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 21 日 (总第 136 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（二）

——美国大型信号情报获取项目

安天研究院

在上一期，我们从战略、能力、产业和技术等方面分析了美国在网络空间的优势，对美国具备网络空间进攻性职能的国家安全机构、多样的信号情报获取项目、全平台全功能的网络攻击装备体系进行了简要介绍，从整体上展现了美国在网络空间中强大的、体系化的情报、攻击、威慑和防御能力。在本期中，我们将聚焦美国的大型信号情报项目，呈现其强大的信号情报（SIGINT）获取能力，以及美国将传统信号情报与网络空间情报作业有机融合的明显趋势。

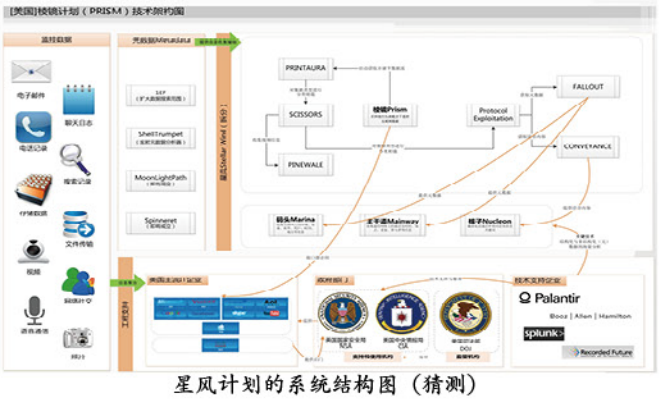
信号情报是一种有效的情报获取方式。早在一战时期，英国情报机构就通过搭接海底电缆的方式截获德国的通信。随着无线电通讯的应用，信号获取变得更加容易，通过轮船、飞机、卫星、地面站等都可以实现对信号的搜集。进入到 21 世纪，计算机网络的发展和普及，使得越来越多的信息通过网络传递，网络就成了情报获取的重要来源。

美国极其重视信号情报工作。斯诺登曾披露了一份美国国家安全局（NSA）的绝密文件《信号情报任务战略规划（2008–2013）》，由 NSA 组织 250 多个单位共同参与完成，目的是提高信号情报重点任务的性能，并将情报及时地转化为重大的国家成果。另一份绝密文件《信号情报战略（2012–2016）》旨在“确保信号情报为全面提升美国国家安全利益提供决定性的优势”。

美国开展了大量的信号情报获取项目和计划，以实现其“监听一切”的目的。这类项目或计划多由 NSA 负责具体实施，包括发起于 20 世纪 60 年代针对卫星通讯的“梯队”（ECHELON）项目、监听目标涵盖美国公民的“星风”（STELLARWIND）计划、针对全球网络安全厂商的“拱形”（CAMBERDADA）计划、针对电话监听的“神奇”（MYSTIC）项目、从网络骨干光缆和交换机上复制光信号的“逆流”（UPSTREAM）项目等。这些项目涵盖了网络、卫星、电话等多种信号情报源，共同支撑起了 NSA 强大的全球信号情报获取能力。

“星风”计划

星风是四个监视项目的统称代号。2001 年 911 事件之后，在《爱国者法案》的授权下，



星风计划的系统结构图（猜测）

NSA 的情报监视范围扩大到了美国公民。早在 2004 年，就有人注意到这些项目并展开了调查，奥巴马上台后，宣布这些项目都于 2011 年结束，但从多种来源分析，针对美国内的监视或已结束（或更为隐蔽），但不论其功能（对外国人应用不违反美国法律）还是数据都仍在使用。

星风包含的四个监视项目分别是：“棱镜”（PRISM）、“主干道”（MAINWAY）、“码头”（MARINA）以及“核子”（NUCLEON）。棱镜是一项由 NSA 自 2007 年起开始实施的绝密级电子监听项目，主要作用是利用美国主要互联网企业所提供的接口进行情报作业。从目前信息看，谷歌、微软、苹果、脸谱等多数美国主流 IT 企业与此计划存在关联。主干道和码头项目分别对通信和互联网上数以亿兆计的“元数据”进行存储和分析（在对电话和互联网监视的语义下，元数据主要指通话或通信的时间、地点、使用设备、参与者等，不包括电话或邮件等的内容）。核子项目负责截获电话通话者对话内容及关键词，相比于主干道和码头，核子项目更加聚焦于内容信息的获取，通过拦截通话以及通话者所提及的地点，来实现日常的监控。

