McAfee
Together is power.

McAfee Labs 威胁报告

2018 年 9 月

本季度的重要事件

想入侵锁定的 Windows 10 设备?询问 Cortana (CVE-2018-8140)

威胁报告:在不能确保安全性的情况下,请勿加入“区块链革命”

AsiaHitGroup 犯罪团伙再次将收费欺诈应用程序潜入到 Google Play 中

在第 2 季度，McAfee Global Threat Intelligence 平均每天分析 1,800,000 个 URL、800,000 个文件和沙盒中的其他 200,000 个文件。

简介

欢迎阅读《McAfee® Labs 威胁报告 2018 年 9 月版》。在本期报告中，我们重点介绍 McAfee Advanced Threat Research 和 McAfee Labs 团队于 2018 年第 2 季度收集的一些值得关注的调查研究和威胁趋势统计数据。

网络犯罪分子继续以追逐金钱为目的。尽管人们对上述说法已习以为常，然而我们最新的威胁报告清晰地表明，随着新的威胁媒介变得愈发有利可图，一些早期的攻击方式正在向新的威胁媒介转变。我们注意到，与第 1 季度的情况相同，加密货币挖掘攻击继续呈上升态势。

在这份报告中，我们详细阐述了 McAfee Labs 通过分析第 2 季度的数据，得出的三项最新发现。您可以在第 5-7 页上阅读每项发现的相关摘要信息。我们研究团队调查的其中一个领域是“数字助理”。在第 2 季度，我们分析了 Microsoft Cortana 中的漏洞。攻击者可利用这项缺陷，登录到锁定的 Windows 设备并执行代码。依照我们的漏洞披露政策，我们在发现这个漏洞后与 Microsoft 进行了沟通；相关的分析内容，已归类在 CVE-2018-8140 中。另外，通过深入了解区块链技术，我们还对加密货币攻击领域进行了研究。在我们的报告中，详细说明了威胁实施者妄图快速获得投资回报而利用的大量漏洞。

此报告的研究及编写人员：

- Christiaan Beek
- Carlos Castillo
- Cedric Cochin
- Ashley Dolezal
- Steve Grobman
- Charles McFarland
- Niamh Minihane
- Chris Palm
- Eric Peterson
- Steve Povolny
- Raj Samani
- Craig Schmugar
- ReseAnne Sims
- Dan Sommer
- Bing Sun

对于恶意软件，我们的报告详细分析了“网络犯罪”这一领域；与那些大肆报道、被大家谈论得“沸沸扬扬”的勒索软件攻击相比，有关“网络犯罪”领域的报告信息，在过去的 18 个月中往往很少提及。“收费欺诈”一度成为了多个威胁实施组织的惯用伎俩。我们检测到 AsiaHitGroup 在其发起的活动中，试图通过官方商店（例如，Google Play）中的应用程序，对 20,000 名受害者收取费用。

在第 2 季度，McAfee Global Threat Intelligence 平均每天都会收到 490 亿次查询。与此同时，新恶意软件的数量已经连续第二个季度呈下降趋势；然而，这或许并不具有重要意义，因为我们看到 2017 年第 4 季度新恶意软件的数量出现飙升，而且在过去的五个季度中，有四个季度的新样本数量都一直保持相对平稳。在第 2 季度，新出现的移动设备恶意软件样本增加了 27%，这是连续第二个季度出现增长态势。加密货币挖掘恶意软件仍然十分活跃；第 2 季度总样本数量增长 86%，恶意软件数据库增加了超过 250 万份的新文件。

很高兴地告诉大家，您现在可以通过 McAfee ePolicy Orchestrator® (McAfee ePO™) 版本 5.10.0 及更高版本的平台，访问我们的所有研究报告。此外，还可以通过我们的常规社交渠道（详细信息如下所示），以及 McAfee Labs 和 McAfee Advanced Threat Research 主页来查看我们的威胁报告。

及时了解安全信息，保障网络安全。

—Steve Grobman，首席技术官

—Raj Samani，McAfee Advanced Threat Research 团队成员和首席科学家

Twitter

@SteveGrobman

@Raj_Samani

关注

共享

目录

本季度的重要事件

想入侵锁定的 Windows 10 设备?询问 Cortana (CVE-2018-8140)

McAfee Labs 和 Advanced Threat Research 团队在 Microsoft Windows 10 的 Cortana 语音助手中发现了一个漏洞。该缺陷会导致执行未经授权的代码，Microsoft 已在 6 月份为此缺陷提供修复。我们解释了如何利用该漏洞，从经过完全修补的 Windows 10 计算机（安装了 6 月份发布的修补程序之前的 RS3 和 RS4）的锁定屏幕上执行代码。在这份分析报告中，我们解释了三个研究层面，并将它们融合在一起提出了 CVE-2018-8140。这三个层面已得到 Microsoft 的综合考虑。第一个研究层面是信息泄漏；我们用一个演示结束了相关工作，该演示介绍了有关登录到锁定的 Windows 设备的整个代码执行过程。作为 Advanced Threat Research 团队负责履行披露政策的一部分，我们在 4 月份向 Microsoft 提交了这个漏洞。该漏洞的提交工作是由网络安全架构师兼资深首席工程师 Cedric Cochin 完成的。

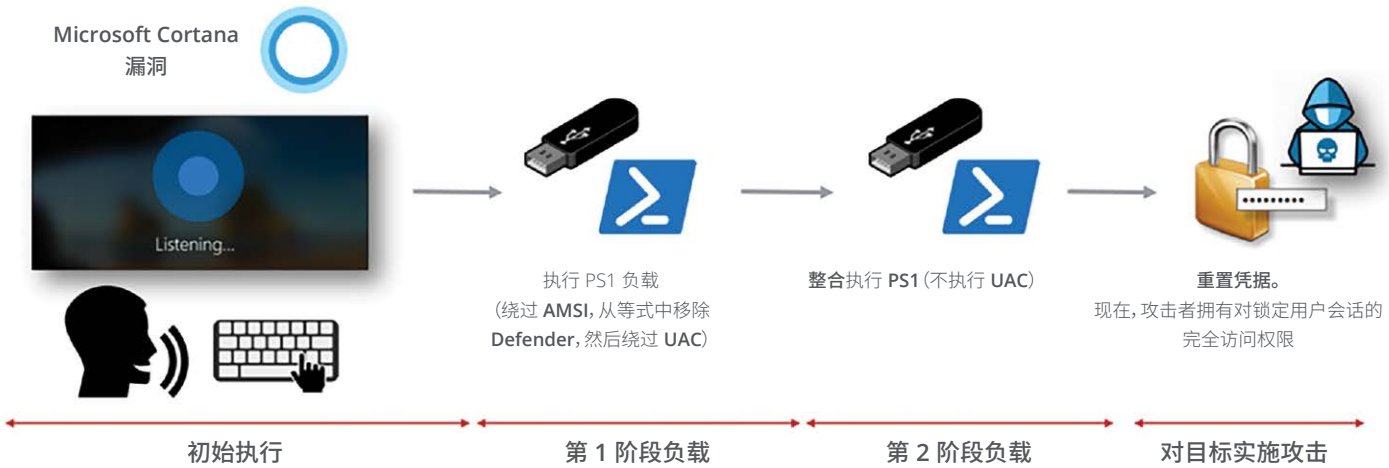


图 1. 攻击者通过四个基本步骤，就可以利用 Cortana，获取对 Windows 10 系统的完全控制权。

关注 共享

威胁报告：在不能确保安全性的情况下，请勿加入“区块链革命”

