安天周观察

安天官方微博　安天官方微信

主办：安天　2018 年 07 月 02 日 (总第 142 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（五）

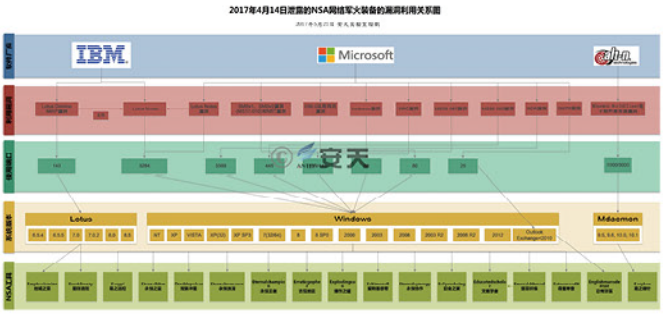
——美国网络空间攻击装备体系

安天研究院

在之前的文章中，我们关注了美国网络空间进攻性能力的支撑体系，对以“湍流”（TURBULENCE）为代表的进攻性能力支撑框架进行了介绍。在这样的支撑体系下，美国得以开展大量的进攻性网空行动，包括网空情报、网空军事行动和网空积极防御中的反制与反击行动等。

2013 年，《华盛顿邮报》披露了美国情报机构进行攻击性网空行动的能力。据称，单是 2011 年就进行了 231 起，其中 3/4 针对被美列为“顶级优先目标”的中、俄、伊朗、朝鲜等。自 2008 年以来美军已经实施了多次的进攻性网空行动，如积极防御行动“扬基鹿弹”（Buckshot Yankee），是对美国中央司令部网络所遭受一次非常严重病毒感染事件的响应行动；针对全球手机监听的“金色极光”（AURORAGOLD）行动，通过收集关于全球移动通讯运营商内部系统的信息，以找到其漏洞，供 NSA 随后的黑客攻击使用，该计划为美国 2011 年对利比亚进行军事干预提供了利方重要人物的通信信息；针对 ISIS 的“发光交响乐”（Glowing Symphony）行动，主要目标是通过关闭、篡改 ISIS 的服务器来控制 ISIS 的网络宣传能力；针对伊朗核设施的“奥运会”（Olympic Game）行动，最终通过“震网”(Stuxnet) 蠕虫，成功入侵并破坏伊朗核设施，严重迟滞了伊朗核计划，成为首个利用恶意代码对实体设施造成重大不可逆损坏的事件。这些行动展现了美国在情报作业、进攻行动和积极防御的反制与反击等方面的能力，这些进攻性能力不仅来自于完善的后端支撑体系，更来自于其强大的网空攻击装备体系。美国的网空攻击装备体系以全平台、全功能为发展目标，并具有模块化特点，使得其能够适应于各种网络环境下的行动作业要求。

自 2009 年正式成立网络司令部以来，美国始终致力于发展一支以全面防御为基础的进攻性网络部队。在这种思想的引导下，NSA、CIA 极其重视网空攻击装备的研发。自 2013 年“斯诺登”事件开始，以及“维基解密”和黑客组织“影子经纪人”（Shadow Brokers）的不断曝光，NSA 与 CIA 的网空攻击装备体系逐渐浮出水面。



泄露的 NSA 网络军火装备与相关漏洞、系统版本关系图

NSA 网络攻击装备库

2014 年，《明镜》周刊揭秘 NSA 旗下高级网络技术部门（ANT），文章披露了软、硬件共 48 种攻击装备资料，能够实现植入、窃取、监听、拦截等多种目的。之后，包括“影子经纪人”在内的其他渠道又进行了多次披露，总共披露的 NSA 网空攻击工具、组件数量已过百。其中有一个名为“IRATEMONK”的装备，该装备的描述与“方程式”组织（Equation Group）的固件修改能力非常相似，怀疑“IRATEMONK”就是“方程式”所采用的固件修改装备。此外，还有一系列针对网络设备的攻击工具，例如针对思科、Juniper 防火墙名为“BANANAGLEE”的攻击工具；针对 Juniper（J、M 和 T 系列）路由器分别名为“SCHOOLMONTANA”、“SIERRAMONTANA”、“STUCCOMONTANA”的植入程序，能够对网络设备进行远程控制；针对华为路由器名为“HEADWATER”的植入程序，也用于对网络设备进行远程控制。