关键得分（X-KEYSCORE）项目

X-KEYSCORE 是斯诺登曝光的 NSA 绝密项目之一，《卫报》对其做了较为详细的报道。它最初是针对邮件和浏览器活动的采集和分析，并建立了庞大的“指纹”系统，随

（下转第三版）

每周安全事件

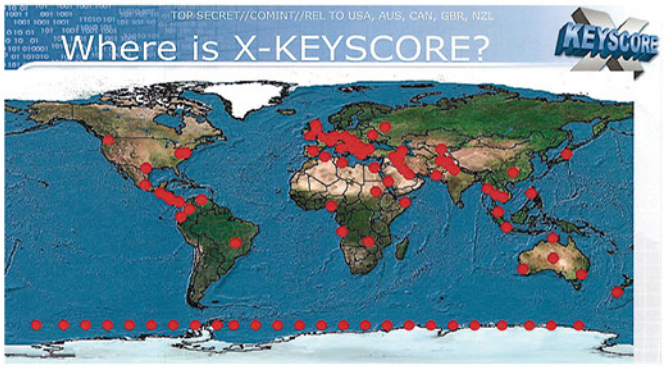
类 型	内 容
中文标题	DDoS 放大攻击新手段：利用 UPnP 协议绕过防御
英文标题	DDoS Attacks Leverage UPnP Protocol to Avoid Mitigation
作者及单位	Catalin Cimpanu
内容概述	研究人员发现，黑客现在采用新的手段来对抗反 DDoS 方案。黑客会使用通用即插即用（UPnP）协议来掩盖网络数据包的源端口。DDoS 解决方案公司 Imperva 表示，它发现至少有两次 DDoS 攻击用到了这种技术。 问题的来源在于通用即插即用（UPnP）协议，这个协议原本的目的是简化在本地网络上发现附近设备的过程。UPnP 协议的特点是它能够将互联网连接转发到本地网络。把连接映射到本地。 此功能能够被用来穿透 NAT，网络管理员也可以远程访问内网里的服务。使用 UPnP 进行 DDoS 可以达到显著的效果，因此如果没有意外的话会被黑客们广泛使用。建议大家如果没有使用的需要就把路由器的 UPnP 功能关闭。
链接地址	https://www.bleepingcomputer.com/news/security/ddos-attacks-leverage-upnp-protocol-to-avoid-mitigation/

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 7 个移动平台恶意代码和 7 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	Trojan/Android.kelefe.a[prv,spy] 2018-05-14	该应用程序伪装成系统应用，运行后会窃取用户短信、联系人、通话录音、位置、照片、微信数据等隐私信息上传服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.tenyent.a[prv] 2018-05-16	该应用程序伪装正常应用的插件，运行后隐藏图标，后台监听用户短信，私自上传用户短信，会造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.ZooPark.a[prv] 2018-05-16	该应用程序包含风险代码，运行私自窃取用户联系人、信箱、通话记录、位置、通话录音等隐私信息上传，会造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Bafors.a[prv,exp] 2018-05-16	该应用程序伪装成手电筒，运行私自发送短信，拦截用户短信并私自转发短信内容到指定号码和邮箱，会造成用户隐私泄露和资费消耗，建议立即卸载。（威胁等级高）
		Trojan/Android.panikrat.a[prv,rmt,spy] 2018-05-17	该应用程序运行隐藏图标，激活设备管理器，开机自启，拦截短信，发送短信，获取联系人信息，联网下载远程数据，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Syncer.a[exp] 2018-05-17	该应用程序重打包正常应用，运行后台联网获取下载信息，私自下载未知应用并动态加载，造成用户流量资费损耗，还会给用户手机带来安全风险，建议卸载。（威胁等级高）
		Trojan/Android.saldex.a[prv,spy] 2018-05-19	该应用程序伪装系统应用，运行隐藏图标，后台联网上传用户短信、通讯录、通话记录、录音等隐私信息，监听、拦截短信，会造成用户隐私泄露和资费消耗，建议卸载。（威胁等级中）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	微软 Office 内存损坏漏洞导致远程命令执行 CVE-2017-11882	Microsoft 微软在例行系统补丁发布中，修复了一个 Office 远程代码执行的严重漏洞，编号 CVE-2017-11882。该漏洞类型为缓冲区溢出，位于 EQNEDT32.EXE 组件。受害用户打开恶意的 Office 文档时，无需交互，就可能执行恶意代码。（威胁等级高）
	较为活跃样本	Trojan/Win32.Tepfer	此威胁是一种窃取用户密码的木马类程序。该家族也可能存在其他的恶意行为，如从浏览器缓存中窃取重要数据，以获取邮箱地址；或通过收集系统数据，为黑客未来的攻击行为做准备。（威胁等级中）
		Trojan/Win32.Inject	此威胁是一种木马类程序。该家族将自身以某种方式注入到其它进程中（避免用户和杀毒软件感知、清除），隐藏自身，并在后台执行恶意行为。因此该病毒家族是一种通过行为来命名、定性的木马类程序。（威胁等级高）
		Trojan[Dropper]/Win32.Dapato	此威胁是一种木马类程序。该家族运行后会释放多个恶意代码。该家族可以注入其它进程，加密用户文件，下载其它恶意代码等。（威胁等级中）
		Trojan[Backdoor]/Win32.Banito	此威胁是一种带有后门的木马类程序，可用于远程控制。该家族进入用户电脑后会为黑客打开后门，进行远程控制系统。（威胁等级高）
		Trojan[Downloader]/Win32.Cabby	此威胁是一种具有下载功能的木马类程序。该家族通过钓鱼网站、未知链接、下载黑客发布的免费软件及垃圾邮件附件等形式进行传播。（威胁等级中）
		Trojan/Win32.VBKrypt	此威胁是一种使用 VB 语言编写的木马类程序。该家族通过恶意网页进行传播。该家族的部分变种通过冒充一些常用软件来盗取信息。（威胁等级中）

