安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 04 月 02 日 (总第 129 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

安天获国家计算机病毒应急处理中心 2017 年度“优秀技术支持单位”称号

日前，国家计算机病毒应急处理中心授予安天“优秀技术支持单位”荣誉称号，以表彰安天在 2017 年度的信息通报工作中做出的支持与贡献。

安天凭借 18 年的技术积累及在威胁检测、海量恶意代码分析体系、高级持续性威胁分析等方面的分析与检测能力，多次在国家重大网络事故和网络安全事件的应急响应中发挥了关键作用。在红色代码、口令蠕虫、心脏出血、破壳、魔窟等重大安全威胁和病毒疫情方面，提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动，进行了深度的解析，对捍卫国家主权、安全和发展利益形成了有力的支撑。参加了十七大、十八大、十九大、2010 年起的历届两会、北京奥运会、上海世博会、广州亚运会、2014 年 APEC 会议、9.3 抗战胜利日阅兵、G20 峰会等重大活动的安保工作，并荣获重大活动信息安全保卫工作突出贡献奖。

未来，安天将继续发挥自身优势，继续与各行业主管部门及国家计算机病毒应急处理中心保持密切协作和配合，对于新发现的威胁及时进行信息报送，为网络与信息安全保驾护航。

北京安天党支部组织全体党员召开党员工作会议

2018 年 3 月 29 日，北京安天党支部 (以下简称“党支部”) 召开党员工作会议，会议对 2017 年党支部的党建工作进行了总结，并制定了 2018 年党支部新的党建工作计划，召开了民主生活会，并对由海淀园工委评选出的“优秀共产党员”进行了表彰，同时为“党建之友”进行颁奖。

北京安天党支部书记陈淑兰表示，党建工作一直在路上，希望党员同志能充分发挥党员的先锋模范作用，以自身实际行动影响周围群众，帮助大家共同进步，壮大党组织。在理论方面积极与党中央靠拢，并组织大家一起对党的十九大修改后的党章进行学习。

在民主评议党员、党支部环节，各位党员同志对自身过去一年来的工作、学习进行了深入反思，并对 2018 年如何更好的进步进行了展望。全体党员均表示将积极参与党支部的理论学习活动，努力提升自身理论水平。

门罗币代码存漏洞，很容易被追踪

门罗币（Monero）是一个创建于 2014 年 4 月的开源加密货币，它着重于隐私、分权和可扩展性。

与比特币衍生的加密货币不同，门罗币基于 CryptoNote 协议，并在区块链模糊化方面有显著的算法差异。门罗币的模块化代码结构还曾得到过比特币核心维护者之一的 Wladimir J. van der Laan 的赞赏。

然而，来自普林斯顿、卡内基梅隆、波士顿和 MIT 的研究人员发现，在 2017 年 2 月门罗币修改代码前，这一货币存在隐私漏洞，相关交易很容易被识别身份。即使在代码修改之后，在交易中识别身份也比用户以为的要简单。这一设计缺陷让不法分子在交易中提取出用户信息成为可能。(**文章来源：** https://arxiv.org/pdf/1704.04299/)

仍有 20% 的 VPN 服务商未解决 WebRTC 漏洞问题

自 2015 年 1 月起，大约有 20% 的 VPN 方案提供商因为 WebRTC 漏洞泄漏用户 IP。但即便在今天，一些 VPN 厂商也并没有对此问题作出改进。

该问题是由安全研究员 Paolo Stagno（VoidSec）发现，他对 83 款 VPN 应用程序进行了安全审计测试，发现了旧版本的 WebRTC IP 泄漏问题。

Stagno 表示在他的调查过程中有 17 款 VPN 会通过网页浏览器直接泄漏用户的 IP 地址。具体的研究成果已经公开在 Google Doc 在线文档中。但 Stangno 表示，自己的工作并不是最完整的版本，因为他没有财力对所有的商用 VPN 服务进行测试。(**文章来源：** https://www.bleepingcomputer.com/news/security/many-vpn-providers-leak-customers-ip-address-via-webrtc-bug/)

