安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 08 月 06 日 (总第 147 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

美国网络空间攻击与主动防御能力解析（八）

——用于漏洞利用的网空攻击装备

安天研究院

上期中，我们对美国国家安全局（NSA）和中央情报局（CIA）用于实现持久化控制的网空攻击性软硬件装备进行了展开介绍，呈现了美方对各类网络设备以及服务器与终端节点全方位覆盖的持久化能力。在本期中，我们将对美方用于实现漏洞利用的网空攻击装备进行介绍，揭示出美方丰富的漏洞储备及强大的漏洞利用能力。

根据我国《信息安全技术安全漏洞等级划分指南》，漏洞即计算机信息系统在需求、设计、实现、配置、运行等过程中，有意或无意产生的缺陷。漏洞一旦被恶意主体所利用，就会对计算机信息系统的安全造成损害，或者干扰系统正常运行，或者非法控制系统并实现包括提升权限、横向移动、持久化等操作。从信息技术开发与运维的质量控制角度来看，随着技术快速变得复杂化，软硬件产品存在漏洞的情况将会变得日益失控。在全球范围内，每年人们都会从不同的平台、系统和软件中挖掘出数量惊人的漏洞。有些漏洞被公开披露，由相关厂商发布补丁，将漏洞修复。而另一些漏洞的发现者则不想公开漏洞，而是将其隐藏起来，用于其他目的，这其中就包括美国的情报部门。

2017 年 11 月 15 日，美国白宫向公众发表了政府关于安全漏洞公平裁决程序（Vulnerabilities Equities Process, VEP）的最新政策信息。VEP 涉及的部门包括美国国防部（包含 NSA）、CIA、国土安全部（DHS）等 10 个美国机构，用于决策 NSA 和其他政府机构发现的硬件、软件、网络设备和工业控制系统组件中的漏洞哪些可以发布给美国公司进行修复，哪些仍作为机密以供情报和执法部门在未来的行动中使用。

根据斯诺登及影子经纪人曝光的资料来看，NSA 具有大量的零日漏洞（从未公开披露的漏洞）储备。2017 年 4 月 14 日，影子经纪人组织曝光了一批 NSA 的网空攻击装备与相关漏洞的资料。其中的 Fuzzbunch 是针对 Windows 操作系统的漏洞利用平台，能够向目标主机植入有效载荷，在植入的过程中可直接内存执行，不需要生成实体文件。平台中还包含数个针对特定类型目标，并且可以直接使用的漏洞，包括“永恒之蓝”（EternalBlue）、“永恒浪漫”（Eternalromance）等。该攻击平台泄露后，其中的永恒之蓝漏洞被“魔窟”（WannaCry）勒索软件利用，肆虐全球，之后的“必加”（NotPetya）和“坏兔子”（Bad Rabbit）勒索软件也同样利用该漏洞进行传播。永恒之蓝漏洞仅是众多泄露漏洞中的一个，其他永恒系列漏洞及其利用工具可能具有同等威胁能力。从泄露的资料来看，这些攻击装备是 NSA 几年前开发的，其漏洞储备和相关的装备能力可见一斑。

相比于 NSA，CIA 的漏洞利用能力也丝毫不逊色。2017 年维基解密披露了名为“7 号军火库”（Vault 7）的一系列 CIA 网空攻击装备的相关文档，其中的“樱花盛开”（Cherry Blossom）具有利用漏洞功能。Cherry Blossom 是一款在目标网络上实现监控并进行攻击的工具集，针对大量主流品牌网络设备，尤其是无线网络设备。一旦在目标网络设备植入，就可以对接入该设备的用户设备执行中间人攻击，将恶意内容注入到数据流中，以利用目标用户计算机上应用程序或操作系统中的漏洞，实现对目标用户计算机的控制。

“7 号军火库”中的“艾尔莎”（Elsa）和“法外之地”（OutLaw Country）则从另一个方面体现了 CIA 强大的漏洞利用能力。Elsa 是一款利用 Wi-Fi 信号进行定位的恶意软件，针对 Windows 操作系统的笔记本电脑，通过植入设备周围的 Wi-Fi 信号确定位置。Elsa 虽然本身并没有漏洞利用功能，但是其获取的数据需要依靠 CIA 利用漏洞从目标设备中检索日志文件的方式取回。OutLaw Country 是针对 Linux 操作系统的恶意软件，允许将目标计算机上的所有出站网络流量重定向到 CIA 控制的机器。OutLaw Country 本身同样没有漏洞利用功能，但其包含一个能够在 Linux 目标上创建隐藏的具有网络过滤的内核模块，该内核模块需要通过漏洞利用注入到目标操作系统中。

