安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 06 月 18 日 (总第 140 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（四）

——美国网络空间安全主动防御体系

安天研究院

之前，我们对美国网络空间安全主动防御体系进行了分析，包括“爱因斯坦”计划的三个不同阶段和积极防御（在之前被称为“主动防御”，但由于该词在杀毒领域已有使用，易引起歧义，因此改为更接近军事意义的“积极防御”，意为分析人员对处于所防御网络内的威胁进行监控、响应、学习和应用知识的过程）系统 TUTELAGE，展现了美国通过不断建设和演进，形成了一套具有完备有效的感知能力、积极防御及反制能力的国家网络空间安全防御体系。本期，我们将聚焦美国网络空间进攻性能力（这些进攻性能力被应用在包括网空情报、网空积极防御和网空军事等行动中），并简单剖析美国在这些能力背后强大的支撑体系及其运作方式。

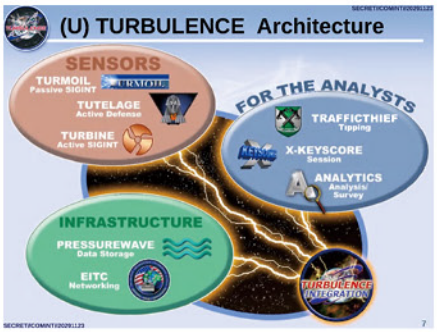
2015 年，美国《国防部网络空间战略》指出，“一旦得到指示，美国国防部（DoD）应有能力发起网络战行动，瘫痪敌对方的指挥及控制网络、与军事相关且不可替代的关键基础设施和装备性能”。2017 年 12 月，美国总统特朗普发布了新版《国家安全战略》，强调了网络空间中的竞争性，美国宣称会考虑采取各种手段威慑和击败针对美国的网络攻击，并“根据需求”对敌对方实施网络行动。目前已进入立法程序的《主动网络防御明确法案》也强调网络防御中的“积极”部分，允许网络空间受害者越过自身网络边界进行带有反击性质的行动，这体现出美国在网络政策中的进攻性色彩愈加浓厚。

美国国防部认为，计算机网络对抗（Computer Network Operations, CNO）即实质操纵计算机和网络，针对计算机或其他网络本身或它们之上的信息、信息系统，实施攻击和防御以及两者所需的支撑行动。按照网空行动目的，可以将 CNO 划分为计算机网络防御（Computer Network Defense, CND）、计算机网络刺探（Computer Network Exploitation, CNE）和计算机网络攻击（Computer Network Attack, CNA），分别对应网空积极防御、网空情报行动和网空军事行动。

为支撑上述能力，美国开展了一系列的网络空间进攻性能力支撑体系建设项目，这些项目主要由国家安全局（NSA）负责开发和实施，其中最大的支撑架构称为“湍流”（TURBULENCE），由多个系统组成，包括主动情报采集系统 TUMULT、被动情报采集系统 TURMOIL、任务逻辑控制系统 TURBINE、进攻性网空行动系统“量子”（QUANTUM）、主动防御系统 TUTELAGE、密码服务 LONGHAUL、数据仓库 PRESSUREWAVE、网络流量分析系统 TRAFFICTHIEF 和信号情报分析系统 CLUSTER WEALTH-2 等。这些系统各司其职，共同支撑信息收集、情报分析、积极防御、决策控制、网络作业等网空行动的攻击性行动环节，共同构成了美国强大的网络空间进攻性能力支撑体系。

“湍流”（TURBULENCE）框架

NSA TURBULENCE 项目由于预算超支和管理不善等问题在 2007 年首次被巴尔的摩太阳报披露。斯诺登曝光的一份绝密文件中也提到了 TURBULENCE 项目，这份绝密文件的日期为 2009 年 8 月。TURBULENCE 项目的文件中解释了将主动与被动方法结合起来以达到从目标网络中渗出数据的过程。TURBULENCE 项目包含传感器（Sensors）、基础设施（Infrastructure）及分析（Analysis）三个模块。



