安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 05 月 14 日 (总第 135 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

编者按：自本期《安天周观察》起，我们将陆续刊登由安天研究院执笔的“美国网络空间攻击与主动防御能力解析”专题解析，本文为概述篇。后续内容将对美国的大型监听项目、攻击支持体系、大型主动防御工程以及攻击装备进行归纳和展示，对其建设背景、功能、场景和防护要点进行介绍，帮助读者深入了解对手的威胁技术、攻击场景和应对手段，敬请关注。

美国网络空间攻击与主动防御能力解析（概述篇）

安天研究院

我国是网络大国，也是面临网络安全威胁最严重的国家之一。近年来，国内金融、能源、交通、教育等行业网络成为战略对手攻击和渗透的主要目标，利用网络攻击造成的信息窃取和破坏事件呈现增长趋势。党的十九大上，总书记“坚持总体国家安全观”、“加强国家安全能力建设”等要求为我国网络空间安全发展指明了方向。为维护我国网络空间主权，保障网络空间安全，实现网络强国的战略目标，必须高度重视网络安全工作。

随着网络空间重要性的日益提升，世界各国纷纷大力建设兼具防御和威慑能力的网络空间安全体系，组建网络部队，以求在网络空间的较量中获得优势。在这方面，美国走在了世界前列。从政府主导的“美国国家网络安全综合纲领”和“爱因斯坦计划”等大规模网络安全倡议和项目，到一系列相关法案、政策、指南，再到“斯诺登事件”、“影子经纪人”及维基解密曝光的网络空间进攻体系，反映出美国在网络空间中强大的、体系化的监听、攻击、威慑和防御能力。这种网络空间优势能力不仅来源于政府的高度重视、持续大量的资金投入和美国的网络技术优势，更离不开其借助产业优势形成的深度军民融合能力。

在战略层面，2017 年 8 月，特朗普总统将网络司令部升级为美军第十个作战司令部，这一举措说明美国在不断调整其国家信息安全战略，逐步将网络安全上升到

美国基础信息产业、网络安全产业、风险投资机构与政府机构关系图

国家安全战略的重要位置，标志着美军的网络战向“成为一种主流战术级军事能力”迈出了关键一步。在能力建设层面，美国的国家安全局（NSA）、中央情报局（CIA）等情报机构，发展出了强大的网络信息采集和网络攻击能力，结合其传统的信号情报（SIGINT）和人工情报（HUMINT）能力，使美国能够在网络空间中继续保持优势；同时，通过国防承包商承担的工程与项目，充分利用安全厂商的技术能力，结合商业安全产品，构建复合的网络安全防御体系。在产业层面，美国一方面通过审查、限制等方式驱离国外安全企业，致使安天等已经走出国门或者正在进军海外的中国安全企业受困于供应链审查，而不得不退回原点；另一方面，大力扶持以火眼（FireEye）为代表的一批本国安全企业，通过政府机构、政府承包商、国防承包商和大厂商（包括大的 IT 寡头和产业集团）的集中商业部署，使其获得迅速的规模成长并进一步转化为技术优势。同时，美国非常重视政府部门、军队与私人公司间的技术与业务合作，大量私人承包商参与到网络空间相关项目中，斯诺登曾就职的博思艾伦（Booz Allen）就是其中之一。在技术层面，美国拥有全球领先的网络空间技术能力，通过思科、IBM、微软、谷歌、英特尔、高通、苹果、甲骨文等“八大金刚”完整布局并实际把持了操作系统、核心芯片、数据库等关键 IT 环节，并通过新兴互联网巨头们形成了对全球数据的有效聚合。

知己知彼，百战不殆。网络空间安全事关国家安全，网络空间战场上的较量是

（下转第三版）

每周安全事件

类 型	内 容
中文标题	Python 连接 SSH 的模块库被曝出存在后门代码
英文标题	Backdoored Python Library Caught Stealing SSH Credentials
作者及单位	Catalin Cimpanu
内容概述	研究人员注意到 Python 用于连接 SSH 的模块库 SSH Decorator（ssh-decorate）存在后门代码，会收集用户的 SSH 凭证并将数据发送到远程服务器。SSH Decorator（ssh-decorate）代码的作者表示，该模块的早期版本已被劫持并被非法上传到 PyPi。
链接地址	https://www.bleepingcomputer.com/news/security/backdoored-python-library-caught-stealing-ssh-credentials/

