安天发布《Trickbot 银行木马变种分析报告》

近日，安天 CERT（安全研究与应急处理中心）在梳理网络安全事件时发现一种名为 Trickbot 的银行木马变种开始活跃。在 2018 年 11 月，Trickbot 曾出现过一个带有密码管理器模块的变种，可以获取多个应用程序和浏览器的访问权限。在 2019 年 1 月，一个新版本的 Trickbot 变种出现了，它拥有更强大的密码及证书抓取功能。

该 Trickbot 木马通过一封伪造的税收通知邮件进行传播，邮件中包含一个启用宏的 Excel 附件，一旦用户打开该文件，恶意宏就会下载并运行 Trickbot 木马。这次的木马变种与 2018 年 11 月的版本比较相似，不同之处是它针对 Virtual Network Computing (VNC), PuTTY, Remote Desktop Protocol (RDP) 这三个平台增加了新功能。通过抓取它们的证书，攻击者将可以远程登录并控制受害者的计算机。为了抓取 VNC 的凭证信息，密码管理模块在 "%APPDATA%\Microsoft\Windows\Recent", "%USERPROFILE%\Documents", "%USERPROFILE%\Downloads" 目录下搜索 "*.vnc.lnk" 后缀的文件，从中读取目标机器的主机名、端口、代理设置等信息，随后访问注册表项 "Software\SimonTatham\Putty\Sessions"，检索可用于登录的 PuTTY 证书，最后使用 CredEnumerateA 这个 API 函数获取 RDP 的凭证信息。最终，模块会从名为 "dpost" 的配置文件中读取一个 C&C 服务器列表，将窃取到的信息通过 HTTP POST 请求发向这些服务器。

安天 CERT 提醒广大政企客户，要提高网络安全意识，在日常工作中要及时进行系统更新和漏洞修复，不要随意下载非正版的应用软件、非官方游戏、注册机等。收发邮件时要确认收发来源是否可靠，更加不要随意点击或者复制邮件中的网址，不要轻易下载来源不明的附件，发现网络异常要提高警惕并及时采取应对措施，养成及时更新操作系统和软件应用的好习惯。确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，而是将运行远程桌面的计算机放在 VPN 之后，只有使用 VPN 才能访问它们。同时也要做好文件的备份，以防止勒索软件加密重要文件后无法恢复。目前，安天追影产品已经实现了对该类恶意代码的检出。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 BD 静态分析鉴定器、YARA 自定义鉴定器、文件来源信息鉴定器、数字证书鉴定器、文件元数据鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、动态（Win7 x86）鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	374ef83de2b254e4970b830bb93a1dd79955945d24b824a0b35636e14355fe05
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	456 KB
MD5	B855B1B7B59668AD991CF0501E4FF4CB
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Mansabo
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=B855B1B7B59668AD991CF0501E4FF4CB

◆ 运行环境

操作系统	内置软件
WinXP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆ 危险行为

行为描述	危险等级
延时	★★★
dll 劫持	★★★★★

◆ 常见行为

获取系统信息（处理器版本、处理器类型等）	★
获取主机内存信息	★★
壳行为填充导入表	★★
复制自身	★★
创建挂起进程	★★
获取系统版本	★★
获取计算机名	★
获取驱动器类型	★
.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 03 月 04 日 (总第 173 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

政协委员肖新光：下好网络安全整体一盘棋

编者按：本文为全国政协委员、安天首席架构师肖新光接受《黑龙江日报》采访的全文。本次刊登对原文中表述不准确之处进行了修订。

当前，网络空间已经成为各国政治、军事、经济等领域斗争的首发“战场”。我省全国政协委员、安天首席架构师肖新光是网络安全领域的一名“老兵”。在安天，他和几位“老兵”带领更多的“新兵”，在我国安全产业的“丛林”中穿行。肖新光的目光敏锐而坚定——国家网络安全一刻也不容松懈。

在哈尔滨安天科技集团股份有限公司，从一楼走到二楼，企业的每一项技术突破或通过大屏幕生动呈现，或通过图表准确表达，甚至通过漫画活灵活现。安天不仅为高安全需求客户提供整体的安全解决方案，其产品与服务还为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航和南极科考等提供了安全保障。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 30 万台网络设备和网络安全设备、超过 15 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。

