安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 10 月 22 日 (总第 156 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（十）

——利用无线信号通信的网空攻击装备

安天研究院

之前的文章中，我们分别展开介绍了美国国家安全局（NSA）和中央情报局（CIA）的多类用于不同攻击作业环节的网空攻击装备，包括突破物理隔离、持久化控制、漏洞利用、命令与控制等，揭示了美方在这些网空作业环节中的强大能力。这些装备的传播、通信、控制大多依赖于目标原有的网络或常规的移动介质，而在本文中，我们将介绍美方的一类不依赖目标网络，而是利用无线信号实现信息传递，进而绕过多数网络安全防护手段，实现信息窃取或内网渗透的网空攻击装备。

德国《明镜周刊》曾曝光了一份长达 50 页的资料，包含 NSA 的各类攻击装备共 48 个，其中绝大部分装备都出自 NSA 下属先进网络技术部（Advanced Network Technology, ANT）之手。在相关文件中，有一组用于室内监控的网空攻击装备名为“愤怒邻居”（ANGRYNEIGHBOR），功能包括计算机屏幕监控、识别定位、键盘记录和音频捕获等。

ANGRYNEIGHBOR 系列装备包括射频发生模块、射频反射模块、解调处理模块等，利用电磁波进行数据传输。射频反射模块能够对不同类型的信息进行采集，通过接收射频发生模块产生的射频信号，以特定的方式对信号进行调制，然后将调制后的信号重新返回给射频发生器，通过这种方式将获取的信息传递出去。射频发生器再将获取的信号进行处理或交给解调处理模块，恢复出屏幕内容、击键信息、音频内容以及识别定位信息等。该系列装备可以用于无法或者极难利用网络收集和处理信号的场景中，据已披露的资料显示，相关装备曾被美方用于对外国使馆和外交人员的监视计划中。

NSA-ANT “愤怒邻居”系列装备关系示意图

射频发生模块主要包括 CTX4000 和 PHOTOANGLO。CTX4000 是一种便携式的连续波雷达单元，不仅能够产生用于辐射目标系统的连续波信号，而且能够对重新辐射回来的信号进行收集并恢复出信息。PHOTOANGLO 是一个 NSA 与英国情报机构政府通信总部（GCHQ）的联合项目，用于开发取代 CTX4000 的雷达系统，根据披露的资料显示，从 2008 年 9 月开始，CTX4000 被 PHOTOANGLO 替换。PHOTOANGLO 同样具有产生连续波并接受返回信号的能力，同时 PHOTOANGLO 的重量非常轻，只有不到 10 磅（约 4.5 公斤），可以安装在小型的公文包中。

射频反射模块主要包括 RAGEMASTER、TAWDRYYARD、SURLYSPAWN 和 LOUDAUTO，分别用于计算机屏幕监控、识别定位、键盘记录和音频捕获等。当射频反射模块接收到射频发生模块发出的射频信号后，能够对信号进行调制，并将调制后的信号重新发送回射频反射模块。RAGEMASTER 用于收集目标计算机屏幕上的显示信息，通常隐藏在连接主机和显示器的 VGA 视频线中。TAWDRYYARD 用于识别和定位已经部署的 RAGEMASTER，作用半径达到 50 英尺（约 15 米）。TAWDRYYARD 的功耗很低，能够依靠纽扣电池运行数月甚至数年。同时，由于其设计简单，因此可以按照需求定制外形。另据披露的资料显示，其后续可能加入返回 GPS 定位的功能。SURLYSPAWN 用于收集目标键盘的输入信息，同样不需要安装任何恶意软件，而是隐藏在键盘的数据线中，兼容 USB 和 PS/2。LOUDAUTO 能够用自带的麦克风收集音频，声音采集的有效距离超过 20 英尺（约 6 米），同样能够按需求定制外形。