“湍流”架构

被动情报采集系统：TURMOIL

TURMOIL 计划是 NSA 的一种全球高速被动信号情报收集系统，用于拦截全球范围内传播的目标卫星、微波和有线通信。据推测，所有这些数据的收集都与互联网数据（DNI）相关。TURMOIL 是在数据包层面的操作，因此它可以采取特殊的方式来处理某些类型的流量，如 VPN 和 VoIP 流量。通过 NSA 的被动能力与积极能力整合工作，TURMOIL 能够识别重点目标的数据特征触发 TURBINE 系统，而且使 NSA 具备可以仿冒任何国家 IP 地址的高级反溯源能力。

任务逻辑控制系统 TURBINE

TURBINE 是任务逻辑系统，由 NSA 使用的 CNE 技术深度集成。当 TURMOIL 的处理分析识别出重点目标，便由 TURBINE 进一步判定是否需要对某个目标进行攻击。一旦判断为需要，则会触发 TURBINE 系统中的程序，试图使用 QUANTUM 侵入目标

（下转第二版）

（上接第一版）

计算机窃取信息。

进攻性网空行动系统 QUANTUM（量子）

“量子”系统是进攻性网空行动系统，能够向互联网侧目标部署作业工具，或操纵已部署工具。“量子”系统部署于 NSA 内网，由定制访问办公室（TAO）远程作业人员操纵，其作业能力覆盖广泛，包括域名系统（DNS）和 HTTP 注入式攻击等多种网络攻击工具、数据库注入工具、僵尸网络控制工具等。“量子”系统可通过多种方式劫持目标，包括应用广泛的“量子插入”（QUANTUMINSERT，针对 HTML 访问）和“量子之手”（QUANTUMHAND，针对 FaceBook 访问）等，在神不知鬼不觉的情况下将用户的正常网络访问劫持到伪装的服务器，并将一些网络攻击框架、系统或工具植入到用户计算机。

集成“关键得分”（X-KEYSCORE）项目

X-KEYSCORE 是可以对各种网上行为进行监视和分析处理的系统，是与谷歌功能类似的分布式数据采集和分析框架，运行于 Linux 系统和 MySQL 数据库。TURMOIL 会筛选出“有意义”的数据包，并将包转发给 X-KEYSCORE，X-KEYSCORE 将会话数据化并通过 XKS 界面为 NSA 人员提供分析和搜索的功能，这样互联网上的一切活动都会尽在 NSA 的掌握之中，从而实现对网络空间攻击目标的发现与确定。

针对恐怖组织的应用案例

2012 年 6 月，美反恐活动部队利用与某恐怖组织头目相关的 Yahoo 筛选条件成功探测到其使用的系统，在“湍流”下，通过“量子”将其劫持到 NSA 的攻击服务器 FOXACID 并在系统中植入恶意程序 UNITEDRAKE，后者在目标系统中植入恶意软件键盘记录程序 GROK 和 USB 监控 / 收集软件 SALVAGERABBIT，通过分析其传回的情报，获得了与该恐怖组织头目一起活动的人员名单，以及其与基地组织之间的通信等重要信息。

在这套支撑体系的支持下，美国的网络攻击行动才能够获得强大的后端支持，包括较完善的信号收集（从网络收集和从其合作伙伴、国防承包商、大型 IT 企业获取的各种信息，涵盖电子邮件、视频音频、消息、社交媒体等）、处理基础设施，包括音频、视频、邮件等大规模网络活动与个人数据库及相关加工处理机制。而攻击行动必然需要具体的攻击装备，美国有哪些网络空间攻击装备，美国的网络空间攻击装备体系有何特点，我们将在后续的文章中为您一一解答。

