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 30 日 (总第 146 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（七）

——用于持久化控制的网空攻击装备

安天研究院

在之前的文章中，我们对美国国家安全局（NSA）和中央情报局（CIA）用于突破物理隔离的网空装备进行了介绍，展现了美国在攻击性的网空作业中，对各类机构的内网体系，特别是对物理隔离网络的穿透能力。在本期中，我们将对美方用于实现持久化控制的网空攻击性软硬件装备进行介绍，展现美方针对各类网络设备以及服务器与终端节点做到全方位覆盖的持久化能力。

持久化的目的是实现对目标网络设备或节点系统的持续控制，这既是进行网络情报获取等攻击性网空行动所依赖的基础，也是开展积极防御反制威慑乃至实现网络战攻击的重要前提。在传统战争中，是在战争开始之时将作战人员和装备投入战场，适应战场以便在战争中获得主动。而在网络空间中，攻击方可以在网络战开始前的数天、数月甚至数年就进行“战场预制”，通过对内网的穿透能力和对生产、运营商、物流链等相关环节的渗透，在网络战争开始前已经按照于己方有利的方式，攻击控制具有潜在战略或战术意义的网络设备和节点系统，从而隐蔽地实现对网络空间战场阵地的预制改造。在战争开始时，就可以迅速地将攻击载荷投递至已被持久化控制的关键位置，或者通过被持久化控制的阵地节点间接对关键位置发起攻击并投递载荷，从而通过攻击行动实现军事作战所需的网空攻击效用。事实上，在现代网络战争中，战争模式早已从战时选取目标开展攻击的早期模式，转变为战时根据作战需要，从已被持久化控制的网络节点中挑选具有战略或战术意义的目标，并展开组合攻击行动的成熟模式。因此，在网络空间的较量，对重要网络设备和节点系统进行持续隐秘控制的持久化能力，已经成为对敌方的重要的战略优势。

在持久化这一问题上，美国一直秉承“持久化一切可以持久化的节点”的理念，将其作为一种重要的战略资源储备，为长期的信息窃取和日后可能的网络战做准备。据斯诺登披露的 NSA 内部文件显示，对网络的监视仅仅是美国“数字战争战略”中的“第 0 阶段”，监视的目的是检测目标系统的漏洞，这是执行后续行动的先决条件。一旦“隐形持久化植入程序”渗入目标系统，实现对目标系统的“永久访问”，那么“第 3 阶段”就已经实现，这一阶段被称为“主宰”，可见持久化能力的重要性。而这些都是为最终的网络战做准备。一旦在目标系统达成持久化，攻击者就能够实现随时从监视到攻击行动的无缝切换，即由计算机网络利用（即 CNE）转换为计算机网络攻击（即 CNA），对目标网络或系统进行破坏和摧毁。

谈及持久化，不得不提“方程式”组织对于固件的持久化能力。2015 年初卡巴斯基和安天先后披露一个活跃了近 20 年的攻击组织——方程式组织，该组织不仅掌握大量的 0day 漏洞储备，且拥有一套用于植入恶意代码的网络武器库，其中最受关注、最具特色的攻击武器是可以对数十种常见品牌硬盘实现固件植入的恶意模块。依靠隐蔽而强大的持久化能力，方程式组织得以在十余年的时间里，隐秘地展开行动而不被发现。方程式组织被认为和 NSA 有较大关联。

根据目前披露的文件显示，NSA 和 CIA 均开发了大量具有持久化能力的网络攻击装备。NSA 的相关装备主要由特定入侵行动办公室（TAO）下属的先进网络技术组（ANT）开发。比较有代表性的装备包括针对 Juniper 不同系列防火墙的工具集“蛋奶酥槽”（SOUFFLETROUGH）和“给水槽”（FEEDTROUGH）、针对思科 Cisco 系列防火墙的“喷射犁”（JETPLOW）、针对华为路由器的“水源”（HEADWATER）、针对 Dell 服务器的“神明弹跳”（DEITYBOUNCE）、针对桌面和笔记本电脑的“盛怒的僧侣”（IRATEMONK）等。

SOUFFLETROUGH 是一种通过植入 BIOS 实现持久化能力的恶意软件，针对 Juniper SSG 500 和 SSG 300（320M/350M/520/550/520M/550M）系列防火墙。它能够向目标注入数字网络技术组（DNT）的植入物“香蕉合唱团”（BANANAGLEE，功能尚不完全明确），并在系统引导时修改 Juniper 防火墙的操作系统。如果 BANANAGLEE 无法通过操作系统