解调处理模块 NIGHTWATCH 是整个架构的重要组成部分，是一款便携式计算机，专门用于精确重建所捕获的计算机屏幕信号，输出视频以供间谍人员查看目标设备显示的内容。该设备恢复的视频信号来自 CTX4000 和 PHOTOANGLO 等雷达单元，也可能由其他的接收器产生。另外据曝光的资料显示，当时 ANT 正在设计 VIEWPLATE 以逐步取代 NIGHTWATCH 系统。

在泄露的 ANT 相关资料中，还有一款名为“火行”（FIREWALK）的攻击装备。FIREWALK 是一款双向网络植入物，隐藏在双层 RJ45/USB 连接器中，能够被动收集千兆以太网流量，还能够按照指令过滤流量和向网络中注入数据包。FIREWALK 除了能够利用目标网络进行通信外，还具有射频收发功能，能够与其他射频收发装备建立无线通信（例如与我们之前介绍过的“吼猴”HOWLERMONKEY），甚至能够与其他射频收发装备建立多跳连接，扩大通信范围。此外，我们在之前文章中介绍过的“水腹蛇 -1”（COTTONMOUTH-I）也是 ANT

（下转第二版）

（上接第一版）

的一款具有无线通信能力的攻击装备，隐藏在 USB 接口中，攻击者可以通过无线信号访问目标设备所在的网络。

CIA 同样开发了大量能够利用无线信号通信的网空攻击装备。在维基解密曝光的包含大量 CIA 网空攻击装备资料的“7 号军火库”（Vault 7）中，包含了一组针对苹果设备的名为“暗物质”（Dark Matter）的攻击装备，其中的“夜空”（NightSkies）是一款固件植入程序，专门针对新出厂的苹果手机，通过物理接触安装。该装备能够让 CIA 作业人员实现对手机的完全监控，包括进行信息窃取、监听等。Vault 7 中的另一款装备“摩天大楼”（Highrise）则针对安卓手机，披露的功能包括短信的窃取和远程控制等。通过这些装备，CIA 能够对重要目标的手机进行控制，利用手机的无线信道通信，获取关键信息。

另一个具有代表性的装备是 CIA 的“哭泣天使”（Weeping Angel）。Weeping Angel 是一款恶意软件，针对三星智能电视，通过物理接触植入，能够利用电视的麦克风实现录音和窃听，并通过 Wi-Fi 通信实现实时监听。由于披露的资料年代较早，并且基于美方网空攻击装备全平台、全能力的特点，可以合理地推测认为美方可能对大量智能硬件设备都进行了针对性地开发和适配。

这些网空攻击装备的植入、通信、控制均不依赖目标网络，而利用无线信号进行信息窃取或内网渗透，实现对多数现有网络安全防御手段的绕过。也因此，相应的软硬件装备（尤其是硬件装备）向目标系统或设备的植入，需要更多地依靠物理接触的方式。美方依靠其强大的 IT 产业优势，形成了供应链上游的控制能力，同时结合其情报机构在人力近场作业方面的能力专长，形成了对更多场景的信息获取和渗透能力。此外，由于隐蔽性需要，硬件装备的体积需要足够小，使用时间要足够长，因此无线信号的发射功率通常也较小，这也要求这类装备在成功部署后的使用过程中，依然需要依赖人力进行近场作业。这就对防御方的供应链安全保障和反人力情报作业能力提出了更高的要求。

