安天周观察

主办：安天　2017 年 4 月 17 日（总第 83 期）试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

2016 安天基础威胁年报（公开版）发布

近日，安天安全研究与应急处理中心（安天 CERT）发布了 2016 安天基础威胁年报《2016 网络安全威胁的回顾与展望》（公开版），在这份几经易稿形成的“观点型”年报中，安天非常谨慎又沉重地提出了以下思考和观点：

1. 高级持续性威胁 (APT) 的普遍存在是网络空间的常态

APT 攻击是网络空间的常态存在，而其增量更多地来自新兴目标场景的拉动和新玩家的不断入场。APT 的攻击重点“转移”到关键信息基础设施既是一种趋势，更是一种既定事实，对超级攻击者来说，关键信息基础设施一直是 APT 攻击的重点目标，这种攻击围绕持续的信息获取和战场预制展开，在这个过程中，CNE(Cyber Network Exploitation，网络情报利用）的行为是 CNA(Cyber Network Attack，网络攻击）的前提准备。

商用攻击平台、商用木马和漏洞利用工具等网络商业军火全面降低了 APT 攻击成本，提升了攻击追溯难度。高级的网络攻击未必使用高级的技巧和装备，APT 攻击者劫持普通恶意代码，包括全面伪装成普通的黑产犯罪，可能会成为一种趋势。

2. 大规模数据泄露导致“威胁情报反用”

网络黑色产业链造成了大量数据泄露，这些海量敏感数据构成了黑产大数据。黑产大数据除了用于精准的广告投放，还会被不法分子滥用，给互联网用户带来更严重、更直接的经济损失。也有部分观点认为大规模数据泄露也是一种威胁情报来源，这些数据其实属于网民个体的信息，同时其数据组织本质上是泄露方的资产。威胁情报不只是防御方的资源，威胁情报也是情报威胁，是攻防双方的公共地带。

3. PC 恶意代码针对重要目标，移动恶意代码快速增长，勒索软件成焦点

2016 年安天捕获的新增传统恶意代码家族数为 1,280 个，新增变种数为 912,279 种，这些变种覆盖了亿级的样本 HASH。传统恶意代码的增量开始放缓，移动和新兴场景的恶意代码开始不断上升。同时，APT 攻击作业中的恶意代码样本，模块化和抗分析的特性进一步增强。而无论 PC 端还是移动端，勒索软件都成为重要威胁。其不再只是一种恶意代码类型，而成为一种典型的黑色经济模式。

4. IoT 威胁影响国家基础设施安全，车联网安全成为威胁泛化的年度热点

安全威胁泛化已经成为常态，安天依然采用与 2014 年、2015 年年报中发布“网络安全威胁泛化与分布”一样的方式，以一张新的图表来说明 2016 年威胁泛化的形势。

5. 供应链主战场的战争序幕正在拉开

随着网络安全威胁范围的逐渐扩张，供应链安全成为当前热点的安全问题，对供应链安全的关注不仅是最终的供给，而且包括了形成供应链的所有环节。供应链从来就不只是网络对抗中的外围阵地，而是更为核心和致命的主战场。

6. 2016 年度工作总结

面对威胁和挑战，安天将选择做具有体系化视野和解决方案的能力型安全厂商。基于自主创新的威胁检测防御核心技术产品服务，推动积极防御、威胁情报与架构安全和被动防御的有效融合，致力于提供在攻击者难以绕过的攻击环节上叠加攻击者难以预测的安全能力，达成有效防护和高度自动化以及可操作化的安全业务价值，这将是未来安天所选择的道路。

以上内容节选自 2016 安天基础威胁年报，报告完整内容可登陆安天官网 http://www.antiy.com/ 或微信公众号“安天”(antiylab) 查看。

每周安全事件

类 型	内 容
中文标题	“无文件攻击”威力初显：仅需一夜轻松窃走俄罗斯 ATM 80 万美元
英文标题	ATMitch-Crooks stole $800，000 from 8 ATMs in Russia using Fileless Malware
作者及单位	Pierluigi Paganini；Security Affairs
内容概述	近日，据卡巴斯基安全实验室消息称，黑客通过新型恶意软件 “ATMitch”采用“无文件攻击”方式，一夜之间成功劫持俄罗斯 8 台 ATM 机，窃走 80 万美元。这起网络劫持事件成功引起了安全专家的注意，他们在分析闭路电视录像时发现一名男子至 ATM 机旁并未与机器交互即可获取现金。据悉，受影响银行的安全团队并未发现任何恶意软件入侵迹象，唯有一家目标银行表示曾在 ATM 中发现两份入侵日志。 银行安全团队表示，他们不仅发现 Microsoft 域控制器 (DC) 的物理内存中存在其代码副本，还发现黑客将恶意代码直接注入受感染内存中与恶意软件一同在 RAM 系统中运行。目前卡巴斯基安全专家已将该此类恶意软件标记为 MEM：Trojan.Win32.Cometer 与 MEM：Trojan.Win32.Metasploit。
链接地址	http://securityaffairs.co/wordpress/57881/cyber-crime/atmitch-fileless-malaware.html

