安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 09 月 10 日 (总第 151 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（九）

——用于命令与控制的网空攻击装备

安天研究院

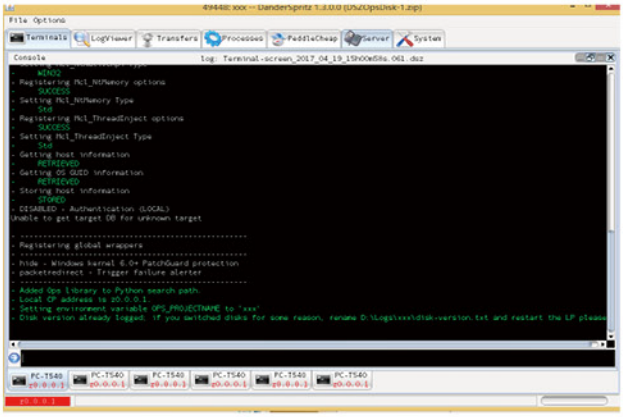
在之前的文章中，我们展开介绍了美国国家安全局（NSA）和中央情报局（CIA）用于实现漏洞利用的网空攻击装备，揭示了美方丰富的漏洞储备及强大的漏洞利用能力。在本期中，我们将对美方用于命令与控制的网空攻击装备与设施进行介绍，展现美方隐蔽而强大的命令与控制能力。

美国国防部军事和相关术语词典将“命令与控制”（Command and Control）定义为：在完成任务期间，由指定的指挥官对指派和附属部队行使权力和指挥，也称为 C2。该定义被延伸到网络空间，通常用以描述攻击者利用命令与控制基础设施向受害者发送命令与控制指令的行为。在通常的网络入侵行动中，攻击者需要和已经进入目标网络 / 系统的恶意代码进行通信，发送指令并获取数据，因此需要使用用于命令与控制的工具，尽可能地以安全、隐蔽的方式实现攻击者与植入恶意代码之间的通信。类比于传统空间中的谍报或特种作战行动，就像是由特工人员使用隐匿交联通道指挥被策反的“鼹鼠”开展情报窃取或蓄意破坏行动的过程。

为实现上述目的，NSA 在全球范围构建了大规模的隐藏基础设施，并通过部署在骨干网节点的“混乱”（TURMOIL）系统，进行数据的捕获和注入。在本专题（四）中，我们曾简要介绍了 NSA“湍流”（TURBULENCE）框架下的信号情报获取系统 TURMOIL，其依靠 RAMPART-A 等项目，能够对互联网数据进行获取和注入。据相关披露，截至 2013 年，NSA 至少已经建立了 13 个 RAMPART-A 站点，通过与其他国家合作的方式，获得互联网接入点。例如 NSA 曾与德国联邦情报局（BND）合作，由 BND 提供进入德国电信公司法兰克福互联网交换机中心的通道，NSA 提供复杂的设备。此外，NSA 还能够从包括海底光缆在内的 70 余种线缆中获取数据，进而获得全球范围的信息获取与流量注入能力，并通过秘密的通信网络将数据回传到 NSA。依靠这些基础设施和 NSA 的先进能力，美方能够将恶意软件获取的数据从其控制的互联网接入点中抽取出来，同样可以将 C2 指令通过其控制的接入点注入到互联网中，并且能够仿冒任何国家的 IP 地址，这使得美方具备了极强的高级反溯源能力。

在具体的 C2 装备方面，美方同样展现出了强大的一面。2017 年 4 月，“影子经纪人”（The Shadow Brokers）曝光了一系列有关 NSA 的资料，其中包括一个名为“SWIFT”的文件夹（SWIFT 即环球同业银行金融电讯协会，为国际银行间结算提供通讯业务），内容为美方对中东和拉美地区银行 SWIFT 系统的几起攻击行动，包括针对 EastNets SWIFT 服务局的攻击行动 JEEPFLEA_MARKET（具体目标为迪拜、比利时和埃及）和针对 BCG SWIFT 服务局的攻击行动 JEEPFLEA_POWDER（目标为巴拿马和委内瑞拉，据资料显示该行动当时并未成功）。

安天 CERT 对上述事件进行了复盘分析，攻击者使用了我们在本专题（七）中提到的“香蕉合唱团”（BANANAGLEE）工具，利用防火墙漏洞进入内网，之后在内网进行横向移动，最终获取了多个服务器的控制权，窃取重要数据。在这一过程中，攻击者使用了 DanderSpritz（DS）平台与植入的恶意软件进行 C2 通信。DS 是一个命令与控制平台，相关披露最早出现在棱镜事件中，后由影子经纪人曝光，该平台上的攻击工具和插件非常丰富且标准化，一旦 DS 的载荷植入远程主机即可方便地实现对植入物的命令与控制。DS 平台可以通过正向、反向、激活包三种方式与受害者建立连接，正向连接即攻击者通过平台主动与植入目标的恶意软件建立连接；反向即攻击者监听指定端口，等待恶意软件发起连接；激活包即攻击者向恶意软件发送一个 trigger 包，用来激活潜伏的恶意软件。同时，通过分析发现，DS 平台在通讯过程中采用严格加密，使得安全分析人员即使捕获了载荷样本也很难破解通信内容。