由于加密货币日益流行，区块链革命愈演愈烈。另外，网络犯罪分子也发现了一些新的攻击角度，包括通过非法货币挖掘和盗窃来获取利润。McAfee Advanced Threat Research 团队在 6 月份发布了一份区块链威胁报告，该报告向区块链技术的用户及实施人员阐述了最新的相关威胁。

即便您没有听说过“区块链”，也很可能会对“加密货币”，尤其是“比特币”有所耳闻，这些是当前最流行的实施方案。加密货币构建在区块链之上，区块链采用去中心化的方式记录各笔交易，它可以在相互并不信任的参与者之间建立信任“账本”。账本中的每个区块都与下一区块相链接，为此就形成了区块链。区块链允许任何人员在无需转到外部源的情况下验证所有的交易。去中心化的货币（例如，比特币）就是根据这个原理来运作的。在这份报告中，我们研究了主要攻击媒介：网络钓鱼、恶意软件、实现漏洞和技术。

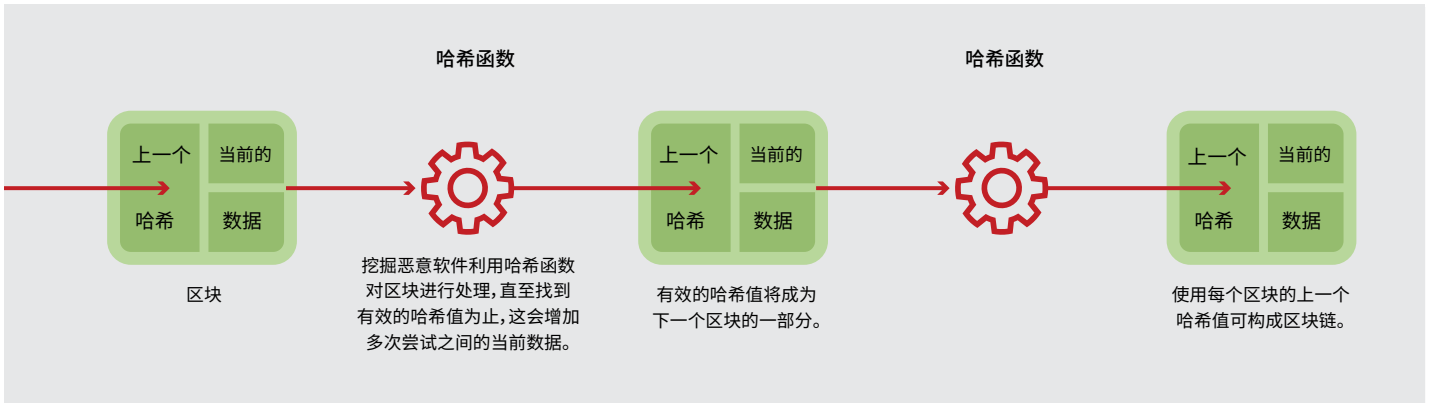


图 2. 证据：构建在每个以往哈希上的工作区块链。资料来源：https://bitcoin.org/bitcoin.pdf

关注 共享

AsiaHitGroup 犯罪团伙再次将收费欺诈应用程序潜入到 Google Play 中

McAfee Mobile Research 团队发现了一个新的收费欺诈活动；2018 年，至少有 15 个收费欺诈应用程序潜入到 Google Play 中。根据报告“Android Security 2017 Year in Review”（2017 年 Android 安全回顾），话费欺诈（包括收费欺诈）是 Google Play 上具有潜在危害的主要应用程序类别。这项新的收费欺诈活动表明，网络犯罪分子一直在伺机寻找新的途径，利用官方商店（例如 Google Play）上的应用程序来窃取受害者的钱财。这次行动的幕后操纵者是 AsiaHitGroup 犯罪团伙，他们至少从 2016 年年底就开始猖獗作乱，不断散布虚假安装程序（fake-installer）应用程序 Sonvpay.A，企图主要从泰国和马来西亚向那些下载常用应用程序副本的用户赚取费用，至少有 20,000 名受害者为此中招儿。一年之后，在 2017 年 11 月，Google Play 上出现了一项新的活动“Sonvpay.B”，该活动利用 IP 地址的地理位置来确认受害者所在的国家/地区，并将俄罗斯的受害者添加到收费欺诈对象行列，以此来提高从毫无戒备的用户那里窃取钱财的可能性。我们的调查报告阐明了此类恶意软件在这些欺诈活动中的运作方式。

图 3. 此前在 Google Play 上发现的、由 AsiaHitGroup 犯罪团伙散布的恶意应用程序。

关注

共享

统计信息

McAfee Global Threat Intelligence

每个季度，McAfee® Global Threat Intelligence (McAfee GTI) 云信息显示板都可以让我们查看和分析各种真实的攻击模式，以便我们为客户提供更好的保护。这些信息体现了我们的客户所面临的攻击数量。McAfee GTI 平均每天会收到 490 亿次查询和 130 亿行的遥测数据，分析 1,800,000 个 URL 和 800,000 个文件，以及沙盒中的另外 200,000 个文件。

- McAfee GTI 可抵御恶意文件（第 2 季度报告了 86,000 个危险的恶意文件，占检测到的 8600 万个文件总量的 0.1%）。
- McAfee GTI 可抵御恶意 URL（第 2 季度报告了 365,000 个危险的恶意 URL，占检测到的 7300 万个 URL 总量的 0.5%）。
- McAfee GTI 可抵御恶意 IP 地址（第 2 季度报告了 268,000 个危险的恶意 IP 地址，占检测到的 6700 万个 IP 地址总量的 0.4%）。