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 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.henbox.a[prv,spy] 2018-06-13	该应用程序是一款间谍软件，运行后隐藏图标，窃取用户短信、联系人、通话记录、地理位置、手机存储文件信息、浏览器记录等隐私信息，私自拍照、录音、静音，并将用户隐私上传。造成用户隐私泄露，建议卸载。（威胁等级中）
	较为活跃的样本	Trojan/Android.Locker.aq[rog,lck]	该应用程序伪装辅助工具，私自提权，卸载指定程序，释放勒索木马到系统目录下，禁用 USB 连接，勒索用户付费解锁，造成用户手机无法正常使用，建议卸载。（威胁等级中）
		Trojan/Android.FakeFB.w[prv]	该应用程序伪装成 Facebook，诱导用户输入账号密码，然后上传到指定服务器，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.SmsSpy.ai[prv,rog,exp]	该应用程序运行诱导替换默认短信应用，而后隐藏图标，私自群发欺诈短信给通讯录联系人，拦截短信，私自通过邮件发送用户短信、联系人、固件信息到指定邮箱，造成用户资费损失和隐私泄露，请立即卸载。（威胁等级高）
		Trojan/Android.AutoSMS.o[prv,exp]	该应用程序运行后会私自发送短信，监听用户短信并上传到服务器，造成用户隐私泄露和资费损耗，建议卸载。（威胁等级高）
		Trojan/Android.Socksbot.d[rmt,prv]	该应用程序伪装成色情游戏，运行后加载恶意子包，接收远程服务器发送的指令，与远控服务器通过 socket 进行通讯，远控端可使用户设备变成 SOCKS 代理，这样远控端可通过用户设备访问设备所属内部网络从而窃取用户内网的隐私信息，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.Trogle.b[prv,rmt,spr]	该应用程序伪装成其他应用，运行后向用户所有联系人发送恶意推广短信，进行恶意传播，在界面上弹出对话框欺骗用户点击安装其恶意子包，并伪装界面骗取用户进行注册，以获取用户手机号、姓名和身份证号等隐私信息，恶意子包监听并拦截短信，并将短信通过短信和 email 方式发送给恶意代码作者，泄漏用户隐私，建议卸载。（威胁等级中）
		G-Ware/Android.CoinMiner.b[exp,rog]	该应用程运行隐藏图标，联网获取 js 脚本，后台私自挖矿，影响用户正常使用，建议卸载。（威胁等级低）
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Adobe Flash 0day 漏洞（CVE-2018-5002）	CVE-2018-5002 是由于 Flash 未能正确处理包含特殊字节码序列的 SWF 文件时产生的栈越界读写漏洞。该漏洞同之前的 CVE-2017-11292 类似，都需要修改 SWF 文件的字节码来触发漏洞。同时该漏洞的利用只需要简单的内存布局，不需要复杂的堆喷，一个样本同时能在 32 位和 64 位系统中稳定运行。（威胁等级高）
	较为活跃样本	Trojan[Downloader]/Win32.Zlob	此威胁是一种具有下载行为的木马类程序。Zlob 家族感染用户电脑后，会修改系统设置，在电脑中下载并执行多个恶意软件。该家族会伪装成 ActiveX 的视频编码欺骗用户下载并安装，安装后，用户会收到伪装成微软警告信息的弹窗，提示用户系统中可能存在间谍软件，需要下载反病毒程序进行清除。在用户点击弹窗后，将下载实为木马的虚假反病毒程序。（威胁等级高）
		Trojan[Ransom]/Win32.Locky	此威胁是一种可以加密用户文件并勒索比特币的木马家族。该家族样本运行后加密多种格式文件并向用户要求支付比特币解锁，有一定威胁。（威胁等级高）
		Trojan[Backdoor]/Win32.Dridex	此威胁是一类可以窃取用户信息的木马家族。该家族样本运行后可以连接远程服务器接受攻击者的恶意操作，可以删除文件、回传敏感信息等。（威胁等级中）
		Trojan[Downloader]/MSWord.Steamilik	此威胁是一种具有下载行为的木马类程序。该家族通过垃圾邮件进行传播，样本为 Word 宏病毒，运行后连接网络下载其它恶意程序并运行。（威胁等级中）

