安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 03 月 19 日 (总第 127 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

肖新光委员：关键信息基础设施防护进入全面提速期

—— 本文为全国政协委员、安天首席架构师肖新光接受新华社《经济参考报》采访的全文。

随着网络技术的不断发展，除互联网+、云计算、大数据等话题引发热议外，网络安全的重要性也提上日程。全国政协委员、安天实验室首席架构师肖新光在接受《经济参考报》记者专访时表示，加强关键信息基础设施的网络安全保障正在进入全面提速期。

“从过去来看，我们对安全的改进更多的是以网站涂鸦篡改、DDoS 攻击、蠕虫传播等比较容易感知到的风险为牵引，对于面向重要信息系统特别是关键信息基础设施的入侵渗透、环境预置、信息窃取乃至进一步的信息战等深度风险缺少系统性的认识与应对。”肖新光指出，此前网络安全法的正式通过，全面界定了网络安全的层次，特别是把关键基础设施的防护要求，以立法的形式确定起来。

肖新光认为，我国在网络安全技术方面相对而言技术门类齐全，没有明显短板。国内网络安全能力型安全厂商在反病毒引擎、主动防御、移动安全、安全大数据分析等单点上已经达到或接近国际先进水平。“若干单点技术优势不值得我们妄自尊大，但也不应妄自菲薄。网络安全的下一步发展，还是要尊重网络安全的整体性、动态性、开放性、相对性、共有性，避免按照割裂、静态、封闭、绝对、孤立的错误思路进行安全实践和投入，须落实中央‘全天候全方位感知网络安全态势和有效防护’的工作要求，实践动态、综合的防护理念，达成安全和发展同步推进。”他说。

肖新光表示，未来将是网络安全的大投入、大建设期。从发达国家的经验看，一方面要发挥立法作用，强调网络安全能力的有效性，形成优胜劣汰机制，网络安全在信息化中的投入占比会不断提升；另一方面，更需要一系列“超级工程”来形成高点能力，以应对复杂的安全挑战和地缘风险。网络安全为人民，网络安全靠人民。网络安全不只是主管和职能部门的事情，也不只是安全厂商的事情，它和每一家机构、每一个用户都息息相关。协同会商，分析敌情，共同摸索，形成合力，每个行业、每个单位、每个区域都能形成既符合安全基本规律，又适配自身特点的有效安全能力。

关于网络安全人才培养问题，肖新光认为，首先，网络安全人才培养必须增强法制教育、道德教育以及爱国主义精神教育，网络安全是一个非常特殊的领域和行业，需要以底线和操守为前提。其次，网络安全需要形成合理的人才结构体系，网络安全本质是人和人之间的对抗，但是它的表现形式却是依托于综合工程体系和能力体系进行博弈，是体系化对抗模式，支撑这种体系化对抗的，是先进可靠的基础能力、产品体系、服务体系、综合规划和综合管理能力，因此这就需要大量的品质纯良、遵守底线，且具有相对成熟职业技能的架构师、开发工程师、分析工程师、服务工程师、配置工程师等。

此外，肖新光还建议，在国家正在进行和将要进行的相关大型网络安全工程建设中，可以考虑在黑龙江等有较好网络安全产业基础的省份，建立镜像节点或子工程体系，从而强化当地产业和人才基础。

安天发布《“挖矿”恶意代码肆虐，安天智甲有效防护》报告

随着虚拟货币被疯狂炒作，疯狂的“挖矿”行为也伴随而来。“挖矿”的本质是计算符合条件的 hash 值并返回，采用的方式为爆破式计算，主要特征表现为消耗主机资源，浪费用户电量。因“挖矿”活动的收益相对稳定，难度较低，且“挖矿”过程中不需要投入其他精力便可坐享其成，故“挖矿”活动日益兴盛。而虚拟货币的增值性和匿名性则促使了恶意“挖矿”活动的兴盛。

