简译版

2018 年上半年无文件攻击飙升 94%

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Fileless Attacks Jump 94% in First Half of 2018		
原文作者	Kelly Sheridan	原文发布日期	2018 年 8 月 28 日
作者简介	Kelly Sheridan 是 Dark Reading 的编辑。https://www.darkreading.com/author-bio.asp?author_id=837		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/endpoint/fileless-attacks-jump-94--in-first-half-of-2018/d/d-id/1332686		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

2018 年上半年无文件攻击飙升 94%

Kelly Sheridan

2018 年 8 月 28 日

虽然勒索软件攻击态势仍然很严峻，但是无文件攻击和 PowerShell 攻击是今年最需要关注的威胁。

安全分析师报告称，通过分析 2018 年上半年的威胁形势，他们发现无文件攻击和 PowerShell 攻击是今年最需要担心的问题。

终端安全公司 SentinelOne 今天发布了《2018 年上半年企业风险指数报告》，该报告显示，1 月至 6 月期间，无文件攻击飙升了 94%。就 PowerShell 攻击统计数字来讲，每 1000 台终端，5 月份攻击次数是 2.5 次，而 6 月份则增加到 5.2 次。勒索软件攻击仍然猖獗，每 1000 台终端遭受的攻击数量从 5.6 次增加到 14.4 次。

SentinelOne 产品管理总监兼本报告的负责人阿维拉姆·什穆利（Aviram Shmueli）指出，无文件和 PowerShell 攻击的兴起并不意外，对于想要实现隐蔽的威胁源来说，这两种攻击方法非常有吸引力。

“无文件攻击更为复杂，不会留下任何痕迹。”他解释说，并补充说，这类威胁在用户数据中越来越常见。PowerShell 攻击的增加向我们传达了这样一个消息，“PowerShell 攻击将会继续存在”，什穆利说。在本报告分析的所有攻击中，无文件攻击、横向移动和文档攻击占了 20%。

他说，无文件攻击和 PowerShell 攻击的威力都很强大，攻击者可以通过其中任何一种攻击造成重大的损害。值得注意的是，这两者存在重叠：威胁源可以通过 PowerShell 攻击访问内部组件，而且可以以无文件的形式执行攻击，从而规避检测。

除了该报告，其他一些安全公司的研究报告也指出了 PowerShell 攻击的肆虐。今年初，迈克菲公司发布的研究结果显示，与 2016 年同期相比，2017 年第 4 季度借助 PowerShell 传播的无文件载体恶意软件飙升了 267%。

当谈到哪种攻击更容易得手时，什穆利说，PowerShell 攻击可能更容易得手。“Windows 系统上已经安装了 PowerShell，因此攻击者无需再安装任何其他东西。”他补充道，“我们认

为，这就是攻击者频繁使用该攻击方法的原因。”

然而，无文件攻击也在增加，这表明攻击者的手段越来越高明，开始转向更高级的网络犯罪活动。他们能够更轻松地创建不会被发现的载荷，增加防御的难度。

研究人员对最近无文件和 PowerShell 攻击飙升的驱动因素进行了调查，但是无法确定具体的原因。这似乎更像是一个整体的增长趋势，而不是与特定活动相关的增长。

虽然勒索软件、无文件和 PowerShell 攻击态势都很严峻，但是什穆利表示，公司应该特别关注无文件攻击。在出现 2018 年的峰值之前，无文件恶意软件的数量已经在持续增加了。

“我认为，我们会看到越来越多的无文件攻击和 PowerShell 攻击。”他补充道。至于勒索软件，他则不太确定。“勒索软件的趋势不是那么稳定，”他指出。SentinelOne 将继续发布此类季度报告。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。安天是中国应急响应体系中重要的企业节点，在红色代码、口令蠕虫、心脏出血、破壳、魔窟等重大安全威胁和病毒疫情方面，提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动，进行了深度的解析，对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上，安天创始人、首席技术架构师作为网络安全领域的发言代表，向习总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了位于哈尔滨科技创新城的安天公司，对安天负责人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com