迁移到云不仅仅是为了省钱

Mark Gonzales / 文　安天技术公益翻译组 / 译

成功的云实现受速度、灵活性和细粒度资源管理的驱动。关注这些驱动因素，就能逐步降低成本。

“我们迁移到云端吧，这样就可以省钱了。”这是我们经常从高管嘴里听到的一句话。他们已经了解到，各种规模的公司通过将计算能力和数据存储迁移到公共云平台，如亚马逊网络服务（AWS），微软 Azure 和谷歌云平台，削减了 IT 基础设施成本。但是他们通常不知道这些公司究竟是如何使用云平台来省钱的。

IT 团队尽职地预测将数据中心的所有内容上传至云平台的成本，这是一种与“基础架构即服务”（IaaS）相关的“直接迁移”（lift-and-shift）方法。他们得出的结论通常是：迁移到云端的成本更高。原因是什么呢？

根据我们自己和客户的经历，我们发现，成功迁移到云平台的公司关注的不是整体基础设施成本，而是三个更重要的驱动因素，依次是速度、灵活性和成本透明。这样一来，公司可以减少计算资源和人员成本的花费，或者将资源和人员解放出来，用于开展更多的业务活动，使其 IT 投资更加高效和经济。

• 速度

到目前为止，将分析和计算基础设施迁移到云服务的最大好处是提高速度。这里说的速度不是提高应用程序的性能，而是缩短决策制定和决策执行之间的时间间隔。

对于大多数公司来说，获取硬件和软件需要经历冗长的采购过程。即使有特定的供应商，获取物理硬件可能也需要几天或几周的时间，之后，至少再用几天的时间对它们进行配

置并集成到数据中心。

而通过云服务，一旦云平台安全地连接到你的网络，你只需要点击几下就能完成配置了。最近，在测试一些架构方案时，我只用几分钟就调配了一个 60 节点的大规模并行处理 SQL 数据库集群。这可以通过 Azure SQL 数据仓库、Hadoop 集群、亚马逊 Redshift 数据库集群、SMP 数据库、数据存储、单个虚拟机和现代数据中心包含的几乎任何东西来完成。决策制定和执行之间的时间间隔被大大缩短，开发人员不必再苦苦等待。你今天想到了办法，明天甚至今天下午就可以实施。

• 灵活性

举个例子，今天你将基于云的 10 节点 MPP SQL 集群整合到了应用程序架构中，明天却发现 20 个节点会更好，该怎么办呢？你可以根据需要随时更改节点数量。如果采用传统数据中心方案，你已经为数据中心购买了 10 节点集群，则需要重新进行采购，等待另外 10 个节点送达。另外一种情况，你配置了 20 个节点，后来发现只需要 10 个节点，该怎么办呢？如果是物理硬件，这属于买多了。然而，使用基于云的服务，你可以根据需要随时撤掉不需要的节点，调整计算资产的规模。

另外，与传统的数据中心相比，云服务通常能提供更加灵活的网络连接和各种服务之间的数据传输。例如，你需要将 Hadoop 集群中的数据发送到分析数据库，并将结果输出到 BI（商业智能）工具。通过云服务，点击几下就成。

• 细粒度的资源管理

云平台的灵活性提供了另一个好处：细粒度的资源管理。你可以根据当天的需要调高和调低计算能力。如果你的数据仓库流程每周需要 8 小时的密集处理能力，你可以将那 8 小时时段内的计算能力调高，其余时段再将其恢复正常。如果你的数据仓库流程需要在工作时间执行分析，则可以为其工作时间分配更多的资源，并在非工作时间将其关闭，以控制成本。

使用云服务的另一个好处是成本透明。云计算和存储服务可以根据应用程序和 / 或功能进行分配，所以特定应用程序所花费的成本是可见的，使得整个计划的成本比以往更加透明。

例如，我们有一位客户完全在云中部署了一个新的分析数据仓库（本地系统定期向云系统上传数据）。运行新系统的总成本每年不到 30 万美元，整个应用程序在 6 个月内开发并投入运行。类似的本地系统通常需要花费数百万美元，而开发、安装、架构和实施花费的时间则远大于一年。

速度、灵活性和细粒度的资源管理是真正推动企业迁移到云的动力。在实施新系统或重构现有系统时关注这些因素，不仅能够在更短的时间内更好地利用客户数据，还可以如管理团队所愿节省资金和资源。