作为安天团队的创始人，肖新光对于网络安全有着更为深刻的思考。他在接受记者采访时表示：“去年我提出了关于‘在网络空间安全领域进行针对性投入和布局应对重大地缘安全风险’的提案，主要是涉及到对安全风险的认识和相应的投入和政策问题。去年的提案，相关部门做出了及时解答和沟通。”

肖新光说，我今年的提案和去年有一定的延续性。我们国家在网络安全的单点技术、单点产品方面已经有了比较好的储备和相应积累，这些产品能够形成相应的单点防御能力。但目前来看，在重要信息系统和关键信息基础设施当中，这些单点能力还没有形成体系性的能力，还存在着一些基础的缺漏和短板情况。在这种情况下，如果只是靠市场的供需关系形成自发驱动，就会加重只顾单点能力建设而不顾体系性建设的倾向，最终导致投入无法有效转化为整体防御能力。

肖新光表示，今年我们希望国家相关主管部门出台一套按照系统工程思维来指导网络安全建设的指南，在信息化的规划、建设、运维的全生命周期过程中，能够实现网络安全与信息化的深度结合与全面覆盖。在这样的过程中，有效地推动网络安全基础能力的夯实，推动能力建设的叠加演进，使相应的安全投入增量能够有效地转化为网络安全防御能力的提升增强，改变我们当前防护不足和防御缺失的局面。

“国家的网信工作是整体一盘棋”，肖新光说，对信息安全来说，决策层和舆论层的引导尤为重要，我们需要一个全景的信息安全视野。而对于从业人员来说，同样要有一个宏观的视野，有一个整体的思想才不至于迷失。当我们看到树叶脉络的同时，也要看到树木，乃至整个森林。

PDF 签名漏洞允许攻击者进行未经授权更改

研究人员发现多个 PDF 查看器和在线验证服务包含漏洞，这些漏洞可被利用来对签名的 PDF 文档进行未经授权的更改，而不会使其数字签名无效。专家进行了三种 PDF 签名攻击试验：通用签名伪造（USF）、增量保存攻击（ISA）和签名包装攻击（SWA），证明几乎所有 PDF 查看器和在线验证服务都容易受到攻击。该漏洞影响 Adobe Reader、Foxit Reader、LibreOffice、Nitro Reader、PDF-XChange 和 Soda PDF 等流行软件，验证服务包括 DocuSign、eTR 验证服务、DSS 演示 WebApp、Evotrust 和 VEP.si。目前所有提供 PDF 查看应用程序的公司都已发布安全补丁来解决这个问题，而一些在线服务尚未解决这些问题。

（来源：https://securityaffairs.co/wordpress/81696/hacking/digital-signature-verification-attacks.html）

数百万公用事业员工密码以纯文本形式存储

研究人员发现美国亚特兰大公司 SEDC 设计的网站的一个常见缺陷—以纯文本形式存储用户密码。研究人员表示一旦网站被破坏，攻击者可以通过转储密码数据库，展开一系列的攻击。研究人员在 80 多家公用事业公司使用 SEDC 的设计网站中发现该缺陷，约为 1500 万左右的员工提供服务。因 SEDC 声称超过 250 家公用事业公司使用其软件，所以受影响的员工可能为目前所发现的数倍。

（来源：https://arstechnica.com/tech-policy/2019/02/plain-wrong-millions-of-utility-customers-passwords-stored-in-plain-text/）

每周安全事件

类 型	内 容
中文标题	新木马攻击形式使用广泛且快速变换的数据
英文标题	Fast-changing Trojan attack identified; masquerades as a paid invoice
作者及单位	Lorita Ba
内容概述	安全团队发现了一种传播广泛、快速变化的木马攻击模式，该模式会更加快速地关闭目标 URL。此次攻击活动中，使用各种不同的主题行、电子邮件内容、电子邮件地址、目标名称和目标 URL。攻击由三个不同的波段组成，每个波段对应一个不同的目标 URL。最初感染点是发送给公司员工的网络钓鱼电子邮件，其带有员工姓名，主题为收据、发票等。发件人电子邮件地址是受到破坏的合法账户，主要来自南美公司。邮件带有的链接自动下载 Word 模板，该文件包含木马。
链接地址	https://www.greathorn.com/fast-changing-trojan-attack-identified-masquerades-as-a-paid-nvoice/

