安天发布《Johnnie 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 Johnnie 的挖矿木马。该木马使用了 powershell 脚本以服务的方式启动，可以较好地隐蔽自身，取证人员很难发现其踪迹。

Johnnie 木马包含多个模块。Dropper 文件 cspsvc.exe 用于加载 powershell 脚本，我们称其为脚本 A。脚本 A 有多种功能，通过其参数可以看出，如 Start，Stop，Restart，Status，Setup，Remove，Service，SCMStart，Control 等。其会获取命令行参数以执行相关操作，会默认启动 setup，其中含有编译 C# 文件的功能，接着从 %fonts% 或 %SoftwareDistribution% 读取配置文件。Service 中包含加密部分，加密内容为一个新的 powershell 脚本，称其为脚本 B。其会新建一个用户，密码从配置文件中读取，然后从 msupdate.info 下载挖矿程序，释放加密的 powershell 脚本 C，此脚本是用于写入计划任务以达到其以多种方式实现持久化的目的。

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（Win 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 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	c765ba5eedcd87b6f98eb503df640f5a8b077d3a30f02c6019feec1b5a553981
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	7 KB
MD5	8790B6B2E718B21EFB581752EC1FAEF5
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Johnnie
判定依据	BD 静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=8790B6B2E718B21EFB581752EC1FAEF5

◆ 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

◆ 静态启发式检测

检测类型	检测点	详细说明
PE 结构	无版权信息	基于海量恶意代码和受信白名单文件名进行数据挖掘，正规软件厂商的文件基本包含版权信息。
PE 结构	非微软的版本信息	非受信厂商的版本信息。具有较低的受信级别。

◆ 常见行为

行为描述	危险等级
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）	★
获取驱动器类型	★

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
192.168.122.111	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.111	1025
192.168.122.111	137	192.168.122.255	137
192.168.122.111	138	192.168.122.255	138
192.168.122.155	138	192.168.122.111	138
192.168.122.111	137	192.168.122.155	137
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.111	68
192.168.122.111	123	13.65.245.138	123

安天周观察
安天官方微博 安天官方微信
主办：安天 2019 年 01 月 01 日 (总第 166 期) 试行 本期 4 版 微信搜索：antiylab 内部资料 免费交流

【铁流鏖战】第六届安天网络安全冬训营即将启幕

本届冬训营基本情况介绍

网络空间威胁对抗与态势感知研讨会暨第六届网络安全冬训营——“铁流鏖战”将于 2019 年 1 月 8、9 两日在哈尔滨太阳岛花园酒店举行。

在网络强国系列讲话中，习近平总书记先后提出了“全天候全方位感知网络安全态势”、“实现全天候全方位感知和有效防护”等工作要求。在今年的全国网络安全和信息化工作会议中，总书记进一步强调要“加强信息基础设施网络安全防护”、“加强网络安全信息统筹机制、手段、平台建设”、“加强网络安全事件应急指挥能力建设”，为网络安全发展指明了方向，“关口前移，防患于未然”更是提出了对网络安全防护的方法要求与效果指引。

本届冬训营以“**战术型态势感知指控积极防御；协同响应猎杀威胁运行实战化**”为主题，态势感知在积极防御体系中对于提供响应决策、支持保障业务弹性和风险控制至关重要。但当前在态势感知实践中，往往更偏重于面向策略调整的宏观态势感知，难以支撑有效积极防御体系。实践化运行的战术型态势感知能够为威胁对抗行动提供实时监控响应能力，指挥对网络潜伏威胁进行猎杀清除，在攻防时间周期上适应高速多变的攻击行动，提升网络安全防护工作的积极性和主动性。本届冬训营上，将有业内专家与安天工程师一同深入分析来自不同层级网空威胁行为体的攻击事件，进一步完善网络空间的敌情想定。分享网络安全实战化运行的心得体会和

战术型态势感知平台的实践探索，研讨如何协同响应猎杀高级威胁。

往届冬训营回顾

自 2014 年起，在相关领导部门和职能机构指导下，安天连续承办了五届网络安全冬训营，提出“直面实际威胁，推动价值落地”的活动导向。根据每一年度的网络安全形势和工作主题，安天为每届冬训营设定了四字营语，此前五届分别是：“凛冬将至”、“北风乍起”、“朔雪飞扬”、“冰峰屹立”和“红旗漫卷”。本届冬训营确定营语为“铁流鏖战”。

从 2016 年开始，为了让议题和内容更为聚焦，安天将冬训营主题化，决定将每届冬训营围绕一个核心主题进行。第三届冬训营主题为“情报的支撑，塔防的实践”，探讨了如何构建有效的纵深防御体系；第四届冬训营以“有效防护，价值输出”为主题，自我批判作为安全厂商和研究者的主观局限和技术优越感，回归安全技术为用户提供有效的防护能力和价值保障的本质；第五届冬训营主题为“敌情想定是前提，网络安全实战化”，旨在以客观充分的敌情想定为前提，以实战化作为网络空间安全防御的第一要求，让安全技术、产品与服务能够随时应对真实的威胁，为客户实现有效的安全价值。