除以上装备外，NSA 还开发了一系列漏洞利用工具，包括针对 Firefox 的漏洞利用工具 FINKDIFFERENT (FIDI)、针对 Juniper 的漏洞利用工具 ZESTYLEAK、针对 Dell PowerEdge 服务器的 BIOS 漏洞利用工具 DEITYBOUNCE 等；Vault 7 中还包括一系列漏洞发现和漏洞利用工

（下转第三版）

每周安全事件

类 型	内 容
中文标题	SamSam 勒索软件获取赎金高达 600 万美元
英文标题	SamSam Ransomware Attacks Extorted Nearly $6 Million
作者及单位	Swati Khandelwal
内容概述	网络安全公司 Sophos 发布了关于 SamSam 勒索软件的详细研究报告，报告发现，自 2015 年 12 月至今，SamSam 勒索软件已经从 233 名受害者那里累计获利约 600 万美元。而且，其利润还在不断上升，平均每个月还能获得净收入 30 万美元。 值得注意的是，SamSam 勒索软件并不是通过垃圾邮件随意分发，也不具有蠕虫传播或病毒传播的特征，主要是通过幕后开发者有计划地针对可能支付赎金的目标手动发起攻击。在 SamSam 的攻击目标中，医疗、政府以及教育领域的受害者占到一半。
链接地址	https://thehackernews.com/2018/07/samsam-ransomware-attacks.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 5 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	Tool/Android.ADTC.a[prv,rmt] 2018-07-30	该应用程序为一款监控工具，运行后激活设备管理器，接收远程控制命令，进行拍照、录音、录像、发送短信、隐藏图标，还会收集用户手机短信、联系人、通话记录、地理位置等信息并上传。请谨慎使用，若非本人安装，建议卸载。（威胁等级中）
		Trojan/Android.zhoffer.a[exp,rog] 2018-07-31	该应用程序伪装系统应用，联网获取数据，模拟点击打开广告页面。上传用户手机号码等信息，造成用户隐私泄露、资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.FakeSetting.a[exp] 2018-07-31	该应用程序伪装设置应用，运行隐藏图标，联网下载恶意插件并动态加载，需警惕该程序私自发送短信，造成用户资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.digi.a[pay,exp] 2018-07-31	该应用程序运行打开色情网址，监听短信并根据短信内容访问网页进行恶意扣费，造成用户经济损失，建议立即卸载。（威胁等级高）
		Trojan/Android.zapto.a[prv,rmt,spy] 2018-08-01	该应用程序是一款间谍软件，运行后隐藏图标，接收远控指令，后台窃取用户短信、联系人、通话记录、地理位置、SIM 卡信息、手机文件等大量隐私信息，拦截用户短信，监听通话，私自录音、录像，下载其他软件，并将用户隐私上传至服务器和指定邮箱。造成用户隐私泄露，建议立即卸载。（威胁等级高）
		Trojan/Android.FakeFbHack.a[prv,exp] 2018-08-02	该应用程序伪装成 Facebook 攻击程序，诱导用户输入 Facebook 账号密码，并发送到指定号码，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.linble.a[prv,spy] 2018-08-02	该应用程序是一款间谍软件，运行后隐藏图标，激活设备管理器，后台窃取用户短信、联系人、通话记录、地理位置，拦截用户短信，监听通话，私自录音，下载其他未知软件，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）
		Tool/Android.Magisk.a[sys] 2018-08-03	该应用程序是一款 Android 框架平台，功能包含 root 模块，对系统隐藏自身，映射域名和 IP 地址，在不修改系统文件的情况下，提供 Xposed 框架一样的定制效果，请谨慎使用。（威胁等级低）
	较为活跃的样本	G-Ware/Android.FakeQB.g[rog,spr]	该应用程序伪装刷 Q 币工具，运行诱导用户分享该程序到 QQ 好友、QQ 群，本身无实际功能，建议不要使用。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft SharePoint 远程代码执行漏洞（CVE-2018-8300）	当软件未能检查应用程序包的源标记时，将触发 Microsoft SharePoint 中存在的一个远程代码执行漏洞。成功利用此漏洞的攻击者可以在 SharePoint 应用程序池和 SharePoint 服务器场账户的上下文中运行任意代码。（威胁等级高）
	较为活跃样本	Trojan[Downloader]/HTA.Locky	此威胁是一类可以下载勒索软件的木马家族。该家族样本是 Html Application 应用程序，运行后连接远程服务器下载 Locky 勒索软件并执行，加密用户重要数据。（威胁等级中）
		Trojan[Backdoor]/Win32.AutoIt	此威胁是一种由 AutoIt 编写的后门类木马程序。样本运行后会连接远程服务器，等待接收上传下载文件、监视用户屏幕、记录键盘击键、查看进程和窗口等控制指令。（威胁等级高）
		Trojan[Backdoor]/Win32.Dridex	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后可以连接远程服务器接受攻击者的恶意操作，可以删除文件、回传敏感信息等。（威胁等级中）
		Trojan[Backdoor]/Win32.Qakbot	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后连接远程服务器接受攻击者恶意操作，包括文件管理，进程查看等。（威胁等级高）