每周安全事件

类 型	内 容
中文标题	微软 Meltdown 补丁引发 Windows 7 更大安全漏洞
英文标题	Meltdown Patch Opened Bigger Security Hole on Windows 7
作者及单位	Catalin Cimpanu
内容概述	1 月份来势汹汹的 Meltdown 漏洞到现在还余威未散。近日，瑞典 IT 研究人员发现微软在 2018 年 1 月发布的 Meltdown 补丁导致 Windows 7 出现更大的安全问题，可以让任意用户级应用读取操作系统内核的内容，甚至向内核内存写入数据。 简而言之，在 PML4 自引用条目中，User/Supervisor 权限位已设置为 User。这使得原本只能由内核本身访问的页表在每个进程中都可被用户模式代码获取。 据了解，微软在 3 月份的修复日修复了这个问题。Windows 7 和 Windows Server 2008 R2 尤其要注意确认，如果 1 月份安装了更新，那么也要尽快安装 3 月份的更新。
链接地址	https://www.bleepingcomputer.com/news/microsoft/meltdown-patch-opened-bigger-security-hole-on-windows-7/

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 9 个移动平台恶意代码和 4 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.arydigital.a[prv,spy] 2018-03-25	该应用程序运行后隐藏图标，窃取用户短信。联系人、通话记录、浏览器历史记录、地理位置等隐私信息，私自拍照、录音，并将用户隐私上传至服务器、造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.IPkik.a[rog,exp] 2018-03-27	该应用程序运行隐藏图标，后台私自通过 socket 连接指定服务器并接收指令，根据指令可以控制用户对指定网站发起 DDoS 攻击，造成用户流量消耗，建议卸载。（威胁等级高）
		Trojan/Android.MargaerySpy.a[prv,exp,rmt,spy] 2018-03-27	该应用程序运行后会隐藏图标，通过短信和网络进行远程控制，监听用户通话及录音，发送短信、拨打电话、上传图片信息等，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
		G-Ware/Android.HamrahMedia.a[pay,rog,exp] 2018-03-29	该应用程序运行诱导用户点击下载其他应用，付费提示不明显，后台私自发送付费短信，拦截短信，可能造成用户资费损失，建议卸载。（威胁等级低）
	较为活跃的样本	Trojan/Android.Joye.h[pay,exp,prv]	该应用程序运行后隐藏图标，上传用户硬件信息，后台联网获取支付信息，通过短信发送扣费短信，会造成用户资费损失，建议立即卸载。（威胁等级高）
		Trojan/Android.Hqwar.l[prv,exp]	该应用程序运行会激活设备管理器，隐藏图标，后台拦截短信，窃取用户银行相关隐私信息。会给用户带来经济损失，建议卸载。（威胁等级中）
		Trojan/Android.JsMiner.e[exp,rog]	该应用程序包含 js 挖矿脚本，运行后会私自执行挖矿脚本进行挖矿，影响用户手机正常使用，请立即卸载。（威胁等级中）
		Trojan/Android.Yzmg.b[exp,rog]	该应用程序伪装成系统应用，安装无图标，运行后私自下载恶意软件，后台推送广告，造成用户资费损耗，建议卸载。（威胁等级高）
		G-Ware/Android.FakeSexApp.f[pay,fra]	该应用程序伪装色情应用，诱导用户点击付费，后台拦截短信，实际跳转到搜狐视频网页，可能造成用户资费损失，建议不要使用。（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 Windows 远程协助信息泄露漏洞（CVE-2018-0878）	Microsoft Windows Remote Assistance 未正确处理 XML 外部实体，在实现上存在信息泄露漏洞，攻击者可利用漏洞获取敏感信息。（威胁等级高）
	较为活跃样本	Trojan[Dropper]/Win32.Miner	此威胁是一种可以释放比特币挖矿机的木马家族。该家族样本运行后释放恶意代码到本机并运行，连接网络下载比特币挖矿机，占用系统资源，影响用户使用。（威胁等级高）
		Trojan[Ransom]/Win32.VKonte	此威胁是一种可以加密用户数据并勒索赎金的木马家族。该家族样本运行后加密指定格式文件，向用户勒索金钱，可能会收集用户系统信息并回传至远程服务器。（威胁等级中）
		Trojan/Win32.Krepper	此威胁是一种可以下载恶意代码的木马家族。该家族样本运行后连接远程服务器下载恶意代码并运行，可能会窃取用户信息并回传。（威胁等级中）