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 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	Tool/Android.TicklePhone.a[prv] 2018-05-07	该应用程序是一款远程控制手机的工具，根据自身设置可实现控制功能：远程拨打电话、发送短信、录制音频、获得通话记录、获取地理位置，建议谨慎使用，避免隐私泄露。（威胁等级中）
		RiskWare/Android.commonSpy.a[prv,spy] 2018-05-09	该应用程序包含风险代码，包含获取用户短信、通讯录、通讯记录、照片、浏览器上网记录、提权修改系统应用权限、删除 app 等一系列风险行为代码，可能造成用户隐私泄露，请谨慎使用。（威胁等级低）
	较为活跃的样本	Trojan/Android.Installerclient.b[exp]	该应用程序运行动态加载恶意子包，私自推送广告，联网下载更新指定应用，静默安装，会造成用户资费损耗，建议卸载。（威胁等级中）
		Trojan/Android.SmsPayment.k[pay,prv]	该应用程序伪装系统桌面，屏蔽用户锁屏界面，运行后联网获取付费内容，私自发送短信订阅付费内容，造成用户资费损失，并且存在拦截屏蔽对应扣费回执短信的行为，请立即卸载。（威胁等级中）
		Trojan/Android.E4AQQspy.ay[prv,spr]	该应用程序运行诱导用户分享盗号程序到 qq 群，盗号程序使用虚假界面诱导使用者输入 qq 账号密码，而后联网上传，会造成他人隐私泄露，建议不要传播和使用。（威胁等级中）
		Trojan/Android.jianmo.cw[rog,lck]	该应用程序伪装成游戏辅助类应用，运行会诱骗用户提权释放子包应用安装到系统目录，子包应用运行会置顶界面勒索用户付费解锁，造成用户手机无法正常使用，建议卸载。（威胁等级中）
		Trojan/Android.Locker.ak[rog,lck]	该应用程序运行后会显示置顶勒索界面，勒索用户付费解锁，包含风险代码，可能删除用户手机文件，影响用户手机的正常使用，建议立即卸载。（威胁等级中）
		Trojan/Android.BankerSpy.h[prv,exp,rmt,spy]	该应用程序伪装正常应用，运行诱导激活设备管理器，隐藏图标，联网获取指令，上传用户信箱、联系人、安装列表、设备固件信息等隐私，私发短信、开启指定应用进行推送，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Microsoft Windows VBScript 引擎远程代码执行漏洞（CVE-2018-8174）	攻击者可能拥有一个通过受影响的 Microsoft 浏览器利用此漏洞的特制网站，然后诱使用户查看该网站。攻击者还可以利用被入侵的网站或接受或托管用户提供的内容或广告的网站，通过添加可利用此漏洞的特制内容。攻击者还可以在托管浏览器渲染引擎的应用程序或 Office 文档中嵌入标记为“安全初始化”的 ActiveX 控件。（威胁等级高）
	较为活跃样本	Trojan[Banker]/Win32.Banbra	此威胁是一种以窃取网络银行敏感信息为目的的木马类程序。该病毒伪装成正常数据，以获取认证。该病毒利用各种途径，使黑客获得数字证书来伪造文件。该病毒还会收集用户的机密信息，如网上银行详细信息和密码等，并将窃取的数据发送给远程黑客。（威胁等级中）
		Trojan[Downloader]/Win32.Zlob	此威胁是一种具有下载行为的木马类程序。Zlob 家族感染用户电脑后，会修改系统设置，在电脑中下载并执行多个恶意软件。该家族会伪装成 ActiveX 的视频编码欺骗用户下载并安装，安装后，用户会收到伪装成微软警告信息的弹窗，提示用户系统中可能存在间谍软件，需要下载反病毒程序进行清除。在用户点击弹窗后，将下载实为木马的虚假反病毒程序。（威胁等级高）
		Trojan[Ransom]/Win32.Zerber	此威胁是一类可以加密用户数据的木马家族。该家族样本是勒索软件，运行后加密用户文件，加密后播放声音提示用户文件已被加密，需支付比特币才可以解密。（威胁等级中）

(接上第一版)

持续不断的高烈度无底线较量。维护国家网络空间安全，建设有效的网络安全防护体系，必须打破旧有以“物理隔离 + 好人假定 + 规定推演”构成的自我麻痹式的安全观，以真实有效的敌情想定作为基础和前提。包括内网已经被渗透、供应链被上游控制、运营商网络的关键路由节点被控制、物流仓储被渗透劫持、关键人员和周边人员被从互联网进行定位摸底、内部人员中有敌特人员派驻或被发展等。只有全面、深入地了解对手的能力，尤其是对手的进攻能力，才能在网络空间安全建设中有的放矢，才能实现真正的“有效防护”。在本系列专题中，我们希望通过层次化地揭示美国在网络空间信息获取、进攻与防御能力，尽可能清晰地展现美国在网络空间安全领域的能力体系，为我国网络空间安全发展提供有益参考和借鉴。