在后续的文章中，我们将对美方的网空攻击装备体系进行分析总结，对美方未来的网空作业能力进行预测，敬请期待。

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 6 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.JsMiner.h[exp,rog] 2018-10-16	该应用程序包含 js 挖矿脚本，运行后会私自执行挖矿脚本进行挖矿，造成用户手机性能降低，建议卸载。（威胁等级中）
		Trojan/Android.HelperPushe.a[rmt,exp,prv] 2018-10-17	该应用程序运行隐藏图标，接收远程指令，弹出未知窗口页面，窃取用户短信，私自发送短信，安装指定 apk。造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.NGSuperShell.a[rmt,spy,bkd] 2018-10-18	该应用程序是一个名为 NG SuperShell 的 ELF 可执行后门程序，会接收远端发送来的文件或指令，并执行该文件或指令，建议立即删除。（威胁等级中）
	较为活跃样本	Trojan/Android.Wsspy.a[prv,spy]	该应用程序运行后隐藏图标，通过拨打指定号码弹出设置页面，上传手机固件信息、短信、位置、联系人、通话记录等隐私信息至指定网址，建议卸载。（威胁等级中）
		RiskWare/Android.Fakejiaoyou.e[fra,exp]	该应用程序伪装交友软件，通过发送虚假诱惑性消息，诱导用户付费，会造成用户资费损失，建议卸载。（威胁等级低）
		Trojan/Android.HalkBank.a[prv]	该应用程序伪装银行应用，窃取用户银行账户密码和收件箱短信，造成用户隐私泄露，建议卸载。（威胁等级中）
		RiskWare/Android.LockerMaker.i[spr,lck]	该应用程序为锁机生成器，用户可用来生成并使用锁机勒索工具，该程序暂未完善，存在恶意制造、传播勒索应用的行为，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	WebLogic 远程代码执行漏洞（CVE-2018-3191）	该漏洞允许未经身份验证的攻击者通过 T3 协议网络访问并破坏易受攻击的 WebLogic Server，成功的漏洞利用可导致 WebLogic Server 被攻击者接管，从而造成远程代码执行。（威胁等级高）
	较为活跃样本	GrayWare[AdWare]/Win32.Otezinu	此威胁是一种有广告行为的灰色软件类程序。该家族通常与正常软件捆绑到一起进行传播，它会在电脑上收集用户信息，并根据这些信息获取用户习惯并推送广告。（威胁等级低）
		RiskWare[Downloader]/Win32.DownloadSponsor	此威胁是一种下载广告软件的风险软件类程序。该家族会自动下载并运行用户不知情或不允许安装的软件，同时它也可以不断地检查更新文件本身。（威胁等级中）
		Trojan/Win64.Patched	此威胁是一种窃取账户信息的木马类程序。该家族样本基于 64 位系统，当用户打开 IE 浏览器时，该家族代码会执行打开文件，并将文件的 shellcode 读到内存中，同时还原 IE 浏览器入口点代码，然后创建一个线程执行恶意操作，并跳转到 IE 原入口地址继续执行。该家族会记录 Windows 登陆账户信息，试图窃取 SQL 账号密码信息，以 URL 方式发送到作者地址中。（威胁等级中）
		Trojan/NSIS.GoogUpdate	该病毒家族是一种使用 NSIS 制作的具有下载行为的木马类程序。该家族样本运行后安装浏览器扩展，收集用户的浏览记录并推送广告，也有可能下载恶意程序。（威胁等级中）
		Trojan/Win32.Bayrob	此威胁是一种可以窃取用户信息的木马程序。该家族样本运行后连接远程服务器，收集用户敏感信息并回传，包括操作系统版本、计算机名、计算机的 IP 地址、关于操作系统和系统设置的信息、MAC 地址及运行服务列表等。（威胁等级中）

并非所有多因子身份验证方法都“生而平等”

Alexandre Cagnoni / 文　安天技术公益翻译组 / 译

与几年前相比，现在更多的人熟悉了“两步验证”、“强身份验证”、“双因子身份验证”（2FA）和“多因子身份验证”（MFA）这些术语。MFA 解决方案旨在保护用户凭证并简化口令管理，其方法是：在身份验证过程中，除了使用口令，还要添加一个或多个验证因子。这些验证因子可能是你拥有的东西（例如令牌）、你本身具备的生物特征（如指纹或虹膜扫描），或者你知道的其他内容（如口令保护问题）。随着安全行业对凭证窃取的日益关注，许多 MFA 解决方案应运而生，涌入安全市场。这引发了一个问题：所有 MFA 方法都同样有效吗？