原文名称	The Cloud Isn't Just About Saving Money
作者简介	Mark Gonzales。Mark Gonzales 是 Elicit 公司的客户技术高级总监。
原文信息	2018 年 6 月 1 日发布于 InformationWeek 原文地址 https://www.informationweek.com/cloud/the-cloud-isnt-just-about-saving-money/a/d-id/1331935?
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《远程访问木马 FlawedAmmyy 分析报告》

近日，安天 CERT（安全研究与应急处理中心）发现了一种新型远程访问木马，名为“FlawedAmmyy”。FlawedAmmyy 是根据之前泄露的远控 Ammyy Admin 版本 3 修改而来，可能与威胁组织 TA505 存在关联。过去四年间，TA505 曾运作了 Dridex，Locky 和 GlobeImposter 等大型攻击活动。

该木马样本运行后会释放 4 个 dll 文件和一个 7z 文件，分别为 System.dll、UserInfo.dll、Nsis7z.dll、nsExec.dll 和 test.7z。样本首先会载入 System.dll，然后多次调用导出函数 System.call，遍历系统中的进程，查找是否存在 avgsvc.exe、a2service.exe、MBAMService.exe 等反病毒引擎。之后载入 UserInfo.dll，调用导出函数 UserInfo.GetAccountType，判断当前进程是否以管理员权限运行。样本创建目录 C:\Documents and Settings\All Users\Application Data\Microsoft\Enc，并在该目录下创建需要解压密码的压缩文件 test.7z，然后调用 Nsis7z.dll 的导出函数 Nsis7z.Extract 将 test.7z 解压，解压密码为 HbMEAKQo6UJ3i3ZdywumRC6J2。test.7z 解压后可得到 test.cab。样本会在 C:\Documents and Settings\All Users\Application Data\AMMYY 目录以及 C:\Documents and Settings\All Users\Application Data\Foundation 目录下查找 wmihost.exe、settings3.bin 和 wmites.exe。若未找到相关文件，则将 test.cab 复制到 \Enc 目录下的 enc.exe。

在运行 enc.exe 之前，样本会调用 nsExec.dll 的导出函数 Exec 来执行 cmd 命令停止 ammyy 和 foundation 服务。enc.exe 运行后，会在内存中释放并运行一个 PE 文件以进行远控。该 PE 文件包含两个资源文件，其中 151 是 32 位的，152 是 64 位的，其作用是获取登录凭证。该 PE 文件运行后会连接 C2 服务器 179.60.146.3:443，若服务器返回“0x2D”数据，表示连接成功。连接成功后，该 PE 文件会收集计算机信息并发送给 C2 服务器，包括计算机型号、计算机名称等。该 PE 文件会对 C2 服务器发送的控制指令进行判断，当指令为“0xC”时，继续发送数据；当指令不为“0xC”时，便根据控制指令执行相应操作。相关操作包括创建进程执行命令、收集计算机信息并发送、载入资源文件并运行、监控键盘操作、监控鼠标操作及文件操作等。

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 YARA 自定义规则鉴定器、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、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。

最终依据静态分析鉴定器将文件判定为木马程序。

概要信息

文件名	1f5d31d41ebb417d161bc49d1c50533fcbff523bb583883b10b14974a3de8984
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	800 KB
MD5	41945BF2BA18BE4551C3F9FE6BDF2C4C
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Agent
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

危险行为

行为描述	危险等级
利用 BAT 实现自删除	★★★★
删除自身	★★★★

常见行为

查找指定内核模块	★
获取系统版本	★★
创建特定窗体	★
获取驱动器类型	★
获取计算机名称	★
请求加载驱动的权限	★
打开自身进程文件	★
读取自身文件	★★
释放 PE 文件	★
遍历进程	★
.....	.....

进程监控

PID	创建	命令行
1740	ns3.tmp	"C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\nsl2.tmp\ns3.tmp" "net.exe" stop ammyy /y
1728	net1.exe	net1 stop ammyy /y
.....	.....	.....