安天发布《ProximityUntilCache32.tlb 挖矿木马样本分析报告》

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 ProximityUntilCache32.tlb 的挖矿木马开始活跃。该挖矿木马的背后是一个僵尸网络，从 2017 年被发现一直活跃。它使用 NSA 泄漏的漏洞利用工具进行传播，感染受害机器并用于挖取门罗币。

该挖矿木马有多个版本，通过不同的 C2 域名进行区分，其中包括 eee.asf3r23.cf、*.drawal.tk 等。样本压缩包中 Crypt 文件为 NSA 漏洞利用工具包，运行后利用该工具进行传播并执行挖矿主程序。Crypt 解压后将文件释放到 %win_dir%\IME\Crypt\ 并执行。spoolsv.exe 会传播 payload DLL 到其他机器中，该 DLL 首先会创建互斥量，检查本机是否存在已感染的文件，之后解压恶意代码并释放，注册自身为系统服务，实现自启动。后续新版本中会包含名为 srv 的 DLL 文件，它可以检查自启动的情况，读取注册表中的 C2 地址，连网请求最新的配置文件，还可以回传当前进程的运行情况。它还使用了 DGA 随机产生域名的手法以逃避检测。

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：

文件被页面手工提交发现，经由文件来源信息鉴定器、文件元数据鉴定器、BD 静态分析鉴定器、数字证书鉴定器、动态(WinXP) 鉴定器、反病毒引擎鉴定器、聚类分析鉴定器、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。

文件名	srv64
文件类型	BinExecute/Microsoft.DLL[:X64]
大小	563 KB
MD5	C70673F416E3C3EE0B194FF0966E0A86
病毒类型	木马程序
威胁名称	Trojan/Win64.Miner
判定依据	反病毒引擎

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=C70673F416E3C3EE0B194FF0966E0A86

◆ 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

◆ 进程监控

PID	创建	命令行
1980	rundll32.exe	"C:\WINDOWS\system32\rundll32.exe" c:\ec847d4149f14d55a23980c61b926099\share\target.dll,DllMain

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.51	1130	192.168.122.1	53
192.168.122.1	53	192.168.122.51	1130
192.168.122.1	67	192.168.122.51	68
0.0.0.0	68	255.255.255.255	67
192.168.122.51	137	192.168.122.255	137
192.168.122.51	123	13.89.190.88	123

◆ 文件元数据分析

描述	值
File Size	562 kB
File Type	Win64 DLL
MIME Type	application/octet-stream
.....	.....

安天周观察
安天官方微博 安天官方微信
主办：安天 2018 年 11 月 19 日 (总第 160 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天发布《Trickbot 银行木马样本分析报告》

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 的银行木马开始活跃。Trickbot 银行木马在 2017 年增加了新模块，此模块功能为规避检测及屏幕锁定。在 2018 年，它又增加了一个密码管理器模块，可以获取多个应用程序和浏览器的访问权限，主要影响加拿大、美国、菲律宾等国家。

攻击者持续利用 Trickbot 的模块化结构，能够从 C & C 服务器下载新模块来不断更新自身，并更改其配置。Trickbot 新增的密码管理器模块名为 pwgrab32 或 PasswordGrabber，会窃取来自 Filezilla、Microsoft Outlook 和 WinSCP 等应用程序的凭据。除了从应用程序窃取凭据外，还会从几个流行的 Web 浏览器窃取信息，例 如 Google Chrome、Mozilla Firefox、Internet Explorer 和 Microsoft Edge。Trickbot 使用 shareDll32 模块在网络中传播自身。它连接 http://185.251.**.**/radiance.png 以下载自身的副本并将其另存为 setuplog.tmp。wormDll32 模块尝试使用 NetServerEnum 和 LDAP 查询识别网络中的服务器和域控制器。networkDll32 加密模块扫描网络并窃取相关网络信息。Wormdll32 是 Trickbot 用于通过 SMB 和 LDAP 查询传播自身的加密模块。它与模块“wormDll”一起用于在网络上传播。injectDll32 模块监视银行应用程序可能使用的网站，它还用于使用反射 DLL 注入技术将代码注入其目标进程。