关注 共享

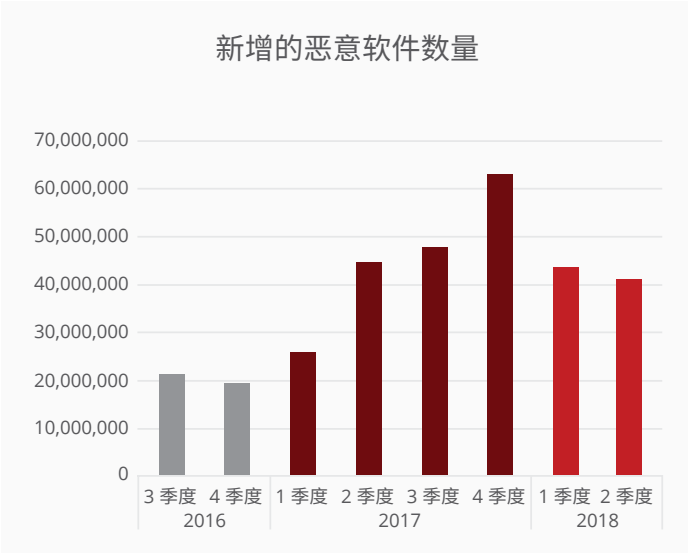
威胁统计信息

10个 恶意软件

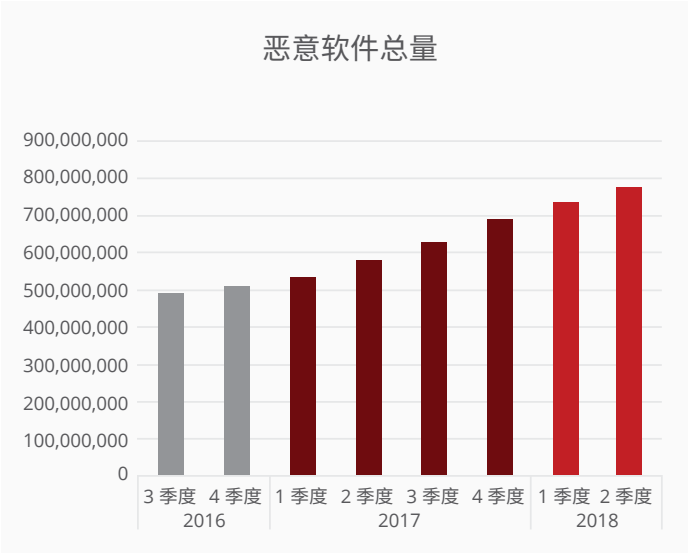
17个 事件

19个 Web 和网络威胁

恶意软件

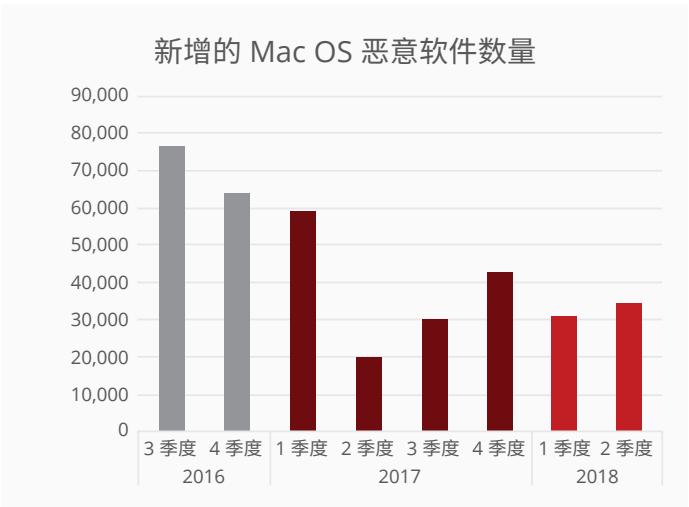


资料来源：McAfee Labs，2018 年。

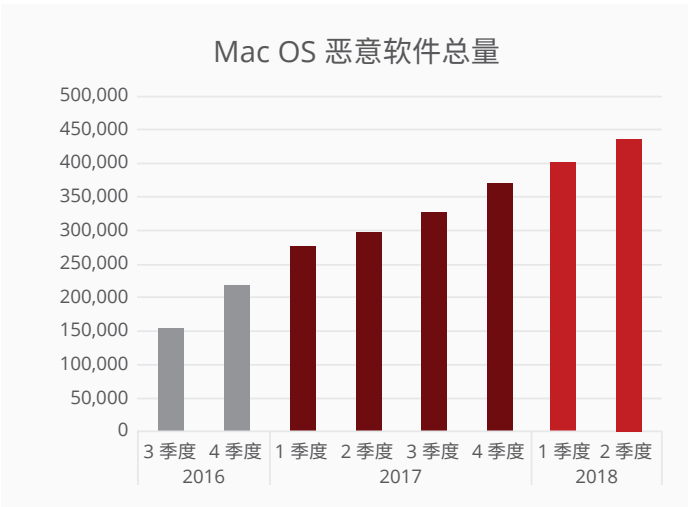


资料来源：McAfee Labs，2018 年。

恶意软件数据来源于 McAfee 样本数据库，其中包括通过 McAfee 垃圾邮件陷阱、爬网程序和客户提交方式收集的恶意文件，以及其他行业来源提供的恶意文件。



资料来源：McAfee Labs，2018 年。



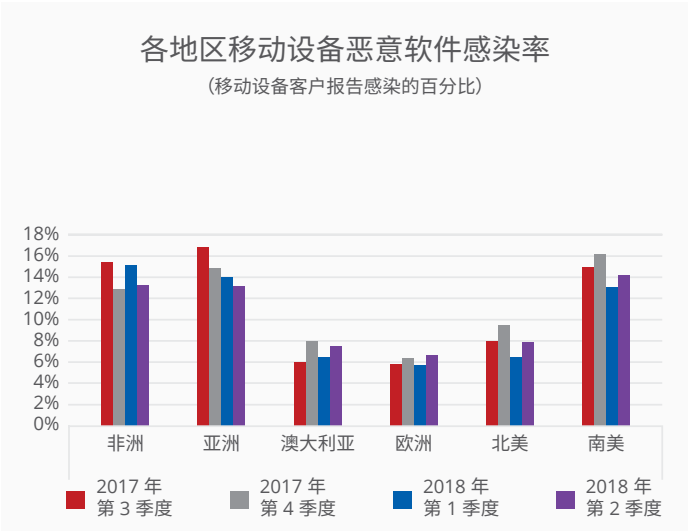
资料来源：McAfee Labs，2018 年。

关注

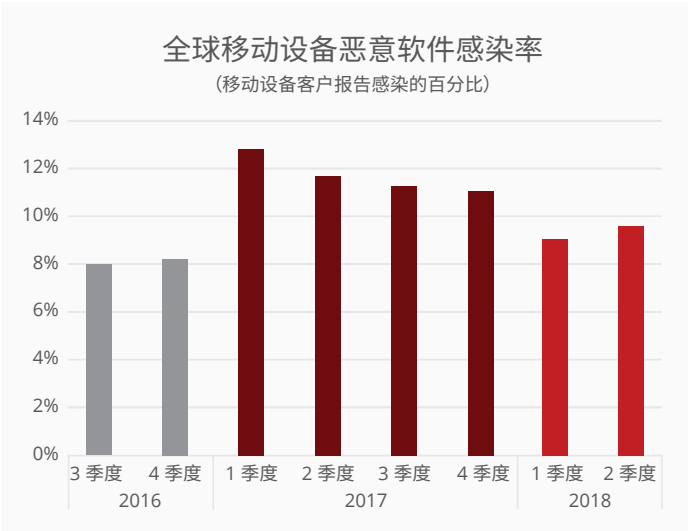
共享

资料来源：McAfee Labs，2018 年。

资料来源：McAfee Labs，2018 年。



