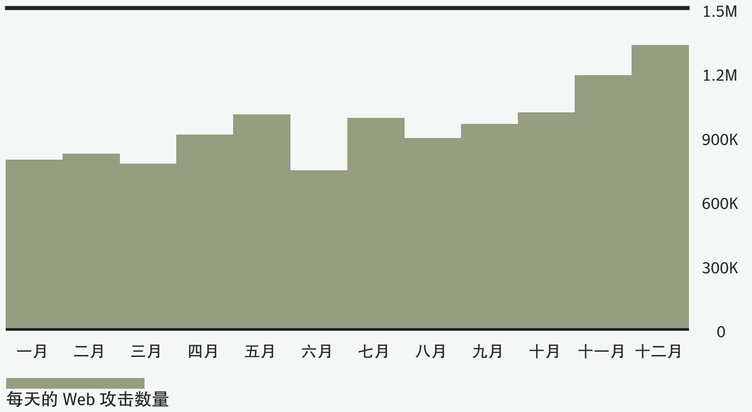
WEB 攻击（年份）

拦截的 Web 攻击总数	平均每天拦截的 Web 攻击次数
348,136,985	953,800

WEB 攻击（月份）



WEB 攻击（每日）



遭感染最多的网站类别（年份）

域分类	2017 (%)	2018 (%)	百分比差
动态 DNS	15.7	16.6	0.8
赌博	7.9	16.3	8.4
托管	8.2	8.7	0.5
技术	13.6	8.1	-5.5
购物	4.6	8.1	3.6
商业	9.0	7.2	-1.7
色情图片	3.2	5.2	2.1
医疗保健	5.7	4.5	-1.2
教育	3.7	3.9	0.2
内容传递网络	2.1	2.6	0.6

恶意 URL（年份）

年份	占总数的百分比	比率	变动百分比
2017	6.4	1/16	
2018	9.9	1/10	3.4

僵尸网络 URL（年份）

年份	占所有 URL 的百分比	比率	占恶意 URL 的百分比	比率	变动百分比	变动百分比
2017	1.2	1/85	18.2	1/5		
2018	1.8	1/54	18.7	1/5	57.6	0.7

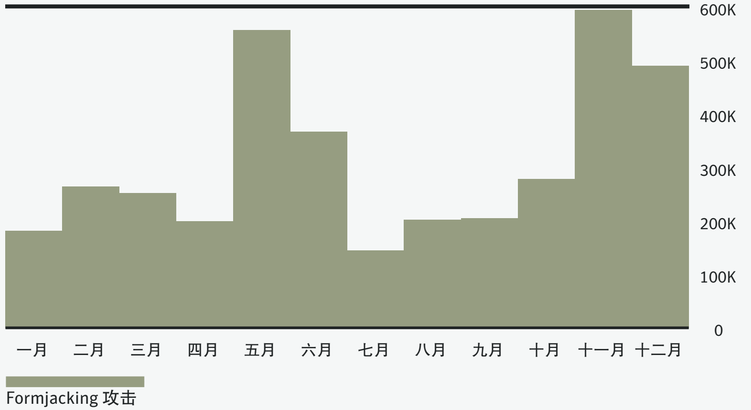
网络钓鱼 URL（年份）

年份	占所有 URL 的百分比	比率	占恶意 URL 的百分比	比率	变动百分比	变动百分比
2017	0.4	1/235	6.6	1/15		
2018	0.6	1/170	5.9	1/17	38.1	0.2

