Symantec

INTERNET SECURITY THREAT REPORT

执行摘要

2019 年《互联网安全威胁报告》

ISTR

第 24 期

执行摘要

Formjacking、目标性攻击、离地攻击，都在觊觎您的业务。

如同蜂蝶追花逐蜜一样，网络不法分子总是青睐最新的漏洞利用，企图以最小的付出快速赚到大钱。勒索软件和挖矿劫持猖獗的时代已经过去，现在是 Formjacking 的天下。

在赛门铁克《互联网安全威胁报告》第 24 期中，我们对全球威胁活动、网络犯罪趋势和攻击者动机进行了深入剖析，提出了自己的最新见解。

我们的分析数据来自全球最大的民用威胁情报网络，即赛门铁克全球情报网络。该网络覆盖全球 1.23 亿个攻击传感器，日均拦截威胁数量达 1.42 亿个，有效跟踪全球 157 多个国家/地区的威胁活动。

{FORMJACKING}

Formjacking 正成为网络犯罪分子快速致富的利器

Formjacking 攻击方法简单且有利可图：网络犯罪分子将恶意代码植入零售商网站以窃取购物者的信用卡详细信息。平均每个月就有 4800 多个独立网站遭到攻击。

无论是知名大企业（例如特玛捷票务和英国航空公司）还是中小型企业都未能幸免。犯罪分子去年一年即从中获利数千万美元。

他们仅需在每个受感染的网站盗取 10 张信用卡信息，即可获得最高为 220 万美元/月的收益，因为在地下销售论坛每张信用卡最高可卖到 45 美元。仅英国航空公司在攻击中就有超过 38 万张信用卡信息被盗，给犯罪分子送去 1700 多万美元的净收益。

RANSOMWARE
勒索软件

CRYPTOJACKING
挖矿劫持

活动有所减缓，但从未停止

勒索软件和挖矿劫持曾是网络犯罪分子首选的赚钱法宝。但随着 2018 年的收益锐减，其活动频率有所减缓。

勒索软件攻击数量自 2013 年以来首次出现 20% 的总体下滑，但针对企业的攻击数量则上升了 12%。

由于加密货币价值暴跌 90%，挖矿劫持的攻击数量在 2018 年也随之下降了 52%。尽管如此，由于门槛低且开销小，挖矿劫持仍然深受犯罪分子青睐；2018 年，赛门铁克拦截的挖矿劫持攻击数量达到上一年度的四倍。

TARGETED ATTACKS
目标性攻击

目标性攻击者具有疯狂的破坏欲

供应链攻击和离地攻击现已成为网络犯罪的主流：2018 年供应链攻击增加了 78%。

离地攻击技术会将攻击者隐藏在合法流程中。例如，去年恶意 PowerShell 脚本使用量暴涨 1000%。

赛门铁克每个月阻止的恶意 PowerShell 脚本多达 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。如果全面阻止所有 PowerShell 活动，势必会干扰到正常业务。这进一步揭示了为何众多目标攻击团伙将离地攻击技术作为首选，就是因为它的活动隐秘性。

MORE AMBITIOUS
更加疯狂

攻击者还愈加频繁地使用鱼叉式网络钓鱼等屡试不爽的方法，对企业进行渗透攻击。尽管攻击者的首要动机是收集情报，但部分团伙同时也专注破坏。目前，近十分之一的目标性攻击团伙借助恶意软件来破坏和干扰业务运营，这一数字比上一年上升了 25%。

一个明显的例子就是 Shamoon，它在沉寂两年之后重新归来，广泛部署数据擦除恶意软件，删除目标企业计算机上的文件，在中东地区造成了恶劣影响。

云

云挑战：云端存储，安全至上

一个配置不当的云端工作负载或存储实例可为企业造成数百万美元损失或重大合规问题。2018 年，因 S3 存储桶配置不当而导致信息泄露或失窃的记录超过 7000 万条。网络上有众多工具可让攻击者识别出配置有误的云资源。

硬件芯片漏洞（包括 Meltdown、Spectre 和 Foreshadow）允许入侵者访问同一物理服务器中所托管云服务上的受保护内存空间。如果这一漏洞被成功利用，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。

AND STEALTHIER
更加隐秘

IoT 物联网

常用的物联网设备是攻击者的最佳目标

尽管路由器和联网摄像机占到受感染设备的 90%，但几乎每一种物联网设备，从智能灯泡到语音助理，都很容易遭受攻击。

目标性攻击团伙对物联网的兴趣与日俱增，将其作为入侵点用来销毁或擦除设备、窃取凭据、数据和拦截 SCADA 通信。

而工业 IT 发展成了潜在的网络战场，诸如 Thrip 和 Triton 等威胁团伙即隐藏在具有感染性的操作和工业控制系统中。

ELECTION INTERFERENCE 2018

2018 年选举干扰事件

您的社交媒体是否影响到选举?

2018 年美国中期选举可谓万众瞩目，所幸的是并未受到重大干扰。但社交媒体仍是一个活跃的战场。

在选举期间，不少仿冒合法政治网站的恶意域被及时发现并关闭，而众多与俄罗斯相关的账户则通过第三方为这些域购买了社交媒体广告。

社交媒体公司在打击选举干预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；而 Twitter 则删除了 10,000 个劝说人们不参加投票的僵尸程序。

在此获得详细信息。下载赛门铁克 2019 年《互联网安全威胁报告》(ISTR)
https://symc.ly/APISTR

关于赛门铁克

赛门铁克公司（纳斯达克：SYMC）是全球领先的网络安全企业，旨在帮助个人、企业和政府机构保护无处不在的重要数据安全。全球企业都青睐选用赛门铁克的战略性集成式解决方案，在端点、云和基础架构抵御复杂攻击。

同时，全球 5000 多万的个人和家庭也在使用赛门铁克的 Norton 和 LifeLock 产品，保护家庭各类联网设备安全，畅享无忧数字生活。赛门铁克经营的在全球规模数一数二的威胁情报网络，能够发现和抵御最高级威胁。如欲了解其他信息，请访问 www.symantec.com.cn 或通过 weibo.com/SymantecChina 联系我们。

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

ISTR