（下转第三版）

一周简讯

- 1、研究人员指出 USB 调试模式攻击难于防御。
- 2、黑客利用 AVTech 设备缺陷构建 Death 僵尸网络。
- 3、WebLogic 中间件漏洞被用于发动大规模攻击。
- 4、Android 银行木马源代码已经在线泄露。
- 5、健身可穿戴设备中存在漏洞会泄露个人信息。

每周安全事件

类 型	内 容
中文标题	蓝牙被曝严重加密漏洞，影响大量主流厂商的数百万设备
英文标题	New Bluetooth Hack Affects Millions of Devices from Major Vendors
作者及单位	Swati Khandelwal
内容概述	某些蓝牙实现中被指出现一个高危加密漏洞，可导致未经认证的远程攻击者在物理临近的目标设备中进行拦截、监控或操纵其交换的流量。 该蓝牙漏洞的编号是 CVE-2018-5383，影响一些主流厂商如苹果、博通、英特尔以及高通等的固件或操作系统软件驱动器，目前该漏洞对谷歌、安卓和 Linux 的影响尚不可知。 该安全漏洞和两个蓝牙功能有关，它们是操作系统软件中安全连接配对的蓝牙低功耗（LE）实现以及设备固件中安全简单配对的 BR/EDR 实现。
链接地址	https://thehackernews.com/2018/07/bluetooth-hack-vulnerability.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	相关描述
移动恶意代码	新出现的样本家族	Trojan/Android.FindTheFish.a[prv,spy] 2018-07-23	该应用程序运行后监听用户短信，上传用户短信内容到服务器。造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.apiempello.a[prv,exp,rog] 2018-07-23	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，私自上传用户邮件地址、Google 账户信息及指定文件列表信息，下载恶意子包，访问钓鱼网址。需警惕该程序造成的用户隐私泄露和财产损失，建议卸载。（威胁等级高）
		Trojan/Android.Bsihai.a[exp] 2018-07-25	该应用程序激活设备管理器，联网上传用户配置信息，通过返回网址数据，下载安装软件。会造成用户资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.lojaok.a[prv,fra,exp] 2018-07-26	该应用程序伪装正常应用，程序运行会隐藏图标，联网下载大量应用图标，打开钓鱼界面诱骗用户输入账号密码信息并联网上传，会造成用户隐私泄露和资费消耗，建议卸载。（威胁等级高）
		Trojan/Android.hzdracom.a[exp,rog] 2018-07-28	该应用程序伪装安全服务，安装无图标，包含风险代码，联网获取未知软件，静默安装，私自加载推送广告。会造成用户流量消耗，建议卸载。（威胁等级高）
	较为活跃的样本	Trojan/Android.QQspy.dl[prv,fra]	该应用程序伪装刷 Q 币工具，运行诱导用户手动输入账号密码、扫码支付等，包含发送短信的风险代码，会造成用户隐私泄露和资费损失，建议卸载。（威胁等级中）
		Tool/Android.JsMiner.g[exp,rog]	该应用程序运行后联网加载 js 挖矿脚本，通过用户点击执行挖矿脚本进行挖矿，造成用户手机性能下降，请谨慎使用。（威胁等级高）
		Trojan/Android.SmsSend.pc[exp,rog]	该应用程序运行后私发大量短信到指定号码，频繁弹出浮动窗口，造成用户资费消耗，影响正常使用，建议卸载。（威胁等级中）
		RiskWare/Android.AppCrack.a[sys]	该应用程序为盗版软件，篡改原始文件，具有一定的风险行为，请使用官方正版应用。（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 Access 远程代码执行漏洞 (CVE-2018-8312)	Microsoft Access 由于没有正确的处理内存中的对象，在实现中存在远程代码执行漏洞，远程攻击者诱使用户打开特制的文档，利用该漏洞安装程序，查看、更改或删除数据或创建新账户。（威胁等级高）
	较为活跃样本	Trojan[Downloader]/Win32.Dapato	此威胁是一种具有自动下载行为的木马类程序。该家族感染用户系统后，系统会自动连接到指定的网站，在本地下载并执行多种恶意软件。（威胁等级中）
		Trojan[Banker]/Win32.Banker	此威胁是一种以窃取网络银行敏感信息(如银行账号、密码、信用卡信息等)为目的的木马类程序。该家族通过恶意网站或已被感染的邮件进行传播。该家族可以监控用户的网络行为，在用户登陆银行网站时记录用户信息，并将所有收集的信息发送给黑客。（威胁等级中）
		Trojan[Backdoor]/Win32.Buterat	此威胁是一种后门类木马程序。该家族会在系统中打开后门，并注入其他的木马家族或恶意软件。该家族还可以允许黑客远程连接被入侵的电脑。（威胁等级中）
		Trojan/Win32.Delf	此威胁是一种由 Delphi 编译器编写的木马类程序。该家族的变种是依据编译器分类的。该家族一般无法主动传播，只能通过将自身伪装成正常软件欺骗用户下载运行，或者通过一些恶意网页的辅助、利用浏览器和插件的漏洞安装到用户的系统中。（威胁等级中）

