安天发布《InnfiRAT 远控木马分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个使用 .NET 编写的名为 InnfiRAT 的远控木马。InnfiRAT 最早在 2017 年被发现，主要通过钓鱼邮件进行传播，目的是窃取用户个人信息和加密货币钱包信息。

InnfiRAT 是一款具有反调试、反虚拟机和反沙箱检测的远控木马。该木马运行后，遍历进程判断是否存在 Process Hacker、Process Explorer 和 Process Monitor 进程，如果存在则退出。远控木马创建计划任务每天执行一次。InnfiRAT 木马包含 11 种控制指令，主要功能包括从指定 URL 下载文件、收集主机信息、获取进程路径、获取浏览器 Cookie 信息、窃取比特币和莱特币钱包、上传可能包含敏感信息的文本文件、获取进程列表、结束指定进程、获取屏幕截图、打开 CMD 以及清除浏览器 Cookie 信息等。

安天 CERT 提醒广大政企客户，应提高网络安全意识。在日常工作中及时进行系统更新和漏洞修复，不随意下载非正版的应用软件，注册机等。收发邮件时应确认收发来源是否可靠，不随意点击或者复制邮件中的网址，不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良好习惯。确保所有的计算机在使用远程桌面服务时避免使用弱口令，如果业务上无需使用远程桌面服务，建议将其关闭。

目前，安天追影产品已经实现了对该远控木马的鉴定；安天智甲已经实现了对该远控木马的查杀。

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、来源信息鉴定器、数字证书鉴定器、元数据信息鉴定器、聚类分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、字符串分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	755894e632485b30d1522058a63b830f4c4c245207141cad4a8b456acee487f5
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.03 MB
MD5	F992DD6DBE1E065DFF73A20E3D7B1EEF
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Razy
判定依据	BD 静态分析

完整报告地址：https://1.119.163.6/vue/details?hash=F992DD6DBE1E065DFF73A20E3D7B1EEF

◆ 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
删除自身	★★★★
通过 WMI 查询 CPU 信息	★★★
通过 WMI 查询 CPU 核数检测虚拟机	★★★★★

◆常见行为

行为描述	危险等级
加载运行时 DLL	★
打开自身进程文件	★
获取系统信息（处理器版本、处理器类型等）	★
获取系统版本	★
检测自身是否被调试	★★
镜像劫持	★★
获取计算机名	★
启动指定服务	★
DNS 请求	★
独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
设置调试器权限	★
.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 09 月 23 日 (总第 201 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天再次接受焦点访谈采访

中国网络空间安全协会副理事长、中国网络安全产业联盟理事长、安天集团负责人肖新光，在国家网络安全宣传周即将开启之际，接受了中央电视台焦点访谈栏目的采访，分享了如何应对高级威胁和关键信息基础设施防御能力建设的思考。

2019 年国家网络安全宣传周于 9 月 16 日正式启动，主题为“网络安全为人民，网络安全靠人民”。作为一个网络大国，我国的网络安全也成了一个大问题，层出不穷的病毒、防不胜防的黑客，盗取数据、破坏电脑，给个人带来麻烦，让企业遭受损失，也对国家安全构成了极大的威胁。“没有网络安全就没有国家安全”，习近平总书记的论断，为网络安全各项工作提供了根本遵循。党的十八大以来，在习近平总书记关于网络强国的重要思想指引下，网络安全保障能力和水平不断提升。

在近 20 年的创业发展中，安天自主研发了全平台、全场景的威胁检测引擎核心技术，通过引擎技术的生态合作，赋予合作伙伴产品的内生安全能力。并在长期威胁检测对抗工作中，逐渐形成了以高级威胁检测防护为特色的产品服务体系。安天通过部署蜜罐网络、诱饵信箱、流量监测等多种环节，实现主动威胁捕获，并根据用户的需求，对安天的智甲终端防御系统、探海流量监测系统、追影沙箱分析系统等产品的事件上报，以及其他使用安天引擎客户所发现上报的疑似威胁进行分析处理。安天与全球七十多家主要安全厂商、应急机构形成了恶意代码样本和威胁情报共享体系。通过“赛博超脑”大规模自动化分析流水线，安天每日可以对百万量级文件实现向量拆解，构成了样本向量大数据空间，与每日十亿级别事件日志和其他威胁情报建立关联。依托监测机制、产品体系和后台支撑，安天对近二十个国家和地区的 180 多个威胁行为体进行分析监测，持续向客户提供特征库、威胁情报、高级威胁追溯包更新等服务。