FORMJACKING 攻击（年份）

年份	FORMJACKING 攻击
2018	3,733,523

FORMJACKING 攻击（月份）



遭受 FORMJACKING 攻击的网站平均数量（月份）

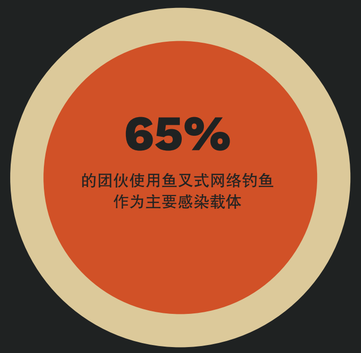
年份	每月网站平均数量
2018	4,818

目标性攻击

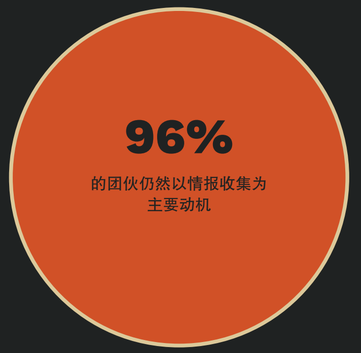
尽管目标性攻击总体数量在去年略有下降，但最活跃团伙在过去三年中攻击的企业平均达到了 55 家，较 2015 至 2017 年之间的 42 家仍有所上升。鱼叉式网络钓鱼电子邮件仍然最受青睐，在所有已知团伙中有 65% 的团伙仍在使用这一攻击方式。96% 的团伙发动目标性攻击是为了收集情报，这也是企业会遭受目标性攻击的最大原因所在。

随着离地策略越来越流行，攻击团伙对零日漏洞的利用有所下降，从 2017 年的 27% 降至 2018 年的 23%。虽然破坏性恶意软件仍是一种小众途径，但其使用率却在持续增长。去年有 8% 的团伙使用了破坏性工具，较 2017 年上涨了 25%。