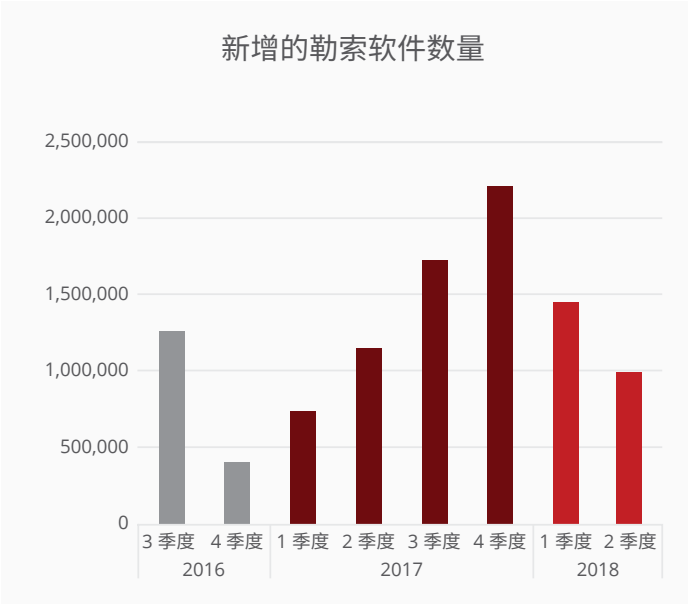
资料来源：McAfee Labs，2018 年。



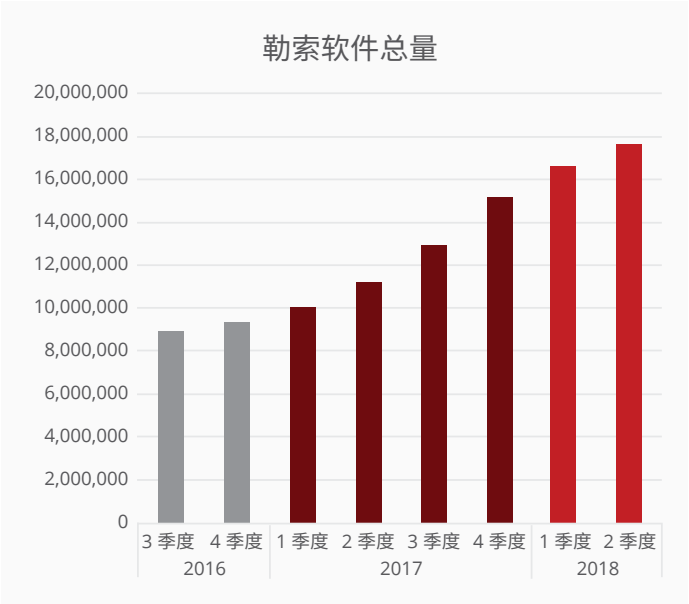
资料来源：McAfee Labs，2018 年。

关注

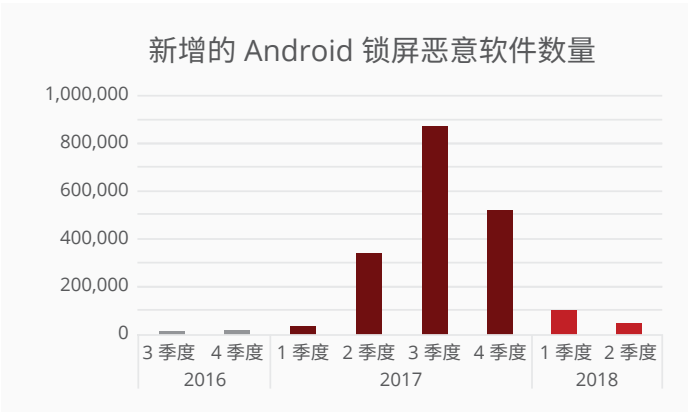
共享



资料来源：McAfee Labs，2018 年。



资料来源：McAfee Labs，2018 年。



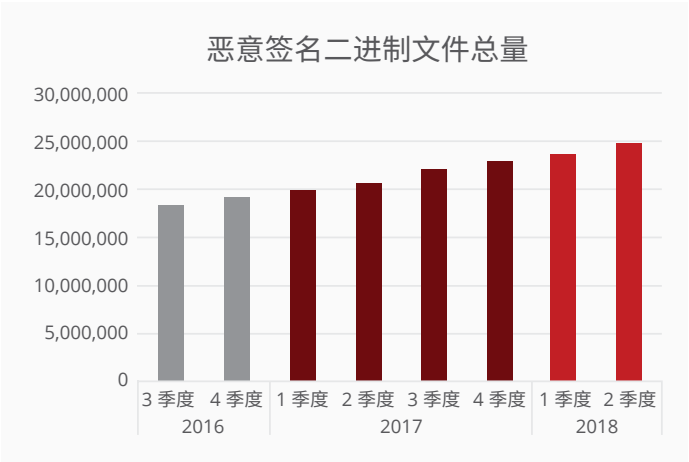
资料来源：McAfee Labs，2018 年。

资料来源：McAfee Labs，2018 年。

关注

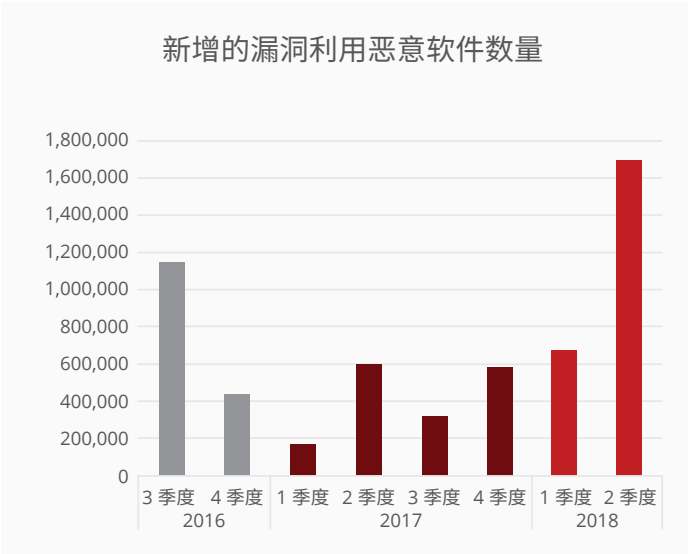
共享

资料来源：McAfee Labs，2018 年。

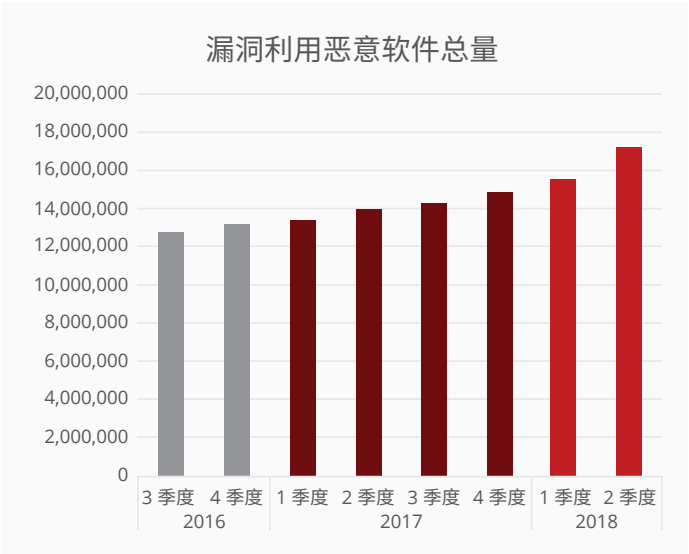


资料来源：McAfee Labs，2018 年。

当二进制文件（应用程序）经过内容提供商签名并验证后，证书颁发机构负责颁发可提供相关信息的数字证书。如果网络犯罪分子通过恶意签名的二进制文件获得数字证书后，发起攻击会变得更加容易。



