简译版

2018——针对性攻击之年？

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	2018 – the year of the targeted attack?		
原文作者	Robert C. Covington	原文发布日期	2018 年 5 月 9 日
作者简介	Robert C. Covington 是 togoCIO.com 的创始人兼总裁。 https://www.csoonline.com/author/Robert-C.-Covington/		
原文发布单位	CSO Online		
原文出处	https://www.csoonline.com/article/3271424/cyber-attacks-espionage/2018-the-year-of-the-targeted-attack.html		
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——针对性攻击之年？

Robert C. Covington

2018 年 5 月 9 日

最近针对亚特兰大城市系统的勒索软件攻击，使居住在该市或附近的人感到不安。此次攻击仍在扰乱其城市网络，处理该事件已经花费了 260 万美元，而且这个数字可能还会增长。该攻击的影响非常广泛，导致全球最繁忙的机场——亚特兰大哈兹菲尔德国际机场（Dallas Hartsfield）——无法连接无线网络。

对很多人来说，涉事勒索软件 SamSam 的大名如雷贯耳，因为它参与了多起此类攻击，包括针对亚当斯纪念医院、医疗软件开发商 Allscripts 和新罕布什尔州法明顿市的攻击，仅在一月份就为攻击者赚取了约 32.5 万美元。

SamSam 被认为出自一个威胁源组织之手，该组织在目标网络上寻找开放的远程访问端口。一旦成功进入一个端口，他们将在网络中横向运动，直到获得足够的权限来发动攻击。他们不断得逞，其中一个原因是他们索要的赎金“合理”，并且通常在受害者付款后提供恢复文件所需的密钥。

SamSam 不是个案，它的一个小伙伴是新版的 SynAck 勒索软件，该版本可以像正常的 Windows 进程一样隐藏自己。Dark Reading 指出，SynAck 将开放的远程访问端口和暴力破解攻击相结合，发动针对性攻击。

对于信息安全领域的人来说，针对性攻击的概念并不新鲜，2014 年的索尼攻击就是一个序幕。在索尼攻击事件中，攻击者显然是蓄意执行破坏的。进入索尼公司的网络后，他们驻留数周或数月而不被发现，在此期间他们窃取了该公司的知识产权和私人通信。

针对性攻击越来越受威胁源青睐，这一点很容易理解。如果威胁源随机发送恶意软件，希望能够感染某些人，他们可能会得到许多低价值的目标，不值得花费这些时间。然而，在针对性攻击中，威胁源知道攻击目标是谁、他们能够找到什么样的资产以及这些资产的价值。根据这些信息，他们知道事后如何销售数据，或者向受害者勒索多少赎金。

SamSam 等针对性攻击的成功引发了一个重要的问题——如果威胁源使用的技术是众所周知的，那么为何还有这么多企业会遭受攻击呢？例如，如果攻击者寻找开放的远程桌面

协议（RDP）端口，那么企业为何不扫描他们网络中的开放端口并将其关闭呢？很少有实例需要开放的 RDP 端口，如果需要的话，可以采取简单的措施来进行保护。

令人遗憾的是，有迹象表明，太多的企业并未严肃对待安全问题，正如最近的一份报告所示，全球有 410 万个开放的 RDP 端口。信息安全是一门需要高度重视细节的学科，成功的唯一途径就是重视细节。

知道你有什么资产

许多企业都有“被遗忘在角落”的资产，指的是网络设备和服务器被置于角落并被遗忘。这些系统通常离得较远，因此会开启远程访问。它们为想要渗透网络的威胁源提供了很好的支点，而且这种访问通常不会被人注意到。你必须知道你有哪些系统以及它们都在哪里，这样才能进行保护和监控。

修复漏洞

如果发现漏洞，请尽快修复，不要因时间紧张而推迟修复。报告显示，在亚特兰大市遭受勒索软件攻击的数月前，就有迹象显示其网络系统存在严重的未修复漏洞。虽然此次攻击和未修复的漏洞之间没有明确的联系，但是发现漏洞后应该立即修复。

不要犯同样的错误

当你采取适当的措施（例如禁用 RDP 访问）防止攻击时，请确保这些措施是到位的。我见过太多这样的情况：网络端口被关闭后，又被不知情的员工重新开启了。请定期扫描你的网络以了解有哪些开放端口，并定期查看防火墙规则。

警惕声东击西的攻击

魔术师有一句谚语——“只让观众看到你想让他们看到的东西”。魔术师经常用一个动作分散观众的注意力，这样他们就不会注意到另一个动作了。威胁源经常使用同样的方法。他们声东击西，用一起攻击掩盖更重要的攻击。在之前的一起小型 DDoS 攻击期间，我就经历了这种事情。DDoS 攻击开始后不久，我就遭到了针对性的“鲸钓”攻击——一种发送给高管的钓鱼邮件。我认为 DDoS 攻击的目的是为了分散安全团队的注意力，与此同时发动鲸钓攻击。在发生攻击时，要确保安全团队的部分人员仍在监控其他攻击的信标，这一点很重

要。

关键问题是：专注于特定、高价值目标的高级威胁源组织明显增多。他们聪明而且有充分的动机，可能会渗透到很多网络中。我们不能为他们的攻击提供可乘之机，应尽可能地保护网络免受攻击，追踪提供威胁线索的威胁情报报告并警惕地监控攻击迹象。

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*