简译版

企业需关注的四类社会工程威胁

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	4 Social Engineering Threats to Keep an Eye on — and How to Stop Them		
原文作者	Jasmine Henry	**原文发布日期**	2019 年 6 月 21 日
作者简介	Jasmine Henry 是一位评论家和自由撰稿人，专门研究分析、信息安全和其他新兴技术趋势。https://securityintelligence.com/author/jasmine-henry/		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/4-social-engineering-threats-to-keep-an-eye-on-and-how-to-stop-them/		
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。		

企业需关注的四类社会工程威胁

Jasmine Henry

2019 年 6 月 21 日

由于成功率低，攻击者对大规模网络钓鱼活动感到厌倦，他们转向了更高级而有效的伎俩。如果说未来的网络安全领域有什么可以确定的，那就是，网络犯罪分子总是妄图获利。他们的战术、技术和规程（TTP）将继续进化，以实现最大的攻击回报。社会工程手段仍然是网络犯罪分子最常用的 TTP，无论是单独使用，还是与其他攻击方法结合使用。

社会工程被定义为对目标进行心理操纵，诱骗他们执行某种行为——最常见的是诱骗受害者主动提供登录凭证、主动提交敏感数据或主动向对方转账。采用社会工程最常用的手段是网络钓鱼，但是，网络钓鱼并非首席信息安全官（CISO）需要担心的唯一攻击手段。最近的网络安全趋势表明，与其他 TTP 相比，高度针对性的社会工程攻击正在增长。企业需了解以下四类社会工程威胁，以便做好防御。

企业需关注的四类社会工程威胁

网络钓鱼邮件仍然是困扰企业的重要威胁，但并非唯一的威胁。根据 PhishLabs 最近的一项研究，越来越多的攻击者开始以“软件即服务”（SaaS）和邮件中的财务凭证为目标，而包含恶意软件的邮件数量则越来越少了。企业比以往任何时候都更有可能遭受精心策划的高级社会工程攻击，这些攻击针对企业内最无防备的人员，包括新员工、高管，掌握敏感数据或资金控制权的人员等。

1. 企业电子邮件泄密

根据 2019 年 IBM《X-Force 威胁情报指数报告》，在 X-Force 事件响应和情报服务团队（IRIS）分析的攻击中，有 29%涉及网络钓鱼邮件；45%涉及企业电子邮件泄密（BEC）或高度针对性诈骗（攻击个人邮件账户以执行未经授权的转账）。

互联网犯罪投诉中心（IC3）将 BEC 描述为一项价值 1200 万美元的诈骗，并指出 BEC 攻击不受行业或企业规模的限制。如果企业缺乏强大的口令监管实践或行为分析方案，无法检测异常模式，对于网络犯罪分子来说，BEC 就是一种既简单又高效的攻击方法。

2. 勒索

勒索攻击正在增加。根据 Digital Shadows 最近的一项研究，此类攻击也非常成功。攻击者从其他攻击中窃取凭证，然后利用这些凭证威胁攻击目标。“性勒索”（sextortion）是一种常见的攻击模式。在此类攻击中，攻击者声称掌握了敏感资料，威胁首席执行官或其他高管支付赎金；如果目标不支付赎金，他们就会发布这些资料。

从最近的趋势来看，攻击者不再局限于直接向受害者索要赎金，他们开始通过众筹模式为敏感内容创收。如果敏感内容是企业知识产权，这就是一种非常有利可图的方式了。一些最知名的勒索活动源于 Digital Shadows 所称的“服务器覆盖五大洲的全球性组织”。

“在任职 Digital Shadows 的三年中，我们总是能看到网络犯罪地下市场和合法企业的相似之处，”Digital Shadows 首席信息安全官里克·霍兰德（Rick Holland）在接受 MIS 培训学院采访时表示，“这让犯罪分子越来越得心应手。”

3. 冒充

根据威瑞森《2018 年数据泄露调查报告》，虽然“冒充”（pretexting）只占社会工程攻击的一小部分，但是其数量正在迅速增长——从 2017 年的 60 起增加到 2018 年的 170 起，几乎翻了两番。在这种高度针对性的社会工程攻击中，攻击者冒充同事或供应商与内部人员对话。他们逐渐获得足够的信任，进而访问内部系统、敏感数据或汇款信息。这种新威胁会导致防御技术的失效。

4. 鲸钓和网络交友诈骗

去年，一位澳大利亚富商遭遇“网络交友”（catfish）诈骗，损失了 100 万美元，这种诈骗将“鲸钓”（whaling）、网络交友或冒充技术结合起来。这位 87 岁富商的助理收到了一封邮件，发件人声称是富商的女友南希·琼斯（Nancy Jones）。这位“南希·琼斯”要求助理转账 100 万美元，助理照做了。

与每季度的数百万封钓鱼邮件相比，针对大公司的鲸钓攻击数量要少得多，但是此类攻击的难度更大。据 InfoSec Institute 估计，针对高管和其他掌握财务控制权的人员的电子邮件攻击，已经导致美国公司损失了至少 18 亿美元。

应对不断进化的社会工程威胁

安全意识培训仍然是对抗大部分社会工程攻击的关键，但是，企业要关注的不仅是基本的安全意识。如今，一些最有利可图的攻击采用前所未见的犯罪方法。毫无防备的内部人员是企业最薄弱的环节，因此，企业需要全面的网络弹性计划，包括模拟训练和强大的弹性恢复能力计划。

攻击者可能会利用员工和企业在社交媒体上共享的信息，来执行社会工程攻击。这意味着，企业不仅要部署基础的安全措施，例如强大的用户监管和培训，还要寻求最先进的网络弹性解决方案，来对抗社会工程威胁。

行为分析是另一个重要保护措施，可以防止 BEC、冒充，以及旧形式的社会工程攻击（如针对云凭证的钓鱼邮件）造成损害。随着网络犯罪分子的不断进化，企业应对包含认知功能的强大安全生态系统进行适当投资，以便为安全团队赋能，帮助他们在高级威胁造成损害（如转账）之前加以检测和阻止。

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，已连续五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