资料来源：McAfee Labs，2018 年。

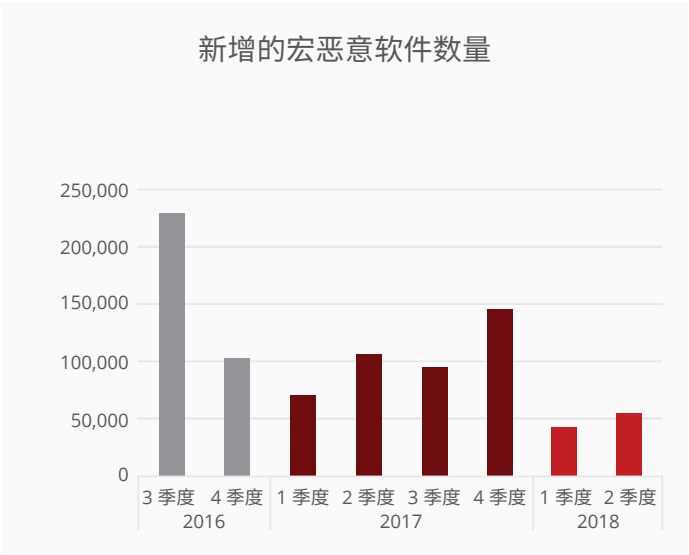


资料来源：McAfee Labs，2018 年。

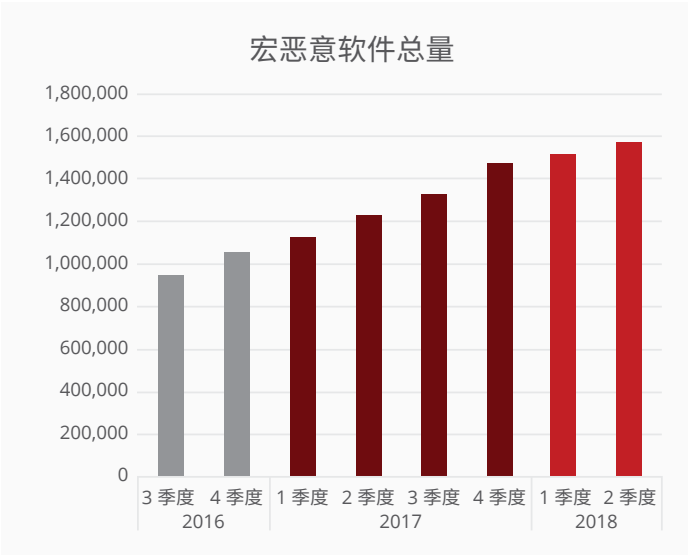
黑客利用软件和硬件中的缺陷及漏洞实施攻击。零日攻击就是成功利用漏洞的示例。相关示例，请参阅 McAfee Labs 发布的“Analyzing Microsoft Office Zero-Day Exploit CVE-2017-11826: Memory Corruption Vulnerability（分析 Microsoft Office 零日威胁 CVE-2017-11826：内存受损漏洞）”。