肖新光在采访中介绍：安天通过一系列的这种技术组合应用，不断进行攻击组织和攻击者行为画像，包括白象、海莲花、方程式、绿斑等这种带有国家或地区政府背景的安全威胁都进行了深度分析。在对手攻击能力不断增强同时，我们本身这种威胁检测、发现分析能力也在提升。

安天从 2010 年的震网事件开始，将应急分析工作的重心转入到高级网空威胁行为体所发动的定向化的高级威胁中，在高级威胁发现、分析、溯源方面取得了一系列进展。在今年 6 月 1 日，安天发布《“方程式组织”攻击中东 SWIFT 服务商事件复盘分析报告》，完整复盘了超级大国网空威胁行为体攻击中东金融服务机构的全过程，这一分析成果被新华社等权威媒体引用发布。

金融、能源、电力、通信、交通等领域的关键信息基础设施，是经济社会运行的神经中枢，也是可能遭到重点攻击的目标。安天为战略客户提供整体安全解决方案、关键产品和服务，安天提出了高信息价值、高防护等级、高威胁对抗的“三高”场景，与业内专家共同翻译引入了 SANS 的滑动标尺安全模型，在此基础上进一步发展了叠加演进的安全模型。在长期进行监管型态势感知平台研发经验教训总结的基础上，正在持续研发战术型态势感知平台，为防御体系打造指挥控制中枢。

肖新光此前在多次接受采访中表示，当前我国关键信息基础设施面临着严重的无效防护问题，为全面改善网络安全防御能力，需要将合规 + 威胁导向的建设模式转入到基于能力导向的建设模式。

本次采访中他指出，随着网络安全的宣传教育普及，整个的防护意识已经有较大增强。从原有这种堆砌产品、零星应对威胁、应付检查的这种工作思路逐步转化到全面建设所有必要之安全环节，使之成为动态、综合网络防御体系的这样一个工作思路。当然要做好这样的工作依然任重道远。

微信扫描二维码阅读原文

网络钓鱼活动窃取亚马逊用户个人信息和财务信息

一个新的亚马逊网络钓鱼骗局正在传播，它诱使用户将他们的个人信息和财务信息（包括信用卡信息）交给攻击者。受害者收到一封据称来自亚马逊的电子邮件，通知其帐户存在可疑活动，试图说服受害者更改亚马逊帐户的密码。然后要求受害者点击“立即更新”以防止他们的帐户被永久禁用。点击更新选项卡后，受害者将被带到看似真实的亚马逊登录页面，登录电子邮件或电话号码和密码。窃取登录凭据后的下一步是询问受害者的帐单地址。点击更新后，受害者将被带到另一个看似真实的亚马逊页面，该页面会询问他们的财务信息。一旦受害者发送财务信息，将被带到另一个页面，通知他们的帐户已被恢复，然后点击下一步将他们重定向到原始的亚马逊网站。

（原文链接：https://www.hackread.com/new-amazon-phishing-scam-stealing-credit-card-data/）

每周安全事件

类 型	内 容
中文标题	研究人员发现针对企业环境的勒索软件 TFlower
英文标题	TFlower Ransomware - The Latest Attack Targeting Businesses
作者及单位	Lawrence Abrams
内容概述	TFlower 勒索软件正通过被黑客攻击的远程桌面服务将其安装在企业网络中。一旦攻击者获得对计算机的访问权，他们就会感染本地计算机，或者试图通过 PowerShell Empire、PSExec 等工具渗透网络。执行时，勒索软件将显示一个控制台，显示勒索软件在加密计算机时执行的活动。
链接地址	https://www.bleepingcomputer.com/news/security/tflower-ransomware-the-latest-attack-targeting-businesses/

