简译版

99%的网络攻击需要受害者的帮忙

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	More Than 99% of Cyberattacks Need Victims' Help		
原文作者	Kelly Sheridan	原文发布日期	2019 年 9 月 9 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/cloud/more-than-99--of-cyberattacks-need-victims-help/d/d-id/1335769		
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。		

99%的网络攻击需要受害者的帮忙

Kelly Sheridan

2019 年 9 月 9 日

研究显示，大多数犯罪分子利用受害者的好奇心和信任，诱骗他们点击、下载、安装、打开文件，以及汇款或发送信息。

大多数网络犯罪分子针对的是人，而不是基础设施：从 2018 年到 2019 年，超过 99%的电子邮件传播恶意软件需要受害者的交互，如点击链接、打开文档、接受安全警告等，才能有效地攻击组织。犯罪分子瞄准的不是各类系统，而是各类人员、人员的角色以及他们可以访问的数据。

以上数据来自 Proofpoint 的研究报告。18 个月来，Proofpoint 研究人员不断观察攻击趋势，并据此编制了《2019 年人为因素》报告。他们发现，随着攻击者从“抢劫式”勒索软件攻击转向精心设计的“企业电子邮件泄密”（BEC）和域名欺诈攻击，针对企业的社会工程活动越来越复杂和普遍了。

“我们发现，绝大多数威胁都依赖于受害者的某种交互。”Proofpoint 威胁情报负责人克里斯·道森（Chris Dawson）说。“我们还发现，硬件或软件漏洞的使用激增，但这些漏洞最终还是会被嵌入到恶意文档中。”即使攻击者利用漏洞和宏，也需要受害者点击链接、打开文档、接受安全警告或完成其他操作。

Proofpoint 报告指出，2018 年，在所有网络钓鱼活动中，电子邮件凭证窃取占了近 25%。而在 2019 年，凭证窃取仍然是一个重点领域，且攻击者转向 Microsoft Office 365 网络钓鱼活动和假冒攻击。云存储、DocuSign 和 Microsoft 云服务网络钓鱼是今年最热门的网络钓鱼诱饵；而在 2018 年，最热门的诱饵是“Brain Food”僵尸网络，该僵尸网络传播与饮食相关的垃圾邮件，旨在窃取受害者的信用卡数据。

道森说，攻击者知道公司正在迁移到云端。而且他们也知道，如果员工在邮件中看到熟悉的内容，即使他们不认识发件人，也会点击这些内容。员工习惯于收到 Office 365 和 Dropbox 链接；通常会不假思索地点击这些链接。

假冒电子邮件的主题正在从“请求”类转向“付款”或“紧急”类。邮件的主题随季节

（2018 年末至 2019 年初，“工资和税收报表”[W-2]相关的攻击很热门）和行业而异。例如，教育行业收到大量的“请求”和“问候”类邮件，而工程公司则通常收到“紧急”和“请求”类邮件。为了跟上业务流程，大多数假冒邮件都会在周一发送，快到周末时渐渐偃旗息鼓。

邮件中有什么内容

与传播勒索软件的大规模攻击活动不同，现在的攻击者倾向于发动精心设计的、更小规模的攻击。他们希望，其恶意软件能够在不触发任何告警的情况下，驻留在受害者的计算机中数天甚至数月。道森解释说，很多攻击者已经开始传播复杂的后门来收集数据了。

“这些措施都是为了驻留在受害者的机器上，以便长期收集数据，方便之后的攻击活动。”他说。安全行业发现了这样一种勒索软件攻击模式：在企业遭到感染的很久之前，企业的网络就已经被攻破了。

我们以 Carbanak 攻击组织为例，该组织使用诱饵和精心制作的文件附件来传播多种恶意软件。在 2018 年的一起攻击活动中，攻击者发送了一份包含附件的电子邮件，声称附件已被加密。一旦受害者点击了如何“解密”附件的说明，就会启动宏并安装 Griffon 后门，而该后门经常被 Carbanak 组织用于攻击活动。

谁会收到钓鱼邮件？

现在的攻击活动越来越有针对性；但是，不同攻击者的攻击目标各有不同，他们的攻击活动也有很大的差异。

“最容易遭受攻击的人群是身份信息公开可见的那些”，道森说。这通常不包括高管——因为高管通常会隐藏他们的在线身份；但是包括销售人员、营销团队和人力资源专家，这些人员中很多都公开了邮箱地址。在“非常易受攻击的人员”（VAP）中，有 36%的相关身份信息可以通过公司网站、社交媒体或其他网站找到。研究人员指出，相比之下，只有 7%的高管的邮箱地址可以在网上找到。

机会犯罪，或发送电子邮件到别名地址（如 HR[@]company[.]com）的攻击很常见。“保护共享账户是非常困难的，”道森在谈到别名电子邮件账户时表示。

如果攻击者使用五个以上的假冒身份，攻击企业内五个以上的人员，则其成功率会大大

提高。他补充说，从一对一攻击，到一对多攻击，再到多对多攻击，“我们发现这个说法很有道理”。攻击者可以假冒几位高管的身份，向员工发送恶意文件；或者他们可以利用一组假冒身份向人力资源部门询问 W-2 数据。

道森说：“利用这种技术，攻击者大获成功。因此，他们大大增加了冒用的身份数量和攻击的目标人数。”

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（如 APT 组织）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