关注

共享

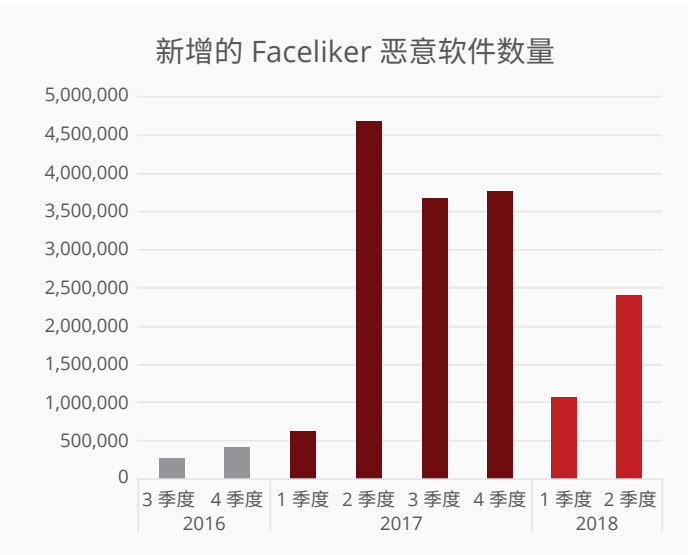


资料来源：McAfee Labs，2018 年。

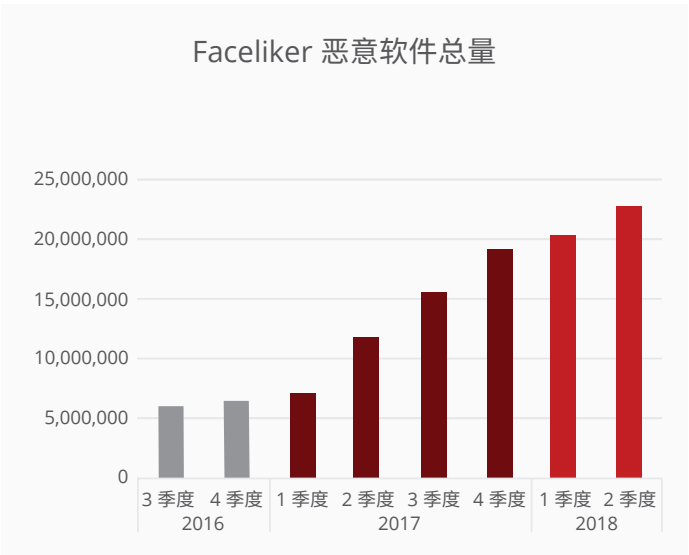


资料来源：McAfee Labs，2018 年。

宏恶意软件通常以垃圾电子邮件或压缩附件中的 Word 或 Excel 文档形式出现。其虚假的文件名很有诱惑力，如果宏已启用，那么受害者一打开文档就会遭到感染。



资料来源：McAfee Labs，2018 年。

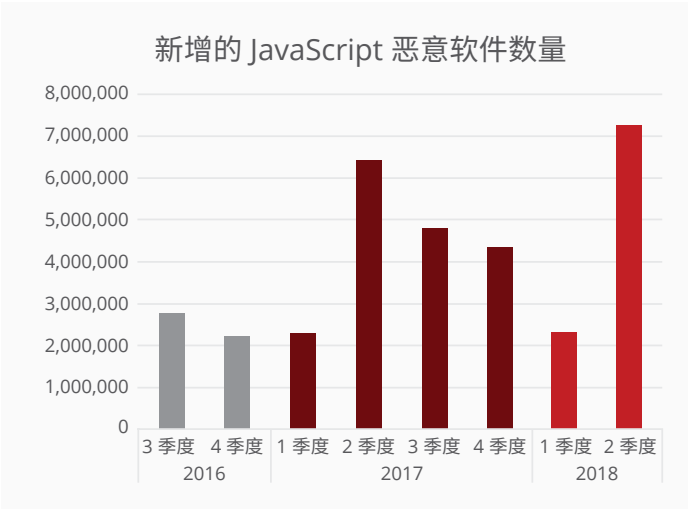


资料来源：McAfee Labs，2018 年。

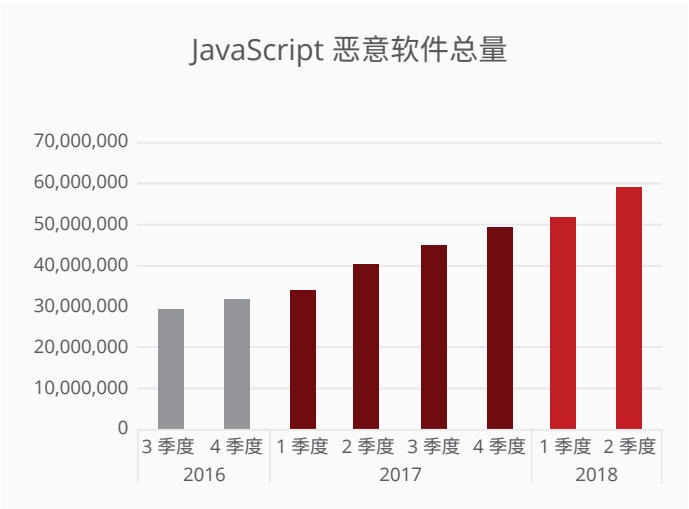
Faceliker 特洛伊木马操纵 Facebook 点击次数，以伪造点“赞”的特定内容。要了解更多信息，请阅读 McAfee Labs 发表的相关文章。