2017 年 5 月 12 日，全球爆发大规模的勒索蠕虫“魔窟”（WannaCry）感染事件，我国大量行业企业内网遭受大规模感染，包括医疗、电力、能源、银行、交通等多个行业均受到不同程度的影响。“魔窟”利用了基于 445 端口的 SMB 漏洞 MS17-010（永恒之蓝），而 2017 年 4 月 14 日“影子经纪人”公布的 NSA“网络军火”中就包含了该漏洞的“武器级（漏洞利用过程具有高稳定性与高可靠性）”利用程序，这是“魔窟”能够迅速感染全球大量主机的重要原因，而“影子经纪人”曝光的“网络军火”系列中还有大量的其他漏洞及其利用工具。

“维基解密”披露 CIA“7 号军火库”（Vault 7）

2017 年 3 月 7 日，“维基解密”曝光了 8761 份据称是 CIA 网络攻击活动的秘密文件。这份数据库的代号为“7 号军火库”（Vault 7），泄露的文件包含 7818 个网页和 943 份附件。在之后的一段时间内，“维基解密”每隔一段时间就放出一组 CIA 网络攻击武器相关文档。本次泄漏事件据称是 CIA 最大规模的机密文档泄漏事件，涉及到的代码有数

（下转第四版）

每周安全事件

类 型	内 容
中文标题	WebAssembly 的修改会使 Meltdown 和 Spectre 补丁失效
英文标题	Changes in WebAssembly Could Render Meltdown and Spectre Browser Patches Useless
作者及单位	Catalin Cimpanu
内容概述	WebAssembly 是去年引入的新技术，大多数主流浏览器均支持该技术，包括 Chrome, Edge, Firefox 和 Safari。浏览器会把 WA 的相关代码转换成机器码直接在 CPU 运行。 但 Forcepoint 的研究员 John Bergbom 表示，WebAssembly 中的新特性会使得 Meltdown 和 Spectre 补丁失效。研究员提出一种时间攻击，其为边信道攻击的一种，造成的后果是直接使用户的 Meltdown 和 Spectre 补丁失效。 攻击者需要做的是精确控制攻击时间段、控制相关参数，还有从加密的数据中恢复出部分信息，以便进行攻击。
链接地址	https://www.bleepingcomputer.com/news/security/changes-in-webassembly-could-render-meltdown-and-spectre-browser-patches-useless/