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

恶意代码类别		名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.ungdungvn.a[prv,rmt,spy] 2019-09-15	高	该应用程序伪装成正常应用，运行后隐藏图标，释放其他恶意软件，加载钓鱼界面诱导用户填写 Facebook 账号和密码，接收远程控制指令，窃取用户地理位置，手机固件信息、通话记录、安装未知应用，删除短信、联系人、私自发送短信，并将用户隐私上传。造成用户隐私泄露，建议卸载。
		G-Ware/Android.Clicker.ag[rog,exp] 2019-09-16	中	该应用程序伪装成正常应用，运行后诱导用户点击，加载广告、跳转到色情网站或者下载链接，导致用户资费损耗，建议不要使用。
		Trojan/Android.Obfus.c[prv,exp] 2019-09-17	中	该应用程序启动隐藏图标，后台私自发送短信，并获取用户短信、电话号码、网络连接等信息上传，会造成用户隐私泄漏及资费消耗，建议卸载。
	较为活跃样本	Trojan/Android.Donot.a[prv,rmt,spy]	中	该应用程序伪装成其他应用，接收远程控制命令，窃取用户短信、联系人、通话记录、地理位置、应用程序列表、Whatsapp 聊天记录等隐私信息并上传，造成用户隐私泄露，建议卸载。
		G-Ware/Android.StealMoneyGame.ed[pay,rog]	中	该应用程序包含风险代码，运行上传手机相关信息，私自发送付费短信，造成用户的资费消耗和隐私泄露，建议卸载。
		G-Ware/Android.HiddenAds.iw[exp,rog]	低	该应用程序包含风险代码，运行隐藏图标，后台推送广告，造成用户的资费消耗，建议卸载。
		RiskWare/Android.FakeQQ.as[fra]	低	该应用程序伪装成 QQ，无实际功能，会将用户输入的账号密码保存至本地，存在一定风险，请使用正版软件。
		RiskWare/Android.PJbocai.q[rog]	低	该应用程序为博彩游戏应用，会给您带来财产损失。此类程序一般以欺骗形式引诱推荐安装，是一种典型的网络赌博诈骗手段，请立即卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows 远程桌面客户端远程代码执行漏洞（CVE-2019-0787）	高	当用户连接到恶意服务器时，Windows 远程桌面客户端会触发远程代码执行漏洞。若要利用此漏洞，攻击者需要控制服务器，然后利用社会工程学、病毒、中间人攻击等手段诱导用户连接到该服务器。成功利用此漏洞的攻击者可以在目标系统上执行任意代码。攻击者可随后安装程序、查看、更改或删除数据，或者创建拥有完全用户权限的新帐户。
	较为活跃样本	RiskWare[Downloader]/Win32.Gena	中	此威胁是一个具有下载器行为的风险软件家族。该家族的样本在执行后会下载样本指定的程序并执行，可能会对系统造成威胁。
		Trojan[Exploit]/JS.RealPlr	中	此威胁是一种以 JS 为载体的木马家族。该家族的样本利用了 SWF 的漏洞，在播放 SWF 文件的时候产生溢出并下载恶意软件从而使执行者的机器完全处于对方控制之下。
		Trojan[PSWTool]/Win32.NetPass	中	此威胁是一个风险软件家族。该家族的样本具有收集并管理用户密码的能力，可能会对用户的隐私造成威胁。
		RiskWare[Dialer]/Win32.PlayGames	中	此威胁是一个风险软件家族。该家族的样本以游戏平台的形式出现，存在着不为用户所知的扣费行为。
		Trojan[Backdoor]/Win32.MoSucker	中	此威胁是一个具有后门行为的木马家族。该家族的样本在执行后，攻击者即获得对此设备的完全控制权限。

特权访问滥用的五个迹象

Todd Peterson/ 文　安天技术公益翻译组 / 译

鉴于 80%的数据泄露与特权访问凭证有关，企业能否有效管理和监控特权账户通常意味着安全和灾难性网络事件之别。一旦攻击者获得企业特权账户的凭证，企业就会遭受数百万美元的经济损失，更不用说声誉损失和客户损失了。