鱼叉式网络钓鱼



情报收集



2015-2017：每个团伙平均攻击 42 个企业
（20 个最活跃的团伙）

2016-2018：每个团伙平均攻击 55 个企业
（20 个最活跃的团伙）

⬇ 23%
使用零日
漏洞的团伙

⬆ 8%
使用破坏性
恶意软件的
团伙

美国当局发起的间谍控诉

中国

俄罗斯

伊朗

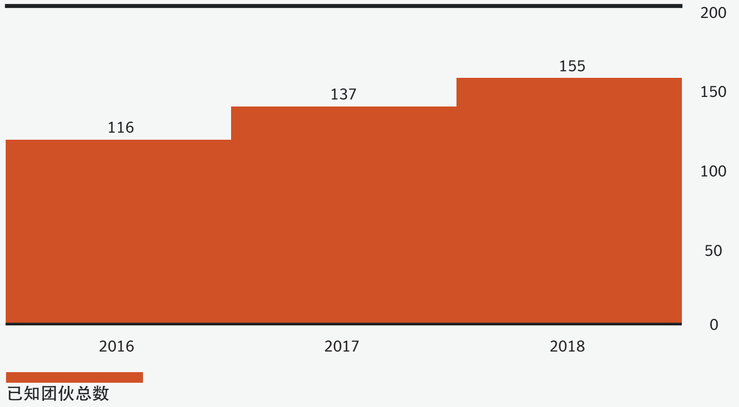
朝鲜

2016

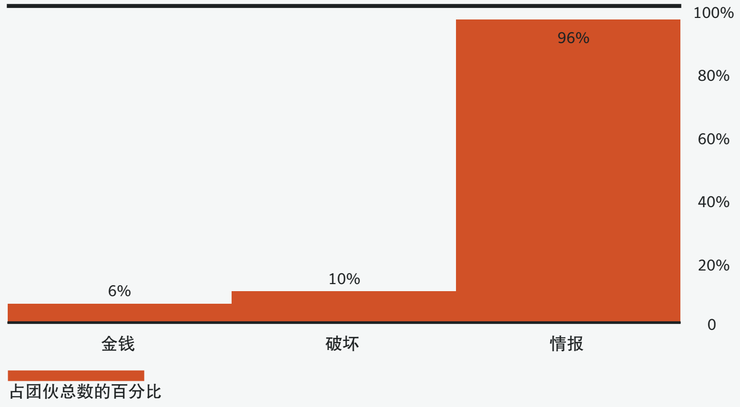
2017

2018

已知目标性攻击团伙（年份）

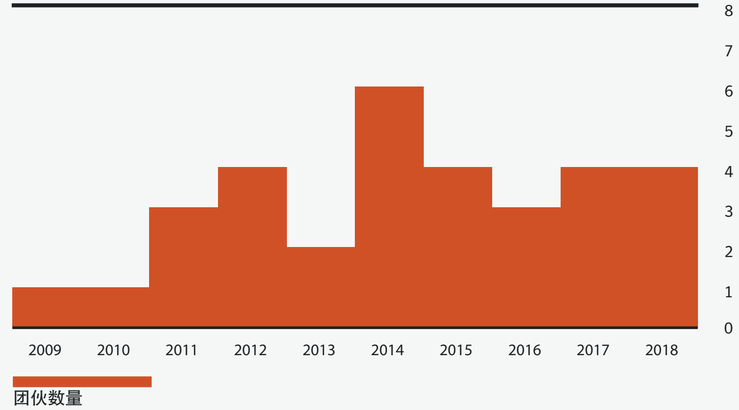


目标性攻击团伙的动机数（一直）

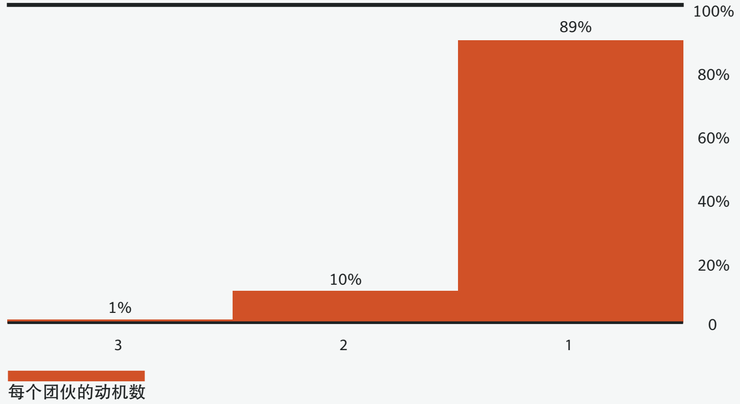


96% 的团伙发动目标性攻击是为了收集情报，这也是企业会遭受目标性攻击的最大原因所在。

赛门铁克公布的目标性攻击团伙（年份）

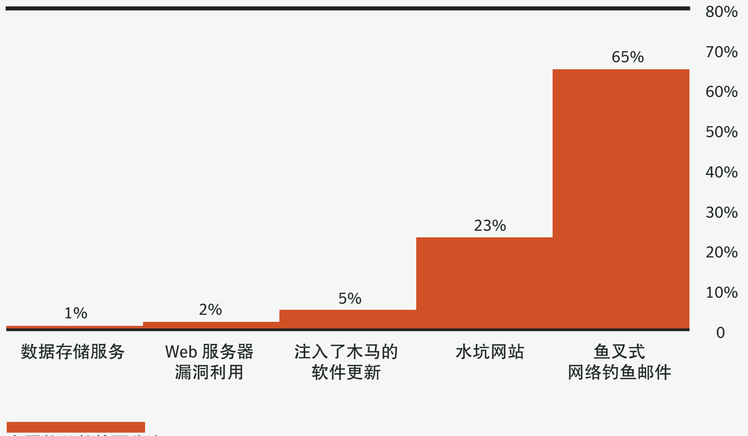