(上接第一版)
具，包括自动化的可利用漏洞识别工具 CRUCIBLE、针对 Android 系统进行漏洞发现的浏览器插件 AngerManagement、针对 Unix 系统的漏洞利用工具 BaldEagle、针对移动操作系统浏览器的漏洞利用工具 HAMR 等，部分装备的具体功能在已披露的材料中并未介绍。

无论是斯诺登、影子经纪人，还是维基解密的披露，都只是 NSA 和 CIA 庞大武器装备库的冰山一角。虽然部分漏洞或相关工具的详细功能还不得而知，但就目前披露的资料看，美方无论在漏洞储备的数量、质量，还是在漏洞针对目标的广泛性上，同样呈现出了全平台、全能力覆盖的特点。NSA、CIA 利用其持有的覆盖各类设备、平台、系统、软件的零日漏洞对各类高价值目标实施网络空间作业，有效支撑了美方的计算机网络利用（CNE）和计算机网络攻击（CNA）。伊朗核设施被攻击的“震网”（Stuxnet）事件就是一个典型的例子，在攻击行动中，攻击者一共使用了 5 个 Windows 的零日漏洞和 1 个西门子的零日漏洞，以一种看似近乎挥霍实则精妙组合利用零日漏洞的方式，实现了通过网络空间作业对伊朗核设施造成物理破坏的效果，几乎永久地迟滞了伊朗核计划，达成了美方的战略意图。从漏洞利用角度来看，“震网”行动体现出了从技术层面零日漏洞到战略层面压制优势的价值转换。

对于我国的关键信息基础设施防护来说，防御体系建设必须对标高能力对手的攻击能力，必须建立有效的敌情想定，以对手的能力来驱动防御能力的演进。而从敌情想定的视角看，我国的关键信息基础设施防护现状不容乐观。一方面，由于对物理隔离的“盲目自信”，由于运维水平局限性而不得不在升级修补与保障运行间“二选一”，由于缺少对供应链的积极管理而造成对补丁的“盲目不信任”，以及由于安全防御运行能力不足导致未能对漏洞进行缓解防护等情况，我国的关键信息基础设施依然存在大量处于敞口暴露状态的陈旧漏洞，这类漏洞极容易被攻击利用，给攻击者留下了巨大的可乘之机；另一方面，大量关键信息基础设施依然没有建立动态综合的网络安全防御体系，而仅靠单一或零散的安全手段很难有效应对零日漏洞的利用。这就造成了关键信息基础设施不仅难以应对高能力对手利用零日漏洞的攻击，甚至较低能力对手利用陈旧漏洞依然能够对我方关键信息基础设施进行持续入侵的现状，这种情况已经被 WannaCry、白象、海莲花等事件的事实情况所证实。客观来看，目前存在着“漏洞研究方面接近国际水平，漏洞防护方面却难以做到有效自保”的“倒挂式”被动局面。

为了在网络空间防御方面转变这种被动局面，一方面必须建立并落实资产管理、漏洞管理、漏洞分析、补丁分析、补丁验证等全方位的安全运行机制，树立“关键信息基础设施上不允许存在敞口漏洞”的准则，解决如何给已发现漏洞打补丁的问题，以及解决如何给无法修补漏洞配备有效缓解防护措施的问题；另一方面，需要通过将网络安全能力与信息技术基础设施和业务应用系统进行深度结合并实现全面覆盖，依托动态综合的防御体系应对利用零日漏洞的高水平攻击行动。例如：对关键信息基础设施中的系统、软件等进行安全配置加固，收缩攻击面，减小漏洞被利用的可能；建立全面覆盖的纵深防御体系，增加发现威胁行为的机会；落实通过情报驱动的态势感知体系，积极发现威胁，进行威胁猎杀，及时缓解攻击行动的影响，降低损失等。

在之后的文章中，我们将继续关注美国网空攻击装备体系，展现美国在其他方面的网空攻击作业能力，敬请期待。

谷歌更新 Play Store 应用市场开发者审查政策 明确禁止挖矿应用上架

谷歌对旗下 Play Store 应用市场的开发者政策进行了更新，禁止了更多种类的应用发行上架，包括进行加密币挖矿、包含“破坏性”广告等应用，但通过远程控制其它设备进行挖矿的应用仍被允许上架。前段时间苹果更新开发者审核指南，明确禁止了挖矿应用。