防止加密货币挖矿攻击的七种方法

Jai Vijayan / 文　安天技术公益翻译组 / 译

最近，Crowdstrike 和其他几家安全厂商称被攻击者劫持系统挖掘门罗币及其他加密货币后，遭受了严重的应用程序和运营中断问题。在许多其他案例中，犯罪分子秘密地在网站上安装加密货币挖矿程序，劫持访问该网站的用户的系统。

与勒索软件和其他恶意软件不同，加密货币挖矿程序通常是合法的软件工具，并不总是能够被反恶意软件产品检测到。像其他许多可能有害的软件工具一样，加密货币挖矿软件主要对那些未遵循基本和经过长期验证的安全措施的企业造成威胁。这些工具像其他任何恶意软件产品一样传播，需要采取相同的措施来阻止。

以下是防御加密货币挖矿工具（以及其他任何恶意软件）需要遵循的最佳实践。

加强端点安全控制

强大的端点保护对于防止加密货币挖矿恶意软件至关重要，CrowdStrike 服务总监布莱恩·约克说。如果不希望加密货币挖矿工具在最终用户和主机系统上运行，请及时打补丁并妥善更新。约克指出，可以考虑使用广告拦截器，禁用 JavaScript 以及使用浏览器扩展；为远程访问实施多因子身份验证；将网络分段以限制横向运动。约克说，端点技术可以帮助检测和阻止与这些工具相关的加密货币挖矿软件和行为。“此外，一些先进的端点技术能够阻止使用无文件恶意软件技术的加密货币挖矿软件通过网络感染和传播。”

考虑实施集中式日志记录功能来检测、限制和捕获恶意活动，Secureworks 公司反威胁部门的高级安全研究员迈克·麦克莱伦补充说。识别出站加密货币挖矿流量的一种方法是使用受监控的出口点来管理出站网络连接流量，特别是使用非标准端口的任何未加密流量。

审查网站安全控制

犯罪分子经常在网站所有者不知情的情况下在网站上安装挖矿软件，然后劫持网站访问者的计算机资源来挖掘门罗币和其他加密货币。

“使用内容安全策略和类似安全机制的 web 服务器可以防止跨站点脚本和跨站点请求伪造的许多常见漏洞利用媒介。”High-Tech Bridge 首席执行官伊利亚·克罗琴科说。请确保你的管理员密码强效且独特，并尽可能实施双因子身份验证。他说，web 应用程序防火墙可以帮助减轻定制代码中未知漏洞的可利用性。“重要的是，持续的安全监控已经成为确保 web 应用程序安全的一种标准。有时候你或你的同事可能会忘记一些东西——但两个人的观察力一定会比一个人强。”

实施强大的访问控制

麦克莱伦说，对系统和应用程序凭证应用最小权限原则，并限制对授权用户和上下文的管理员级访问。“对于 Windows 系统，请考虑使用微软的本地管理员密码解决方案（LAPS）来简化和加强密码管理。”对可从外部访问的服务实施双因子身份验证。他说，与其使用标准端口和服务，不如考虑使用定制服务来实现远程管理等功能。

使用安全的第三方软件和组件

The Media Trust 首席执行官克里斯·奥尔森说，不要让存在漏洞的第三方代码破坏你的网站安全。审查所有为你的网站运营提供代码的合作伙伴，并将你的数据隐私政策传达给合作伙伴。他说，不要不好意思与那些不合规的供应商终止合作关系。“对所有已知合作伙伴的网站进行评估对于沟通期望和强化合规性至关重要，持续的网站监控是检测流氓代码且一旦其执行就可立即阻止的唯一方法。”

保护云帐户

BMC 产品管理副总裁丹尼尔·尼尔森说，黑客已经开始劫持大公司的公有云帐户来挖掘加密货币了。“企业应该实施政策自动化解决方案，例如 SecOps Policy Service，以持续监控、评估和修复容器堆栈。”

确保你可以检测到云盲点。“如今影子 IT 非常活跃，”纳尔逊说。即使 IT 部门知道在云中配置的所有服务器，他们也很有可能不知道安装在这些服务器上的所有软件，因此了解云使用的程度至关重要。