每个目标性攻击团伙的动机数（一直）

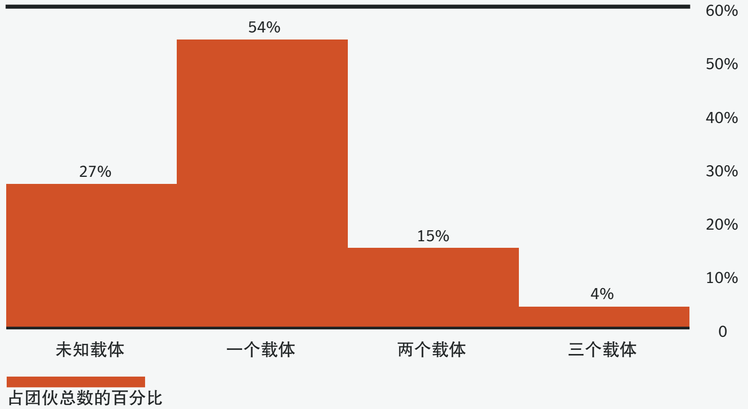


鱼叉式网络钓鱼电子邮件仍然最受青睐，在所有已知团伙中有 65% 的团伙仍在使用这一攻击方式。

目标性攻击团伙使用的感染载体数（一直）



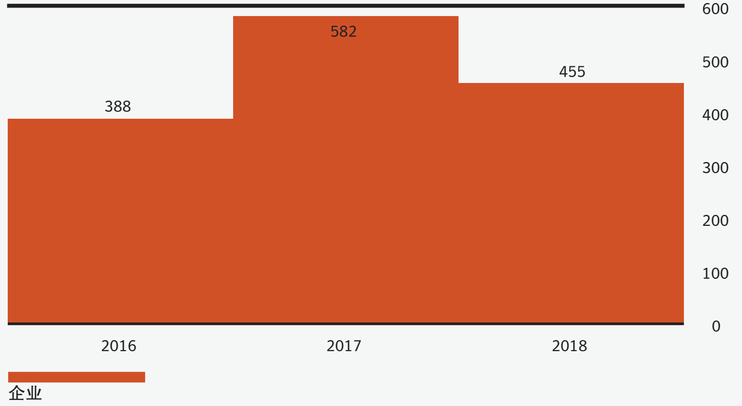
每个目标性攻击团伙的感染载体数（一直）



目标性攻击团伙影响最大的国家/地区 (2016-2018)

国家/地区	攻击
美国	255
印度	128
日本	69
中国	44
土耳其	43
沙特阿拉伯	42
韩国	40
中国台湾	37
阿联酋	30
巴基斯坦	28

受目标性攻击影响的企业数量（年份）



20 个最活跃团伙所用工具的数量 (2016-2018)

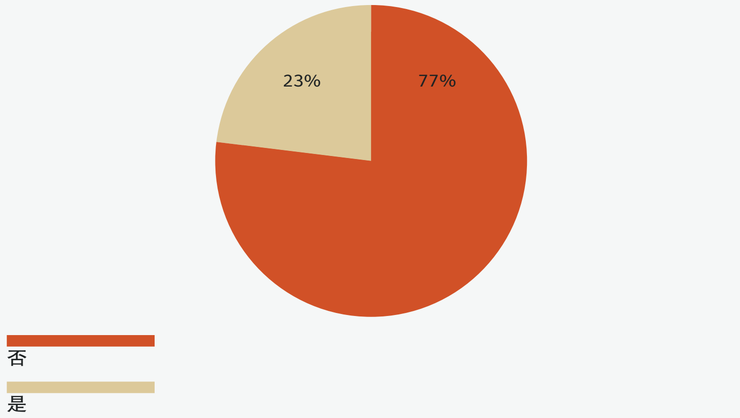
最小值	最大值	平均值
1	18	5

20 个最活跃团伙平均攻击的企业数量 (2016-2018)

