安天发布《利用新型黑客工具传播挖矿木马活动的分析报告》

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由 RADMIN 和 MIMIKATZ 组合而成的新型黑客工具，被用来在 Windows 系统上植入门罗币恶意挖矿程序。它会扫描开放端口 445 并利用 Windows SMB 服务器漏洞 MS17-010（2017 年已发布补丁）进行感染和传播。目前，该攻击活动主要针对中国和意大利的公司。

在攻击时，攻击者首先通过 MIMIKATZ 工具收集系统的账户信息和凭证信息，随后利用 RADMIN 工具获取管理员权限，并在系统中安装其他恶意软件。在安装过程中，最初会在 Windows 目录下释放一些随机命名的不相关的文件，分析显示，只有最后一个释放的文件是门罗币恶意挖矿程序。由于这种随机命名性和看似合法的 Windows API 函数调用，使得它有可能逃避开安全软件的检测。最初感染用户机器的恶意木马是通过用户访问不良网站或者经过其他恶意软件的释放来安装的，然而该木马本身并不下载挖矿软件，它只会连接到几个 IP 地址，发送本机信息，随后获取攻击端 RADMIN 传回的命令，来远程下载和安装恶意挖矿软件。该攻击活动高发在今年 1 月到 2 月之间，即使在年后也并没有减弱的迹象。

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、数据证书鉴定器、文件元数据鉴定器鉴定器、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、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	bdbfa96d17c2f06f68b3bcc84568cf445915e194f130b0dc2411805cf889b6cc
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	197 KB
MD5	59B18D6146A2AA066F661599C496090D
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Fsysna
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=59B18D6146A2AA066F661599C496090D

◆ 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	★★★
伪装 svchost 进程	★★★★
通过 CMD 隐藏删除自身	★★★★

◆ 常见行为

行为描述	危险等级	行为描述	危险等级
释放 PE 文件	★	启动指定服务	★
创建挂起进程	★★	获得计算机用户名	★
获取驱动器类型	★	访问文件尾部	★
设置调试器权限	★	添加计划任务	★★
获取系统信息（处理器版本、处理器类型等）	★	独占模式打开，防止复制读取，防止杀毒软件扫描上报	★
查找窗口	★	获取当前光标位置	★
设置文件属性为隐藏	★★	获取计算机名	★
隐藏 PE 文件	★★	复制文件到系统目录	★★
Run 自启动	★	获取驱动加载权限	★
对照发现设置自启动	★	读取自身	★★
创建服务	★	安装 LSP 协议	★★
疑似桌面控制	★	疑似查找浏览器进程	★★

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 11 日（总第 174 期）试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

全国政协委员、安天首席架构师肖新光做客凤凰两会直播间

编者按：2019 年 3 月 7 日，全国政协委员、安天首席架构师肖新光做客凤凰两会直播间，接受吴小莉现场访谈，本文根据现场访谈音频整理。

主持人：今天两会直播间我们邀请到的是全国政协委员、安天科技集团的首席技术架构师肖新光，就信息技术发展、网络安全等话题来进行分析。肖委员，您好！

肖新光：小莉，您好！

主持人：其实我们刚才已经提到，您是网络安全领域的专家，现代社会中，网络本身的发展越来越快，政府工作报告中也多次提到了信息、信息技术的发展，而基础设施进一步强化之后关于个人信息的保护已经成为了焦点。我们很想知道，在过去一年中，世界范围内，包括中国，网络安全领域有哪些比较突出的变化？

肖新光：去年，我们国家在 4 月 20 日到 21 日，召开了全国网络安全和信息化工作会议，习总书记作出了一系列重要工作要求，包括“关口前移、防患于未然”，为网络安全提出了以防护效果为导向的工作要求。过去几年，是各种类型的网络安全事件多发、频发的一个时段，一方面，出现大量带有政府背景、大国博弈和地缘安全背景的网络安全威胁和攻击，像去年 8 月央视在焦点访谈上曝光的“绿斑”攻击组织，就是长期以大陆的各种关键信息系统和军工科研为目标进行入侵、渗透和攻击。同时，也有以逐利为目的的各种网空攻击，像一些肆意传播的勒索软件，包括一些 DDoS 攻击等。还有一个值得关注的，就是有大量的、不同类型的信息泄露的事件。

主持人：就像您提到的，网络安全其实跟每个人都息息相关，我们现在有大量的个人信息都是通过网络在传递，那我们也很想知道，在大国博弈中，中国的网络安全防御能力是怎样的？