每周值得关注的恶意代码信息

经安天检测分析，本周有 8 个移动平台恶意代码和 5 个 PC 平台的恶意代码值得关注

平台分类	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.alexnuclear.a[prv，exp]2017-04-10	该应用程序感染恶意模块，运行后会获取手机固件信息、安装程序列表信息和 root 相关信息并联网上传；以 USB 防护申请辅助功能，检测手机内置安全软件，禁用 USB 调试、开发者选项和恢复出厂设置，会导致应用无法卸载；同时包含激活设备管理器风险代码，造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.GpsSys.a[prv，exp，rmt]2017-04-10	该应用程序伪装成系统服务，运行后会隐藏图标，接收短信指令，获取用户位置信息，造成用户隐私泄露和资费损耗。（威胁等级中）
		Trojan/Android.Vitamio.a[exp]2017-04-13	该应用程序伪装成正常应用，连网下载推广视频，诱导用户点击跳转推广页面，会造成用户资费损耗，建议立即卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.FakeInst.ej[prv，exp]	该应用程序伪装成色情、杀软等应用，运行后会关闭 wifi，打开移动数据流量，诱导用户点击下载其他应用，获取用户手机号码和固件信息，加载风险网页，并触发 JS 文件模拟点击，后台拦截屏蔽短信，给用户造成隐私泄露和资费损失，建议立即卸载。（威胁等级低）
		Trojan/Android.LockScreen.y[rog，lck]	该应用程序伪装成其他应用，无实际功能，程序运行后会强制置顶界面勒索用户付费解锁，建议卸载。（威胁等级中）
		Trojan/Android.emial.fc[prv，exp]	该应用程序伪装成其他应用，运行后获取 root 权限，卸载某安全应用，隐藏图标；发送激活信息到指定号码，监听拦截短信、广播，通过邮件转发信息，造成用户隐私泄露和资费损耗，建议立即卸载。（威胁等级高）
		Trojan/Android.SmsSpy.s[prv，exp]	该应用程序为间谍应用，运行后会隐藏图标，监听短信获取短信信息联网上传，包含发送短信、删除短信等风险代码，会造成用户隐私泄露和资费消耗。（威胁等级中）
		Trojan/Android.QQspy.ba[prv，exp]	该应用程序运行后会诱导用户输入 QQ 账号密码通过短信转发，造成用户隐私泄露和资费损耗，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	Microsoft Office OLE 功能远程代码执行漏洞 (CVE-2017-0199)	Microsoft Office 是微软公司开发的一套基于 Windows 操作系统的办公软件套装。在实现上存在远程代码执行漏洞，可使攻击者执行任意代码，完全控制受影响系统。攻击者通过电子邮件向目标用户发送含有 OLE2 嵌入式链接对象的 Microsoft Word 文档，当用户打开文档时，winword.exe 将会向远程服务器发出 HTTP 请求，以索取恶意 HTA 文件。服务器返回的文件是一个带有嵌入式恶意脚本的假 RTF 文件。Winword.exe 通过 COM 对象查找 application / hta 的文件处理程序，从而导致 Microsoft HTA 应用程序 (mshta.exe) 加载并执行恶意脚本。（威胁等级高）
	较为活跃的样本	Trojan[Downloader]/Shell.Agent	此威胁是一类具有执行 Shell 语句行为的恶意代码的家族的统称。该家族的样本在执行后会利用 ShellExecute 等函数来执行特定的语句，会对系统造成潜在危害。（威胁等级中）
		Trojan[DDoS]/BAT.Agent	此威胁是一类基于批处理脚本的恶意代码的家族的统称。该家族的样本具有后门行为，所有感染者在攻击者需要的时候可以发起 DDoS 攻击。（威胁等级中）
		Trojan[Exploit]/SWF.Angler	此威胁是一类通过 SWF 漏洞进行传播的木马家族。该家族因 Angler Exploit Kit 而得名。该家族的样本使用了 SWF 的漏洞对用户的设备进行感染，从而执行任意恶意代码。（威胁等级中）
		Trojan[Downloader]/WinLNK.Powedon	此威胁是一个以快捷方式为载体的恶意软件家族。该家族的样本通常是一个下载 / 加载器，使用快捷方式调用 Powershell 在后台执行下载任务并执行。（威胁等级中）