每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码和漏洞值得关注

关注方面		名称与发现时间	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.DatactrlSpy.a[prv,exp,sys,rmt] 2019-02-25	该应用程序是间谍件，接收远程指令，运行后会上传用户联系人、通话记录、通话录音、社交应用聊天记录、位置信息、浏览器书签等隐私信息，私自发送短信、拨打电话、下载安装指定应用、修改手机设置，会造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.loaloveme.a[prv,spy] 2019-02-26	该应用程序运行后强制要求激活设备管理器，而后隐藏图标，监听用户手机短信，窃取用户短信、地理位置等信息，显示钓鱼界面诱导用户输入银行相关账号密码。造成用户隐私泄露和经济损失，建议立即卸载。（威胁等级中）
		Trojan/Android.BadCamera.a[exp,prv] 2019-02-27	该应用程序均伪装为相机相关应用，运行后隐藏图标，部分应用会将用户图片上传到指定的服务器，可能用于恶意的目的，同时诱导用户下载更新已获取处理过的图片，部分应用推送广告，利用钓鱼页面获取用户隐私信息，造成用户的隐私泄露和资费消耗，建议卸载。（威胁等级高）
	较为活跃的样本	RiskWare/Android.CSJapp.a[exp]	该应用程序是广告测试程序，运行后台获取广告内容，会造成用户流量消耗，建议不要使用。（威胁等级低）
		RiskWare/Android.locazilla.a[exp,rmt,rog]	该应用程序包含风险代码，运行后隐藏图标，联网获取未知数据，使用辅助功能，模拟点击操作用户界面，存在一定风险，请谨慎使用。（威胁等级中）
		G-Ware/Android.ismailkya.a[prv,rog]	该应用程序运行后隐藏图标，后台搜集用户手机固件信息，Facebook、Instagram 等安装信息，并通过邮件将信息上传。造成用户隐私泄露，建议不要使用。（威胁等级中）
		RiskWare/Android.clickoon.a[exp,rog]	该应用程序是一个在线刷量工具，运行后加载广告，下载广告进行刷量操作，存在一定风险，建议不要使用。（威胁等级低）
		Trojan/Android.bulgakovSpy.a[prv,rmt,spy]	该应用程序是一款间谍软件，伪装系统应用，运行后接收远程指令，窃取用户短信、联系人、通话记录、地理位置等隐私信息。造成用户隐私泄露，请立即卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 脚本引擎内存损坏漏洞（CVE-2019-0590）	脚本引擎在 Microsoft Edge 中处理内存中的对象时可能触发该漏洞。成功利用该漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理权限登录，攻击者便可以任意安装程序，查看、更改或删除数据。（威胁等级高）
	较为活跃样本	Trojan/Win32.Winsecsrv	此威胁是一种具有窃密行为的木马家族。该家族的样本在执行后会获取用户的信息，与远程的控制端通讯并接受后续的控制，控制端具有对用户机器的完全控制权。（威胁等级中）
		Trojan[Downloader]/JS.Shadraem	此威胁是一种基于 Javascript 脚本的、具有下载器行为的木马家族。该家族使用混淆过的 Javascript 编写，在执行后会启动一个下载进程来下载其它程序到用户的机器中执行。（威胁等级中）
		RiskWare[RiskTool]/Win32.Ocna	此威胁是一种风险软件家族。该家族的样本在执行后可能会对用户的计算机造成破坏，影响用户的正常使用。（威胁等级低）
		Trojan/Win32.Mokes	此威胁是一种具有后门行为和窃密行为的木马家族。该家族的样本在执行后会让远程的控制端取得用户设备的完全控制权限。该家族利用代码注入技术在内存中驻留，并且会在用户机器上收集信息并回传给控制端，造成泄密。（威胁等级高）
		RiskWare[Downloader]/Win32.4Shared	此威胁是一种有广告行为和下载行为的风险软件家族。该家族的样本在执行后会连接远程的服务器，下载广告并在用户的 PC 上弹出。该家族的样本具有多种签名形式和变种。（威胁等级低）

