

光打补丁还不够，机构还需采取“零信任”方法

非官方中文译文·安天技术公益翻译组 译注

简译版

| 文档信息 | | | |
|--------|--|--------|-----------------|
| 原文名称 | Patching Not Enough; Organizations Must Adopt Zero-Trust Practices | | |
| 原文作者 | Kevin Townsend | 原文发布日期 | 2018 年 9 月 19 日 |
| 作者简介 | Kevin Townsend 是 SecurityWeek 的高级作家。 | | |
| 原文发布单位 | SecurityWeek | | |
| 原文出处 | https://www.securityweek.com/patching-not-enough-organizations-must-adopt-zero-trust-practices-report | | |
| 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.antivy.cn 安天公益翻译板块 | | |
| 免责声明 | <ul style="list-style-type: none"> 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。 | | |

光打补丁还不够，机构还需采取“零信任”方法

Kevin Townsend

2018 年 9 月 19 日

黑客可以通过社会工程手段获得网络访问权限，然后等待新的零日漏洞出现，利用它来提升权限。

在 2017 年黑帽大会上，安全公司 Thycotic 对 250 名黑客进行了调查，以了解他们在入侵网络的过程中遇到过哪些困难以及哪些是容易攻击得手的。在今年的黑帽大会上，该公司对 300 名自认为是黑客的受访者进行了类似的调查。

“今年，” Thycotic 公司首席安全科学家约瑟夫·卡森 (Joseph Carson) 告诉《安全周刊》 (SecurityWeek)，“我们希望能够更好地了解目前存在的黑客类型，以及他们执行黑客行动的动机。”

根据受访者的自我定位，黑客可以分为三类：白帽 (70%)，灰帽 (30%) 和黑帽 (5%) (译者注：三个括号中的百分比原文如此)。“白帽”遵守法律规范——他们将自己的技能和知识用于良好的目的。“灰帽”也遵守法律规范，但他们承认有时会越界。”卡森说，“他们的动机也是让社区受益；但承认他们的一些做法可能是违法的。”

“灰帽”通常是独立研究人员，他们的贡献往往不为人所知，因为“他们倾向于匿名报告他们的发现”，卡森说。

第三种是“黑帽”——他们为了非法目的和谋取私利而执行黑客行动。只有 5% 的受访者承认自己是黑帽，但他们都不是专门从事网络犯罪活动的。执法机构会一直监视黑帽黑客；对“未就业的”黑帽尤其关注。

这 5% 的黑帽很可能有合法的工作，他们很可能是代表雇主参加黑帽大会的。这就证实了今年夏天 Malwarebytes 公司的调查结果——很多公司都有那么一到两名正式员工下班后，会从事“黑帽”活动。

“我们想要研究的另一个问题是，”卡森说，“及时更新软件是否能够防御黑客攻击。”具体来说，Thycotic 公司想要知道当前的操作系统是否容易受到攻击，于是问了这样一个问题，“在过去的 1 年里，你攻破的最强大的操作系统是什么？”

“答案是 Windows 10，这令人非常惊讶。”卡森说，“虽然 Windows 10 是微软推出的最新、最安全的操作系统，但是黑客仍然可以轻松攻破。在被攻破的操作系统中，Windows 8 和 10 超过了三分之一。这违背了一个被普遍接受的观点——使用最新的、完全打补丁的操作系统可以保证安全。而现在，我们知道这样是不足以保证安全的。”

受访者最常使用的攻击方法（56.03%）是社会工程手段，这比使用零日漏洞更容易，也更便宜。“受访者证实，50%的漏洞源于口令重用，即员工重复使用已经在其他数据泄露事件中暴露的口令，这使得黑客能够轻松地进入网络。”报告指出。

很明显，很多用户仍然不了解其口令的弱点。“强口令不仅仅是很多杂乱字符的堆叠，”卡森说，“它必须具备三个特征：复杂、独特、未在其他数据泄露事件中暴露过。”

“我们发现，通过社会工程手段，黑客并不能获得高级访问权限和完全的网络控制。他们获得初步的访问权限后，会等待新的零日漏洞出现，然后利用它来提升权限。”卡森说。

卡森指出，几周前就有这样一个 Windows 10 零日漏洞被披露了。“这很可能意味着，在过去几周内非特权帐户被攻破的许多公司，现在面临着严重的攻击风险。通过社会工程手段，攻击者一只脚已经踏入公司，然后他们等待时机，当出现他们可以轻松利用的配置错误或新漏洞时，他们就能升级攻击了。”

基于这两项调查结果——打补丁并不能阻止黑客攻击，大多数黑客攻击利用社会工程手段，卡森给出了他的结论：机构需要采取“零信任”方法。“我们从去年的研究中了解到，最低权限和多因子身份验证方法能够增加黑客的攻击难度。”卡森说。

“今年，我们了解到，尽管这两种方法是有效的，但仍有 75% 的公司还未采用。”零信任方法是指，我们假设帐户已被攻破，然后采用多因子身份验证进行证实或证伪。这种方法适用于从互联网到公司网络的连接，以及从公司网络的一个网段到另一个网段的连接。

“综合采用最低权限和零信任方法将会增加黑客的攻击难度，他们很可能会放弃攻击采取这些方法的公司，然后转向更容易攻击的目标。”卡森说。为了达到攻击整个网络的目的，这些黑客不得不一个一个地攻破网络中各个机器及其帐户，而不能再像以前那样采用社会工程手段攻破非特权帐户，然后利用一个零日漏洞就能打穿整个网络。

“每当犯罪分子在被攻击网络中寻找下一个目标时，他们都会再次面临挑战，必须使用多种更复杂的方法来维持其攻击。”卡森说，“综合采用最低权限和零信任原则并不能 100%

地保证安全，但能够有效遏制日常的黑客攻击。”

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>