肖新光：我国的信息化发展实际上是一个后发的过程，在之前比较长的时间内，我们还是处于信息化先行、网络安全补课的状态，由于较长时间缺乏整体的规划指引，整个的预算投入不足，当前来看，我们的安全防护能力还是亟待加强的。

主持人：说到投入不足，我知道您去年就提到了希望在网络空间的安全领域要有针对性的投入和布局，后来这个提案提出之后，得到怎样的回应？

肖新光：这个提案提出后，得到了国家网信办，包括其他的相关部委的回复。当然，我们本身作为一家有代表性的网络安全企业，我们自己也是要积极的参与到相关的工作中去。

主持人：那么今年又带来了哪些提案，能够进一步强化您这份提案的后续？

肖新光：今年我们主要提出了通过加强系统规划指引、预算投入保障和问责机制落实，来全面强化政府以及央企的网络安全。从一个国家的网络安全能力建设来看，防控能力建设是以国家大型工程为主干，以各政企机构建设管理的每一个重要信息系统和信息基础设施的安全为基石。从过去的情况来看，我们在政企网络安全防御工作中，缺少系统规划指引，特别是在当前经济下行压力加大的大环境下，政企机构信息化投入普遍放缓，导致网络安全建设缺少预算支撑。另外，我们国家整个的网络安全责任制，也需要形成有效的落地机制。所以，从这份提案中，我们希望国家相关部门通过帮扶赋能的视角，为整个政企机构如何建设网络安全防护能力，形成比较清晰的战略指引和体系化、框架性防护规划指引，把网络安全建设从合规要求基础上简单堆砌部分产品应对各类单点威胁的模式，转入到全面建设必要的网络安全防御能力，并将其有机结合以形成动态综合网络安全防御体系的能力导向建设模式。然后，基于这个规划指引，再提供充分的预算保障。同时，我们也建议进一步强化问责机制，把国家监察体系和网络安全责任的执行落实结合起来。

主持人：您觉得，当前情况下，中国可能会面临哪些网络安全上的危机或者是可能的攻击？

肖新光：像金融、电力、能源、交通这些关键信息基础设施，它所面临的就是被威胁行为体入侵、控制、窃取、毁瘫等这样的风险，会给我们的国计民生、社会发展运行，包括在遇到一些紧急情况下的战争潜力，带来潜在的影响。因此，我们的重要信息系统和信息基础设施的网络安全防护是当前的重中之重，是必须得到强化的。

主持人：网络安全涉及到国家安全，在这方面，中国如何与其他国家进行合作来加强中国的网络安全？

肖新光：总书记指出，要共同构建网络空间命运共同体。在网络空间如何建立

（下转第二版）

（上接第一版）

起相应的合作生态，共同应对重大的安全事件和风险，共同打击网络中包括恐怖主义在内的犯罪行为，是各国间进行合作的结合点。

主持人：网络安全与我们息息相关，但目前也只是涉及到个人信息泄露、信息窃取这个层次的问题上，可随着网络技术的进一步的加强，包括人工智能，5G或者物物相联、物联网的诞生，所有东西都在网络上进行之后，像好莱坞影片中那种如果一个系统被网络的骇客给攻击了，整个城市就造成了非常大的安全隐患的情况可能发生么？

肖新光：随着信息化的发展，网络安全威胁的连接性和发生风险的后果也随之放大，在这种情况下，信息化越发达，如果不能够同步做好网络安全工作，就等于叠加了更大的风险，对此必须进行有效的应对。不管是包括像物联网所支撑的智慧城市，大数据和云平台，还是其他的各种信息系统的建设，必须在系统的规划、建设、运维全生命周期考虑网络安全问题，通过整体系统的安全框架去落实网络安全的能力，实现能力建设的叠加演进。

主持人：我们常常说“未来已来”，但是这个未来到底是一个非常便利的未来，还是可能充满着安全隐患的未来？我们可能现在就要做好准备，您觉得无论是政府、企业或个人，如何在未来的网络世界中保护网络空间的安全？

肖新光：网络安全本身，与安全的每一个层次都息息相关的，包括国家安全、社会安全、政企机构安全和个人安全。同时，它又和总体国家安全的每一个方面，包括政治安全、经济安全、科技安全、军事安全等，也都发生关联。从政府的角度，要以总体国家安全的视角，深入考虑到网络安全相关的关联和相应的影响，切实把投入转化为有效的网络安全防御能力，实现和提升人民群众的获得感、幸福感和安全感。