安天提醒广大政企客户：

1、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，不要随意下载非正版的应用软件、非官方游戏、注册机等。

2、收发邮件时请确认收发来源是否可靠，不要随意点击或复制邮件中的网址，更不要轻易下载来源不明的附件，发现网络异常时要提高警惕并及时采取应对措施。

3、确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，必要时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。

4、做好文件备份工作，防止出现如勒索软件加密重要文件后无法恢复等情况。

安全厂商披露 INDRIK SPIDER 组织攻击演进路线

INDRIK SPIDER 是一个复杂电信诈骗组织，自 2014 年 6 月以来一直在使用 Dridex 进行攻击。在 2015 年和 2016 年间，Dridex 是市场上最多产的银行木马之一。2017 年 8 月，名为 BitPaymer 的新勒索软件变种攻击了英国的国民健康服务（NHS）。BitPaymer 的加密和赎金功能在技术上并不复杂，但恶意软件包含多个与 Dridex 重叠的反分析功能，分析表明 BitPaymer 是 INDRIK SPIDER 开发的。

在最近的 BitPaymer 活动中，攻击者入侵的合法网站，利用社交工程诱骗用户下载和运行恶意可执行文件。下载后 Dridex 加载程序和 PowerShell Empire 在受感染的主机上运行。Dridex 加载程序有收集有关主机上当前用户信息的功能。PowerShell Empire 是一种专为渗透测试而开发的后期开发代理，用于在主机之间横向移动。PowerShell Empire 会在受害者网络的服务器上部署 Mimikatz 模块。研究人员发现两种下载 BitPaymer 的方法，一种是直接在这些服务器上下载和执行 BitPaymer 恶意软件。另一种是 BitPaymer 恶意软件被下载到受害者网络中的网络共享，并且调用启动脚本 gpupdate.bat 通过域控制器的组策略对象（GPO）推送到网络上的所有主机。BitPaymer 恶意软件的两种变体都具有多种阻碍分析的技术。

（原文链接：https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/）

Lazarus 使用韩国和美国服务器进行 APT 攻击

研究人员发现了一个执行后门（RAT）的二进制（EXE）文件，该文件 2018 年 11 月 7 日创建。分析发现，该文件与 2018 年 2 月发现的文件具有类似结构和代码重叠。恶意文档使用英语编写，但代码页 949 表明这是在韩语环境中编译的。提示显示要求用户打开宏。宏运行之前，恶意函数不会被调用，而英文版的 Office 将导致宏运行。恶意宏会连接特定网站安装其他恶意软件。研究人员发现，与 C2 通信的代理，功能和结构与 2 月发现的样本几乎相同，但 C2 地址被部分改变。恶意软件使用两个韩国 IP 和两个美国 IP 与四个 C2 通信，并且美国的 IP 还被用于恶意文件存储。

（原文链接：http://blog.alyac.co.kr/1978）

每周安全事件

类 型	内 容
中文标题	Nginx 修补了 Web 服务器多个拒绝服务漏洞
英文标题	Nginx server security flaws expose more than a million of servers to DoS attacks
作者及单位	Pierluigi Paganini
内容概述	Nginx 开发团队发布了版本 1.15.6 和 1.14.1，解决了两个 HTTP/2 实现漏洞。这些漏洞可能导致 Nginx 版本 1.9.5 到 1.15.5 受到 DoS 攻击。其中 CVE-2018-16843 会导致过多的内存消耗，CVE-2018-16844 则会导致过多的 CPU 使用率。Nginx 团队还修复了影响 ngx_http_mp4_module 模块的漏洞 CVE-2018-16845，攻击者可利用该漏洞通过让模块处理特制的 MP4 文件导致工作进程崩溃或内存泄漏。该漏洞影响 nginx 1.1.3 及更高版本以及 1.0.7 及更高版本。
链接地址	https://securityaffairs.co/wordpress/77866/hacking/nginx-server-dos-flaws.html