保护关键基础设施

Seema Haji / 文 安天技术公益翻译组 / 译

IT 和 OT 团队都应该能够快速访问和分析与其需求相关的所有数据。

要想保持关键基础设施（如电网、核设施、石油和天然气精炼厂、污水处理厂、制造厂等）的运行和安全，工业控制系统（ICS）是关键。事实上，全球生产和提供的商品和服务，无论是生产、运输还是运营方面的，很大一部分都依赖于某种形式的 ICS。在我们的生活中，这些 ICS 系统不可或缺，因此，我们有充分的理由关注它们的安全性。

我们的首要目标是实现“物理安全”（safety）——即，保护类似机场等关键基础设施不会给人类带来伤害、其自身运行的环境不遭到破坏或者抵御其他形式的威胁。除以上首要目标外，其他目标包括知识产权（IP）保护和服务可用性等。要实现这些目标，需要保持 ICS 系统的运行，维持强健的安全态势并优化资源使用。以下是我们需要关注的四大趋势。

智能运营技术将成为标配

廉价设备和传感器的爆炸式增长，以及可访问数据技术的发展，正在彻底改变工业领域。随着前瞻性企业找到利用“运营技术”（OT）数据的创新性方法，物联网（IoT）逐渐蔓延到制造业和运输业等工业环境。这种互联的网络可以自动执行繁琐的任务，改善工人的安全环境状况并释放更多的资源。

该趋势将移动技术引入了员工层。“自带设备”（BYOD）的普及导致了攻击面的扩大；与此类似，IoT 设备和传感器扩展到工业环境，在提高生产效率的同时也增加了风险。单纯提高工作效率，但是又不增加风险的情况很难存在。鉴于此，企业必须实现对其设备（这些设备是 IT 和 OT 堆栈的一部分）的可视化和控制。

机器学习驱动的预测性维护将成为主流

鉴于智能技术在工业环境的使用激增，

更多企业开始采用预测性措施来补充其防御工作。将更多的数据点与更好的数据处理方式 / 可视化相结合，企业就能优化维护周期和资源使用。随着运营的开展和进行，制造主管和运营经理都可以专注于网络安全，而不必经常担心成本和物理安全了。

维护和运营模式转变的核心是机器学习和人工智能——在即将发生事件时，它们不仅会发出告警。例如，基于机器学习构建的异常检测和告警触发将会越来越无缝链接，使运营经理能够专注于高优先级的问题和任务。企业不要错过这一飞跃。

针对制造商的工作条例和监管措施促进质量控制和安全保证

企业必须牢记监管和合规性，特别是在汽车和医疗等行业。由于更严格的合规要求不断出台，这些行业的制造变得更加复杂。企业必须跟踪和监控所有组件、制造设备及操作员操作的合规性。

云和工业 IoT 的爆炸式增长（新技术和流程的引入），可能会使企业的合规性变得更加困难。随着新工具、流程和培训的引入，在符合新标准和法规方面，新技术可能是一把双刃剑。意外必然会发生，因此企业要做好准备并采取严格的措施来保证质量和合规性。

OT 和 IT 融合

近年来，工业环境中的 OT 和 IT 系统日益融合。人机界面（HMI）通常用于向现场或工厂设备发送命令。OT 网络中的智能设备连接到 IT 基础设施，以实现更好、更快的数据驱动的决策。因此，网络分段策略已成为这些环境中的常见做法。但是，更多的集成，以及可视化和控制的缺乏，给 OT 带来了风险。攻击可以从 IT 或 OT 环境开始，然后进行横向移动。想象一下，如果连接到阀门、仪表或设备的 ICS 受到损害，会带来什么后果。

随着工业环境变得更加复杂，企业需要采用不受数据类型和数据源影响的技术。IT 和 OT 团队都应该能够快速访问和分析与其需求相关的所有数据。

简而言之，ICS 安全至关重要，企业需要不断完善其保护措施。IoT 将成为常态；智能技术将增强运营管理和执行；随着跨系统的互联变得更加普遍，IT 和 OT 堆栈将会融合。企业应做好准备，避免因工业系统受损而导致严重的后果。

原文名称	Got Critical Infrastructure? Then You Should Know How To Protect It
作者简介	Seema Haji。Seema Haji 是 Splunk 公司产品营销负责人，负责其物联网和业务分析解决方案。
原文信息	2019 年 2 月 20 日发布于 Security Week 原文地址 https://www.securityweek.com/got-critical-infrastructure-then-you-should-know-how-protect-it
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，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。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。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。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，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。