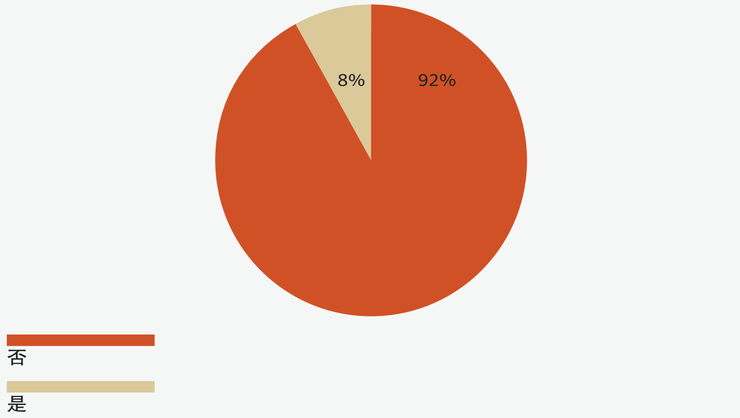
2016-2018
55

虽然破坏性恶意软件仍是一种小众途径，但其使用率却在持续增长。使用破坏性恶意软件的团伙从 2017 年年末的 6% 上升至 8%。

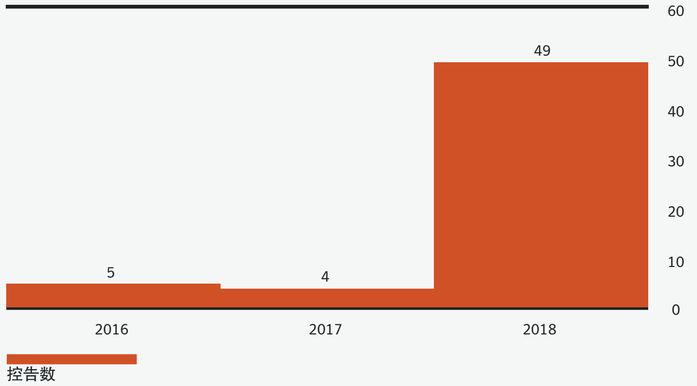
已知团伙中使用零日漏洞的百分比（一直）



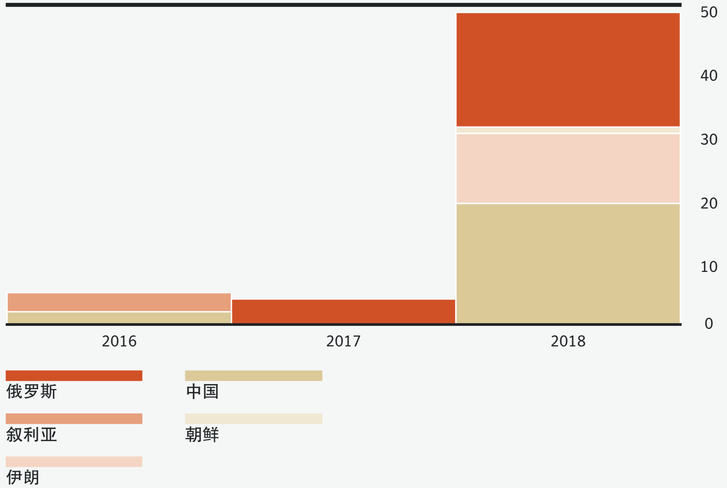
已知团伙中使用破坏性恶意软件的百分比（一直）



美国当局发起的间谍控诉总数（年份）



美国当局针对各国家/地区发起的间谍控诉（年份）



物联网

物联网 (IoT) 攻击在 2017 年大幅增加后，攻击数量在 2018 年趋于稳定，当年针对赛门铁克物联网诱捕系统的攻击平均每月达到 5200 次。目前，路由器和联网摄像机是物联网攻击的主要来源，占诱捕系统所遭攻击总量的 90% 以上。2018 年，攻击中所用的受感染摄像机比例大幅增加。联网摄像机在攻击中占比 15%，较 2017 年的 3.5% 有大幅上升。攻击者也日益将 Telnet 视作一种攻击途径。使用 Telnet 发起的攻击占比从 2017 年的 50% 上升至 2018 年的 90% 以上。

以联网摄像机为目标的攻击从 2017 年的 3.5% 上涨至 2018 年的 15%

路由器和联网摄像机

是物联网攻击的主要源头

占据全部活动的

90%

以上

物联网设备平均每月遭受 5200 次攻击

物联网攻击的主要来源国（年份）

国家/地区	百分比
中国	24.0
美国	10.1
巴西	9.8
俄罗斯	5.7
墨西哥	4.0
日本	3.7
越南	3.5
韩国	3.2
土耳其	2.6
意大利	1.9

物联网攻击中最常用的密码（年份）

密码	百分比
123456	24.6
[BLANK]	17.0
system	4.3
sh	4.0
shell	1.9
admin	1.3
1234	1.0
password	1.0
enable	1.0
12345	0.9

物联网攻击中最常用的用户名（年份）

用户名	百分比
root	38.1
admin	22.8
enable	4.5
shell	4.2
sh	1.9
[BLANK]	1.7
system	1.1
enable	0.9
>/var/tmp/.ptmx && cd /var/tmp/	0.9
>/var/.ptmx && cd /var/	0.9