在这种情况下，采取严格的特权账户访问管理措施，对于保护企业免受潜伏在企业内外的网络威胁至关重要。现实情况是，传统的验证不足以保证特权账户的安全。一旦“IT 管理员”使用特权账户登录，IT 安全团队通常就不会再对其或其活动进行进一步验证了。

除了标准的身份鉴别控制措施和策略之外，IT 安全团队还需要了解如何在特权访问会话中有效地识别可疑活动，以减轻威胁。接下来，本文将介绍特权访问滥用的五个迹象，帮助企业识别“冒充的”特权用户。

异常账户登录时间

登录时间是可疑活动的一个重要迹象。特权用户通常在工作日工作，因此，如果管理员在星期六凌晨 3 点登录账户，IT 团队就应该警惕并发布告警了。

跟踪登录时间，可以为特权访问增加一定的置信度和额外的验证层。对于大多数企业而言，这是最简单的策略，应该作为第一道防线。

新的、不同的打字风格

打字风格就像人的指纹一样：世界上没有两个指纹相同的人，也没有两个打字风格相同的人。每个人的大脑工作方式不同，记忆模式不同，因此其打字节奏也各不相同。

为了确定使用特权账户的人是否是授权用户，IT 管理员可以采用生物识别分析技术，利用高级机器学习来了解每位用户的击键行为，例如打字速度和连续击键之间的延迟。这些信息能够帮助 IT 管理员轻松发现可疑活动；此外，最终用户几乎不会察觉到这种持续的身份鉴别方法。

异常窗口标题

在监控潜在攻击者方面，诸如应用程序窗口标题这样简单的内容，也有助于识别攻击者。最简单的方法是，像攻击者一样思考问题。具体而言，只考虑管理员能够执行的活动，这些活动通常涉及访问敏感系统和数据，而这些系统和数据就是攻击者的最终目标。

对于特定标题，例如与认可用户和网络犯罪分子均相关的输出，该如何处理呢？在这种情况下，企业可以收集用户的所有标题。这将有助于企业创建基准，了解哪些标题是常见的。当出现异常标题时，这种基准可以帮助安全团队快速识别攻击活动，以便在攻击发生之前予以阻止。

非典型地理位置

了解特权用户的标准地理位置，有助于 IT 安全团队更快地识别恶意活动。在分析特权用户的地理位置时，IT 安全团队需要考虑两个重要因素：（1）特权用户是否在其典型地理位置登录；（2）登录次数。

为了确认威胁，首先要查看特权用户的 IP 地址，以确定其是否在典型地理位置。如果 IP 地址出现异常，IT 安全团队应立即检查该账户登录的次数。在如今的互联世界中，全球超过 70%的特权用户每周至少远程工作一次，且在旅行中工作的情况越来越普遍。因此，特权用户偶尔改变地理位置或 IP 地址不足以触发告警，但是其短期内多次在异常地址登录就是一种攻击迹象了。

会话长度突然改变

无论是管理活动目录（Active Directory），还是数据库管理员使用 SQL Server Studio，特权账户都会执行非常具体且明确定义的任务。考虑到这一点，应用程序启动的时间以及特定凭证的登录时间，可能是恶意威胁的迹象。例如，如果特权访问用户只负责设置新的租用账户，但是却在短时间内多次登录公司财务系统，这可能意味着该账户已被盗用。

为了确认这并非是特权用户在执行新的活动，企业需要记录可疑用户的新活动。这样，企业就能很容易地发现与用户新活动不一致的会话，从而识别网络中的威胁和犯罪分子。

特权账户是各种规模的企业控制、监控和审核其信息的基础流程，因此企业面临的问题不再是特权账户是否存在风险，而是如何主动和更准确地识别可疑活动。通过向安全团队赋予特权会话活动的全面可见性，企业可以在损害发生之前快速识别并阻止网络犯罪分子。

原文名称	5 Signs of a Privileged Access Abuser
作者简介	Todd Peterson。Todd Peterson 是 One Identity 解决方案的产品营销负责人。
原文信息	2019 年 9 月 16 日发布于 Security Boulevard。 原文地址 https://securityboulevard.com/2019/09/5-signs-of-a-privileged-access-abuser/
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。