本报告分析了恶意“挖矿”的类型及投递方式，并给出了判别“挖矿”行为的方法及解决方案。若电脑经常卡顿、CPU 使用率莫名其妙居高不下；或浏览网页时，打开的明明是静态页面却很卡顿并出现 CPU 占用率过高的情况，便可能存在“挖矿”行为。面对恶意“挖矿”软件，安天智甲终端防御系统（英文简称 IEP）采用行为分析结合终端资源监控的防御方案，可有效防御恶意“挖矿”行为。

报告原文

每周安全事件

类 型	内 容
中文标题	远程桌面协议存在严重漏洞通杀所有 Windows 版本
英文标题	CredSSP Flaw in Remote Desktop Protocol Affects All Versions of Windows
作者及单位	Mohit Kumar
内容概述	近日，微软发布了 CVE-2018-0886 的补丁，该漏洞由 Preempt 的研究人员发现。该漏洞包含 RDP（远程桌面协议）和 Windows 远程管理（WinRMI）使用的凭据安全服务提供程序协议（CredSSP，该协议负责将凭据安全的转发到目标服务器）中的逻辑缺陷。攻击者可以采用中间人攻击的方式利用该漏洞，以实现在受害网络中未中招的计算机上远程运行代码的目的。 在很多真实的场景中，受害者的网络中存在有漏洞的网络设备，攻击者可使用该漏洞在网络横向移动甚至给城控安装恶意软件。目前 Preempt 还没有在野外检测到该漏洞的利用。 这是一个逻辑漏洞，影响目前所有的 Windows 版本。
链接地址	https://thehackernews.com/2018/03/credssp-rdp-exploit.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 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.Kxqp.a[exp] 2018-03-12	该应用程序运行后动态加载风险子包，有私自推送广告和更新下载行为，会造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.tttGRun.a[exp,rog] 2018-03-12	该应用程序是非官方应用，植入了恶意代码，运行后会加载恶意插件，后台私自加载广告，造成用户流量消耗，建议卸载。（威胁等级高）
		Trojan/Android.Silentio.a[prv,spy] 2018-03-13	该应用程序运行后隐藏图标，监听用户短信、通话记录和邮件信息并上传，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.DropboxSpy.a[prv,exp,rmt,spy] 2018-03-14	该应用程序运行后会隐藏图标，利用短信远程控制，拦截特定短信，根据短信指令上传短信信息、联系人信息、通话记录、位置信息以及设备信息等，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.BankInteza.a[prv] 2018-03-14	该应用程序伪装银行相关应用，运行隐藏图标，拦截短信，上传用户短信内容到指定网址，会造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.ASspy.a[prv,exp,spy] 2018-03-14	该应用程序是间谍件，私自拦截上传用户收件箱短信，访问指定网址，加载 js 脚本，私自点击，私发短信，可能用于订阅，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.asus.a[prv,exp] 2018-03-15	该应用程序伪装其它应用，运行会请求激活设备管理器，隐藏图标，后台联网推送广告，窃取用户短信信息，私自发送短信，造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.Locker.ae[rog,sys,lck]	该应用程序运行请求 root 权限，在系统目录安装勒索子包程序，之后重启手机并禁用 USB 连接，恶意置顶勒索界面，要求付费解锁，影响用户手机的正常使用，建议卸载。（威胁等级高）
		Trojan/Android.mspyonline.d[prv,rmt,spy]	该应用程序是一款间谍程序，运行后接收控制消息，窃取用户短信、通话记录、联系人、地理位置等隐私信息，并上传至云端。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 Windows 远程代码执行漏洞 CVE-2018-0886	微软凭证安全支持提供程序协议（CredSSP）中存在远程代码执行漏洞。 成功利用此漏洞的攻击者可以中继用户凭据并使用它们在目标系统上执行代码。CredSSP 是为其他应用程序处理验证请求的验证提供程序； 任何依赖 CredSSP 进行身份验证的应用程序都可能容易受到此类攻击。（威胁等级高）
	较为活跃样本	Trojan[Backdoor]/Win32.ZSpy	此威胁是一种可以窃取用户信息的木马类程序。该家族样本运行后连接远程服务器接受攻击者恶意操作，收集用户信息并回传。（威胁等级高）
		Trojan[Exploit]/SWF.SwfDrop	此威胁是一种可以利用漏洞的木马类程序。该家族使用 SWF 文件利用 Adobe Flash Player 相关的漏洞，具有连接网络发送和接收数据、读取和写文件到磁盘的功能。（威胁等级高）
		Trojan[Spy]/Win32.Tiny	此威胁是一种具有间谍功能的木马类程序。该家族的样本运行后会记录用户击键记录，获取屏幕截图并发送给远程服务器。（威胁等级中）