DanderSpritz 远程控制平台

通过 DanderSpritz 攻击平台，情报作业人员可以使用数百个插件进行组合来实现相

（下转第三版）

每周安全事件

类 型	内 容
中文标题	研究人员指出 Wireshark 三个 DoS 漏洞的 PoC 已出现
英文标题	Wireshark can be crashed via malicious packet trace files
作者及单位	Zeljka Zorz
内容概述	Wireshark 是世界上最受欢迎的网络协议分析仪。该软件是免费和开源的。研究人员发现 Wireshark 存在三个严重漏洞 :CVE-2018-16056、CVE-2018-16057 和 CVE-2018-16058，影响 Wireshark 的三个组件：蓝牙属性协议（ATT）解剖器，Radiotap 剖析器和音频 / 视频分发传输协议（AVDTP）解剖器。 研究人员称可以公开获得每个漏洞的概念验证（PoC）的利用代码。攻击者可以通过将格式错误的数据包注入网络、受影响的应用程序处理、或者诱使目标用户打开恶意数据包跟踪文件来利用这三个漏洞。
链接地址	https://www.helpnetsecurity.com/2018/08/31/wireshark-dos-vulnerabilities/

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 6 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	AdWare/Android.lladscat.a[ads] 2018-09-03	该程序包含 lladscat 广告插件，通过插屏、积分墙等形式推送广告，请谨慎使用。（威胁等级中）
		Trojan/Android.LockScreen.bn[rog,lck] 2018-09-04	该程序伪装为百度网盘，点击后进入色情图片勒索页面，要求付费解锁，建议卸载。（威胁等级中）
		Trojan/Android.Triout.a[prv,spy] 2018-09-05	该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、浏览器历史记录、手机存储文件、社交软件记录等大量隐私信息，私自拍照、录音、录像，监听通话和短信，并将隐私信息上传至服务器，造成用户隐私泄露，建议立即卸载。（威胁等级高）
	较为活跃的样本	G-Ware/Android.HiddenAds.fh[exp,rog]	该程序伪装成系统应用，运行后隐藏图标，后台推送广告，造成用户资费损耗，建议卸载。（威胁等级低）
		Trojan/Android.Socksbot.e[prv,bkd]	该应用运行后隐藏图标，后台私自通过 socket 连接实行端口转发，上传用户手机基本信息、地理位置、IP 地址信息，警惕程序存在后门，窃取用户隐私信息，建议卸载。（威胁等级中）
		Trojan/Android.Mobilespy.ay[prv,spy]	该程序加壳，运行时隐藏图标，运行后获取用户短信、通讯录信息、通话记录、微信消息等信息，并通过网络上传造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Locker.au[rog,lck]	该应用伪装游戏工具，运行后置顶色情图片，要求用户添加 QQ 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）
		G-Ware/Android.Subapp.a[exp,rog]	该程序是非官方应用，运行私自下载推广应用，伪装升级诱导安装，同时会推送广告，造成用户流量资费损耗，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	Windows VBScript Engine 代码执行漏洞（CVE-2018-8373）	该漏洞影响 Windows 最新版本的 VBScript 引擎，攻击者可利用该漏洞执行 shellcode。（威胁等级高）
	较为活跃样本	Trojan[PSW]/Win32.Overg	此威胁是一种可以窃取密码信息的木马类程序。该家族的样本运行后会窃取用户账户信息，如账号密码等。（威胁等级中）
		Trojan[Spy]/Win32.Spybox	此威胁是一种可以监视用户系统的木马类程序。该家族样本运行后监视用户操作系统并记录敏感信息，如击键等。（威胁等级中）
		Trojan[Backdoor]/Win32.BasicHell	此威胁是一种带有后门的木马类程序。该家族的样本运行后可以使攻击者访问受害系统，可以窃取系统信息，执行远程命令。（威胁等级中）
		Trojan[Dropper]/Win32.DNet	此威胁是一种木马程序。该家族的样本运行后可以安装其他恶意代码或者用户不想安装的软件。（威胁等级中）
		Trojan[Backdoor]/Win32.Zdemon	此威胁是一中木马程序。该家族的样本运行后允许攻击者远程控制计算机。它可以监听任意的端口，默认监听的端口有 31、556 和 6051。（威胁等级中）

