安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 07 月 09 日 (总第 143 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（六）

——用于突破物理隔离的网空攻击装备

安天研究院

上一期中，我们对美国国家安全局（NSA）和美国中央情报局（CIA）的网络攻击装备体系进行了整体的概述，介绍了其全平台、全功能的武器装备库，体现了对手在网空进攻作业中的全方位能力。在本期中，我们将聚焦用于突破物理隔离的网空攻击装备，展现超级大国在网空攻击作业中，对各类机构的内网体系，特别是对其物理隔离网络的穿透能力。

根据我国《计算机信息系统国际联网保密管理规定》，物理隔离网络即不直接或间接与国际互联网或其他公共信息网络相联接的网络。物理隔离属于一种能够产生效果的安全防护手段，能够从传播途径一侧阻断大量的安全威胁，提高攻击者的攻击难度，曾经在很长一段历史时期里，在某种程度上保障了关键内网的安全。但在当前形势下，由于存在广泛的人员交换、设备接入和信息交换等情况，采取物理隔离措施的网络，早已在事实上成为开放的网络体系。习近平总书记在 4·19 讲话中明确告诫我们，“‘物理隔离’防线可被跨网入侵，电力调配指令可被恶意篡改，金融交易信息可被窃取，这些都是重大风险隐患”。尤其在面对来自网络空间中高能力国家行为体的网络攻击时，仅靠物理隔离已经不足以保障内网安全。

据美国媒体报道，美国当地时间 5 月 9 日，CIA 副局长吉娜·哈斯佩尔（Gina Haspel）出席了国会参议院情报委员会关于 CIA 局长提名的听证会，当被问到面对中国崛起，“今日的 CIA 在设备和架构上，是否能够应对这种多方面的挑战”时，哈斯佩尔表示中国崛起成为全球大国是“更具有战略性的威胁”，之后称在中国问题上，CIA 有着惊人的专长。CIA 作为美国最重要的对外情报部门之一，在面对“中国问题”时，是不是也包含着网络空间中“惊人的专长”，值得我们深思。

为采用网络空间技术配合其情报作业或隐秘行动，需要能够突破物理隔离以渗透到对手隔离内网中进行信息窃取或展开破坏的能力。为此，CIA 开发了一系列能够用于突破物理隔离的网络攻击装备，其中比较具有代表性的攻击装备包括“冲击钻”（HammerDrill）和“野蛮袋鼠”（Brutal Kangaroo）。

由于保密要求，非涉密机向涉密机的数据传递通常会使用光盘作为存储介质。“冲击钻”恰恰针对这种情况，利用光盘突破物理隔离防线。“冲击钻”能够收集计算机读取的 CD/DVD 内容并保存到指定的文件夹中，更关键的是，当用户使用 Nero 软件（一款常用的光盘刻录软件）刻录光盘时，“冲击钻”可以向可执行文件注入 Shellcode，一旦光盘插入其他计算机并执行可执行程序时，Shellcode 就感染到计算机上，自动运行。

“野蛮袋鼠”是 CIA 另一种用于突破物理隔离的网络攻击装备。使用时首先需要入侵一台接入互联网的主机，并在这台主机上安装“野蛮袋鼠”恶意软件，然后“野蛮袋鼠”会自动感染插入这个主机的 U 盘，并在由于信息交换等目的将 U 盘带入隔离网络并插入计算机时实现入侵，随后还能够利用这种“U 盘摆渡”方式传递数据和控制信息。CIA 甚至能够在多个被控制的内网主机间建立隐蔽网络，进行数据交换和任务协作。

需要注意的是，与 NSA 的大规模监听和情报获取不同，人力情报（HUMINT）作为 CIA 的传统能力，当前依然是 CIA 的主要情报作业方式。2015 年 CIA 改组成立数字创新处（DDI），负责开发网络攻击装备，被称为“给了传统‘斗篷与匕首’任务更好的 IT 工具”，可见人力情报作业依然是 CIA 工作的重点，而网络攻击装备则赋予了 CIA 更加丰富的情报获取能力。据披露，CIA 早在 10 多年前就开始通过“黑袋行动”（Black Bag Jobs）的方式，以人工方式破门入屋，入侵那些难以通过互联网遥控攻击的目标电脑，完成其内部竞争对手 NSA 的大规模窃听计划所不能完成的情报收集任务。