在过去的几届冬训营上，我们邀请了一批来自客户、安全研究机构、知名大学和安全厂商的演讲嘉宾，同时也有安天的优秀工程师担任讲师，共同分享工作心得和前沿探索。对充分认识威胁挑战，让网络安全技术探索转化为客户价值产生了积极的作用，受到相关机构和行业领域专家的好评。

网络安全是当前大国博弈的焦点领域，是持续性对抗的领域。在网络强国战略思想的指引下，安天希望与您一道，携手共进，将网空防御力量打造成滚滚“铁流”，不惧艰险，“鏖战”强敌！（更多信息请登录冬训营官网：wtc.antiy.cn）

每周安全事件

类 型	内 容
中文标题	黑客利用虚假亚马逊订单活动传播 Emotet 木马
英文标题	Is that you Amazon?
作者及单位	EdgeWave
内容概述	EdgeWave 威胁检测中心发现一项新网络钓鱼活动，钓鱼邮件首先会伪装成合法亚马逊订单，并要求用户确认。用户点击确认按钮后，随即下载 Word 文档，该文档被打开后，随后就会触发位于印度尼西亚的宏，并下载名为 keyandsymbol.exe 的文件，即 Emotet 银行木马，Emotet 将通过在美国休斯顿和兰辛的受感染服务器下载其它组件。Emote 会在后台静默运行，进行键盘记录、窃取帐户信息及其它活动。
链接地址	https://www.edgewave.com/phishing/is-that-you-amazon/

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.HdsSmspay.a[pay,exp] 2018-12-24	该应用程序中包含恶意代码，安装后无图标显示，后台拦截特定短信，联网获取订阅信息，私自发送订阅短信。造成用户资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.LockScreen.bv[rog,lck] 2018-12-25	该应用程序包含恶意代码，运行后会锁定屏幕并勒索用户来进行付费解锁，影响用户手机的正常使用，建议卸载。（威胁等级中）
		Trojan/Android.FakeInst.ff[pay,fra] 2018-12-26	该应用程序伪装色情应用或正常应用，私自发送或拦截短信，造成用户资费损耗，建议卸载。（威胁等级中）
	较为活跃的样本	RiskWare/Android.repackKbackup.a[rog]	该应用程序非官方应用，经过重打包处理，可能被恶意篡改并已植入广告，存在一定的使用风险，建议卸载该应用，下载安装官方正版应用。（威胁等级低）
		RiskWare/Android.pubgtool.a[rog]	该应用程序为 PUBG 游戏辅助软件，运行后会向系统请求 root 权限，可能存在一定安全风险，请谨慎使用。（威胁等级低）
		G-Ware/Android.CoinMiner.d[exp,rog]	该应用程序伪装系统应用，运行后隐藏图标，后台私自挖矿，影响用户正常使用，请卸载。（威胁等级中）
		RiskWare/Android.PettygainVpn.a[fra]	该应用程序使用开源代码，运行后通过配置文件利用运营商漏洞，伪装流量，开启 VPN。请用户谨慎使用。（威胁等级低）
		Trojan/Android.Delta.a[prv,exp]	该应用程序运行后隐藏图标，拦截窃取用户短信，窃取用户手机号码，监听用户通话，窃取来电号码，并将相关隐私信息联网上传。造成用户隐私泄露，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	Microsoft PowerPoint 安全漏洞（CVE-2018-8628）	当 Microsoft PowerPoint 软件无法正确处理内存中的对象时，就会触发该漏洞。攻击者必须诱使用户使用 Microsoft PowerPoint 打开经特殊设计的文件，才能利用此漏洞。成功利用此漏洞的攻击者可以在当前用户权限下执行恶意代码。（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/MSIL.AGeneric	此威胁是一种采用 MSIL 中间语言编写的具有广告行为的灰色软件家族。该家族根据通用定性进行分类，这类恶意代码没有统一的行为与功能，是以通用定性策略定性进行的恶意代码分类。（威胁等级低）
		Trojan[Downloader]/Win32.Morstar	此威胁是一种可以连接网络下载推广应用的木马家族。它会下载恶意代码和广告软件到感染者的计算机中，占用系统资源，影响用户使用。（威胁等级中）
		GrayWare[AdWare]/Win32.Midia	此威胁是一种有广告行为的灰色软件类程序。该病毒家族运行在 32 位平台下，可以监视感染者计算机上浏览器的活动，并在网页中注入代码，修改计算机注册表以实现开机自启等功能。（威胁等级中）
		RiskWare[RiskTool]/Win32.SpeedUpMyPC	此威胁是一种风险软件家族。该家族样本运行后连接网络下载并安装工具栏，该软件可以在用户访问网页时弹出广告，占用系统资源，影响用户使用。（威胁等级低）
		RiskWare[Downloader]/Win32.Somato	此威胁是一种具有下载行为的风险软件类程序。该家族样本运行后，会在用户访问网页时弹出广告，占用系统资源，影响用户使用。（威胁等级中）

