精译版

金融服务行业成为网络犯罪分子的头号目标

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	Financial Services Sector the #1 Target of Cybercriminals		
原文作者	Kelly Sheridan	原文发布日期	2017 年 5 月 1 日
作者简介	Kelly Sheridan 是 Dark Reading 的副编辑。http://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/endpoint/financial-services-sector-the--1-target-of-cybercriminals/d/d-id/1328775?		
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。		

金融服务行业成为网络犯罪分子的头号目标

Kelly Sheridan

2017 年 5 月 1 日

2016 年最常被攻击的行业是金融服务行业，其遭受的攻击同比增长了 29%。

网络犯罪分子通常追着钱走，越来越多的攻击者开始瞄准金融服务机构。在 2016 年，数据泄露事件，漏洞数量，通过物联网执行的 DDoS 攻击都出现了增加。

金融服务行业已经成为犯罪分子的头号目标，遭受的攻击比其他行业高出 65%。该行业遭受的攻击同比增长了 29%，从 2015 年的 1310 起增加到 2016 年的 1684 起。

威瑞森（Verizon）高级网络工程师戴夫·高兰德（Dave Hylender）说："攻击者的主要目标是赚钱，这是大多数攻击的驱动力。"

金融服务机构削减了网络犯罪分子与资金之间的中间步骤。黑客们也可以通过攻击医疗机构获得大量数据，但是他们必须采取额外的步骤才能将这些数据变现并开立诈骗账户。

他解释道，如果能够在银行系统中植入恶意软件，就可以更容易地获取资金。威胁源可以执行一系列非法活动，如获取用户名和密码、提取资金、创建假借记卡等等。

IBM X-Force 威胁研究员米歇尔·阿尔瓦雷斯（Michelle Alvarez）指出："如果能够成功感染金融服务机构，攻击者就能获得可观的利润。攻击医疗和零售机构也能够获利，但是攻击金融服务机构能够省去许多中间环节。"

在 2016 年，金融服务机构被攻击次数猛增 937%，达到 2 亿次。高兰德指出，网络犯罪背后有很多动机，除了经济利益之外，威胁源的目标也可能是知识产权和商业机密。

攻击从何而来呢？对金融服务机构来说，内部人员造成的攻击占 58%，而外部攻击只占 42%，但是大多数内部人员并不知道他们造成了伤害。

超过一半（53%）的内部攻击源自"疏忽人员"，他们在无意间遭到了钓鱼攻击，或者来自其他连网系统的内部攻击。报告指出，在"疏忽人员"造成的威胁方面，金融服务机构面临的威胁最为严重。

高兰德说，拒绝服务攻击和网络攻击也是很严重的问题。威瑞森上周发布的《2017 年数据泄露调查报告》显示，与信息服务公司相比，金融和保险公司遭受的网络应用程序攻击数量高出 5 倍（364 起）。

他继续说，一些企业能够承受将其网站下线一天。但是金融服务机构不能，尤其是开通了重要网络业务的大银行。三至四年前，针对银行的网络应用程序攻击开始增加，目前仍然是该行业的最大威胁。

“如果你是金融服务机构，那么你需要保护你的网络业务。”高兰德说，“你的大部分资产和业务就在网络上，你需要对其进行控制。”

研究人员还发现，用于攻击商业银行账户的恶意软件数量有所增加。商业恶意软件重出江湖了，IBM 对经常遭到 SQL 注入和 shell 命令注入攻击的客户进行了监控。

阿尔瓦雷斯说：“从 2014 年中期开始，这一趋势就开始了。一些恶意软件，包括 Dyre，Dridex，GozNym 和 TrickBot，开始瞄准商业银行服务。”

她建议各公司评估其网络安全“免疫系统”，找出自己的漏洞，并考虑以下问题：你的终端安全吗？你对当前的威胁有足够的了解吗？你具有适当的身份管理解决方案吗？

高兰德建议密切关注员工的活动，确保每个人只能获得他们真正需要的信息。他说，企业还应该为所有网络应用程序实施多因素身份验证。

阿尔瓦雷斯补充说，员工培训也很重要。企业应该教员工识别可疑的电子邮件，这样企业就可以避免成为网络钓鱼诈骗的受害者，并降低“疏忽人员”造成的攻击风险。