旅行路由器和 NAS 盒易遭攻击

Chris Brook / 文　安天公益翻译小组 / 译

近日，一位研究人员 Jan Hoersch 只用了 20 分钟，展示了市场上最受欢迎的物联网设备的脆弱性。Jan Hoersch 是慕尼黑小型渗透测公司 Securai GmbH 的 IT 安全顾问。在卡巴斯基实验室的安全分析师峰会上，他发表了演讲，介绍了目前影响物联网设备 (如旅行路由器和视网膜扫描仪) 正常运行的漏洞。

Hoersch 探讨了 TP-LINK 制造的旅行路由器 M5250，指出攻击者能够通过短信获取该设备的管理员凭证。他指出，如果攻击者向该路由器发送短信，路由器就会以明文形式发回数据，包括名称、SSID 和管理员密码等登录信息。Hoersch 表示："路由器甚至不需要连网，只需要打开就行。" Hoersch 在演讲中介绍的大多数设备都是旅行路由器，M5250 是其中之一。

此外，Hoerch 指出 StarTech 制造的路由器问题可能最为严重。如果攻击者能够通过网络或 LAN 端口访问该路由器，就能投放并传播载荷。Hoersch 说："我曾经把它带到会议室用过一次。我们把它连接起来，打开 telnet 功能，输入用户名和密码，得到一个 shell。我们发现它有一个硬编码的 root 密码，因此我们无法修改密码。"

"我们经常遇到硬编码的密码，大多数时候它们就像后门一样，等着黑客来利用。" Hoersch 在演讲中说。

Hoersch 去年研究了一款摄像头设备，甚至在安装更新之后，他都能够获 root

shell 和密码。他尝试通过 Google 搜索找到密码，居然真得在 2014 年的一篇文章的评论中找到了完全相同的密码哈希值。"我得出的结论是，这个漏洞与 FTP 设置漏洞是一样的，是基本的命令注入，不是高级的内存破坏漏洞。" Hoersche 说，"攻击者很容易得到 shell 和密码备份并登录摄像头。"

Hoersch 还指出，Hootoo TripMate 旅行路由器通过 bash 文件处理固件更新。如果改变一些设置，就可以不需身份验证地在任何地方上传一个 bash 脚本，更改凭证，并以 root 身份触发固件更新。

TrendNet 制造的旅行路由器 TEW714TRU，也很容易执行命令注入。他说，攻击者可以通过 LAN 端口不需身份验证地注入命令，并将这些命令与另一层中的远程代码执行漏洞进行组合。

Hoersch 指出，松下制造的视网膜扫描仪 BM-ET2000 也存在验证绕过漏洞。该设备的登录系统有问题，可能允许攻击者以 root 用户或管理员身份重定向到设备。Hoersch 承认该设备并不属于消费设备。"并不是每个人都会在家门口安装视网膜扫描仪，但我曾经安装过。" Hoersch 说。虽然多个电子网站已经将该设备标记为停产，但是一些用户仍然在使用，因此他们面临风险。

Hoersch 原本计划讨论 10 款设备的漏洞，但是在他发表演讲之前，供应商已经修复了其中的 4 个漏洞。Hoersch 警告说，包括 TP-Link 路由器和 HooToo 路由器在内的多款设备很容易从亚马逊上买到，但是，它们的漏洞会导致广泛的攻击。

Hoersch 发现了西部数据 MyCloud 设备的 85 个漏洞，他原本想进行研究。但是，Exploitee.rs 的研究人员抢先公布了这些漏洞。Exploitee.rs 研究人员指出，许多设备和 NAS 盒仍然是很脆弱的。即使西部数据推出了 EX2/EX4 和 Mirror 的更新，但该团队还是发布了推文，指出："大多数型号仍然易受 83 个远程代码执行漏洞的影响。"

Hoersch 说："你先得到一些参数，然后用它们编写命令并执行，这样就能够为所欲为了。" Hoersch 并没有披露西部数据漏洞的细节，只在演讲的结尾强调了研究人员和供应商之间的沟通至关重要。

"我们如何报告 85 个漏洞呢？每报告一个漏洞，我需要用 45 分钟的时间来向供应商解释问题，这实在是太费时了。" Hoersch 指出，更多的公司应该设立漏洞赏金计划。就算不为别的，此项目也可以作为研究人员的联系渠道。他说："大多数研究人员都会选择公布漏洞，因为向供应商报告漏洞实在是太麻烦了。这种情况应该得到改善。"

原文名称	Travel Routers，NAS Devices Among Easily Hacked IoT Devices
作者简介	Chris Brook，Threatpost 的副编辑。
原文信息	2017 年 4 月 10 日发布于 Threatpost 原文地址 https://threatpost.com/travel-routers-nas-devices-among-easily-hacked-iot-devices/124877/
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《僵尸网络 Nitol 分析报告》