NSA 则以信号情报（SIGINT）为主，其下属部门特定行动办公室（TAO）负责开发各种网络攻击装备，实施网络控制、窃取、监视（被称为计算机网络利用，即 CNE）和破坏、摧毁（被称为计算机网络攻击，即 CNA）。为了配合美方军事力量抵近展开秘

（下转第三版）

一周简讯

- 1、Mozilla 发布 Firefox 61 修复以往 18 个漏洞
- 2、安天联合猎豹发布 testServiceSpy 分析报告
- 3、研究表明超三分之二的旧存储卡敏感信息可被恢复
- 4、Facebook 拉黑功能设置出错影响 80 万用户
- 5、攻击者利用社工手段传播 Mac 木马 Dummy
- 6、VMware 发布安全更新修补越界读取漏洞
- 7、新型剪贴板木马监视着超过 230 万的数字钱包地址

每周安全事件

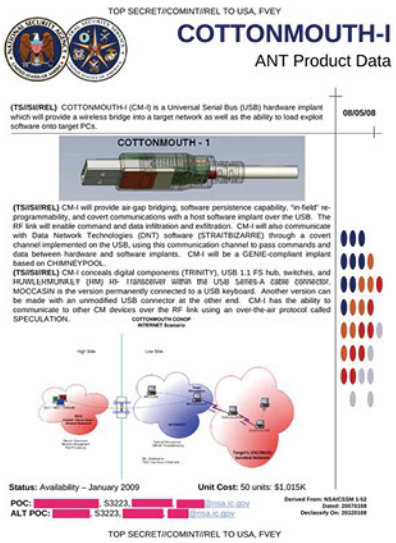
类 型	内 容
中文标题	Adidas 宣称数百万用户数据泄漏
英文标题	Adidas Announces Data Breach
作者及单位	Catalin Cimpanu
内容概述	运动服装制造商 Adidas 宣布了一次数据泄露事件，并指出这对使用其美国网站的购物者产生了影响。该公司表示，在 6 月 26 日得知有一未经授权的组织声称已获得 Adidas 客户的详细信息后，发现了此次信息泄露事件。 “根据初步调查，泄露的信息仅限于联系信息、用户名和加密密码，”Adidas 发言人表示，并补充道，“Adidas 没有理由相信这些消费者的信用卡或健康信息受了到影响。”
链接地址	https://www.bleepingcomputer.com/news/security/adidas-announces-data-breach/