微软详述不同形式的加密货币挖矿程序

Kelly Sheridan / 文　安天技术公益翻译组 / 译

微软在一份新报告中探讨了合法和恶意加密货币挖矿程序在企业中出现的不同方式。

数字货币的未来可能还不明朗，但它们对网络犯罪的影响是很清楚的。加密货币改变了犯罪分子的动机和网空攻击的本质。在消费者不断探索数字财富新前沿的同时，网络犯罪分子和恶意软件开发人员也在探索。加密货币的匿名性及其价值的飙升吸引了威胁源，最典型的例子是，他们在勒索软件攻击中要求受害者支付比特币作为赎金。

与加密货币有关的犯罪活动推动了不同形式加密货币挖矿程序（也称矿工）的激增。微软 Windows Defender Research 团队的研究员发布了一份新报告，详述了各种加密货币挖矿程序及其在企业中的存在情况。研究人员解释说："挖矿是运行维护区块链账本所需的复杂数学计算过程。"挖矿本身并不是恶意的，但它确实需要大量的计算资源才能生成加密货币。许多个人和企业向设备投资，执行合法的挖矿。有些人则不希望进行这种基础设施投资，而是想方设法在其他人的计算资源中植入加密货币挖矿代码。

植入木马的加密货币挖矿程序

网络犯罪分子经常修改现有的加密货币挖矿程序，并通过恶意软件、社会工程手段和漏洞利用包将其投放到目标计算机上。微软表示，在 2017 年 9 月至 2018 年 1 月期间，平均每月有 64.4 万台机器遭到加密货币挖矿恶意软件感染。有些挖矿恶意软件更为复杂，利用漏洞利用包或自传播恶意软件进行传播。

"绝大多数攻击都是出于经济动机，并基于攻击者的投资回报率。"Proofpoint 公司威胁运营中心副总裁凯文·爱泼斯坦（Kevin Epstein）指出。在消费者安全意识不断增强的

情况下，勒索软件活动不再那么有利可图，许多犯罪分子开始转向加密货币挖矿程序，将加密货币挖矿代码整合到木马中来赚钱。

之前，漏洞利用工具包主要用于部署银行木马和勒索软件；现在，它们则用于传播加密货币挖矿程序。研究人员以 DDE 漏洞利用包为例进行说明：该恶意软件的一个样本作为恶意 Word 文档传播，能够执行 PowerShell 脚本并下载植入了木马的门罗币加密货币挖矿程序 XMRig。一些犯罪分子使用社会工程手段，即利用一个名为"flashupdate"的、伪装成 Flash Player 的恶意文件（该恶意文件也使用 XMRig 的修改版本）。

一旦加密货币挖矿程序进入目标机器，其目标就是待在那里。"对于加密货币挖矿程序来说，持久性是一个关键因素，"微软研究人员解释说，"它们留在内存中且未被发现的时间越长，利用被盗的计算资源挖矿的时间就越长。"犯罪分子使用计划任务、自动启动注册表项、代码注入和其他无文件技术来规避检测，从而持续驻留在计算机中。

基于浏览器的挖矿程序

一些加密货币挖矿脚本托管在网站上，这种趋势也被称为"挖矿劫持"（译者注：cryptojacking，即劫持用户的设备，利用 CPU 或其他处理器进行挖矿）。随着犯罪分子对加密货币的兴趣不断增加，这种趋势愈演愈烈。这些网站利用访问者的计算能力来挖掘加密货币。有的网站会提示访问者挖矿脚本的运行，有的则不会。