近日，安天追影小组发现互联网的 DDoS 攻击有很大一部分攻击者所使用的僵尸网络是 Windows 系列的“肉鸡”群，而活跃在 Windows 环境下的 DDoS 家族尤其繁多，其中比较具有代表性的家族是病毒名为 Trojan[DDoS]/Win32.Nitol 的病毒家族。

Nitol 家族是暴风 DDoS 家族、鬼影 DDoS 家族的统称，其功能代码是从网上的同一套源码改造而成。某杀毒软件将其统称为 Nitol 家族，该家族并没有像常见的 DDoS 僵尸网络家族那么活跃，他们一般有以下 2 个特点：

1. Nitol 家族兼有 DDoS 僵尸网络和 RAT 恶意程序特色

Nitol 家族主要具有 DDoS 僵尸网络中的 DDoS 攻击的功能特点，分为 syn flood、udp flood、http flood、icmp flood、tcp flood、cc flood、dns flood 等 7 种 DDoS 攻击类型；同时还初步具备 RAT 恶意程序的远程 cmd、文件更新下载窗口弹出等功能。通过长期的监控和统计分析得知，Nitol 家族的幕后操纵者，经常通过远程文件更新下载指令，将部署在 HTTP File Server 服务器上的各种病毒木马进行远程植入，实现同一台设备被植入多种类型木马，严重危害设备安全。

2. Nitol 家族不易被清除

Nitol 家族为了长期保持对“肉鸡”的控制权限，其研发者使用了 lpk.dll 劫持技术，该技术是目前病毒传播较常用的一种方法，而正常系统本身也会存在 lpk.dll 文件，这足以说明这类病毒的危险性。系统本身的 lpk.dll 文件位于 C:\WINDOWS\system32 和 C:WINDOWS\system\dllcache 目录下。lpk.dll 病毒的典型特征是感染存在可执行文件的目录，并隐藏自身，删除后又再生成，当同目录中的 exe 文件运行时，lpk.dll 就会被 Windows 动态链接，从而激活病毒，进而导致不能彻底清除。

经过安天追影小组的长期监控与跟踪，发现 Nitol 家族每天都在进行非法的 DDoS 攻击以获取更多的非法利益，已经威胁到互联网安全，损坏了广大用户的利益。安天提醒广大网络用户，要提高自身的安全意识，对于来源不明的邮件，不要轻易点击或者复制邮件中的网址，更不要轻易下载附件，以防止钓鱼邮件中的恶意代码感染。

风险软件

安天【追影高级持续威胁分析系统】无需更新病毒库，依据行为即可实现对上述风险软件进行有效检测，以下为其自动形成的分析报告：

文件被内部组件发现，经由 BD 静态分析鉴定器、美国软件交叉索引（NSRL）鉴定器、可交换信息（EXIF）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、静态分析鉴定器、动态行为鉴定器、智能学习鉴定器将文件判定为风险软件。

根据动态行为（默认环境）得出该文件具有以下行为：使用 cmd 删除自身、删除自身、延时、填充导入表（疑似壳）、打开自身进程文件、释放 PE 文件、复制自身文件、创建服务、获取驱动器类型、启动服务、查找指定内核模块、创建特定窗体、获取计算机名称、请求加载驱动的权限、获取主机用户名称、访问 dns、连接网络、获取 CPU 信息、独占打开文件、获取系统内存、获取 socket 本地名称、自启动。

文件名	1242cabae9718d87032d5061f720bbf9
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	21 KB
MD5	1242CABAE9718D87032D5061F720BBF9
病毒类型	风险软件
恶意判定 / 病毒名称	GrayWare[AdWare]/Win32.ServStart.d
判定依据	BD 静态分析

◆ 危险行为

行为描述	危险等级	行为描述	危险等级
使用 cmd 删除自身	★★★★	删除自身	★★★★
延时	★★		

◆ 其他行为

行为描述	危险等级	行为描述	危险等级
填充导入表（疑似壳）	★★	打开自身进程文件	★
释放 PE 文件	★	复制自身文件	★★
创建服务	★	获取驱动器类型	★
启动服务	★	查找指定内核模块	★
创建特定窗体	★	获取计算机名称	★
获取主机用户名称	★	请求加载驱动的权限	★
连接网络	★	访问 dns	★
获取系统内存	★★	获取 CPU 信息	★★
自启动	★	独占打开文件	★
获取 CPU 信息	★★	获取 socket 本地名称	★

报告地址：https://antiy.pta.center/_lk/details.html?hash=1242cabae9718d87032d5061f720bbf9