一、美国具备网络空间进攻性职能的国家安全机构

美国国防部（DoD）是美国作战部门的最高领导机关，2006-2008 年间，总统就曾允许 DoD 举行大规模网络作战演习，发起网络攻击，夺取对方指挥控制权。作为 DoD 的重要组成部分，NSA 专门负责收集和分析国内外的信号情报，为美国提供决策优势。NSA 下属的特定入侵行动办公室（TAO）是 NSA 的一个重要职能部门，负责针对特定目标收集情报、潜入外国计算机和电信系统、破解密码、窃取数据等，NSA 称这些行动为计算机网络利用（CNE），TAO 对目标造成直接影响的其它行动，例如瘫痪服务、破坏文件等，则被称为计算机网络攻击（CNA）。NSA 拥有完善的音频、视频、邮件等信号情报的收集、处理机制，并且针对 CNE、CNA 和网络防御（CND）等多种任务建立了稳定、完备的基础设施。

CIA 是美国唯一一个独立的情报机构，也是美国最重要的情报机构之一。CIA 的传统任务包括人工情报、全源情报分析和秘密任务。2015 年，CIA 进行了重大重组，增设了数字创新处（DDI），专门负责为传统的人工情报开发数字装备和手段，使得 CIA 能够更好地为国家决策者的战略评估提供情报支撑。

二、多样的监听手段获取全球信息

美国通过在产业、技术上的优势，逐步实现了对全球网络空间的全面布局并具备了事实上的控制能力。斯诺登事件相关文件表明，美国具有多种情报收集方式，包括为 NSA 提供数据的 30 多个国家的合作伙伴、在全球范围内的计算机上植入恶意软件以及与大型 IT 企业合作等。

2004 年，美国政府启动“星风”（STELLARWIND）计划，进行大规模的情报搜集、监听，后因法律等问题，将“星风”拆分为“棱镜”、“主干道”、“码头”、“核子”等项目，由 NSA 接管。谷歌、微软、脸谱、雅虎等 IT 企业均与“棱镜”项目有关联。“拱形计划”（CamberDADA）是在斯诺登披露的一份绝密文件中提到的，NSA 对俄罗斯网络安全厂商卡巴斯基进行监听，通过监听样本上报渠道，从中分析安全厂商是否已发现、掌握其网络攻击武器。该计划后续目标包括安天等 22 家全球重点网络安全厂商。

三、全平台、全功能的网络攻击装备体系

在“全面拒止威慑”的积极防御思想引导下，NSA、CIA 极为重视网络攻击装备的研发。“震网”、“毒曲”、“火焰”、“方程式”等事件均被认为与美国有关。

从斯诺登和“影子经纪人”泄露的资料看，NSA 具有强大的网络攻击装备和丰富化的漏洞储备，2017 年 5 月席卷全球的“魔窟”（WannaCry）勒索软件事件就是由 NSA 的装备库泄露直接导致。

2017 年 3 月起，维基解密陆续曝光了包含大量 CIA 网络攻击装备资料的“7 号保险库”（Vault 7），功能涵盖了突破物理隔离、信息窃取、持久化能力、隐蔽信息传输、边信道传输、直接漏洞利用等众多方面，同时体现了强大的多平台能力。其中，部分装备被安全厂商发现与以往发生的 40 多起网络安全事件关联。

实现网络强国的战略目标离不开深度的网信军民融合，正是因为对手的强大，我国的网信军民融合才肩负着更重要的使命。以多领域民间领先技术和优秀产品为军队提供支撑，以军队的资源、体系和能力优势支持民间抵御来自国家行为体和非国家行为体的威胁，各尽其能，共同构建我国军民融合的网络空间安全能力体系。

开发者误读芯片厂商调试文档导致出现新内核漏洞

美国计算机安全应急响应中心 (以下简称 CERT) 日前发布公告称，Windows、macOS、Red Hat、Ubuntu、SUSE Linux、FreeBSD、VMware 和 Xen 等系统都可能受到一个重大安全漏洞（CVE-2018-8897）的影响，这个漏洞是由于操作系统开发者曲解了英特尔和 AMD 两大芯片厂商的调试文档所致。

不过，这个漏洞的利用需要一定的条件，攻击者需要使用已经感染带有恶意软件的计算机，或者必须使用已经登录的帐户才能运行利用此漏洞的恶意代码。如果顺利入侵，攻击者可以将其代码的访问权限提升到内核级别，然后使用此访问权限执行其他操作。通俗来说，攻击者可以利用操作系统的 API 获取敏感内存信息，或控制低级操作系统功能。