此外政策更新还限制了重复模仿性的应用（Repetitive Apps），指那些模仿已有应用提供同样功能体验的 APP，这些 APP 完全重复其它应用的内容，不增加任何独特的或新的功能，还可以包括由自动生成工具、向导服务、或者基于模板的应用等。

此外，政策更新还限制了与武器或者武器配件相关的应用，为爆炸物、火器、弹药或者武器配件提供销售的应用将会被封禁；表面看上去面向儿童的应用，却提供成人主题的应用也在禁止名单中。

文章来源：https://www.cnbeta.com/articles/tech/751147.htm

恶意网站忽悠 iOS 用户拨打假冒的 Apple Care 客服电话

来自印度的“技术支持诈骗”，最近又被发现玩出了新花样 —— 因为诈骗者会向苹果用户发去网络钓鱼电子邮件，将之忽悠到虚假的苹果网站，然后拨打所谓的 Apple Care 客服电话。由于普通用户难以了解网络钓鱼的复杂性和网页的格式，导致其很容易错误地相信自己的设备已经“因为非法活动而被苹果官方给锁定”。在受害者打去电话之后，诈骗者就会沿用老套路来索取钱财。

移动安全服务提供商 Lookout 的威胁情报研究员 Jeremy Richards 表示：“人们在使用移动设备时更加分心，且对其更加地信任，因此针对移动设备的网络钓鱼攻击的成功可能性更大。”

万幸的是，安全研究人员已经将钓鱼欺诈网站的技术细节传递给了苹果安全团队成员。尽管该恶意网站仍处于活跃状态，但谷歌和苹果都已经将它标记为“欺诈”。

文章来源：https://arstechnica.com/information-technology/2018/07/click-on-this-ios-phishing-scam-and-youll-be-connected-to-apple-care/

安天发布《“圣甲虫”勒索软件变种分析报告》

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Scarab“圣甲虫”勒索软件变种开始活跃，其名为Scarabey。其传播方式不同于其他变种，载荷代码亦不相同。

与大多数勒索软件一样，Scarabey加密系统上的文件后要求受害者支付比特币。然而，Scarabey并不像原始的Scarab那样通过Necurs malspam进行传播，而是针对俄罗斯用户并通过服务器和系统上的RDP功能或手动方式进行传播。另外，Scarabey是由Delphi编写的，而Scarab使用C++，并且勒索信息和使用语言也与其他样本不同。对受害者而言，Scarabey与其他Scarab勒索软件之间的主要区别在于勒索信息中使用的恐吓策略。在Scarab样本中，勒索信息是英文内容，但看起来像是将俄语逐字翻译成英文，而不知道正确的英语语法。Scarabey是用俄语写的，但有趣的是，若将Scarabey的勒索信息使用Google翻译时，将出现与Scarab的勒索信息相同的语法错误。

从整体代码来看，Scarabey和Scarab几乎是逐字节相同的，因此很可能是来自同一作者。此外，其生成的子进程、删除的文件、使用的加密方法以及使用的互斥量也都是相同的，这也是Scarabey被认为是Scarab变种的原因。Scarabey使用的加密算法是AES256，其加密密钥会写在注册表键值中。在磁盘加密完成后，它会遍历网络文件夹和磁盘并进行加密，最后弹出勒索信息。

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。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、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BD静态分析鉴定器和静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	d3a28327df38c258a8af00e5eb89abbef5ccf12c22e31b83b72a153d2b15f469
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	189 KB
MD5	9A02862AC95345359DFC3DCC93E3C10E
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.SGeneric
判定依据	BD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

◆ 常见行为

查找指定内核模块	★
创建特定窗体	★
获取驱动器类型	★
获取计算机名称	★
请求加载驱动的权限	★
读取自身文件	★★
释放PE文件	★
复制自身文件	★★
获取主机用户名称	★
打开自身进程文件	★
获取系统版本	★★
查找特定窗体	★
独占打开文件	★

◆ 进程监控

PID	创建	命令行
1624	cmd.exe	"C:\WINDOWS\system32\cmd.exe" /c copy /y "C:\9ebefc743edc473b8232539d2ed72351\share\target.exe" "C:\Documents and Settings\Administrator\Application Data\sevnz.exe"
1720	C:\9ebefc743edc473b8232539d2ed72351\share\target.exe	"C:\9ebefc743edc473b8232539d2ed72351\share\target.exe" runas

◆ 文件扫描

文件名	文件MD5	家族相似性	yara扫描
target.exe	9a02862ac95345359dfc3dcc93e3c10e	N/A	N/A
target.exe.dmp	7915768333b9ed5c89953438d29bde45	N/A	N/A