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	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.InfoStealAd.a[prv,exp] 2018-07-01	该应用包含恶意代码，运行后加载虚假警告，诱骗用户点击，后私自跳转至 Google Play 下载页面，模拟点击广告，并会窃取用户手机设备基本信息，接收用户短信并上传。造成用户隐私泄露和流量消耗，建议卸载。（威胁等级高）
		Trojan/Android.pblSpy.a[prv,spy] 2018-07-01	该应用程序是一款间谍软件，伪装正常应用，运行后激活设备管理器，窃取用户短信、地理位置，私自录音，并上传至指定网址。造成用户隐私泄露，建议卸载。（威胁等级中）
		Tool/Android.RAMZ.a[rmt] 2018-07-03	该应用程序是一个远程控制工具，可以通过短信指令，让受控端手机执行振动、响铃、静音、拨号、短信发送地理位置信息等操作，以及对 WIFI、GPS、GPRS 流量、设置呼叫转移的开关控制等，若非本人安装，建议谨慎使用。（威胁等级中）
		Trojan/Android.hbkysmjj.a[pay,rog,exp] 2018-07-04	该应用程序运行后私自发送付费短信，包含流氓广告，会通过插屏、悬浮窗、添加桌面快捷方式等手段展示，点击即下载应用，会造成用户资费损失和流量消耗，建议不要使用。（威胁等级高）
		Trojan/Android.6etv.a[prv,spy] 2018-07-05	该应用程序是一款间谍软件，运行后窃取用户短信、联系人、通话记录、地理位置，私自录音、录像，并上传至服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.Locker.ar[rog,lck]	该应用程序是勒索程序，运行隐藏图标，置顶勒索界面，要求用户付费解锁，造成用户资费损耗，请卸载。（威胁等级中）
		Trojan/Android.smssteal.b[prv,exp]	该应用程序是一款测试应用，监听解析用户短信内容，发送用户短信内容到指定号码，通过判断短信内容私自拨打电话和播放音乐，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.HiddenApp.bf[rmt,exp]	该应用程序运行后隐藏图标，接收远程指令，可能加载广告、私自下载安装应用，造成用户资费损耗，建议卸载。（威胁等级中）
		G-Ware/Android.Dropper.be[exp,rog]	该应用程序包含风险代码，运行后释放恶意子包，联网后下载恶意文件尝试获取 root 权限且私自安装恶意应用，然后加载广告，造成用户资费消耗，建议卸载。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Acrobat/Reader 远程代码执行漏洞 (CVE-2018-4999)	Adobe Acrobat 是一套 PDF 文件编辑和转换工具，Reader 是一套 PDF 文档阅读软件。Adobe Acrobat/Reader 存在远程代码执行漏洞，成功利用后可使攻击者远程执行任意代码。(威胁等级高)
	较为活跃样本	Trojan[DDoS]/Win32.Mavros	此威胁是一种可以实行 DDoS 攻击的木马家族。该家族样本运行后连接远程控制服务器并向其发送上线包，接受攻击者控制，有一定威胁。（威胁等级中）
		Trojan[Backdoor]/Win32.DarkKomet	此威胁通常通过垃圾邮件附件、恶意链接及网上的免费应用下载等方式传播。该木马会监控用户行为，并为黑客打开系统后门，导致用户的信息被窃取。该木马会将窃取到的信息发送给攻击者，同时其还会下载其他恶意软件。（威胁等级高）
		Trojan[Downloader]/Win32.Adload	此威胁是一种木马类程序，运行后会释放可执行文件，并访问远程服务器，会下载其它恶意可执行程序，添加注册表信息，并添加计划任务，用来执行恶意程序。（威胁等级中）
		Trojan[Downloader]/Win32.Banload	此威胁是一种木马类程序，运行后复制自身到 %system32%\csrss\ 下，连接网络、下载病毒文件，修改注册表，添加启动项，以达到随机启动的目的，该家族下载的文件可以盗取用户银行账号和密码，它是基于特定行为来命名的家族。（威胁等级中）

（上接第一版）


TOP SECRET//COMINT//REL TO USA, FVEY

COTTONMOUTH-I

ANT Product Data

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.

08/05/08

COTTONMOUTH - 1

(TS//SI//REL) CM-I will provide air-gap bridging, software persistence capability, "in-field" re-programmability, and covert communications with a host software implant over the USB. The RF link will enable command and data infiltration and exfiltration. CM-I will also communicate with Data Network Technologies (DNT) software (STRAITBIZARRE) through a covert channel implemented on the USB, using this communication channel to pass commands and data between hardware and software implants. CM-I will be a GENIE-compliant implant based on CHIMNEYPOOL.

(TS//SI//REL) CM-I conceals digital components (TRINITY), USB 1.1 FS hub, switches, and HUWLEHMUNKLY (HM) HI- [illegible] within the USB SERIES-A cable connector. MOCCASIN is the version permanently connected to a USB keyboard. Another version can be made with an unmodified USB connector at the other end. CM-I has the ability to communicate to other CM devices over the RF link using an over-the-air protocol called SPECULATION.