每周值得关注的恶意代码信息

经安天【CERT】检测分析，本周有 9 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	Tool/Android.linkdroid.a[prv,rmt] 2018-06-25	该应用程序是一款手机远控软件，能接收远程控制命令，进行拍照、录音、录像、发送短信、截屏、隐藏图标，收集用户手机短信、联系人、通话记录、地理位置、手机基本信息、浏览器历史记录等信息，并上传。若非本人安装，建议不要使用。（威胁等级低）
		Trojan/Android.poph5.a[exp] 2018-06-26	该应用程序安装无图标，包含风险代码，后台联网上传用户手机基本信息，获取未知脚本和插件，私自下载未知软件，并静默安装，造成用户流量消耗。警惕脚本存在私自发送短信行为，请立即卸载。（威胁等级中）
		Trojan/Android.nbank.a[prv] 2018-06-26	该应用程序运行后强制要求激活设备管理器，监听用户拨打电话，私自替换拨打号码，伪装拨打电话界面，可能会造成用户资费损耗；后台窃取用户联系人、信箱、通话记录等隐私信息，造成用户隐私泄露，建议立即卸载。（威胁等级中）
		Trojan/Android.flongjce.a[sys,exp,rtt] 2018-06-26	该应用程序运行隐藏图标，解密加载子包，下载提权相关文件，私自提权，修改多个系统 API 调用的返回值，联网获取数据模拟点击注册 Google 账号，还会私自下载未知文件，造成用户资费损耗和影响手机正常使用，建议卸载。（威胁等级高）
		Trojan/Android.ServeBlog.a[prv,spy] 2018-06-27	该应用程序伪装系统应用，运行诱导激活设备管理器，隐藏图标，后台窃取用户联系人、通话记录、短信、设备信息、通话录音等隐私上传，造成用户隐私泄露，建议卸载。（威胁等级中）
		Trojan/Android.ScamMiners.a[fra] 2018-06-28	该应用程序伪装挖矿应用，无实际功能，运行推送广告，以合作挖矿、分享报酬的名义，诱导用户下载、刷评价，达到快速推广目的，后期可能恶意利用该程序窃取用户加密货币钱包凭据，非法牟利，造成用户财产损失，建议卸载。（威胁等级中）
		Trojan/Android.Metasploit.a[prv,bkd] 2018-06-28	该应用程序被植入了后门程序，会连接远程服务器，联网获取 dex 文件，并动态加载执行，接收远程指令窃取用户手机各项隐私信息，造成用户隐私泄露，存在安全隐患，建议卸载。（威胁等级中）
		Trojan/Android.BycSpyLocker.a[prv,rmt,exp,lck] 2018-06-28	该应用程序伪装游戏外挂，运行诱导用户激活设备管理器，私自提权，拦截短信，私自拍照，获取用户短信内容、联系人、通话记录、固件信息、照片并上传到指定 ftp 服务器，还会根据远程指令进行锁屏勒索，会造成用户隐私泄露和资费损失，建议立即卸载。（威胁等级中）
		Trojan/Android.wm01.a[prv,rmt,spy] 2018-06-29	该应用程序是一款间谍软件，运行后隐藏图标，接收远程控制指令，窃取用户短信、联系人、通话记录、地理位置，私自拍照、录音、录像、截屏，并将用户隐私上传至服务器，造成用户隐私泄露，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	Drupal 核心远程代码执行漏洞（CVE-2018-7602）	Drupal 官方发布新补丁和安全公告，修复了编号为 CVE-2018-7602 的远程代码执行漏洞，此漏洞源于 3 月 28 日更新版中对编号为 CVE-2018-7600 的漏洞不完全修复，导致补丁被绕过，可以造成任意代码执行。目前此漏洞被利用来传播门罗币挖掘恶意软件。（威胁等级高）
	较为活跃样本	Trojan[Dropper]/Win32.Agent	此威胁是一种以基因片段定性的木马类程序。该家族以捆绑安装为主要传播手段，将木马程序与正常软件捆绑，并将捆绑后的文件上传到下载网站中。（威胁等级高）
		Trojan[Banker]/Win32.Banker	此威胁是一种以窃取网络银行敏感信息（如银行账号、密码、信用卡信息等）为目的的木马类程序。该家族通过恶意网站或已被感染的邮件进行传播，可以监控用户的网络行为，在用户登陆银行网站时记录用户信息，并将所有收集的信息发送给攻击者。（威胁等级中）
		Trojan[Backdoor]/Win32.Thunkan	此威胁是一种后门程序。该家族样本使用了简单的加壳手段隐藏自身的关键字符串，运行后会建立后门，可以从远程服务器下载其他恶意代码并运行，有一定威胁。（威胁等级高）
		Trojan[Ransom]/Win32.Cryptor	此威胁是一种可以加密用户文件并勒索赎金的木马家族。该家族样本运行后遍历系统磁盘并加密文件，向用户勒索赎金以解密，有一定威胁。（威胁等级中）