最常见的物联网威胁（年份）

威胁名称	百分比
Linux.Lightaidra	31.3
Linux.Kaiten	31.0
Linux.Mirai	15.9
Trojan.Gen.2	8.5
Downloader.Trojan	3.2
Trojan.Gen.NPE	2.8
Linux.Mirai!g1	1.9
Linux.Gafgyt	1.7
Linux.Amnesiark	1.1
Trojan.Gen.NPE.2	0.8

臭名昭著的 Mirai 分布式拒绝服务 (DDoS) 蠕虫仍然十分活跃，在所有攻击中占比 16%，是 2018 年第三大常见的物联网威胁。

路由器和联网摄像机最易受到感染，它们的感染比例分别占到 75% 和 15%。

受物联网威胁攻击最多的协议（年份）

目标服务	百分比
telnet	90.9
http	6.6
https	1.0
smb	0.8
ssh	0.6
ftp	<0.1
snmp	<0.1
cwmp	<0.1
upnp	<0.1
modbus	<0.1

受物联网威胁攻击最多的端口（年份）

TCP 端口号	说明	百分比
23	Telnet	85.0
80	www HTTP	6.5
2323	Telnet（备用）	5.8
443	HTTP（采用 TLS/SSL）	1.0
445	Microsoft Directory Services	0.8
22	SSH 协议	0.6
8080	HTTP（备用）	0.1
2223	Rockwell CSP2	<0.1
2222	SSH 协议（备用）	<0.1
21	文件传输协议[控制]	<0.1

执行物联网攻击的常见设备类型（年份）

设备类型	百分比
路由器	75.2
联网摄像机	15.2
多媒体设备	5.4
防火墙	2.1
PBX 电话系统	0.6
NAS（Network Attached Storage，网络接入存储）	0.6
VoIP 电话	0.2
打印机	0.2
警报系统	0.2
VoIP 适配器	0.1