COTTONMOUTH CONOP

INTERNET Scenario

Status: Availability – January 2009

Unit Cost: 50 units: $1,015K

POC: S3223, [redacted]@nsa.ic.gov

ALT POC: S3223, [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

密行动，也需要能够突破物理隔离并渗透进入对手内网的作业能力，NSA 也开发了一系列着重于突破物理隔离防护机制的工具和技术，“水腹蛇 -1”（COTTONMOUTH-1）是其中最具代表性的一个。

“水腹蛇 -1”是一套无线信号收发系统，可以隐藏在 USB 接口中。植入了“水腹蛇 -1”的 USB 接口，外表看起来和普通的 USB 接口没有不同，但内部却集成了无线信号收发模块，通过该模块，作业者可通过无线信号访问目标设备所处的隔离内网。“水腹蛇 -1”可以将目标系统中收集的数据发送到 NSA 的外场接收站，并接收来自指挥控制节点的指令。该工具可通过供应链感染、物流链劫持等方式植入，具有高度隐蔽性。一份斯诺登披露的文件可以证明，NSA 会使用物流链劫持的方式，拦截发送到目标地区的计算机和网络设备，然后由 TAO 的情报和技术人员完成设备或固件的篡改，并重新打包发送到目标地区，采用这种方法突破物理隔离防线。

除了上述装备外，NSA 和 CIA 还开发了大量其它装备，通过多种方式突破物理隔离。例如，NSA 的可用于对离线室内活动（如高密级会议、研讨等）进行信号采集的“愤怒的邻居”（Angry Neighbor）装备，能够主动收集视频、音频、无线信号，并转换为特定波段的射频信号，通过隐蔽通信通道回传；NSA 利用物理隔离网络中的 Wi-Fi 信号（物理隔离网络中常常因为管理不到位而存在违规私接的 Wi-Fi 网络）的漏洞进行重定向并

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

入侵的“床头柜”（NIGHTSTAND）装备；CIA 针对三星智能电视开发的攻击装备“哭泣天使”（Weeping Angel），能够在电视看起来是关闭的状态下，利用电视的麦克实现录音和窃听，并能够通过 Wi-Fi 使攻击者实现实时监听，等等。

基于本文对美方攻击装备的介绍，结合“震网”（Stuxnet）、“黑色能量”（BlackEnergy）、“魔窟”（WannaCry）等重大安全事件，可以发现突破物理隔离、进入内网已经成为代表不同利益和诉求的各种攻击组织的基础能力，而大量的事实已证明仅靠物理隔离不足以在网络空间有效抵御高能力对手的威胁。突破物理隔离不是一个简单的单一操作，而是一个结合了人力情报作业与网络攻击作业，通过物理接触、电磁波信号获取、供应链污染、物流链劫持等多种手段，对物理隔离防线造成突破效果的过程，是一种体系化的进攻过程。但长期以来，我们被笼罩在一种“物理隔离绝对安全”的假象之下，而各政企机构出于对物理隔离的迷信和对安全厂商的不信任，导致安全厂商的安全能力难以深入到关键信息基础设施内部，或者即使进入内部也难以有效更新维护，继而成为无支持的孤岛。总体来看，以上这些问题导致各种安全投入难以产出有效的安全价值，更导致无法形成全面的网络安全态势感知能力，客观上造成了威胁易于流入而难以有效被发现的现状，形成了巨大的安全隐患。

仅靠物理隔离不足以在网络空间有效抵御高能力对手的威胁并不代表要放弃物理隔离，而是需要在物理隔离的基础上，对网络进行体系化加强。2018 年 4 月 20 日，习近平总书记在全国网络安全和信息化工作会议上强调，要构建“关口前移，防患于未然”的网络安全体系。“关口前移”是对落实网络安全防护方法提出的重要要求，而“防患于未然”则形成了鲜明地以防护效果为导向的指引要求，这是对如何解决当前面临问题的深刻回答。