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.NomoSpy.a[prv,exp,rmt,spy] 2018-11-12	该应用程序伪装 Google Play，运行诱导激活设备管理器，联网接收远程指令进行发送短信、拨打电话、打开浏览器、恶意注入、修改手机设置等高危行为，同时上传用户通讯录、短信、位置、安装列表等隐私，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.acplus.a[exp,rog] 2018-11-13	该应用程序包含恶意子包，运行后释放脚本，联网获取电商购物商品数据，模拟操作进行刷单行为，请谨慎使用避免资费消耗。（威胁等级中）
		Trojan/Android.Hqwar.o[prv,exp,spy] 2018-11-14	该应用程序伪装系统应用，运行会隐藏图标，联网上传用户短信、通讯录、通话记录、录音、位置信息等隐私信息，私自发送指定短信，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级中）
	较为活跃样本	Tool/Android.CallRecorder.b[prv]	该应用程序是一款电话录音工具，登陆后录音可以通过邮件上传，可能造成用户隐私泄露，请谨慎使用。（威胁等级低）
		RiskWare/Android.chima.a[prv,rmt,sys]	该应用程序为雷电 os 相关，安装无图标，运行会频繁连接网络，收集手机相关信息，并能够执行远程命令，有一定的风险，请用户谨慎使用，若非自主安装，建议卸载。（威胁等级中）
		RiskWare/Android.mmHook.a[sys]	该应用程序运行后隐藏图标，会 hook 微信相关 api，可能会影响手机的正常运行，存在一定风险，请谨慎使用。（威胁等级低）
		Trojan/Android.ludo.a[prv]	该应用程序植入恶意代码，会私自收集用户短信、拦截短信、无提示私自发送短信，造成用户隐私泄露、资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.emial.gt[prv,exp]	该应用程序运行后隐藏图标，监听用户短信信息并拦截短信，发送短信内容到指定号码，造成用户隐私泄露和资费消耗，建议立即卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash Player 越界读取漏洞（CVE-2018-15978）	Adobe Flash Player 31.0.0.112 及更早版本中存在越界读取漏洞，成功利用可导致信息泄露。（威胁等级中）
	较为活跃样本	Trojan[Exploit]/PDF.AGeneric	此威胁是一种以 PDF 为载体的木马类程序。该家族利用了 PDF 的格式溢出漏洞并释放出文件执行，它没有特定的行为，是以启发式检出的家族。（威胁等级中）
		RiskWare[RiskTool]/Win32.NetFilter	此威胁是一种会安装浏览器扩展插件的风险软件类程序。该家族样本在执行后会安装浏览器扩展程序并更改主页，同时在启动项中添加自身。还会注入其他进程，让自身难以清除。（威胁等级低）
		RiskWare[Downloader]/NSIS.SoftBase	此威胁是一种具有下载行为的木马类程序。该家族的样本使用 Nullsoft 安装程序打包器，在执行后会启动下载器在后台下载恶意代码文件。（威胁等级中）
		Trojan[Backdoor]/PHP.Agent	此威胁是一种以 PHP 页面为载体的且有后门行为的木马类程序。该家族的样本在执行后会开放一个后门给攻击者，在后台接受攻击者的命令并执行。（威胁等级中）
		RiskWare[Downloader]/Win64.Wajam	此威胁是一种具有下载行为的风险软件类程序。该家族的样本基于 64 位操作系统，会在执行后启动一个下载器，在后台下载其他恶意代码文件并执行。（威胁等级中）

2018 年：数据泄露最严重的年份之一

Jai Vijayan/ 文 安天技术公益翻译组 / 译

在 2018 年的前九个月，各机构报告了 3676 起数据泄露事件，涉及的记录超过 36 亿条。

一份总结 2018 年前九个月数据泄露事件的新报告指出，对于各机构来说，2018 年又是艰难的一年。

今年 1 月 1 日至 9 月 30 日期间，各机构报告的数据泄露事件比去年同期下降了 8%，泄露的记录数量则下降了 49%。尽管如此，各机构仍然报告了 3676 起数据泄露事件，涉及的记录超过 36 亿条。

