简译版

“网络杀伤链”的转变

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	The Cyber Kill Chain Gets A Makeover		
原文作者	Kelly Sheridan	**原文发布日期**	2018 年 9 月 25 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	http://www.darkreading.com/threat-intelligence/the-cyber-kill-chain-gets-a-makeover/d/d-id/1332892		
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。		

“网络杀伤链”的转变

Kelly Sheridan

2018 年 9 月 25 日

一份新报告显示，随着犯罪分子寻求更快的方式来发起针对性攻击，传统的“网络杀伤链”的前五个阶段已经合并。

根据《2018 年重要发现报告》，Alert Logic 公司的研究人员审查了 2017 年 4 月 1 日至 2018 年 6 月 30 日期间的 254,274 起安全事件，与这些安全事件相关的 720 万次活动，以及 12 亿次异常情况。他们有五个重要的发现，其中最重要的是,不同类型的网络攻击正在转变其传统的（七阶段）杀伤链模式。

他们报告称，自 2011 年以来，典型的网络杀伤链包括七个阶段：侦察（收集凭证、电子邮件地址等），武器构建（使用漏洞利用代码和后门制作可发送的载荷），载荷投递，漏洞利用（在目标系统上执行漏洞利用代码），恶意软件安装，命令与控制（C&C），目标达成。

在上述模型中，每个阶段都有对应的中断和遏制方法。在越早的阶段处理掉威胁，威胁造成损害的可能性就越小。公司可以在侦察阶段检测到攻击者，拒绝攻击者访问数据，阻止数据发送给攻击者，反击 C&C，以及进行网络分割。

Alert Logic 公司首席威胁研究员马特·唐宁（Matt Downing）解释说，传统的攻击方法是典型的“高级持续性威胁”（APT）攻击，在 21 世纪 10 年代中后期的网络犯罪中很常见。

“这七个阶段构成了网络杀伤链。”他说。“攻击者对你感兴趣，是因为你拥有有价值的信息或者有价值的身份。他们首先进行侦察以找出你的攻击面……这是典型的针对性攻击场景。”

根据在侦察阶段收集的信息，攻击者会将受害者的漏洞与他们的漏洞利用代码相匹配，然后利用这些漏洞攻击受害者。

研究人员发现，攻击者已经修改了这个杀伤链，将前五个阶段合并，加快了识别存在漏洞的系统和发动攻击的过程。当攻击者利用预定义的、武器化的工具包攻击目标时，侦察、武器构建、载荷投递、漏洞利用和恶意软件安装这五个阶段就合并了。研究人员报告称，88%的攻击都采用了这种合并的杀伤链。

这种杀伤链的一个重要用例是挖矿劫持（cryptojacking）。研究人员发现，许多攻击采用这种杀伤链的原因正是挖矿劫持。大多数（88%）WebLogic 攻击都是挖矿劫持尝试，虽然这类网络犯罪不会窃取数据或劫持系统，但是能够说明目标系统容易受到其他恶意软件的攻击。

“在挖矿劫持中，互联网上的每一台主机都是有价值的。”唐宁说。拥有挖矿软件的攻击者不需要进行侦察，他们可以简单地发送武器化的载荷，然后载荷就可以按预定顺序执行相关活动了。勒索软件与此类似；但是，有几个因素增加了挖矿劫持的吸引力。

许多人认为挖矿是一种良性的活动。“这些人的道德标准比较低，”Alert Logic 公司产品营销总监克里斯丁·迈耶斯（Christine Meyers）指出。“他们认为这种活动是无害的，而勒索软件则是有害的。”

唐宁说，从操作上看，挖矿劫持很容易实现。从道德上看，它“有点模棱两可”。但是，对于出于经济动机、想要挖掘数字货币的网络犯罪分子来说，挖矿劫持的吸引力越来越大。

在更广泛的层面上，研究人员发现，自动化攻击和“广撒网”（spray and pray）攻击不断增加。各行业的 Web 应用程序仍然是主要的攻击媒介，包括零售和酒店（85%）、非营利组织（82%）、媒体和娱乐（80%）、信息技术和服务（77%）、教育（74%）和金融服务（71%）。

为了降低风险，研究人员建议回归基本的安全措施。漏洞扫描，尤其是针对低级别漏洞的扫描，对于了解攻击者是如何轻松访问环境的至关重要。“这是一个基本的安全问题，”唐宁说，并指出“了解漏洞和打补丁”是防御这种新型杀伤链的关键。

迈耶斯建议定期评估安全状况——而且频率要高一些。她说：“这不是一劳永逸的事儿，你需要不断地评估风险。”

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，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、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有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

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厂商、IT 厂商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、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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，为捍卫国家主权、安全和发展利益提供了有力支撑。

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的发言代表，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*