深入落实“关口前移”的前提是深入理解“关口”的内涵意义，这里不能将“关口”片面窄带化为网关或网络入口，而是应理解为落实安全能力的重要控制点，有效解决安全能力的“结合面”和“覆盖面”问题，即安全防御能力与物理、网络、系统、应用、数据与用户等各个层级的深度结合，并将网络安全防御能力部署到信息化基础设施和信息系统的“每一个角落”，最大化覆盖构成网络的各个组成实体。重要的是，在网络安全体系建设实施的过程中，必须在投资预算和资源配备等方面予以充分保障，以确保将“关口前移”要求落到实处，在此基础上进一步建设实现有效的态势感知体系。

在做好“关口前移”的基础上，进一步加强网络安全防护运行工作，除了采用定期检查和突发事件应急响应等偏被动的常规机制外，还需提升安全防护工作的主动性，将安全管理与防护措施落实前移至规划与建设等系统生命周期的早期阶段，将态势感知驱动的实时防护机制融入系统运行维护过程，实现常态化的威胁发现与响应处置工作，从而实现“防患于未然”。

在后续的文章中，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。

安天发布《GandCrab 勒索软件 V4 版本分析报告》

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 GandCrab 勒索软件出现了第 4 个版本，新版本具有许多变化，包括不同的加密算法、新的加密扩展名、新的赎金数额和新的 TOR 支付链接。

GandCrab V4 通过一个虚假的软件破解网站传播，勒索软件开发者会在软件破解网站上发布提供破解软件下载链接的博客，当用户下载并运行这些破解软件时，GandCrab 就会被安装到计算机上。根据安全研究员在 GandCrab V4 中发现的调试信息，该勒索软件看起来已经将其加密算法切换为 Salsa20，GandCrab 的作者还向发明 Salsa20 算法的伊利诺伊大学芝加哥分校的计算机教授 Daniel J. Bernstein 发送了一条消息："@hashbreaker Daniel J. Bernstein let's dance salsa <3"。

GandCrab V4 样本运行后，将扫描计算机和所有的网络共享，当匹配到相应格式的文件时，加密文件，然后将 .KRAB 扩展名附加到加密文件原有的扩展名后。在加密文件时，勒索软件还会创建名为 KRAB-DECRYPT.txt 的勒索信息，其中包含受害者文件发生变化的信息、付款的 TOR 地址以及勒索软件开发者恢复文件所需的密钥。如果用户访问了 TOR 支付网站，他们将获得赎金金额以及如何支付以获得 GandCrab Decryptor 解密工具的说明。目前赎金金额是价值 1200 美元的 DASH（达世币）加密货币。

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、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、安全云鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、动态行为鉴定器、静态分析鉴定器、安全云鉴定器将文件判定为木马程序。

概要信息

文件名	ef7b107c93e6d605a618fee82d5aeb2b32e3265999f332f624920911aabe1f23
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	206 KB
MD5	97A910C50171124F2CD8CFC7A4F2FA4F
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.TSGeneric
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

危险行为

行为描述	危险等级
查找游戏进程	★★★★
添加 IPC 共享	★★★
延时	★★★

常见行为

遍历进程	★
获取主机用户名称	★
获取计算机名称	★
查找反病毒程序	★★
获取驱动器类型	★
扫描驱动器类型	★★
查找指定内核模块	★
独占打开文件	★
文档篡改	★★
打开自身进程文件	★
获取系统内存	★★
创建特定窗体	★
查找浏览器进程	★★
访问 dns	★
连接特殊 URL	★
获取 socket 本地名称	★
连接网络	★
设置调试器权限	★
设置文件属性为隐藏	★★

进程监控

PID	创建	命令行
3676	wuauclt.exe	"C:\WINDOWS\system32\wuauclt.exe" /RunStoreAsComServer Local\[3dc]SUSDS9b4ff92a86ba6d448de6269af01fac71
2884	dumprep.exe	C:\WINDOWS\system32\dumprep.exe 988 -dm 7 7 C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\WERc0ae.dir00\svchost.exe.mdmp 16325836412031264
.....	.....	.....