简译版

多阶段攻击技术增加了网络防御的难度

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	Multi-stage attack techniques are making network defense difficult		
原文作者		原文发布日期	2019 年 7 月 15 日
作者简介			
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/07/15/multi-stage-attack-techniques/		
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。		

多阶段攻击技术增加了网络防御的难度

Help Net Security

2019 年 7 月 15 日

Sophos 公司指出，由于缺乏安全专业知识、预算和最新技术，IT 管理人员面临着来自各个方向的网络攻击，每天都在费力应对。

在该研究中，Sophos 公司对美国、加拿大、墨西哥、哥伦比亚、巴西、英国、法国、德国、澳大利亚、日本、印度和南非的中型企业的 3100 名 IT 决策者进行了采访。

网络犯罪分子使用多种攻击方法和载荷来实现影响最大化

Sophos 的研究显示，攻击者的攻击技术多种多样，而且通常是多阶段的，这增加了网络防御的难度。在接受调查的 IT 管理人员中，有五分之一不知道他们是如何遭到攻击的。攻击方法的多样性意味着，没有任何一种防御策略是万能“银弹”。

“网络犯罪分子正在改进攻击方法，并且经常使用多个载荷来实现利润最大化。在 23%的事件中，软件漏洞是初始入口点；但是在所有攻击中，此类漏洞占 35%左右。这说明，软件漏洞被用于攻击链的多个阶段中。” Sophos 公司首席研究科学家切斯特·维希涅夫斯基（Chester Wisniewski）说道。

“如果企业仅为面向外部的高风险服务器打补丁，而忽视了内部服务器，则内部服务器就很容易遭到攻击了——网络犯罪分子正在利用这种漏洞。”

事实证明，广泛、多阶段和大规模的攻击是有效的。例如，在遭受网络攻击的受害者中，有 53%遭遇了网络钓鱼邮件攻击，30%遭遇了勒索软件攻击，41%则遭遇了数据泄露事件。

安全薄弱环节导致更多的供应链感染

研究显示，75%的 IT 管理人员将软件漏洞、未修复的漏洞和/或零日威胁视为最严重的安全风险。而 50%的 IT 管理人员认为网络钓鱼是最严重的安全风险之一。

令人惊讶的是，只有 16%的 IT 管理人员认为供应链是最严重的安全风险之一。这是网络犯罪分子很可能会利用的一个攻击向量。

“网络犯罪分子一直在寻找进入企业的途径，而供应链感染越来越受他们的青睐。IT 管理人员应该优先考虑供应链安全风险，但并非出于认为这些攻击是由国家攻击者对知名目标实施的原因。

维希涅夫斯基说：“一些国家可能参与了供应链攻击的规划。但是，一旦这些攻击技术被公布，就会被其他网络犯罪分子采用，以便降低成本，提高攻击成功率。”

“供应链攻击也是网络犯罪分子执行自动化、主动攻击的有效方式。在此类攻击中，他们可以从更大的潜在客户群中选择受害者，然后通过手动-自动技术和横向移动来规避检测，到达目标系统。”

缺乏安全专业知识、预算和最新技术

受访的 IT 管理人员指出，其安全团队平均将 26%的时间用于安全管理。另外，86%的受访者认为其安全团队需要增强安全专业知识；80%的受访者希望创建更强大的安全团队，以检测、调查和应对安全事件。

此外，企业还面临人才招聘的问题。79%的受访者表示，在招募具备所需网络安全技能的人才方面，企业面临着严峻的挑战。

在预算方面，66%的受访者表示，其企业的网络安全预算（包括人员和技术）低于其预期。企业能否掌握最新的技术也是一个问题——75%的受访者表示，对他们的企业来说，掌握最新的网络安全技术也面临着严峻的挑战。

企业缺乏安全专业知识、预算和最新技术，这意味着 IT 管理人员只能费力地响应已经发生的网络攻击，无暇主动规划和处理接下来将会发生的攻击。

“要想掌握威胁的来源，需要安全专业知识。但是 IT 管理人员往往很难招到合适的人才，或者没有适当的安全系统，这使他们无法快速有效地响应攻击。”维希涅夫斯基说。

“如果企业可以采用一种安全系统，使其产品协同工作以共享情报并自动应对威胁，那么 IT 安全团队就可以跳出‘永远在事后处理攻击’的怪圈，更好地防御明天将要发生的攻击。”

“建立安全系统有助于缓解 IT 管理人员面临的安全技能差距。通过部署简单易用的工具，使其在整个企业中相互协调，企业可以提高安全性，节省时间和成本。”

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，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

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，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（APT）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“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