主持人：这个安全感非常的重要。非常感谢肖委员来到现场，为我们科普了一下网络安全的重要性。谢谢！

肖新光：好。谢谢小莉！

每周值得关注的恶意代码信息

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平台的恶意代码值得关注

关注方面		名称	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.Mazap.a[prv,spy] 2019-03-01	该应用程序是一款远控工具软件，运行后通过设置激活设备管理器权限、获取root权限和隐藏图标，监听用户手机短信、通话，获取地理位置、通话记录，截屏、录音、拍照，并将用户隐私上传至服务器。会造成用户隐私泄漏，若非自主安装请卸载。（威胁等级中）
		Trojan/Android.Mobispy.a[prv,spy] 2019-03-02	该应用程序是一款间谍工具，运行后会隐藏图标，窃取手机用户的短信、地理位置、社交软件记录、通话记录及录音、浏览器历史记录等隐私信息，联网并将这些信息上传至服务器，造成用户的隐私泄露。请谨慎使用，非自主安装建议卸载。（威胁等级中）
		Trojan/Android.concern4u.a[prv,spy] 2019-03-03	该应用程序是一款间谍软件，能够伪装成系统应用，运行后窃取用户短信、联系人、通话记录、固件信息、地理位置、照片、视频等隐私信息。造成用户隐私泄露，请立即卸载。（威胁等级中）
	较为活跃的样本	RiskWare/Android.iappTool.b[rog]	该应用程序是使用裕语言编写的程序，大多是推广、刷钻、破解工具类的应用，存在一定安全风险，请谨慎使用。（威胁等级低）
		Trojan/Android.backdroid.a[prv,spy]	该应用程序伪装系统应用，安装后无图标显示，程序运行后会联网并上传用户设备信息、GPS位置信息、短信信息，造成用户隐私泄露，建议卸立即载。（威胁等级中）
		G-Ware/Android.weiduanGame.a[pay,rog]	该应用程序是一款风险微端应用，运行后诱导用户点击下载指定付费应用，且付费信息不明显，造成用户资费消耗，建议不要使用。（威胁等级低）
		Trojan/Android.isitdown.a[prv,rmt]	该应用程序伪装为正常应用，包含风险代码，触发后会启动并激活设备管理器，拦截短信，接收指令，执行获取手机相关信息、下载文件、发送短信等操作，并将这些信息上传至指定网址，造成用户的隐私泄露和使用不便，建议卸载。（威胁等级中）
		Trojan/Android.vorona2.a[exp,rog]	该应用程序伪装成其他应用，运行后激活设备管理器，联网后私自下载未知子包，并加载其他应用。造成用户流量消耗，存在安全隐患，建议卸载。（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 Office 访问连接引擎远程代码执行漏洞（CVE-2019-0671）	当 Windows Office 访问连接引擎处理内存中的对象时存在远程代码执行漏洞。攻击者可以通过向目标主机发送经特殊设计过的文件，通过诱导受害者打开该文件来利用此漏洞，成功利用此漏洞的攻击者可以在受害者系统上执行任意代码。（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/NSIS.Zaitu	此威胁是一种具有广告行为的灰色软件类程序。该家族样本使用NSIS打包，NSIS（Nullsoft Scriptable Install System）是一个开源的 Windows 系统安装程序的制作程序。该家族样本通过NSIS打包可以捆绑其他恶意代码到用户系统中。该家族软件运行后会在受感染计算机的浏览器中显示广告。该家族能通过安装自动更新程序来获取自身的最新版本。（威胁等级低）
		Trojan[Dropper]/Win32.Recodrop	此威胁是一种具有捆绑行为的木马类程序。该家族会在后台记录和收集用户信息并回传。（威胁等级中）
		GrayWare[AdWare]/Win32.Techsnab	此威胁是一种有广告行为的灰色软件类程序。该家族劫持被感染者的浏览器，更改浏览器主页，跳转到指定网站。该家族会下载恶意软件，在受感染的计算机上显示广告。（威胁等级中）
		Trojan[Downloader]/JS.Cryptoload	此威胁是一种下载类木马程序。该家族样本通过JS脚本语言编写主要是用来下载勒索软件。该家族木马通过电子邮件附件传播。（威胁等级中）

防御新兴的社交媒体攻击

Mark Stone / 文　安天技术公益翻译组 / 译

对企业来说，最严重的威胁通常是：攻击者利用社会工程手段从员工手中窃取信息或数据。对攻击者来说，这种方法无需多么高超的技能，门槛很低。

更糟糕的是，社交媒体的迅速普及进一步降低了这一门槛。无论企业是否制定了限制社交媒体使用的规则，都无法阻止员工全天候地使用它们。随着攻击者不断利用社交媒体来渗透企业网络，企业应该采取哪些防御措施呢？