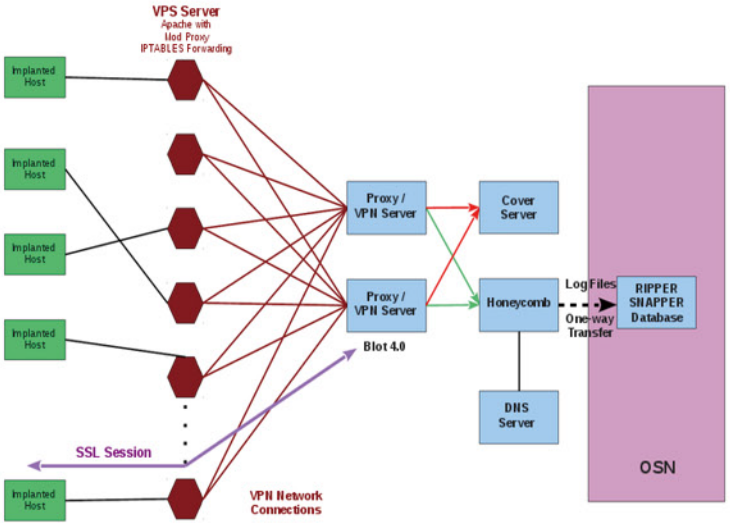
(上接第一版)

应功能，对目标设备进行全方位的控制。这些插件体现了如下架构风格——不再采用功能高度复杂的单一木马模式，而是把功能拆解成高度独立的小模块，这种拆解的粒度，几乎到了“原子化”的程度，即使在简单如获取系统信息的操作中，也把类似获取环境变量、语言集、网络状态等都作为一个独立的小模块，这将保证系统作业可以完全按需展开，从而最大化的保证作业的谨慎和静默，以规避网络与主机侧基于特征检测机制的匹配发现，从而确保命令与控制行为的隐蔽性，进而保证其进攻性网空行动的安全性。

此外，NSA 先进网络技术组（ANT）开发的“拇指水”（HALLUXWATER）和“水源”（HEADWATER）装备也包含命令与控制模块。HALLUXWATER 是针对华为防火墙的装备，利用“涡轮熊猫”（TURBOPANDA）注入工具与 NSA 的攻击者通信，使攻击者能够隐蔽地对内存进行读写操作和执行程序。HEADWATER 是针对华为路由器的攻击装备，利用数据网络技术组（DNT）的“粉碎机”（HAMMERMILL）注入工具来控制驻留型后门，捕获并检查通过主机路由器的所有 IP 数据包。

CIA 同样开发了各种用于命令与控制的装备。2017 年 5 月，维基解密在“7 号军火库”（Vault 7）中披露了“雅典娜”（Athena），该装备能够感染所有版本的 Windows 设备（Windows XP 至 Windows 10），并实现对目标设备的远程命令与控制，一旦安装在目标设备上，恶意软件就会提供包括配置和任务处理在内的远程命令与控制功能。

另一款 CIA 的攻击装备“蜂巢”（Hive）则更具代表性。Hive 是一款具有隐蔽通信能力的命令与控制平台，在 Vault 7 及后续的“8 号军火库”（Vault 8）中都进行了披露。通过 Hive，CIA 情报作业人员能够以安全隐蔽的方式与被控设备进行通信。首先，被植入主机发出的流量会通过虚拟专用服务器发送到 CIA 的代理服务器，Hive 会通过特定的方式区分主机的正常流量和植入物发送的流量，把流量分配到不同的服务器，对于正常的流量会返回正常的结果，对于植入物发送的流量会在识别后分配到 CIA 的后台服务器进行处理。同时，Hive 的控制端与植入物之间通过加密通信传输 C2 指令和数据，这样即使植入物被发现，由于难以掌握攻击者通信的特征和加密方式等，也很难通过互联网溯源到 CIA。



Hive 架构

对于物理隔离的网络，美方也能通过多种方法实现命令与控制。在本专题（六）中，我们曾介绍过一款 CIA 用于突破物理隔离的恶意软件“野蛮袋鼠”（Brutal Kangaroo），能够通过感染 U 盘进入内网，并能够在多个控制的内网节点间建立隐蔽的通讯网络，之后通过 U 盘摆渡的方式实现命令与控制，传递数据和指令；NSA 的“吼猴”（HOWLERMONKEY）是一组中近距离射频收发器，大小只有几毫米到几厘米，十分便于隐藏，能够分别配合其他装备进行射频通信，结合人力情报作业，实现不依赖于网络连接的命令与控制；NSA 的“阴暗恶棍”（SOMBERKNAVE）则试图利用目标自带的 802.11 设备建立无线网络连接，该恶意软件能够控制计算机的 802.11 网络设备，尝试搜索无线接入点，一旦有可用的网络连接，该软件便能够与攻击者建立通信，接受指令，下载新的载荷，进行进一步的入侵。