事实上，MFA 包括很多种方法。相比来说，其中一些方法的安全性要更好一些。下面，我们将分析一些常见的 MFA 方法，并探索哪些验证因子更加有效。

短信动态口令（OTP）

使用短信作为第二个身份验证因子的方法很常见。该方法通过短信将随机的六位数验证码发送到用户的手机号码上。理论上说，只有持有该手机号码的人才能进行身份验证，但事实并非如此——有几种经过验证的方法能够破解短信 OTP。例如，2018 年 6 月中旬，攻击者通过短信拦截攻破了新闻和娱乐网站 Reddit。虽然该攻击并未导致太多私密信息泄露（而且 Reddit 出色地响应了攻击），但它表明短信身份验证并不像通常所认为的那样安全。举例来说，黑客可以利用蜂窝网络的漏洞来拦截短信；也可以在受害者手机上安装恶意软件，将短信重定向到攻击者的手机。此外，黑客还可以对手机运营商发动社会工程攻击，获得与受害者号码相关联的新 SIM 卡，从而接收 OTP 消息。事实上，美国国家标准与技术研究院（NIST）早在 2016 年就不赞成使用短信身份验证了，指出该方法已经不再安全。不幸的是，许多公司到现在仍然依赖短信 OTP，他们给用户带来一种虚假的安全感。

硬件令牌

硬件令牌验证是仍在使用的最传统的 MFA 方法之一，令牌通常采用密钥卡（key-fob）格式，有一个显示屏，用于显示基于时间同步的 OTP。在该方法中，硬件本身会保护其内部唯一密钥。但是该方法也存在缺点，包括：必须随身携带、价格昂贵、需要物流运送、必须不时更换等。某些硬件令牌还需要与电脑的 USB 连接，如果用户通过手机或平板电脑进行身份验证，可能会非常棘手。

手机令牌

最常见的手机令牌运作原理跟硬件令牌一样，只不过它们是手机应用程序。与硬件令牌相比，手机令牌最大的优势是：除了智能手机，用户不需携带其他任何东西。在该方法中，最重要的步骤是检查唯一密钥是如何生成的，即检查“激活过程”。通过二维码（例如 Google Authenticator 二维码）提供所有密钥和凭证，并不是一个好主意，因为任何获得该二维码副本的人都能够克隆令牌。

基于推送的身份验证令牌

在手机令牌和短信验证基础上，出现了安全推送验证技术。随着其可用性的提高，该方法越来越受欢迎。与短信不同，推送消息不包含 OTP。相反，它包含的是加密消息，只能由用户手机上的特定应用程序解密。因此，用户能够根据情境信息确定正在发生的登录尝试是否是真实的，然后快速同意或拒绝身份验证。如果同意验证，则用户手机上的令牌会生成唯一的 OTP，并将其发回以进行验证。并非所有 MFA 解决方案都会生成 OTP 进行验证，这会增加“推送消息”被模仿或伪造的风险。

基于二维码的身份验证令牌

基于推送的令牌需要手机的数据连接，而基于二维码的身份验证则可以脱机工作，并通过二维码提供情境信息。用户使用身份验证应用程序扫描屏幕上的二维码，该应用程序会根据唯一密钥、时间和情境信息生成一个 OTP，用户只要输入该 OTP 就行了。这种流畅的用户体验非常重要，这就是基于推送和基于二维码的令牌受欢迎的原因。如果 MFA 方法过分地减慢登录过程，人们可能不会再使用它，因而可能更容易受到不安全口令的影响。