限制不必要的服务

如果不需要某个服务，请将其禁用，麦克莱伦说，包括 SMBv1 等内部协议。如果应用程序没有合法的业务功能，请将其删除。限制对无法删除但对大多数用户完全不必要的系统组件的访问权限，例如 PowerShell。

保护物联网网络

“数以百万计的用于处理或存储机密或个人信息的物联网设备甚至没有基本的密码保护选项，或者无法更改的硬编码的管理员密码。”克罗琴科说。物联网设备的 web 界面和开源组件往往充斥着可被利用的关键漏洞。

原文名称	7 Ways to Protect Against Cryptomining Attacks
作者简介	Jai Vijayan。Jai Vijayan 是一位经验丰富的技术记者，在 IT 新闻领域拥有超过 20 年的经验。
原文信息	2018 年 3 月 22 日发布于 Dark Reading 原文地址 https://www.darkreading.com/cloud/7-ways-to-protect-against-cryptomining-attacks/d/d-id/1331301
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。

安天发布《可卸载反病毒程序的勒索软件“AVCrypt”分析报告》

近日，安天 CERT（安全研究与应急处理中心）发现一例试图卸载反病毒程序的勒索软件“AVCrypt”。该勒索软件运行后试图在加密计算机之前卸载现有的安全软件，删除包括 Windows Update 在内的一些服务，警告信息只有几个字母，因此安天分析人员认为它可能是一个 wiper。

“AVCrypt”运行时，会试图从受害者的计算机上删除已安装的安全软件。有两种方式，一种是单独针对 Windows Defender 和 Malwarebytes，另外一种是查询已安装的 AV 软件，然后尝试删除它们。首先，“AVCrypt”将删除正确运行 Malwarebytes 和 Windows Defender 所需的 Windows 服务，操作命令为“cmd.exe /C sc config "MBAMService" start= disabled & sc stop "MBAMService"& sc delete "MBAMService"”。然后查询在 Windows 安全中心注册的 AV 软件并尝试通过 WMIC 删除：“cmd.exe /C wmic product where (Vendor like "%Emsisoft%") call uninstall /nointeractive & shutdown /a & shutdown /a & shutdown /a”。同时，在该勒索软件启动时会试图删除各种 Windows 服务，包括：“MBAMService MBAMSwissArmy MBAMChameleon MBAMWebProtection MBAMFarflt ESProtectionDriver MBAMProtection Schedule WPDBusEnum TermService SDRSVC RasMan PcaSvc MsMpSvc SharedAccess wscsvc srservice VSS swprv WerSvc MpsSvc WinDefend wuauserv”，这些服务被删除后 Windows 仍然能够正常工作，但可能会出现问题。此外，勒索软件创建的警告信息不提供任何联系信息，只有“lol n”字样，因此分析人员认为该勒索软件并未开发完成，而是正在测试中。

安天 CERT 提醒广大网络使用者，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及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。目前，安天追影产品已经实现了对该类恶意代码的检出。

勒索软件

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述勒索软件进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 YARA 自定义规则鉴定器、文件来源信息分析鉴定器、文件元数据分析鉴定器、数字证书鉴定器、静态分析鉴定器、动态行为（默认环境）鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。

最终依据动态行为鉴定器、静态分析鉴定器将文件判定为勒索软件。

概要信息

文件名	58c7c883785ad27434ca8c9fc20b02885c9c24e884d7f6f1c0cc2908a3e111f2
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	2.91 MB
MD5	248144F924D49B37312DA171F14F4131
病毒类型	勒索软件
恶意判定 / 病毒名称	VCS/PEStruct.NoVersion
判定依据	静态分析

运行环境

操作系统	内置软件
Windows XP 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	★★★
删除自身	★★★★
关闭 UAC	★★★

常见行为

获取计算机名称	★
设置调试器权限	★
关机	★
查找指定内核模块	★
创建特定窗体	★
查找特定窗体	★
获取驱动器类型	★
获取主机用户名称	★
打开自身进程文件	★
读取自身文件	★
释放 PE 文件	★★
.....	.....

文件扫描

文件名	文件 MD5
1688	cmd.exe
1704	cmd.exe
.....	.....