安天发布《Beapy 挖矿木马分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Beapy 的恶意软件。这种挖矿木马主要借助钓鱼邮件进行传播，一旦受害者点击邮件附件中的 Excel 文档，Beapy 就会释放“双脉冲星”后门，并利用“永恒之蓝”漏洞在内网中传播扩散。Beapy 不仅利用“永恒之蓝”漏洞进行传播，还会使用工具 Mimikatz 来收集和使用受感染计算机的口令，以便操纵整个内网网络。

Beapy 由 Python 和 PowerShell 组件组成，当受感染计算机安装“双脉冲星”后门后，就会执行 PowerShell 命令，与 C2 服务器进行连接，并下载一个门罗币挖矿程序。之后 Beapy 会使用“永恒之蓝”漏洞利用工具进行内网传播，重复此过程，最终导致内网主机大面积感染该恶意软件。虽然该恶意软件不会窃取用户数据，但感染该恶意软件会造成诸多不良影响。如设备性能的下降、电池过热、设备老化、无法使用等，影响工作效率导致生产力下降。增加基于 CPU 使用量计费的云计算业务花销、增加电力使用量，导致 IT 成本上升。此外，感染该挖矿木马后的清除程序比较繁琐，很大情况下还会出现内网传播的情况。

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类挖矿木马的鉴定；安天智甲已经实现了对该挖矿木马的查杀。

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、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、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	f5ab73390a126bc8c2326f0f9dd72651294b0ee664afdc9c844fc6e77dddee02
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	159 KB
MD5	F79CB9D2893B254CC75DFB7F3E454A69
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
判定依据	BD 静态分析

完整报告地址：https://1.119.163.6/vue/details?hash=F79CB9D2893B254CC75DFB7F3E454A69

◆ 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

◆文件操作

操作	文件路径
新建	c:\windows\system32\svhost.exe

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.121	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.121	1025
0.0.0.0	68	255.255.255.255	67
192.168.122.121	137	192.168.122.255	137
192.168.122.1	67	192.168.122.121	68
192.168.122.121	123	13.65.245.138	123
192.168.122.86	137	192.168.122.121	137

◆进程监控

PID	创建	命令行
1384	target.exe	"c:\443e25ac33f74fbb8dc4cd250e0f5b33\share\target.exe"

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 09 日 (总第 199 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

安天集团：把党建作为企业发展精神动力 做中国网络空间的保卫者

编者按：近日，哈尔滨新闻联播系列报道《党建在基层》，以“把党建作为企业发展精神动力 做中国网络空间的保卫者”为题对安天集团进行了报道。安天集团党委宣传委员刘雪、党委纪检委员王海江、党委办公室主任薛正光接受了记者的采访。

党员“流动”而不“流失”

几年来，安天集团党委把党建作为企业发展的精神动力，强化党组织的核心功能，发挥党员先锋模范作用，形成以党建促进企业发展的良好局面。安天集团员工平均年龄 28 岁，党员大多数为 80 后、90 后。集团党委结合自身实际主动占领网络虚拟阵地，创建“网上党建工作”新模式，运用党务 APP、内部信息系统、多地同步视频会议等方式，使“三会一课”、主题党日和民主评议等组织生活在网上得到延伸拓展。通过网络平台开展活动、沟通思想、交流业务，让 70 余名外地分公司的党员能够经常感受到党组织的“辐射”作用，实现党组织与党员之间的顺畅沟通，让党员“流动”而不“流失”。

刘雪：“通过网上党建工作，我们希望能让党员在业余时间学、工作闲暇学，时时刻刻利用碎片化的时间把党的方针政策学习好，把公司的历史文化领略好，把自己的岗位职责掌握好。”

“线上党建”和“线下党建”有机结合

安天不断提高党建工作专业化水平。近年来，集团党委在企业打造党组织公开设立、公开聘用、公开活动，党务工作人员纳入公司中层、活动经费纳入公司预算，党员技术骨干奖励纳入公司福利的“三公开三纳入”党建工作机制，积极开展“把党员培养成生产技术骨干，把技术骨干培养成党员，把党员中的技术骨干推荐到公司管理层”的“两培一推”活动，让党员站前台、唱主角，激发公司员工实在实干、想为愿为的内生动力。安天还采取党委会成员与法人治理结构的“双向进入、交叉任职”，使党委集体决策意图能够贯穿到公司决策执行和监督的各环节，近年来集团党委提出的合理化建议均被公司采纳。截至目前，集团公司技术创新项目已向国家知识产权局提交专利申请 957 项，获授权专利 322 项。

王海江：“作为党员，就代表着一份责任和担当。这样就要求对待每一份工作都要做到脚踏实地。通过党员在企业、在组织中任职可以充分发挥党员的先锋模范带头作用，使党员能够深入到群众，更好地为群众服务，体现党的优越性。”