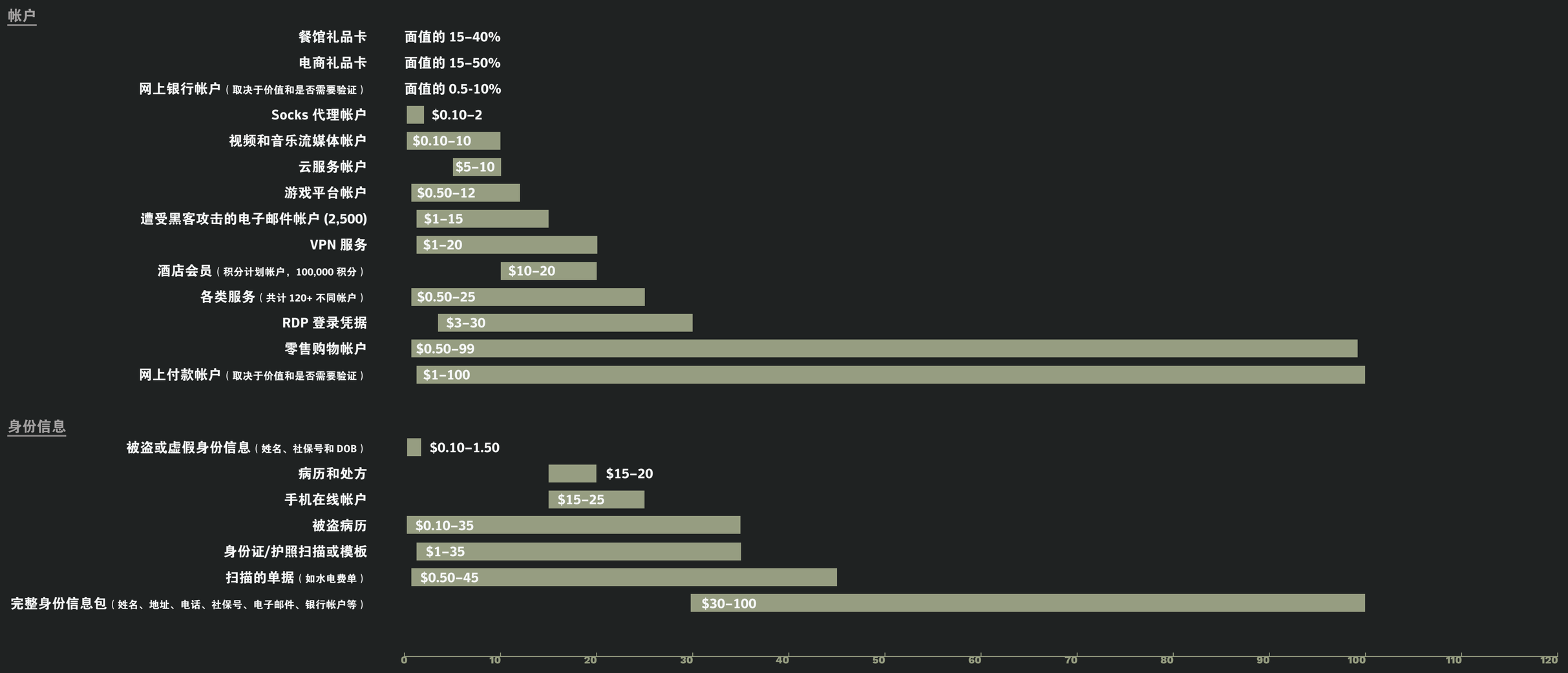
物联网设备遭到的攻击（年份）

年份	攻击总量	变动百分比
2017	57,691	
2018	57,553	-0.2

物联网设备遭到的攻击平均数（月份）

每月
5,233

地下经济


帐户
餐馆礼品卡
面值的 15–40%
电商礼品卡
面值的 15–50%
网上银行帐户（取决于价值和是否需要验证）
面值的 0.5-10%
Socks 代理帐户
$0.10–2
视频和音乐流媒体帐户
$0.10–10
云服务帐户
$5–10
游戏平台帐户
$0.50–12
遭受黑客攻击的电子邮件帐户 (2,500)
$1–15
VPN 服务
$1–20
酒店会员（积分计划帐户，100,000 积分）
$10–20
各类服务（共计 120+ 不同帐户）
$0.50–25
RDP 登录凭据
$3–30
零售购物帐户
$0.50–99
网上付款帐户（取决于价值和是否需要验证）
$1–100
身份信息
被盗或虚假身份信息（姓名、社保号和 DOB）
$0.10–1.50
病历和处方
$15–20
手机在线帐户
$15–25
被盗病历
$0.10–35
身份证/护照扫描或模板
$1–35
扫描的单据（如水电费单）
$0.50–45
完整身份信息包（姓名、地址、电话、社保号、电子邮件、银行帐户等）
$30–100
0
10
20
30
40
50
60
70
80
90
100
110
120

地下经济

身份信息（续）

虚假医疗保健卡	$50–220
包裹投递信箱	$70–240
虚假身份证、驾照、护照等	$25–5,000

转账服务

银行帐户的套现服务	面值的 0.1–15%
在线支付系统的套现服务	面值的 1–5%
用比特币支付 100 美元，获得 1000 美元的转账	$100
套现服务	面值的 5-20%

恶意软件

Office 宏下载程序生成器	$5–10
DDoS bot 软件	$1–15
间谍软件	$3–50
加密货币恶意窃取软件	$4–60
加密货币挖矿软件（例如门罗币）	$10–200
勒索软件工具包	$0–250
常见银行木马工具包及支持	$10–1,500

地下经济

服务

机票和酒店预订	面值的 10%
洗钱服务（现金或加密货币）	4–40%
套现服务（银行帐户、ATM 卡和假身份证）	$350
雇佣黑客	$100+
自定义网络钓鱼页面服务	$3–12
DDoS 服务，持续 1 小时以下（以防护等级为中等的对象为目标）	$5–20
DDoS 服务，持续 24 小时以上（以防护等级在中等偏上的对象为目标）	$10–1,000