（上接第一版）



X-KEYSCORE 全球分布

“拱形”计划目标分布

后发展为覆盖 VoIP、社交聊天等各种网上行为的监视和分析系统。X-KEYSCORE 在全球 150 个站点有 700 台服务器（2013 年数据），可对 3 天内的数据进行暂存，被称为 NSA 的谷歌系统。分析人员可以通过姓名、电话号码、IP 地址、浏览器等多种关键字来查找目标网络活动的内容数据和元数据。凭借该系统，NSA 可对互联网上特定目标的一举一动尽收眼底。据报道，仅 2008 年以前，X-KEYSCORE 就协助定位了 300 余名恐怖分子。

X-KEYSCORE 还具有良好的扩展性，可以与 NSA 的“湍流”（Turbulence）网络攻击作业体系集成或交互，对其他渠道采集的网络信息进行自动分析，并触发任务逻辑；也可以接受来自其他项目任务的数据（如外国卫星通信收集 SKIDROW 项目的数据），并提供分析处理功能；X-KEYSCORE 也为“五只眼”情报联盟各国使用和共享情报提供支持。此外，X-KEYSCORE 在建设中也充分引入了民间技术能力，例如大数据公司 Palantir 的海量数据分析和可视化分类服务能力为 X-KEYSCORE 提供了有力支撑。

“拱形”计划

2015 年斯诺登披露的一份 NSA 绝密文档介绍了拱形计划，该计划始于 2007 年，信息保障局（Information Assurance Directorate,IAD）和 NSA 威胁行动中心（NSA/CSS Threat Operations Center, NTOC）两个部门参与了该计划。该计划以俄罗斯反病毒厂商卡巴斯基等为目标，通过监听其样本上报渠道，从中分析安全厂商是否已发现、掌握其网络攻击武器。但“五只眼”情报联盟国家的反病毒厂商并不在内，可能说明“五只眼”相关情报机构与所在国安全厂商有直接的互动方式和沟通渠道，而无需通过监听的方式。该计划后续目标包括安天等 22 家全球重点网络安全厂商。

美国的大型信号情报获取项目众多，覆盖面广，持续时间长，使美国获得了强大的信号情报搜集能力。这些项目在打击犯罪、反恐、国家政策制定、重大问题决策等方面起到了重要作用，并为美国获得网络空间安全防御与反制、威慑、攻击等全方位优势奠定了基础。那么，运行这些监控项目需要什么样的支持体系，美国政府在这些项目中如何借助民间的技术和能力，这些监控行动如何与积极防御和反制相结合，监控如何与攻击行动结合，我们后续的文章会为您一一解答，敬请期待。

两大加密协议 PGP 与 S/MIME 被曝明文漏洞

近日，几名欧洲安全研究人员发现常用的 PGP 和 S/Mime 电子邮件加密协议存在两个严重漏洞，会以明文形式泄露用户加密邮件内容，以前发送过的邮件内容也可能被泄露。研究人员将相关漏洞命名为 EFAIL，并在周二早上发布了两个漏洞的详细研究报告。