总结

在上文中，我们介绍了各种身份验证方法的优点和潜在的缺点。但在选择 MFA 解决方案时，我们还需要考量其他一些因素。例如，大多数人认为硬件令牌比使用推送和二维码技术的手机令牌更安全——事实并非如此。假设，一名俄罗斯攻击者试图使用窃取的凭证，连接到一家公司的虚拟专用网（VPN）。如果用户拥有硬件令牌，攻击者可能会使用社会工程手段（打电话或发送钓鱼邮件），诱骗用户提供 OTP——很多用户都会上钩。现在我们假设，该用户收到了一条推送消息：“你的帐户正在从俄罗斯的一台计算机登录，试图连接你的 VPN，是否同意？”这样的消息很难说服用户同意连接。

现在有许多不同类型的身份验证方法，但并非所有方法都能提供相同级别的安全性。如果你要使用某种 MFA 解决方案，请确保克服它的缺点，并清楚地了解使用该方法能够获得的安全性和风险级别。

原文名称	Not All Multifactor Authentication Is Created Equal
作者简介	Alexandre Cagnoni。Alexandre Cagnoni 是 WatchGuard Technologies 公司的身份验证总监。
原文信息	2018 年 10 月 11 日发布于 Dark Reading 原文地址 https://www.darkreading.com/endpoint/authentication/not-all-multifactor-authentication-is-created-equal/a/d-id/1332991
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

安天发布《Danabot 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种名为 Danabot 的银行木马开始活跃。DanaBot 银行木马初始被发现时是针对澳大利亚和欧洲银行，但新的研究表明目前其活动也开始针对美国银行。

DanaBot 是一种用 Delphi 编写的模块化的银行木马程序，试图从网络银行网站窃取账户凭据和信息。它会通过各种方式来窃密，例如截取活动屏幕截图，窃取表单数据或记录用户击键等。然后收集这些被盗信息并将其回传命令和控制服务器。研究人员首次发现 DanaBot 时，一个小组正在使用它来攻击澳大利亚银行。随着时间的推移，其他攻击者开始使用 DanaBot 攻击其他地区。随着从流量中发现更多不同 ID 的攻击者，研究人员推测 DanaBot 可能已经被公开出售或者租用，卖家可以从中获取利润。此次攻击北美的活动是通过垃圾邮件传播，邮件伪装成来自 eFax 的传真，提示用户下载 Word 文档，该文档是一个包含恶意宏代码的文档，文档会引诱用户点击启用宏的按钮，之后会下载 DanaBot 和其他恶意代码，研究人员发现，新的 DanaBot 活动的目标包括美国银行、富国银行、道明银行、皇家银行和摩根大通。

安天 CERT 提醒广大政企客户，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。确保没有任何计算机运行直接连接到 Internet 的远程桌面服务，而是将运行远程桌面的计算机放在 VPN 之后，只有使用 VPN 才能访问它们。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：

文件来源于内部组件，经由 BD 静态分析鉴定器、文件来源信息分析鉴定器、文件元数据分析鉴定器、数字证书鉴定器、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 静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	288615e28672e1326231186230f2bc74ea84191745cc40369d49bf385bf9669b
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	451 KB
MD5	00EFE74D64877E267420B35A19B7D84C
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Generic
判定依据	BD 静态分析

报告链接：https://antiy.pta.center/_lk/details.html?hash=00EFE74D64877E267420B35A19B7D84C

◆ 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	行为描述	危险等级
删除自身	★★★★	延时	★★★

◆ 常见行为

行为描述	危险等级
释放 PE 文件	★
获取驱动器类型	★
查找指定内核模块	★
创建特定窗体	★
连接网络	★

◆ 文件扫描

文件名	文件 MD5	家族相似性	yara 扫描
target.exe	00efe74d64877e267420b35a19b7d84c	N/A	N/A
target.dll	7bde107ca19dd9b4528658829f2dd98d	N/A	N/A
target.exe.dmp	e956388d8a411e9eb66d6e42609e3e61	N/A	N/A
target.dll	2ffb876b49e3be2750c9ce33bccea59c	N/A	N/A