付款卡

单张信用卡	$0.50–20
含全部信息的单张信用卡 (fullz)	$1–45
转储的磁轨 1/2 数据（例如通过浏览数据）	$5–60

社交媒体

社交媒体平台上 100 个赞	$0.10–3
500 名社交媒体粉丝	$2–6
100,000 次社交媒体视频观看	$200–250

这些价格来自可公开访问的地下论坛和网络黑市 TOR 网站。封闭式私人论坛的价格往往更低。我们无法验证商品是否真的以所标的价格出售，其中有些可能是虚假价格。

METHODOLOGY 调研方法

赛门铁克建立了全球最大的威胁信息收集网络赛门铁克全球威胁情报网络 (GIN)，通过该网络收集全球各个角落的网络安全威胁信息。

Symantec GIN 配备了逾 1.23 亿个攻击传感器，每秒可记录数千个活动，记录的安全威胁数据高达 9 PB 以上。该网络还监控着全球 30 多万家采用赛门铁克安全防护的企业和机构遭到的威胁攻击活动。赛门铁克威胁防护产品组合提供的遥测数据可帮助我们 3800 名网络安全研究人员和工程师确定影响威胁态势的主要趋势。

各种赛门铁克电子邮件安全技术每日要处理 24 亿多封电子邮件，并详尽分析垃圾邮件、网络钓鱼以及电子邮件恶意软件趋势。这些技术包括：Symantec Messaging Gateway for Service Providers、Symantec Email Security.cloud、Symantec Advanced Threat Protection for Email、Symantec's CloudSOC™ Service 和 Symantec Probe Network。赛门铁克还通过一个由企业、安全供应商和合作伙伴组成的反欺诈社区收集网络钓鱼信息。

赛门铁克专属的 Skeptic™ 技术每日过滤 3.22 亿多封电子邮件以及逾 15 亿个 Web 请求，在此基础之上构建的 Symantec Email.cloud 和 Web Security.cloud™ 服务运用高级机器学习、网络通信分析和行为分析来检测最隐蔽和最顽固的威胁。此外，赛门铁克的 Advanced Threat Protection for Email 通过增添云端沙盒、鱼叉式网络钓鱼防护以及独特的目标性攻击识别功能，让狡猾的电子邮件攻击无处遁形。

Symantec Secure Web Gateway 解决方案包含 ProxySG™、Advanced Secure Gateway (ASG) 和 Web Security Solution (WSS)，借助实时 WebPulse Collaborative Defense 技术和 Content Analysis 系统每月处理和分析数十亿个 URL，识别并抵御恶意负载并控制敏感的 Web 内容。

Symantec Endpoint Protection Mobile (SEPM) 的移动威胁信息用于预测、检测和防御各种已知威胁和未知威胁。SEPM 的预测性技术采用基于海量众包威胁情报的分层保护技术，同时提供基于设备和服务器的分析服务，能够主动保护移动设备抵御恶意软件、网络威胁、应用程序和操作系统漏洞利用攻击。此外，Appthority 的移动技术与 SEPM 相结合，可以分析移动应用程序的恶意功能及不安全和不宜行为，例如漏洞、敏感数据丢失风险和隐私侵犯行为。

这些资源为赛门铁克分析师提供了最全面的数据来源，并据此发现和分析网络攻击、恶意代码活动、网络钓鱼和垃圾邮件，并提供新兴趋势的中肯评论。赛门铁克《互联网安全威胁报告》正是分析师结合上述资源的智慧结晶，为大型企业、中小型企业和个人用户提供了当前和未来有效保护系统所需的必要信息。

作者名单

小组

Brigid O'Gorman

Candid Wueest

Dick O'Brien

Gillian Cleary

Hon Lau

John-Paul Power

Mayee Corpin

Orla Cox

Paul Wood

Scott Wallace

撰稿人

Alan Neville

Alex Shehk

Brian Duckering

Chris Larsen

Christian Tripputi

Dennis Tan

Gavin O'Gorman

Parveen Vashishtha

Pierre-Antoine Vervier

Pravin Bange

Robert Keith

Sean Kiernan

Sebastian Zatorski

Seth Hardy

Shashank Srivastava

Shaun Aimoto

Siddhesh Chandrayan

Tor Skaar

Tyler Anderson

Yun Shen

INTERNET SECURITY THREAT REPORT

《互联网安全威胁报告》

02/19

赛门铁克中国地区办事处
北京 电话:(010)58746999
上海 电话:(021)60377266
广州 电话:(020)28017160
安全产品售后技术支持热线: 800 810 3992

www.symantec.com.cn