目前暂时没有针对这个漏洞的可靠修复方案，研究人员提示，如果用户使用 PGP/GPG 或 S/MIME 加密敏感通讯，那么应当立刻在电邮客户端中禁用。此外，最好也禁用 Thunderbird、macOS Mail、Outlook 等邮件客户端中的相关加密插件。将加密插件从上述邮件客户端移除后，邮件就不会被自动加密。如果用户接收到了 GPG 加密的消息，也不要解密。

报告链接：https://securityaffairs.co/wordpress/72487/hacking/pgp-s-mime-tools-flaws.html

Adobe 修复 Acrobat、Reader 和 Photoshop 中将近 50 个漏洞

Adobe 修复了 Acrobat、Reader 和 Photoshop 中将近 50 个漏洞，包括 24 个严重的内存损坏漏洞，可被攻击者利用，在目标用户的上下文中执行任意代码，还会导致信息泄露或安全绕过等问题。

Adobe 通知用户，已经在 2017 年 10 月 15 日停止了对 Acrobat 和 Reader 11.x 的支持，11.0.23 版本是最终版本。建议用户更新到最新版本的 Acrobat DC 和 Acrobat Reader DC。此外，Adobe 还发布了针对 Windows 和 MacOS 版本 Photoshop CC 的安全更新。Photoshop CC 2018 的 19.1.4 版本和 Photoshop CC 2017 的 18.1.4 版本修复了在目标用户上下文中用于任意代码执行的临界越界写入问题。

报告链接：https://www.securityweek.com/adobe-patches-two-dozen-critical-flaws-acrobat-reader

安天发布《“熊猫”银行木马分析报告》

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款攻击世界多个国家银行的恶意代码，其名为“熊猫”。

“熊猫”银行木马在 2016 年被发现，它从 Zeus 银行木马中借用代码并在地下论坛中以工具包形式出售。2017 年 11 月，“熊猫”银行木马的攻击者利用黑色搜索引擎优化在搜索结果中置入恶意链接。2018 年 3 月，最新的“熊猫”银行木马开始针对日本金融机构进行攻击。

在 2016 年的早期版本中，“熊猫”木马通过网络钓鱼邮件传播，主要针对 Windows 操作系统。主要功能包括 Web 注入、用户活动屏幕截图、键盘输入记录、剪贴版粘贴（抓取密码并将其粘贴到表单）以及攻击 VNC 桌面共享系统。在今年最新的版本中，采用与之前相同的攻击技术，可以记录击键，劫持流行的 Web 浏览器和 VNC 会话并窃取个人信息。除了金融服务，它还针对加密货币网站，Facebook 和 Instagram 等主要社交媒体平台，以及 Skype 等消息应用程序和 Youtube 等娱乐平台。而针对不同国家地区的版本也有区别，针对日本时，攻击者删除了内容安全策略头文件：remove_csp−1，CSP 头是用于防止跨站点脚本（XSS）、点击劫持和其他代码注入攻击，这些攻击可以从其他可信站点执行恶意代码。针对拉美金融机构的攻击，其中大部分在阿根廷、哥伦比亚和厄瓜多尔，攻击目标包括社交媒体、搜索、电子邮件、娱乐和技术提供商等。

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。

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、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、动态行为鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	https://antiy.pta.center/_lk/details.html?hash=35A7E666942EB0C70E73D5DC502A97D2
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	200 KB
MD5	35A7E666942EB0C70E73D5DC502A97D2
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

◆ 危险行为

行为描述	危险等级
其他进程写入可疑数据	★★★
注入其他进程	★★★★
删除自身	★★★★

◆ 常见行为

获取计算机名称	★
请求加载驱动的权限	★
查询 windows product key	★★
获取驱动器类型	★
遍历进程	★
打开自身进程文件	★
读取自身文件	★★
释放 PE 文件	★
篡改系统文件创建时间	★★
查找指定内核模块	★
创建挂起的进程	★★
访问其他进程内存	★
自启动	★
自删除	★★

◆ 进程监控

PID	创建	命令行
1476	(null)	C:\WINDOWS\system32\svchost.exe
1876	(null)	C:\WINDOWS\system32\svchost.exe
1772	Desktop.exe	"C:\Documents and Settings\Administrator\Application Data\Foxit Software\Foxit Reader\StartPage\Skins\Normal\Black\ScrollBar\Horz\Desktop.exe"
1240	cmd.exe	"C:\WINDOWS\system32\cmd.exe" /c "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\upddb39c274.bat"