（上接第一版）

引导启动，可以安装驻留型后门（PBD）与BANANAGLEE的通信结构协作，以便之后获得完全访问权。该PBD能够发出信标并且是完全可配置的。如果BANANAGLEE已经安装于目标防火墙，则SOUFFLETROUGH可以执行远程升级。

JETPLOW是针对思科500系列PIX防火墙，以及大多数ASA防火墙（5505/5510/5520/5540/5550）的恶意软件，功能与SOUFFLETROUGH基本相同，能够注入BANANAGLEE并安装PBD。类似地，FEEDTROUGH针对Juniper Netscreen防火墙，能够注入BANANAGLEE和另一款名为“兴趣点泄露”（ZESTYLEAK，功能尚不完全明确）的恶意软件。此外，还有一系列针对Juniper路由器的BIOS注入工具，包括“学院蒙塔纳”（SCHOOLMONTANA）、“山脊蒙塔纳”（SIERRAMONTANA）和“灰泥蒙塔纳”（STUCCOMONTANA）等，分别是针对Juniper J、Juniper M和Juniper S系列路由器，用以完成DNT相关植入程序的持久化。

HEADWATER是一个驻留型后门工具集，针对华为路由器。HEADWATER后门能够通过远程运营中心（ROC）远程传输到目标路由器。传输完成后，后门将在系统重启后激活。一旦激活，ROC就能够控制后门，捕获并检查通过主机路由器的所有IP数据包。HEADWATER是针对华为公司路由器的PBD的统称，相关文件还提到，NSA和CIA曾发起联合项目“涡轮熊猫”（TURBOPANDA）使用PBD来利用华为的网络设备。

DEITYBOUNCE提供一个软件应用程序，利用主板的BIOS和系统管理模块驻留在戴尔PowerEdge服务器中，操作系统加载时能够周期性的执行。该技术能够影响多处理器系统（RAI硬件和Microsoft Windows 2000、2003和XP操作系统），针对戴尔PowerEdge 1850/2850/1950/2950服务器。通过远程访问或物理访问，ARKSTREAM在目标机器上重新刷新BIOS，以植入DEITYBOUNCE及其有效载荷。

IRATEMONK通过注入硬盘驱动器固件，针对桌面和笔记本电脑提供持久化能力。通过主引导记录（MBR）替代以获得执行。这种技术针对不使用磁盘阵列的系统，支持西部数据、希捷、迈拓、三星等品牌的硬盘，支持的文件系统格式包括FAT、NTFS、EXT3和UFS。通过远程访问或物理访问，将硬盘驱动固件发送至目标机器，以植入IRATEMONK及其有效载荷。

根据维基解密披露的CIA“Vault 7”文档显示，CIA同样开发了大量具有持久化功能的网络攻击装备，包括“暗物质”（DarkMatter）、“午夜之后”（AfterMidnight）和“天使之火”（AngelFire）等。

DarkMatter是一组针对苹果主机和手机的恶意软件和工具，能够通过多种方式实现持久化，包括伪装成雷雳接口转换设备或进行固件植入，可通过人力作业或物流链劫持实现。AfterMidnight是一个恶意代码植入框架，能够向目标远程投放恶意软件，其主程序具有持久化能力，能够伪装成Windows系统的.dll文件。AngelFire是一个针对Windows计算机的恶意代码植入框架，能够通过修改引导扇区的方式，在Windows系统中安装持久化的后门。

通过以上介绍可以看出，美方的情报部门开发了大量针对各类网络和终端设备的持久化工具，这既是美方“持久化一切可以持久化的节点”理念的体现和实践基础，也从一个侧面反映了美方网络空间攻击装备全平台、全能力覆盖的特点。

无论是NSA还是CIA的持久化装备，其目的都是对关键网络或系统实现长期、隐秘的控制，为持续的情报窃取和未来可能的攻击行动、甚至发动网络战做准备。在这种情况下，我们应该认识到，关键信息基础设施的保护应该不仅仅是数据的保护，更重要的是要确保对网络与系统控制权的掌控。攻击者一旦获得了在关键信息基础设施中的“主宰”能力，能够实现随时从CNE到CNA的快速切换，关键信息基础设施安全便无从谈起。根据“敌情想定”的原则，有必要改变之前根据“既成损害事实”对潜伏网络威胁进行研判的传统模式，转为从总体国家安全观高度来确认支撑关键信息基础设施的网络设备和节点系统的国家安全重要性级别，并且将高级别关键信息基础设施中出现的攻击受控事件与持久化潜伏威胁作为必须“第一时间发现、第一时间猎杀、第一时间全网清除”的“零容忍”目标。