根据已公开的数据泄露事件，采用自动化、自有处理方法或者其他办法，Risk Based Security 公司的分析结果显示：自 2005 年以来，2018 年全年的数据泄露事件数排在第二位，而其对应的泄露数据总量则排在第三位。

今年有 7 起事件泄露的记录量超过了 1 亿条。在所有被泄露的记录中，10 起规模最大的事件占了 80 % 以上。今年遭受重大数据泄露的公司包括 Facebook，Under Armour，Ticketfly 和 Hudson's Bay Company。

与去年同期相比，2018 年前九个月的数据泄露事件数量和泄露的记录数量都有所减少，这可能是因为，攻击者将很大一部分精力放在了挖矿活动上。直到 9 月底，也没有爆发像 2017 年“魔窟”（WannaCry）和 Petya/NotPetya 的灾难性事件。但这并不意味着威胁减少了。

“数据泄露问题不会消失；也没有好转。”Risk Based Security 公司执行副总裁因加·顾德金（Inga Goddijn）说，“窃取敏感和机密数据仍然可以赚钱。”

尽管监管压力越来越大，但是今年，各机构首次发现与公布数据泄露的时间间隔几乎没有缩短。在 2017 年，各机构公布数据泄露的平均间隔是 47 天；而今年这一数字为 47.5 天。

虽然各机构在数据泄露检测和响应方面进行了大量投资，但是他们大多是在收到外部通知后才发现数据泄露的。Risk Based Security 指出，在报告的 3676 起事件中，只有 483 起（13% ）是各机构自己发现的。超过一半的数据泄露事件（2171 起），涉事机构都是在收到第三方通知后才得知数据泄露的。

顾德金说：“绝大多数泄露事件都是外部发现的，例如执法部门或银行检测到了诈骗活动，然后提醒各机构注意。除非各机构能够从内部更快地检测到数据泄露，否则他们在数据泄露的报告方面不会有太大的改进。”

正如多年来的情况一样，对各机构的数据来说，内部人员是最大的威胁。Risk Based Security 公司采用“舞弊”（fraud）一词，来描述内部人员非法访问数据的恶意活动或非技术方法。该公司称，在数据泄露事件中，内部人员的“舞弊”占了近 36%。

事实上，今年发生的一些最具破坏性的事件，源于内部人员售卖包含敏感数据的数据库，顾德金说。前九个月，在涉及知识产权的 51 起数据泄露事件中，有 30 多起源于各机构的内部人员。除了恶意活动之外，许多机构的员工和具有内部访问权限的人员对资产处理不当，也会导致数据泄露。

电子邮件地址、口令、姓名和地址是最常被泄露的数据类型。但是，18% 的泄露事件涉及社保号，15%涉及信用卡数据，11%涉及出生日期。

虽然内部人员泄露了大量记录，但是外部黑客攻击仍然是大多数机构遭受安全事件的主要原因。

顾德金说：“通常情况下，黑客攻击出于经济动机，无论是窃取并售卖数据，还是利用系统访问权限执行其他操作来获取收入。”她补充说，外部黑客行为也有其他动机，包括政治动机和好奇心等。

今年，在遭受数据泄露事件的各机构中，约有 35% 没有或未能公布受影响的记录数量。考虑到目前的监管压力，这一点让人惊讶。

讽刺的是，各机构拒绝公布数据泄露的规模，会导致更严重的后果。实际上，超过 48 % 的事件泄露的记录数量在 1 到 1000 条之间。“我们已经习惯了在新闻头条上看到数十万甚至数百万条的记录泄露事件。当遭泄露的记录数量‘不予公布’时，人们倾向于往最坏的情况考虑。”她指出。

原文名称	2018 On Track to Be One of the Worst Ever for Data Breaches
作者简介	Jai Vijayan。Jai Vijayan 是一位自由撰稿人。
原文信息	2018 年 11 月 12 日发布于 Dark Reading 原文地址 https://www.darkreading.com/vulnerabilities---threats/2018-on-track-to-be-one-of-the-worst-ever-for-data-breaches/d/d-id/1333252
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。