关注

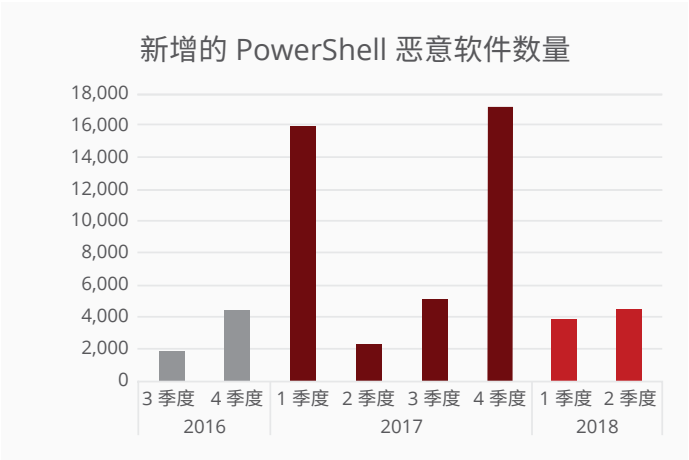
共享



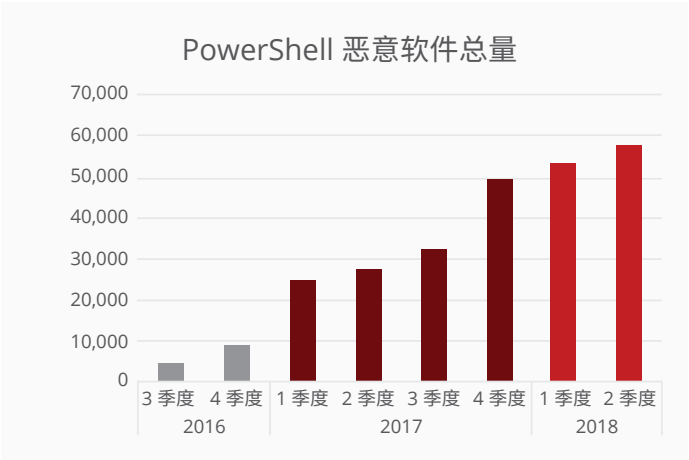
资料来源：McAfee Labs，2018 年。



资料来源：McAfee Labs，2018 年。



资料来源：McAfee Labs，2018 年。



资料来源：McAfee Labs，2018 年。

有关 JavaScript 和 PowerShell 威胁的更多信息，请阅读 McAfee Labs 威胁报告早期版本中的“基于脚本的恶意软件兴起”。

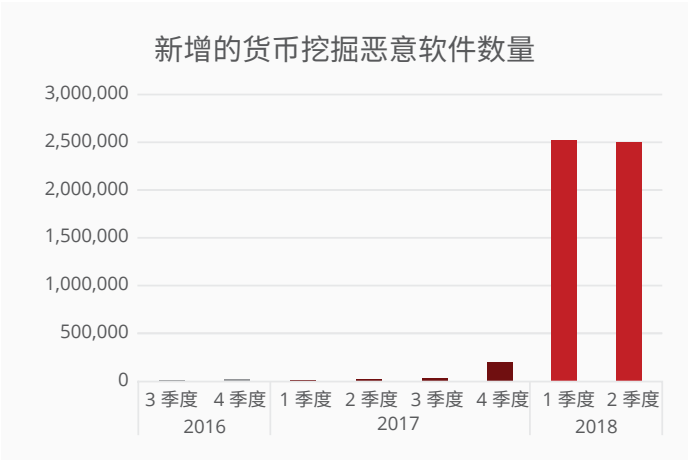
关注

共享

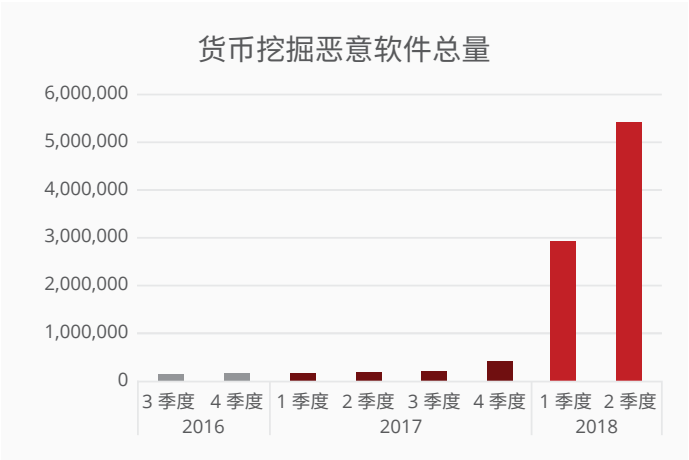
资料来源：McAfee Labs，2018 年。

资料来源：McAfee Labs，2018 年。

网络犯罪分子不断利用 .lnk 快捷方式来秘密提供恶意 PowerShell 脚本和其他恶意软件。



资料来源：McAfee Labs，2018 年。



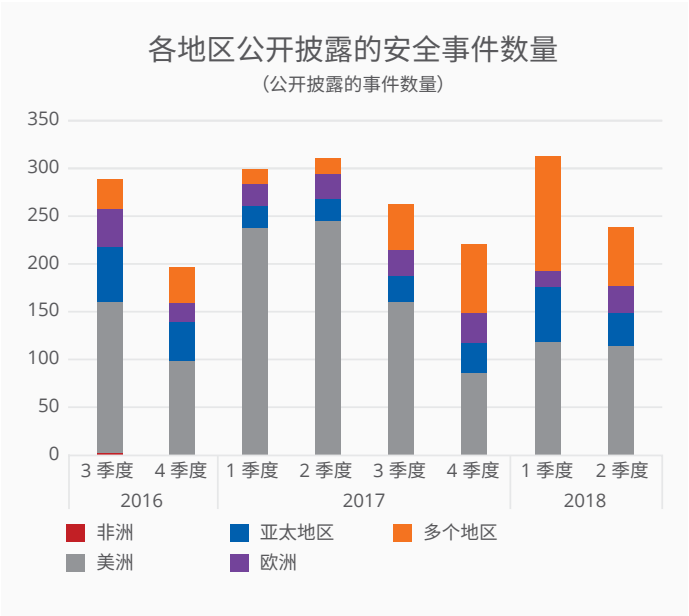
资料来源：McAfee Labs，2018 年。

在未经受害者同意或知情的情况下，货币挖掘恶意软件劫持系统以创建加密货币（“矿”）。2018 年，新的货币挖掘软件威胁大幅增加。

关注

共享

事件



资料来源：McAfee Labs，2018 年。

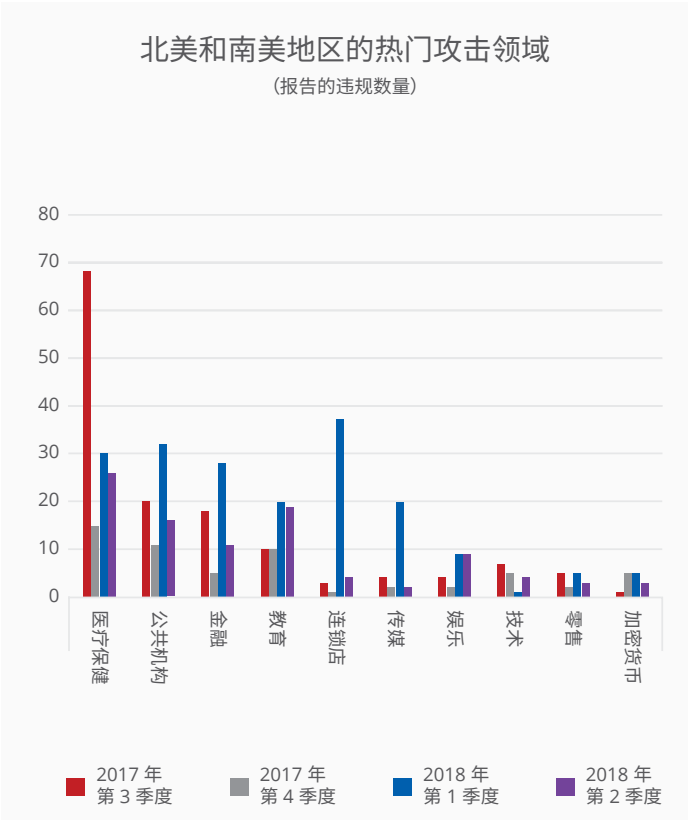
资料来源：McAfee Labs，2018 年。

安全事件数据是使用多种来源编译的，其中包括 hackmageddon.com、privacyrights.org/data-breaches、haveibeenpwned.com 和 databreaches.net。