党建引领聚合力 红色引擎促发展

十几年来安天始终跟随党的步伐，坚持威胁检测技术的自主创新，在业内积淀了深厚的技术优势和良好口碑。党建为企业的快速发展插上了红色引擎、注入红色力量。

薛正光：“安天作为国际、国内知名的网络安全企业，今后将按照关于加强和改进非公有制企业党的建设工作的意见要求，深入扎实地开展企业、党的各项工作，为推动企业的发展提供强大的精神动力和组织保证。”

Android 智能手机容易受到高级短信网络钓鱼攻击

研究人员发现某些 Android 智能手机中存在高级网络钓鱼攻击的可能性，其中包括三星、华为、LG 和索尼。在这些攻击中，远程代理可以欺骗用户接受新的电话设置，例如，通过受攻击者控制的代理路由的所有 Internet 流量。该攻击向量依赖于称为空中（OTA）供应的过程，该过程通常由蜂窝网络运营商用于将网络特定设置部署到加入其网络的新电话。但是，任何人都可以发送 OTA 配置消息。这种攻击流程使任何拥有廉价 USB 调制解调器的人都可以诱骗用户在手机上安装恶意设置。为了攻击一些易受攻击的手机，攻击者需要知道受害者的 IMSI 号码，这些号码可以通过具有 READ_PHONE_STATE 权限的 Android 应用程序中获得。

（原文链接：https://research.checkpoint.com/advanced-sms-phishing-attacks-against-modern-android-based-smartphones/）

每周安全事件

类 型	内 容
中文标题	Astaroth 木马利用 Cloudflare Workers 平台逃避检测
英文标题	Astaroth Trojan Uses Cloudflare Workers to Bypass AV Software
作者及单位	Sergiu Gatlan
内容概述	新的恶意攻击活动通过滥用 Cloudflare Workers 无服务器计算平台来积极分发新的 Astaroth 木马变种，以避免检测并阻止自动分析。Cloudflare Workers 是 Cloudflare 服务器上运行的脚本，允许用户执行任何 JavaScript 代码而无需担心基础架构维护。Cloudflare Workers 被 Astaroth 的运营者用作第三阶段感染步骤的一部分，首先是网络钓鱼电子邮件，包含混淆 JavaScript 代码的 HTML 附件并链接到位于 Cloudflare 基础架构后面的域名。此域名以 JSON 格式提供多种类型的有效载荷，允许攻击者为不同位置的目标快速更改恶意文件。并且为了避免被阻止，会基于文件类型分发给他们的潜在受害者计算机。
链接地址	https://www.bleepingcomputer.com/news/security/astaroth-trojan-uses-cloudflare-workers-to-bypass-av-software/

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.MobOk.b[pay,exp,rog] 2019-08-31	高	该应用程序伪装为系统应用，安装无图标，动态加载恶意子包，推送广告，通过注入恶意 js，私发订阅短信，植入收件箱短信，上传未知信息，会造成用户资费损耗，请卸载。
		Trojan/Android.MobOk.a[pay,sys,rog] 2019-09-02	中	该应用程序内嵌恶意代码，动态加载恶意子包，关闭 wifi，访问推广页面和付费订阅页面，私自订阅付费服务，会造成用资费损耗，请卸载。
		Trojan/Android.nicro.c[exp,rog] 2019-09-03	中	该应用程序捆绑恶意插件，会从远程服务下载其他未知插件加载，可能后台加载广告插件，造成用户资费损耗，建议卸载。
	较为活跃样本	Trojan/Android.Venus121Spy.a[prv,rmt,spy]	中	该应用程序是一款间谍软件，运行后联网下载恶意子包，窃取用户通话记录、手机序列号，sim 卡信息，私自录音、录像，并将用户隐私上传至指定云盘。造成用户隐私泄露，建议卸载。
		Trojan/Android.HoneyHunterSpy.a[prv,spy]	中	该应用程序是间谍软件，运行隐藏图标，私自上传短信、联系人、通话记录、位置等信息，造成用户隐私泄露，请卸载。
		Trojan/Android.BRATA.a[prv,rmt,spy]	中	该应用程序伪装为知名应用，运行隐藏图标，后台解析控制指令，窃取用户 Google 账号、手机固件信息，私自键盘记录，模拟键盘输入信息，造成用户隐私泄露，建议卸载。
		Trojan/Android.ConsoleSpy.a[prv,rmt,spy]	中	该应用程序是间谍软件，运行隐藏图标，接收远程指令，窃取用户短信、安装列表信息、启动截屏并上传该文件，会造成用户隐私泄露，请卸载。
		Trojan/Android.fonetracker.a[prv,spy]	中	该应用程序是一个名为 fonetracker 的间谍工具，伪装系统服务，可以通过设置隐藏图标，后台收集用户短信、邮件、位置、通话记录等隐私信息到远程服务器，造成用户隐私泄露，建议卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows VBScript 引擎远程代码执行漏洞（CVE-2019-1183）	高	Windows VBScript 引擎处理内存中对象的方式中存在远程代码执行漏洞。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员用户权限登录，那么攻击者就可以控制受影响的系统。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	Trojan/Win32.Reveton	中	此威胁是一个勒索软件家族。该家族被 Blacole 和 Axpergle 这两个 Exploit Kit 所利用。该家族的样本在执行后会加密系统中的文件，并在加密后全屏显示勒索信以索求赎金。该家族的样本会创建一个快捷方式放置在启动项中，确保每次开机的时候都会下载并执行这个勒索软件。
		Trojan[Monitor]/Win32.ActualSpy	中	此威胁是一种具有监视行为的木马家族。该家族的样本在执行后会监视并记录键盘按键，对屏幕进行截图并获取剪贴板的内容。
		RiskWare[Downloader]/Win32.Soft32	中	此威胁是一个具有下载行为的风险软件家族。该家族的样本在执行后会下载其他的恶意软件到用户的设备中，对用户的设备进行感染。
		RiskWare[RemoteAdmin]/Win32.RMS	中	此威胁是一个具有远程控制行为的风险软件家族。该家族可以对用户的设备进行集中管理，方便地进行远程控制。但对用户的隐私可能有潜在的泄露风险。
		GrayWare[AdWare]/Win32.SuperJuan	中	此威胁是一类具有窃密和远控行为的木马类程序。该家族的样本在执行后会驻留在启动项中，并在后台与 C&C 服务器通信回传数据，接受并执行对方发送的命令。