目前，各大厂商都已知晓这个漏洞，并积极应对。Red Hat、Ubuntu 和苹果 MacOS 都已经着手推出补丁。而早在 2018 年 3 月，Linux 内核已经解决了这个问题，4.15.14、4.14.31、4.9.91、4.4.125 以及更早的 4.1、3.16 和 3.2 版本都有相应的补丁。

微软也做出了回应，其 Windows 7 到 Windows 10 以及 Windows Server 2008 到 1803 版本都推出了补丁。Xen 4.6 到 4.10 版本也推出了修补程序。VMware 的虚拟机管理程序没有风险，vCenter Server 有对应的解决方案，vSphere 集成容器正在等待修复，但专家认为，二者都“可能受到影响”。

来　源：https://www.theregister.co.uk/2018/05/09/intel_amd_kernel_privilege_escalation_flaws/

安天发布《某钓鱼邮件事件样本分析》

安天捕风小组在一次外出取证过程中，发现了一起钓鱼邮件攻击事件。攻击者通过钓鱼邮件对目标进行攻击，其主要的攻击方式有两种：一种是仿冒链接，诱骗邮箱密码；另一种是通过附件放马。

通过邮件附件放马是一种常见的攻击手段。该事件中附件的名称是“Technology Promotion Points For Review.docx .zip”，解压之后是一个 exe 文件：“Technology Promotion Points For Review.docx .exe”，该文件名在“.docx .exe”之间存在大量的空格，以此来伪装成 doc 文件诱导受害者点击。用户在不知情的情况下点击“Technology Promotion Points For Review.docx .exe”后，该程序会在 c:\intel\logs 目录下释放 mobisynce.exe。mobisynce.exe 是一个下载器，可能会下载其他的木马到用户机器，从而获取更多有价值信息。

Mobisynce.exe 运行后，会先对程序中的加密字符串通过单字节密钥进行解密，以得到需要的字符串。然后通过查找当前进程列表名中是否有包含“avg”字符串的进程，以此来判断是否存在 avg 相关的杀毒软件。如果不存在与 avg 相关的杀软进程，则创建新线程，并在该线程中判断是否存在注册表启动项“HKCU\Software\Microsoft\Windows\CurrentVersion\Run\igfxmsw”，如果不存在该注册表项，则创建后门进程并通过管道的方式接收执行后续的攻击者指令。之后，创建注册表启动项“HKCU\Software\Microsoft\Windows\CurrentVersion\Run\igfxmsw”，并设置 Mobisynce.exe 为自启动。Mobisynce.exe 会尝试连接 C&C 控制服务器：wingames2015.com。如果连接成功则开始搜集系统信息并拼装成 HTTP GET 请求，并将 HTTP GET 请求发送到 C&C 服务器的 ldtvtvqs/accept.php? 页面。最后，mobisynce.exe 会循环监听执行后门命令，当 C&C 服务器向木马发送含有“Yes file”字符串的指令时，木马会在指令中提取“[“与”]”中间的命令，并通过 ShellExecuteA 函数执行该命令。

安天建议广大网络使用者及时进行弱密码检查，将所有弱密码修改为强密码；不要轻信各种以管理员身份发送的通知邮箱故障、即将到期、即将封闭等通知；谨慎对待陌生人发来邮件的各类附件；安装邮件过滤软件，以阻止多数初级的钓鱼邮件。企业应加强人员安全意识，企业 IT 团队应定期开展内部防网络钓鱼活动，真正帮助提高意识。目前，安天追影产品已经实现了对该类样本的检出。

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、数字证书鉴定器、文件元数据分析鉴定器、动态行为鉴定器、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、静态分析鉴定器将文件判定为木马程序。

概要信息

文件名	EF8B828E2D2E7E0F2FC22F15DB9D9F30
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	398 KB
MD5	EF8B828E2D2E7E0F2FC22F15DB9D9F30
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	★
打开自身进程文件	★
读取自身文件	★★
查找特定窗体	★
释放 PE 文件	★
获取计算机名称	★
获取驱动器类型	★
请求加载驱动的权限	★
获取主机用户名称	★
遍历进程	★
获取系统内存	★★
访问 dns	★
连接网络	★
获取系统版本	★★
设置文件属性为隐藏	★★
隐藏文件	★

文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.exe	ef8b828e2d2e7e0f2fc22f15db9d9f30	N/A	N/A
target.exe.dmp	50938815e89650127492cc1d7a7c1c71	N/A	N/A
mobisynce.exe	6a3f0de81242e55a35571a6a231c5b2c	N/A	N/A
Normal.dot	347b44ff630ee597656dc805e040a16e	N/A	N/A