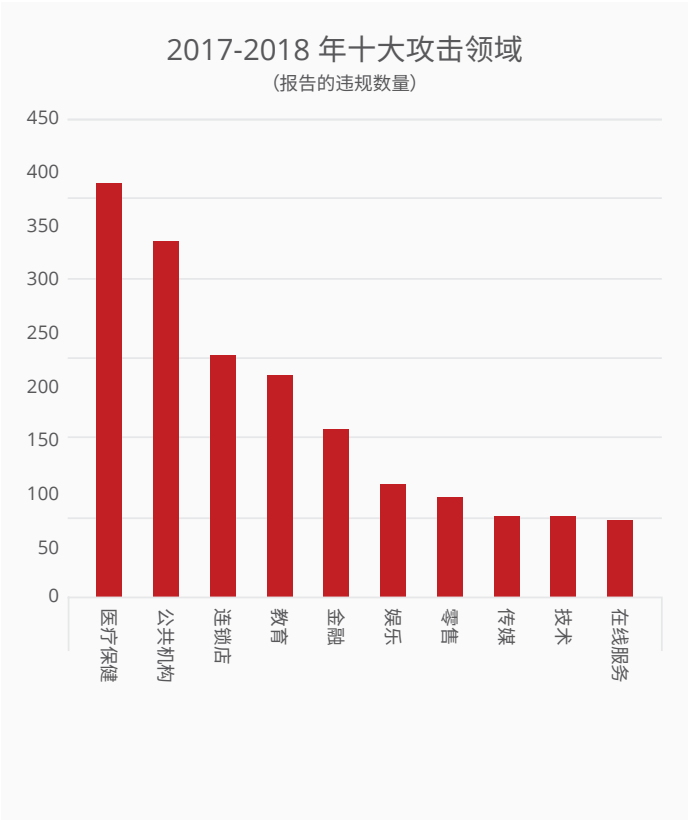
大多数攻击媒介都是未知或尚未公开报道的。

关注

共享



资料来源：McAfee Labs，2018 年。

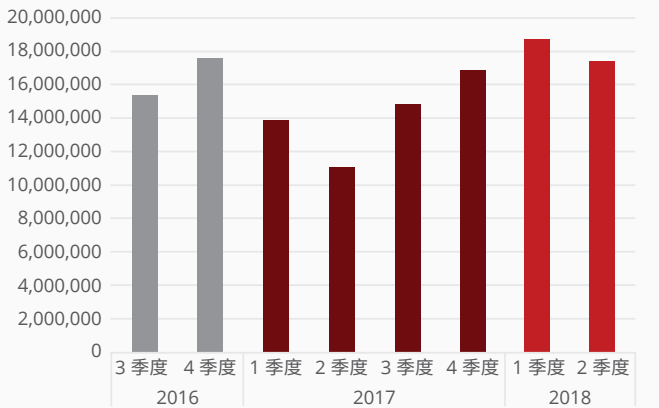


资料来源：McAfee Labs，2018 年。

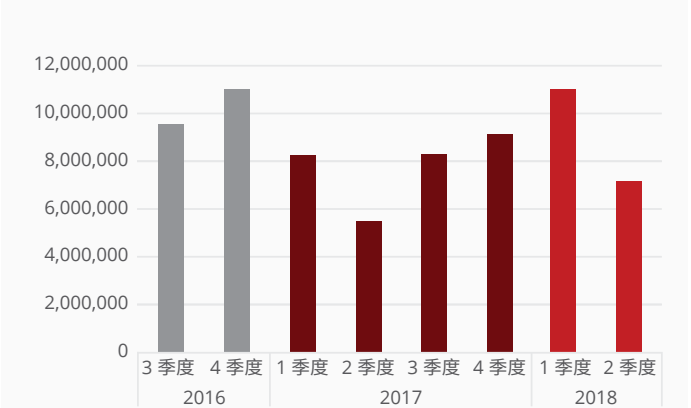
关注

共享

Web 和网络威胁

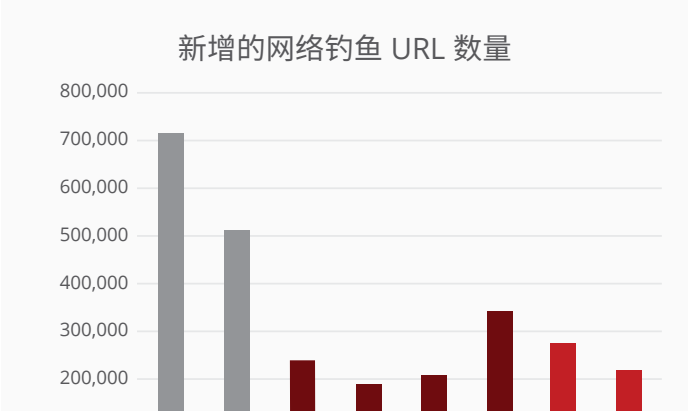


资料来源：McAfee Labs，2018 年。



资料来源：McAfee Labs，2018 年。

资料来源：McAfee Labs，2018 年。



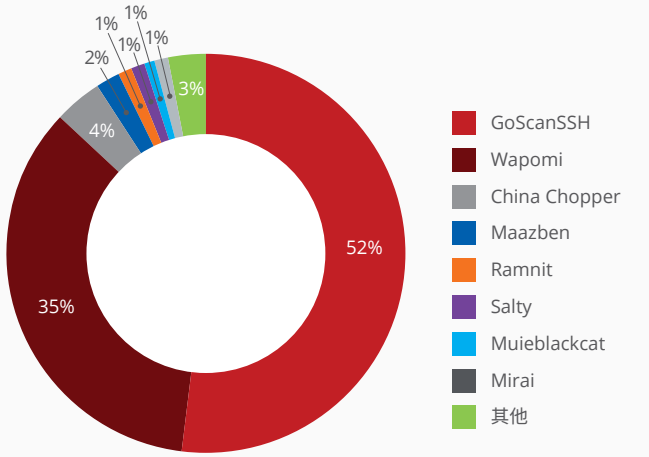
资料来源：McAfee Labs，2018 年。

McAfee® TrustedSource™ Web 数据库包含按网站信誉归类的 URL（网页），可与过滤策略一起用于管理网络访问。可疑 URL 的数量指的是那些评为高风险或中等风险的站点的总量。恶意 URL 部署代码，其中包括“路过式”可执行文件和特洛伊木马程序，旨在劫持计算机的设置或活动。恶意下载内容的源站点可让用户在不知情的状况下，无意间下载有害或恼人的代码。网络钓鱼 URL 是一些网页，通常以盗用用户帐户信息的恶作剧电子邮件形式出现。

关注

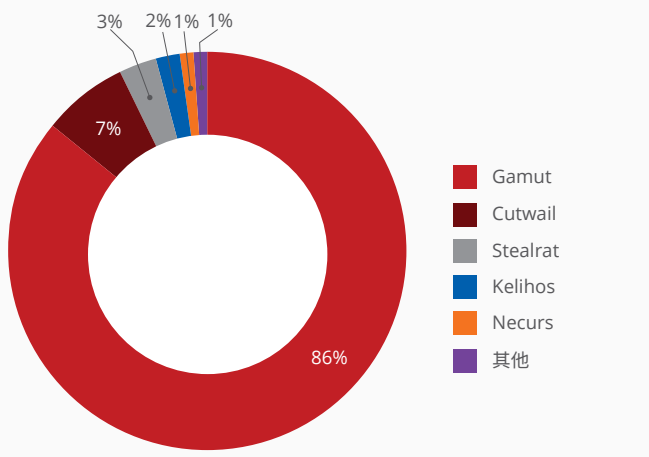
共享

第 2 季度连接到控制服务器的热门恶意软件



资料来源：McAfee Labs，2018 年。

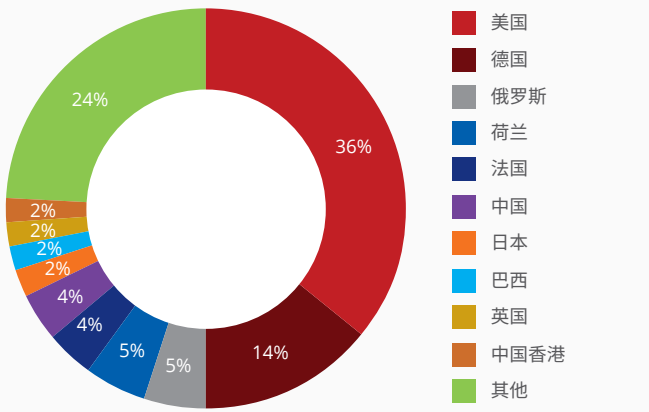
第 2 季度流行的垃圾邮件僵尸网络占比



资料来源：McAfee Labs，2018 年。

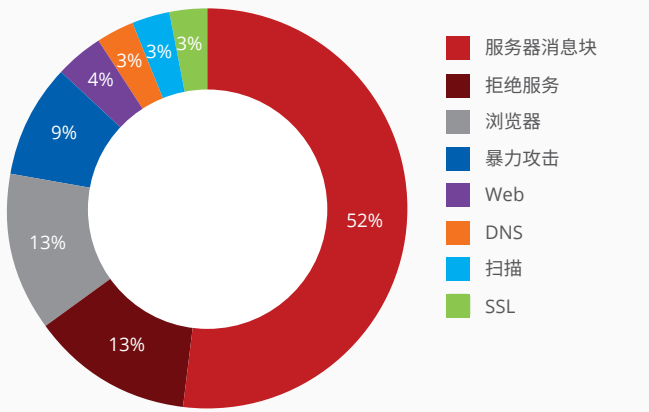
第 2 季度，Gamut 垃圾邮件僵尸网络的增长速度超过了所有其他网络威胁。尤其值得注意的是，它大规模实施了“加拿大税务局”(Canada Revenue Agency) 网络钓鱼诈骗。最近的活动与虚假工作岗位有关，通常称作“钱骡”招募伎俩。

第 2 季度托管僵尸网络控制服务器的主要国家/地区



资料来源：McAfee Labs，2018 年。

第 2 季度的热门网络攻击



资料来源：McAfee Labs，2018 年。

关注

共享

关于 McAfee

McAfee 是设备到云网络安全公司。在协同工作思想的启迪下，McAfee 研发出了适用于企业用户和家庭用户的解决方案，让网络环境变得更为安全。通过构建与其他公司产品集成的解决方案，McAfee 能够帮助企业部署真正集成的网络环境，通过协作的方式及时进行威胁检测和纠正，从而保护网络安全。通过保护用户的所有设备的网络安全，McAfee 能够随时随地为他们的数字化生活提供安全保障。McAfee 与其他安全参与者同心协力，致力于打击网络犯罪分子，以保护所有用户的利益。

www.mcafee.com/cn.

关于 McAfee Labs 和 Advanced Threat Research

McAfee Advanced Threat Research 团队领导的 McAfee Labs 是威胁研究、威胁情报和网络安全先进理念的全球领先来源之一。利用从跨主要威胁媒介（文件、Web、消息和网络）的数百万传感器获取的数据，McAfee Labs 和 McAfee Advanced Threat Research 团队可提供实时威胁情报、关键分析和专家意见，以便增强保护并降低风险。

www.mcafee.com/cn/mcafee-labs.aspx.

McAfee™
Together is power.

北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层，100013
电话：8610 8572 2000
www.mcafee.com/cn

2018 年 9 月