选择适合自己的人工智能战略

Jessica Davis / 文　安天技术公益翻译组 / 译

Dun & Bradstreet 公司正在转变自己的人工智能（AI）和分析战略，同时帮助客户进行分析和机器学习转型。

在人工智能应用方面，你的企业与同行相比如何呢？你是否觉得自己落后了？放心吧，即使你还没有人工智能计划，你也多的是伴儿。

如果你想要清楚地了解企业目前的人工智能应用情况，会发现各个企业都有所不同。一些企业可能非常先进，其他企业则可能还挣扎于数据管理和治理工作。此外，还有很多公司处在这两个极端之间。

Dun & Bradstreet 公司首席分析官尼帕·巴苏（Nipa Basu）就公司目前的分析战略发表了自己的观点。她在公司牵头人工智能转型，并帮助不同垂直行业的、各种规模的客户进行人工智能转型。在纽约举行的 H2O World 2018 会议上，她分享了一些看法，并接受了《信息周刊》（InformationWeek）的采访。

• 人工智能的现实：没有通用方法

对于刚开始接触人工智能的企业而言，需要特别注意的一个问题是：没有通用的方法。巴苏告诉《信息周刊》，企业的人工智能战略应该关注核心业务元素。

例如，Dun & Bradstreet 公司的一项核心任务是：在高级分析方面超越同行。巴苏说，她的团队由数学家、计量经济学家、统计学家和数据科学家组成，他们专注于高级分析，而

非构建人工智能软件或平台。她的团队中没有数据工程师。

但是，其团队使用的平台不仅仅是让客户点击按钮并获得答案，因为这样客户自己就能做到。Dun & Bradstreet 价值定位的核心是：提供先进的分析洞察力。

巴苏说，一家大型会计师事务所的代表也在 H2O World 2018 会议上发表了演讲。该公司的核心任务不是为客户提供分析服务，但它在核心任务中应用了高级分析技术。例如，该公司的一个核心任务是确定金融风险与价值，因此，它应该在这方面应用机器学习和人工智能技术。

• 选择适合自己的平台

巴苏说，每个企业都必须选择适合自己需求的平台，这具体取决于他们处于什么发展阶段。你不会把大学生放到幼儿园班上，反之亦然。

“这取决于公司的情况。如果你的公司拥有一支先进的数据科学家团队，那么你应选择一个有助于这些年轻和有抱负的数据科学家加速分析的平台。”她说。“如果你的公司没有数据科学家，那么你可以寻找成本更低、更容易使用的平台。总之，要找到适合你自己的平台。”

• Dun & Bradstreet 的转型之旅

Dun & Bradstreet 目前处在哪个阶段呢？巴苏表示，公司的工作方式出现了很多积极的变化。在流程方面，公司采用了精益和敏捷方法，并从中获得了好处。此外，公司还拓宽了建立技术合作伙伴关系的途径。

“我们从知名公司和工业级系统开始，”巴苏说，“我们目前是这样做的。但作为分析领域的领导者，我觉得很有必要与近年来在硅谷成立的公司合作。”

对有着 175 年历史的 Dun & Bradstreet 来说，这些改变可不算小。

• 基本要素——人

机器学习、人工智能和分析技术的进步，将会改变我们的工作方式和员工队伍，但这并不意味着它们将替代员工。巴苏说，要使这些技术良好地运作，需要人的参与。

“有的企业可能太过依赖于机器了。”她说，“我认为，真正好的解决方案是将人类智慧和人工智能结合起来。”

巴苏说，人类智慧能够产生专业知识，“这非常重要”。

原文名称	The Right Fit: Choosing an AI Strategy
作者简介	Jessica Davis。Jessica Davis 是 Enterprise Apps 的高级编辑。
原文信息	2018 年 6 月 19 日发布于 InformationWeek 原文地址 https://www.informationweek.com/big-data/ai-machine-learning/the-right-fit-choosing-an-ai-strategy/d/d-id/1332072?
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《Samsam 勒索软件新变种分析报告》

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 SamSam 勒索软件开始活跃，它在新版本中增加了更多功能和变化，使分析人员在检测和追踪时更加困难。