总书记强调：“我们必须深入研究，采取有效措施，切实做好国家关键信息基础设施的安全防护。”但在我国的信息化建设中，由于信息基础设施的不完备，信息化建设的“小生产化”等原因，我国在基础结构安全和纵深防御层面存在严重的先天基础不足；同时，由于在信息化建设过程中，没有充分考虑安全需求，导致更高级的安全手段，如态势感知、威胁情报等无法叠加在现有的网络环境中，难以形成动态综合的防御体系，难以有效对抗高等级威胁。因此，需要认真落实信息化和安全的同步建设，从信息化建设的开始就深入考虑安全需求，切实做到“安全与发展同步推进”。

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。

电子邮件网络攻击急剧上升，邮件安全风险增大

网络安全公司Mimecast近期发布了《2018邮件安全现状》报告，报告显示，攻击者持续针对终端用户发起邮件攻击，邮件攻击数量急剧上升。

调查显示，最容易出问题的人恰恰是公司的管理层。40%的受访者认为公司的CEO是公司网安的薄弱环节；另外，31%的高管会不小心将敏感信息发送给无关的人（普通员工的比例只有22%）。此外，2017年有92%的勒索软件都是通过邮件分发，造成了较大危害。90%的组织都表示邮件钓鱼攻击数量有所增长。但是，只有11%的企业不断培训员工识别网络攻击，而52%的企业每年只组织一次培训。Mimecast CEO表示，电子邮件攻击持续增长，除了常规的防御之外，企业还需要采取其他应对措施来确保安全。

原文链接：https://www.infosecurity-magazine.com/news/emailbased-attacks-a-growing-risk/

安天发布《Magniber 勒索软件分析报告》

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一种名为 Magniber 的勒索软件开始在亚洲地区活跃，其利用 Magnitude 漏洞利用工具包进行传播，使用多种混淆技术，并可根据地区判断是否主动进行感染。

自 2017 年起，Magnitude 漏洞利用工具包便开始向外传播 Cerber 勒索软件，但只针对于少数几个亚洲国家。2017 年 10 月，其开始传播开发者自己编写的勒索软件，Magniber。此次的攻击行动仅针对韩国，Magniber 会检测返回的国家代码，如果不符合要求就会自删除。恶意代码在初始阶段使用 VBScript 利用 CVE-2018-8174 漏洞，一旦漏洞利用成功，脚本会执行一段负责下载的 shellcode。它会下载经过混淆的载荷，使用 xor 进行解密。载荷运行后会加密系统文件，弹出勒索信息，给出到洋葱页面的链接。因其使用了 AES 算法加密，故每个密钥都是唯一的。

目前，Magniber 的感染区域已经开始扩展，影响区域包括马来西亚、新加坡以及中国的香港、澳门、台湾等地区。虽然 Magniber 勒索软件初期的代码简单且没有使用混淆，但其开发者在持续开发新版本，编码质量也在不断提高，对此应予以重视。

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、智能学习鉴定器、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、静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfbe293aa9dfc
文件类型	BinExecute/Microsoft.DLL[:X86]
大小	81 KB
MD5	72FCE87A976667A8C09ED844564ADC75
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.TSGeneric
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

◆ 文件元数据分析

描述	值
File Size	80 kB
File Type	Win32 DLL
MIME Type	application/octet-stream
Machine Type	Intel 386 or later, and compatibles
Time Stamp	2018-07-06 01:38:07+08:00
PE Type	PE32
Linker Version	11.0

Code Size	28160
Initialized Data Size	4776960
Uninitialized Data Size	0
Entry Point	0x4c80
OS Version	6.0
Image Version	0.0
Subsystem Version	6.0
Subsystem	Windows GUI

◆ UDP 信息

源 IP	源端口	目的 IP	目的端口
0.0.0.0	68	255.255.255.255	67
192.168.122.1	67	192.168.122.246	68
192.168.122.246	137	192.168.122.255	137
192.168.122.246	1025	192.168.122.1	53
192.168.122.1	53	192.168.122.246	1025
192.168.122.246	123	52.163.118.68	123
52.163.118.68	123	192.168.122.246	123
192.168.122.246	138	192.168.122.255	138

◆ 文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.dll	72fce87a976667a8c09ed844564adc75	N/A	N/A