为防止访问者离开网站，一些恶意网站托管视频流。研究人员还发现，与加密货币挖矿程序一样，技术支持诈骗网站的数量也翻倍了。访问者被弹出窗口吸引并留在网站上，此时，犯罪分子会在后台利用其计算资源挖矿。

非法使用合法挖矿程序

企业面临的一个日益严重的问题是：人们在企业环境中使用合法但未经授权的加密货币挖矿程序。这些挖矿程序导致了电力消耗和成本，对安全团队来说更难检测（因为它们不是通过传统的感染媒介到达计算机的）。

微软在 2018 年报告称，运行 PUA（potentially unwanted application，可能有害的应用程序）防护的 Windows 企业用户在 1800 多台企业机器上发现了加密货币挖矿程序。随着企业对这些程序的密切关注，这个数字预计会增加。PUA 不同于植入木马的挖矿程序（被视为恶意软件）和"有害软件"（被认为是有害的，因为它们在没有用户控制的情况下更改 Windows 设置）。安全管理员可以使用 PowerShell cmdlet 或 Microsoft Intune 配置默认情况下在 System Center Configuration Manager 中启用的 PUA 防护。

研究人员解释说，当用户试图安装符合特定条件的 PUA 时，Windows Defender 会阻止它们。这些主要包括捆绑了程序的软件、浏览器修改器和声誉不佳的程序。加密货币挖矿程序所占比例越来越大，其在 2017 年 9 月占 PUA 的 2%，2018 年 1 月则达到了 6%。

原文名称	Microsoft Report Details Different Forms of Cryptominers
作者简介	Kelly Sheridan。Kelly Sheridan 是 Dark Reading 的编辑
原文信息	2018 年 3 月 13 日发布于 Dark Reading 原文地址 https://www.darkreading.com/endpoint/microsoft-report-details-different-forms-of-cryptominers/d/d-id/1331266
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《远控木马“Olympic Destroyer”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注意到，一例在平昌冬奥会中使用的恶意代码比较活跃，名为“OlympicDestroyer”。据媒体报道，平昌奥运会的组织者证实，他们正在调查一起网络攻击事件，在正式开幕式之前暂时使 IT 系统瘫痪，关闭显示器，使 Wi-Fi 失效以及破坏奥运会网页，以致游客无法打印门票。

该恶意代码样本为 VC++ 编写的可执行文件，编译平台为 Visual Studio 2015 之后。样本运行后，一旦过了 60 分钟，它就清除 Windows 事件日志，重置备份，从文件系统中删除卷影副本，禁用 Windows 启动菜单中的恢复项目，禁用系统上的所有服务并重新启动计算机。同时它也可以连接网关服务器，窃取用户凭证，内网横向渗透攻击。当同时运行两个实例时，后运行的实例会创建 notepad.exe 进程，并对 notepade.exe 进行注入。注入后的 notepad.exe 会对原样本文件进行修改，修改后，样本文件会自删除。该恶意代码使用钓鱼邮件投放，钓鱼邮件的目标是冬奥会官方合作伙伴的网络，攻击者可能会去官方网站查找合作伙伴公司的名称，收集他们的域名及已知的电子邮件地址，并开始用钓鱼邮件轰炸他们。

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，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。目前，安天追影产品已经实现了对该类恶意代码的检出。

恶意程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述高级威胁进行有效检测，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。

最终依据静态行为鉴定器将文件判定为恶意程序。

概要信息

文件名	edb1ff2521fb4bf748111f92786d260d40407a2e8463dcd24bb09f908ee13eb9
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	1.78 MB
MD5	CFDD16225E67471F5EF54CAB9B3A5558
病毒类型	恶意程序
恶意判定 / 病毒名称	VCS/Instruction.PEEPOCheck
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	★★★

常见行为

查找指定内核模块	★
获取计算机名称	★
设置调试器权限	★
释放 PE 文件	★
从资源中释放 PE 文件	★
获取驱动器类型	★★
填充导入表（疑似壳）	★
打开自身进程文件	★★
读取自身文件	★
.....	.....

监控预警

PID	创建
0	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\jjbjz.exe
1812	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tbvsb.exe
1920	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp_kex.exe
436	dumprep.exe
.....	.....