为何说“有条件访问”对企业很重要

Adam Case/ 文　安天技术公益翻译组 / 译

实施“有条件访问”（conditional access）是“零信任”战略的关键部分。但是请反思一下，对企业的访问是否总是有条件的：在用户输入用户名和口令的情况下，是否会向其授予对企业系统和数据的访问权限？诚实回答就可以了。“有条件访问”是指特定的网络安全管理方法。接下来，我们将介绍什么是有条件访问，以及为何说有条件访问对企业很重要。

在企业转向移动设备和云的趋势下，有条件访问是指：IT 安全团队使用一组自动化策略来验证设备和用户，以保护网络和数据的流程。这些策略可能涉及特定使用情境或各种因素，例如用户个人信息、设备的性质、时间、地理位置以及用户试图访问的数据类型等。鉴于此，“知情访问”（informed access）这一术语应运而生，用于描述下一级授权，即向系统告知特定用户是真实、合规和可信的，以便系统进行授权。

通过有条件访问，企业可以动态确定每个访问尝试的结果，甚至可以基于有效的风险评估和访问策略实时监督和控制每个会话。有条件或知情访问提供了一种可扩展的方式，可以解决用户或设备被认为可疑的各种场景。例如，用户从某个城市访问企业网络；一小时后，同一位用户（或看似同一位用户）却试图从地球另一端的另一个城市访问企业网络。在这种情况下，有效的访问策略就会阻止一小时后的那次访问。

更典型的例子是，合法用户使用安装了过时操作系统的设备来访问企业网络。访问解决方案能够检测到过时的系统，然后拒绝用户的访问。此外，访问解决方案还会告知用户更新操作系统，以便被授予访问权限，并提供更新操作系统的指导。这种自助服务流程的另一个优势是：减少用户对技术服务台的咨询，并且无需 IT 人员干预。

如何配置有条件访问策略

企业可以根据定义的条件，配置访问策略和规则。例如，企业可以使用软件提供商预定义的访问策略，也可以根据企业的特定需求创建自己的策略。

移动设备的访问策略，可能要求设备在公司的移动管理工具中注册（托管）。移动设备可以分为以下三类：

1. 在公司的移动管理工具中托管，并完全符合企业的 IT 策略；

2. 在公司的移动管理工具中托管，但是操作系统过时或因其他原因不合规；

3. 没有在公司的移动管理工具中托管。

企业可以根据移动设备的状态，以及用户尝试访问的系统或数据的敏感性，对这三种设备条件进行不同的处理。

企业可以采用多种访问策略和配置，以下示例简单介绍了如何应用这些策略。企业应根据用户试图访问的网络或数据，选择特定的策略。

- **低敏感数据。**允许托管设备（合规或不合规）的用户进行访问。但是，非托管设备的用户，必须通过额外的双因子身份验证（2FA）才能获得访问权限。
- **中等敏感数据。**允许托管、合规设备的用户访问。托管但不合规设备的用户必须完成 2FA 才能获得访问权限。非托管设备的用户将被阻止访问。
- **非常敏感的数据。**托管、合规设备的用户，通过 2FA 后可以访问。托管、不合规设备的用户和非托管设备的用户都会被阻止访问。

为云和移动世界提供便利

在如今的企业环境中，移动性和便利性对于企业的客户和员工都至关重要。即使不在公司，员工也希望像在线购物一样，能够快速和方便地访问工作相关的系统和信息。有条件和知情访问解决方案提供了一种系统的方法，能够以最少的 IT 参与、最快的速度和简单性，为用户提供快速、方便和安全的访问。

原文名称	What Is Conditional Access, and Why Does It Matter to You?
作者简介	Adam Case。Adam Case 是 IBM Security 云身份技术产品经理。
原文信息	2019 年 8 月 30 日发布于 Security Intelligence。 原文地址 https://securityintelligence.com/posts/what-is-conditional-access-and-why-does-it-matter-to-you/
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。