简译版

银行木马 CamuBot 通过社会工程手段传播

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	Attackers Employ Social Engineering to Distribute New Banking Trojan		
原文作者	Jai Vijayan	**原文发布日期**	2018 年 9 月 4 日
作者简介	Jai Vijayan 是一位自由作家。https://www.darkreading.com/author-bio.asp?author_id=1912		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/attacks-breaches/attackers-employ-social-engineering-to-distribute-new-banking-trojan/d/d-id/1332731		
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。		

银行木马 CamuBot 通过社会工程手段传播

Jai Vijayan

2018 年 9 月 4 日

CamuBot 银行木马伪装成必需的安全模块，攻击巴西几家主要银行的企业客户。

身份未明的攻击者开始使用一种新的、复杂的银行木马“CamuBot”，从巴西几家主要银行的企业客户手里窃取资金。攻击者经常将巴西当作测试金融恶意软件的试验场，之后便会在全球范围内传播这些恶意软件。

IBM X-Force 公司安全研究人员一直在追踪 CamuBot，认为它综合使用三种攻击方式：高度定向的社会工程学手段、恶意代码以及设备劫持。攻击者将 CamuBot 伪装为必需的安全模块（包含银行的标识和品牌图标），诱骗目标将它下载到系统上。

银行经常将指纹识别器、U 盾和其他第三方安全外围设备，用作验证用户身份的附加机制。令人不安的是，CamuBot 能够劫持这些设备的驱动程序。

IBM Security 公司安全顾问利莫·凯瑟姆（Limor Kessem）表示，CamuBot 的部署和使用不同于其他银行木马。“首先，它的传播非常有针对性。攻击者会给潜在的受害者打电话，诱骗他们访问被感染的网页，从而将恶意软件下载到他们的设备中。”她说。

攻击者的目标通常是：最有可能持有公司银行账户凭证的人员。他们伪装成银行员工，要求受害者浏览某个网页，以检查其公司的银行安全模块是否已经升级为最新版为幌子。检查结果伪装为“未升级为最新版”，然后他们就会欺骗目标下载安全模块的“最新”版本。

如果受害者下载“安全模块”，前台就会显示一个假的应用程序，而后台则会秘密安装 CamuBot，并与其 C&C 服务器建立连接。然后，受害者被重定向到银行的在线门户网站，然后被提示输入登录凭证，攻击者则会迅速捕获这些凭证。

“其次，CamuBot 不会试图隐藏安装进程。”凯瑟姆说。“相反，通过伪装成安全模块，CamuBot 在设备上的执行是由被骗的受害者促成的。”

在需要强身份验证的情况下，CamuBot 会安装一个驱动程序。通过该驱动程序，他们能够远程共享连接到受害者计算机的任何基于硬件的身份验证设备。攻击者设法让受害者同意共享设备，这样他们就能拦截银行生成的、用于验证用户身份的一次性验证码。IBM 表

示，有些设备支持生物识别身份验证，如果用户授权进行远程共享，可能会破坏生物识别身份验证系统。

“操纵 CamuBot 的网络犯罪分子窃取受害者的账户访问凭证，然后欺骗他们生成一次性验证码。”凯瑟姆指出，“通过这些手段，他们的假会话就能够通过身份验证，成功地从受害者账户中划走资金。”

由于 CamuBot 的传播非常有针对性，并且一次只能攻击一家受害企业，因此与其他银行木马相比，CamuBot 的攻击数量比较有限。

凯瑟姆指出，CamuBot 攻击再一次为企业敲响警钟——“人”往往是安全链中最薄弱的环节。“企业的出路是，采取能够有效防止诈骗的安全控制措施。而这会导致，网络犯罪分子日益转向社会工程手段。”她说。

事实上，一些最严重的损失源于企业邮件攻击（BEC）诈骗，犯罪分子利用社会工程手段，诱骗公司员工将资金汇入他们的账户。今年初，美国联邦调查局曾警告说：BEC 诈骗正在急剧增加，给全国各地的公司造成了巨额经济损失。

“有组织的网络犯罪团伙，如 Dridex、TrickBot 和 QakBot，将社会工程手段和恶意软件功能组合起来欺骗目标。”凯瑟姆说，“现在，CamuBot 也走上了这条路。”

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，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，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，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。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，提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动，进行了深度的解析，对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上，安天创始人、首席技术架构师作为网络安全领域的发言代表，向习总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了位于哈尔滨科技创新城的安天公司，对安天负责人说，“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*