保障“智慧城市”的安全和连续运行

Oussama El-Hilali/ 文 安天技术公益翻译组 / 译

如今，几乎我们生活中的每一个方面都是由新兴技术支持的，包括从预测分析、人工智能到物联网（IoT）的各种技术。我们先是有了智能手机，后来又有了智能手表，现在则有了“智慧城市”。

目前，世界上一半以上的人口居住在城镇。到 2050 年，这一比例可能会增加到 66%。因此，各城市需要部署解决方案，以有效管理其基础设施，应对不断增长的人口压力，同时又能跟上现代化进程。

智慧城市能够提供很多便利，例如公用设施和智能交通系统的无线连接。通过物联网，智慧城市可以提供有效和创新的解决方案，以应对不断增长的挑战。例如，如果启用了传感器的交通信号灯出现故障，维护人员就会及时收到消息，这样能够保证公共安全并节省宝贵的时间和资金。

智慧城市的安全漏洞和风险

显然，启用物联网的城市能够为人们提供巨大的便利。但是，这些便利伴随着一系列挑战和风险，安全风险就是其中之一。当然，城市管理员会试图阻止攻击；但是，他们也有可能出现疏忽——完全依靠他们就太天真了。历史证明，即使安全措施存在非常小的漏洞，也会被犯罪分子迅速识别和利用。在这方面，智慧城市也不例外。

物联网正在迅速发展，但是却没有得到足够的保护。智慧城市技术正是依赖于数字网络的，因此，网络犯罪分子可以远距离利用数字网络的各种漏洞。

由于软件的安全性不足，很多智慧城市系统只具有最低程度的端到端安全性——很多设备都低估了部署环境的安全风险以及用户社区的规模。市政资金紧张，预算不足导致各城市经常使用多年未升级的老旧系统，因此很容易遭受网络攻击。

网络攻击或极端天气（如风暴或大雨），可能会导致数百万居民失去电力供应。对智慧城市来说，这些都是非常真实的威胁。此外，在这些超级互联的环境中，服务中断可能会产生级联效应。例如，如果电网受到攻击，家庭、工作场所和各种基础设施就会断电，导致不说千万级，但是至少也有几十万的居民在数小时甚至数天内无法供电或供热。这类似于乌克兰在 2015 年遭受的“黑色能量”（BlackEnergy）网络攻击——黑客攻击了电厂系统，造成停电，导致整个城市的 23 万名居民无法供电或供热。（译者注：参见安天对“黑色能量”的分析报告 http://www.antiy.com/response/A_Comprehensive_Analysis_Report_on_Ukraine_Power_Grid_Outage/A_Comprehensive_Analysis_Report_on_Ukraine_Power_Grid_Outage.html；http://www.antiy.com/response/BlackEnergy/BlackEnergy.html）

保障智慧城市连续运行的预防措施

过去，解决攻击或服务中断的标准方法是“恢复”，但是现在，这种方法已经不足以保护我们的安全了。

即使是最新和最具弹性的技术也无法完全消除安全风险和漏洞，因此，如果我们不采取预防措施，智慧城市就会面临风险。那么，当安全风险和漏洞出现时，我们应该如何应对以保障智慧城市的连续运行呢？

随着各城市不断采用智能技术，我们应该将数据安全作为优先事项，这一点很重要。如今，智能设备在家庭中日益普及，这些设备生成大量新的数据流，可以为智慧城市服务提供信息——前提是这些信息是安全的。例如，智能家居的安全监控探头记录的实时视频，可以为警方提供线索。但是，这也为网络攻击者入侵家庭设备提供了机会，可能会给家庭带来网络层面的安全和连续运行问题。很多智能设备基本不具备安全功能，因此，使用这些设备的城市系统很容易遭受攻击，使用这些设备的家庭的在线隐私也会受到侵犯。

云技术的引入有助于保障智慧城市的连续运行——其系统可以迅速备份和恢复。启用云还能为关键系统提供“物理隔离”——当这些系统遭到黑客攻击或面临风险时，可以强行将其关闭。这样，我们就有时间修复漏洞了，有助于防止更严重的损坏并恢复运行——这样不仅能够避免大规模服务中断，还能在服务中断后迅速恢复。

随着智慧城市从概念转为现实，保护城市的基础设施变得越来越重要。如果决策者不能实施正确的流程来保护基础设施，公众就会面临风险。虽然部署安全解决方案会有所帮助，但是，以连续运行为框架构建弹性恢复能力才是智慧城市的发展方向。我们必须投资于正确的解决方案，确保城市能够迅速恢复和运行（例如迅速恢复供热和供电）——除此之外，没有任何可替代方案。

提前对云备份和灾难恢复进行高质量的投资势在必行。采取主动而非被动的方法，有助于保护城市系统的安全，使其在可预见或不可预见的攻击和服务中断中保持弹性恢复能力。

原文名称	Delivering security and continuity for the cities of tomorrow
原文作者	Oussama El-Hilali.Oussama El-Hilali 是 Arcserve 公司的产品副总裁。
原文信息	2018 年 12 月 18 日发布于 Help Net Security 原文地址 https://www.helpnetsecurity.com/2018/12/18/delivering-security-smart-cities/
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。