Samsam 的新版本与早期版本有一些区别，唯独有一件事没有变化：勒索软件的载荷是动态解密的。这就是为什么找到实际的有效载荷代码非常困难。新版 Samsam 有 5 个组成部分，其中 4 个是实体文件，第 5 个由攻击者直接参与。组件 1 是一个批处理文件，包含勒索软件的一些设置，它执行一个 .NET 文件。攻击者使用密码作为其命令行参数来执行目标计算机上的批处理文件。在旧版本中，这个批处理文件并不存在，攻击者可能直接执行 .NET 组件。组件 2 则是载荷的解密器和启动器，该文件没有使用混淆，功能也比较简单，它会查找目录中扩展名为 .stubbin 的文件，该文件是加密的勒索软件，它会立即从文件中读取内容到内存并自删除。该文件由 AES 加密，所以即使获取该文件，分析人员也不能进行分析，除非能获得攻击者独有的密码。组件 3 解密代码包含在单独的 DLL 中，而在旧版本中，则在包含在启动器中。组件 4 就是加密的恶意代码载荷 *.stubbin。

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、文件元数据分析鉴定器、静态分析鉴定器、安全云鉴定器等鉴定分析、智能学习鉴定器。

最终依据 BD 静态分析鉴定器和静态分析鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	9c8ad4147f5cbdda51317a857d75720c84bddb16338dabe374a3e60c64c2f0de

文件类型	Text/ISO_IEC.UTF8[:No bom]
大小	276 Bytes
MD5	46602C08BC8A96B55D7998CD695DABAA
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

（上接第一版）

亿行。

“7 号军火库”所泄露的文件包含了一个庞大的攻击装备库，其平台面覆盖非常广泛，支持的操作系统不仅包括了 Windows、Linux（含 Debian、RHEL、CentOS 等发行版）、OS X、iOS、Android 等常见的操作系统，还包括了基于 POSIX 的操作系统如 Solaris 与 FreeBSD 等；支持的设备不仅包括个人电脑、服务器、路由器、交换机等传统网络和终端设备，也包括智能电视、手机、平板电脑等智能设备。装备功能包括了突破物理隔离、信息获取、武器定制、远程控制、监听、欺骗等可以与 CIA 人力情报作业紧密结合的攻击作业能力，也包括了代码混淆、痕迹清除、文档追踪等作业支撑与行动安全保障能力。

利用全平台、全功能的网空攻击装备体系，美国能够通过物流链劫持、运营商劫持、源代码污染等实现战场预制；通过大规模信息采集形成终端、设备、软件、用户身份的信息库，绘制网络地形、寻找关键目标；通过移动介质摆渡攻击、物流链劫持、近场作业等方式突破物理隔离防线；在内网横向移动，建立持久化据点，投递载荷；通过摆渡攻击、开辟侧信道、隐信道等方式实现远程控制，最终实现目标。在针对伊朗核设施的“震网”事件中，美国在攻击伊朗核工业网络之前，已经完全渗透了伊朗的核工业体系，包括设备生产商、供应商、软件开发商等，在完整研究与模拟了伊朗核工业体系之后才进行了载荷投递并最终对伊朗核设施进行破坏。

今天的网络攻防处于一种防御方更加透明、攻击者更加隐蔽的状态。具有国家行为体为背景的攻击者可以无节制承担攻击成本和动用资源，攻防双方进一步朝着不对等化发展；而且，一旦国家行为体的网空进攻性能力向恐怖组织等非国家行为体扩散，可能会造成灾难性的现实后果。面对国家级攻击行为体，应当以敌情想定为前提，一方面持续分析国外网络空间能力进展，充分了解对手；另一方面，我们也应意识到只有采取系统化的应对策略建立有效的能力体系才能应对系统化的进攻，所以必须积极推进军民融合，整合产业先进有效的技术能力，建立国家级防御体系。

那么，美国的网空攻击装备具体有哪些功能？装备的模块化组合有哪些优势？应该如何防御？在之后的文章中，我们将对美国 NSA、CIA 具有代表性的网空攻击装备进行介绍，并探讨可能针对哪些环节展开有效防御，敬请期待。