通过上述的介绍可以看出，以 NSA、CIA 为代表的美方情报部门开发了一系列具有命令与控制能力的攻击平台和武器装备，功能原子化、目标全覆盖，且针对不直接与互联网联通的“物理隔离网络”也进行了能力适配，再次体现了美方网络空间攻击装备模块化、全平台、全能力的特点。面对这种情况，对于我国的关键信息基础设施防护来说，必须建立客观的敌情想定，立足于与被保护关键信息基础设施业务重要作用相适应的威胁假设，设计、建设与实施综合的防御体系。假定敌方已经侵入我方内网，以及假定敌方已经建立了 C2 通道，开展积极协同的网络安全对抗。

具体来说，参考网络安全叠加演进模型，首先在基础结构安全方面，需要设计合理的网络架构，增强网络的可管理性，认真落实漏洞与补丁管理、策略管理、统一信任管理等安全措施，并通过合理配置与安全加固，收缩攻击面，提升对手获得控制权的难度与成本。在全面纵深防御方面，要确保安全防护措施与信息系统物理和环境、网络和通信、设备和计算、应用和数据等各个逻辑层次深度结合，并全面覆盖信息系统的每一个角落，在对手可能的通信路径上，设置多个安全监测点与防御点，并通过合理的安全规则设置（如防火墙规则等），进一步限制对手的行为。同时，坚持“面向失效的设计”理念，考虑每一项安全手段失效的“后手”，做到层层防御，提高发现威胁的可能。对于某些高信息价值、高防护等级的网络来说，可以根据业务情况，构建基于白名单的安全环境，限制程序、主机的网络访问行为，对于白名单规则以外的访问行为一律认为非法。在基础结构安全和全面纵深防御的基础上，需要建设全面持续的监测系统，通过对信息的汇聚和分析，实现全天候全方位的态势感知能力，同时结合内外部威胁情报，及时发现威胁，并依靠相应的安全团队和响应与处置系统，进行威胁猎杀，及时止损。

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。

安天发布《njRAT 木马及其变种 H-Worm 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 njRAT 木马及其变种 H-Worm。njRAT 远控工具被发现于 2013 年，也被称为“Bladabindi”，在中东非常流行。它可以对受害者的机器进行完全控制，攻击者几乎可以看到受害者的所有信息。攻击者一般使用流行的游戏或者应用软件的破解及注册机来传播该远控，攻击受害者。H-Worm 是一个基于 njRAT 的远控，但它是用 VBS 脚本编写。与 njRAT 相同，它也使用动态 DNS 及相同的控制，不同的是，它使用了 POST 请求将用户信息放在 HTTP User-Agent 段回传给攻击者。

njRAT 包括控制端和被控端，其被控端是由控制端根据自身的 IP 自动生成的。被控端机器上线后，通过控制端可以看到下列内容：屏幕缩略图、被控端编号、受害者 IP、受害者机器名、用户名、被感染的时间、标记、国家、操作系统、摄像头、版本、延迟、当前活动窗口等。控制端可以对被控端做如下操作：管理（包括文件、进程、连接、注册表、远程 shell 及服务的操作）、运行文件（包括通过网络下载文件后运行）、远程桌面查看、远程摄像头、麦克风控制、获取密码、键盘记录器、开启与被控端的聊天窗口等。H-Worm 是 njRAT 的变种，控制端的功能与 njRAT 如出一辙，其被控端被绑定了应用软件的安装程序，运行后启动安装对话框，释放载荷 VBS 脚本，该脚本经过了多层加密，其中包含 C&C 的域名 si******.zapto.org 及端口 7895。

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	bd36dfdb6de9b3785f089dca00c2bbcbdd01a158b6112c5505119c3c9464ef9f
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	262 KB
MD5	E2476ED98A57BBB14F45FD1E04D4C43C
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.SGeneric
判定依据	静态分析

完整报告地址：https://antiy.pta.center/_lk/details.html?hash=E2476ED98A57BBB14F45FD1E04D4C43C

◆ 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	262 kB
File Type	Win32 EXE
MIME Type	application/octet-stream
Machine Type	Intel 386 or later, and compatibles
PE Type	PE32
Linker Version	8.0
Code Size	2560
Initialized Data Size	2048
Uninitialized Data Size	0
Entry Point	0x1000
OS Version	4.0
Image Version	0.0
Subsystem Version	4.0
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
.....	.....	.....	.....

◆ 文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.exe	e2476ed98a57bbb14f45fd1e04d4c43c	N/A	N/A