了解攻击者的社交媒体策略

企业首先需要知道，攻击者可以通过社交媒体轻松地攻击其员工。

Comparitech.com网站的隐私倡导者保罗·比肖夫（Paul Bischoff）说：“利用一点点信息渗透企业网络并不难。”他指出，如果某位员工在其社交媒体资料中列出了公司名，一旦攻击者知道了该员工的名字，就能利用其资料中的信息对公司发动攻击了。

如果目标公司规模较大，攻击者甚至不需要知道某位员工的名字——他们可以做一下猜测。确定目标员工之后，攻击者可以采用以下攻击方法。第一种方法是，利用在其他公司的数据泄露事件中泄露的口令，破解该员工的社交媒体帐户。第二种方法是，尝试与该员工建立联系，并通过网络钓鱼攻击来获取所需信息，例如访问其企业邮件帐户。攻击者甚至可以将自己标记为该员工的朋友；或者破解其现有朋友的帐户，冒充他们与其进行通信。

通过社交媒体，攻击者可以评估公司内外的目标。人们在社交媒体上分享了大量的个人信息，这些信息通常包含有关其工作的宝贵

数据。一旦攻击者获得了员工帐户（通常是企业邮件帐户）的访问权限，其下一步可能就是渗透公司网络了。

“一旦攻击者攻破了员工的电子邮件帐户，就会造成严重的破坏。”比肖夫补充说，“他们不仅能获得现有的电子邮件，还能编写新的电子邮件。此外，电子邮件帐户通常会为各种在线帐户发送双因子身份验证PIN码、口令重置链接等敏感信息。”

一旦攻击者登录到受害者的电子邮件帐户，他们就可以通过更改口令和/或恢复邮件地址来锁定帐户，为自己争取时间。受害者需要一段时间来解决这些问题，攻击者可以趁这段时间冒充受害者，向公司中的其他人发送以假乱真的钓鱼邮件。

探索一些简单的预防技术

访问敏感公司数据的一种有效方法是信息克隆，即：使用从目标用户的真实社交媒体帐户中窃取的照片和相关数据，来创建假的Facebook（或Instagram或其他社交网络）帐户。

“通过信息克隆创建Facebook帐户，攻击者可以冒充熟人与目标建立联系。”比肖夫说，“他们甚至可以克隆目标现有朋友的信息——你是否注意过，一个在Facebook上发帖不多的人，第二次请求添加你为朋友？针对该问题，Facebook的应对方法是：如果有人向你发送了添加朋友的请求，Facebook会向你展示此人与你有多少共同朋友。但不是每个人都会注意到这一点。”

为了阻止此类攻击，比肖夫建议员工不要在他们的社交媒体资料中列出公司名。如果必须提供公司名，他们可以“创建”一个，而不要从下拉列表中选择。这样可以防止员工沦为以公司为目标的攻击者的“垫脚石”。

此外，正如安全专家反复强调的那样，对员工开展常见钓鱼策略的培训至关重要，公司甚至可以向员工发送钓鱼邮件进行实时测试。我们必须对企业的所有团队进行培训和测试，并提供基于角色的教育和意识培训课程。最后，比肖夫建议制定相关规则，在共享信息之前进行二次身份验证。

抵御新兴的社交媒体攻击

我并不是说，企业应该决定员工如何以及何时使用社交媒体——因为这将是徒劳的。特别是在这个“自带设备”（BYOD）时代，即使在工作场所，社交媒体的使用也只会不断增加。我清楚地记得，即使在Facebook早期，试图监控其使用也是一项非常艰巨的任务。我无法想象，现在这项工作会有多难了。

社交媒体上的诱惑太多了，用户难以抗拒。与其因噎废食，我们不如直面现实，尽最大努力让员工意识到潜在的社交媒体攻击。与其限制员工的在线行为，不如让他们成为安全流程的一部分——为他们提供相关知识，使其成为企业安全保护层的一部分。

原文名称	When Combating Emerging Social Media Attacks, Don’t Try to Swim Against the Current
作者简介	Mark Stone。Mark Stone是内容营销撰稿人，擅长技术、商业和娱乐领域。
原文信息	2019年2月26日发布于Security Intelligence 原文地址 https://securityintelligence.com/when-combating-emerging-social-media-attacks-dont-try-to-swim-against-the-current/
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。