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 04 日 (总第 138 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（三）

——美国网络空间安全主动防御体系

安天研究院

之前，我们对美国的大型信号情报获取项目进行了介绍，包括监听目标涵盖美国公民的“星风”（STELLARWIND）计划、网上行为监视和分析的关键得分（X-KEYSCORE）项目、针对全球网络安全厂商的“拱形”（CAMBERDADA）计划等，全面地展现了美国强大的信号情报获取能力。在本期中，我们将聚焦美国网络空间安全主动防御体系，呈现其全面的网络空间安全防御能力，以及美国将信号情报与主动防御相结合，全面拒止威胁的能力。

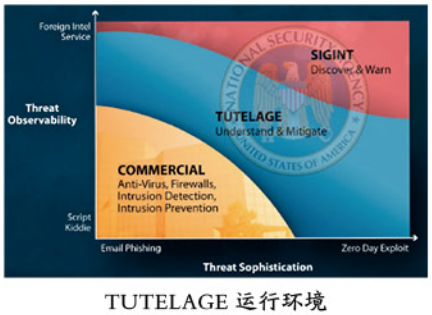
2008 年 1 月 8 日，时任美国总统布什签署了第 54 号国家安全总统令 / 第 23 号国土安全总统令，即《国家网络安全综合计划》（Comprehensive National Cybersecurity Initiative,CNCI）。该计划旨在从国家层面建设一个综合的网络空间安全防御系统，抵御美国遭受到的网络攻击，保护美国的网络空间安全。CNCI 自签署以来，就以涉及国家安全的原因被列为高度机密，至 2008 年底仅公开了 12 项计划的基本信息。

2010 年，为了体现“实现前所未有的政府开放性”的承诺，奥巴马政府公开了一份关于 CNCI 的摘要，其中包括“部署一个由遍布整个联邦的感应器组成的入侵检测系统”和“寻求在整个联邦范围内部署入侵防御系统”，即“爱因斯坦 2”（EINSTEIN 2）计划和“爱因斯坦 3”（EINSTEIN 3）计划。

“爱因斯坦”计划是美国联邦政府主导的一个网络空间安全自动监测项目，由国土安全部（Department of Homeland Security, DHS）下属的美国计算机应急响应小组（US-CERT）开发，用于监测针对政府网络的入侵行为，保护政府网络系统安全。美国政府启动了 CNCI 后，爱因斯坦计划并入 CNCI，并改名为国家网络空间安全保护系统（National Cybersecurity Protection System, NCPS），但依然被称为“爱因斯坦”计划。

“爱因斯坦”计划经历了三个阶段。“爱因斯坦 1”自 2003 年开始实施，监控联邦政府机构网络的进出流量，收集和分析网络流量记录，使得 DHS 能够识别潜在的攻击活动，并在攻击事件发生后进行关键的取证分析。“爱因斯坦 2”始于 2007 年，在“爱因斯坦 1”的基础上加入了入侵检测（Intrusion Detection）技术，基于特定已知特征识别联邦政府网络流量中的恶意或潜在的有害计算机网络活动。“爱因斯坦 2”传感器产生大量关于潜在网络攻击的警报，DHS 安保人员会对这些警报进行评估，以确认警报是否具有威胁，以及是否需要进一步的补救，如果需要，DHS 会与受害者机构合作解决。“爱因斯坦 2”是“爱因斯坦 1”的增强，系统在原来对异常行为分析的基础上，增加了对恶意行为的分析能力，使得 US-CERT 具备更好的态势感知能力。2010 年，DHS 计划设计和开发入侵防御（Intrusion Prevention）来识别和阻止网络攻击，即“爱因斯坦 3”。根据奥巴马政府公布的摘要，“爱因斯坦 3”将利用商业科技和政府专业能力相结合的方式，实现实时的完整数据包检测，并能够基于威胁情况对进出联邦行政部门的网络流量进行决策，在危害发生前，对网络威胁自动检测并正确响应，形成一个支持动态保护的入侵防御系统。

根据目前披露的资料，“爱因斯坦 3”的入侵防御能力主要来自于美国国家安全局（National Security Agency, NSA）开发的一套名为 TUTELAGE 的系统。TUTELAGE 是一套具有网络流量监控、主动防御与反击功能的系统，用于保护美军的网络安全，相关文件显示早至 2009 年以前就已投入使用。传统基于日志的防御方法具有时效性差、通常在攻击成功实施后才能发现和应对的问题，而 TUTELAGE 可以和信号情报（SIGINT）、商业防护工具一起，协作应对威胁。TUTELAGE 通过 SIGINT 提前发现对手的工具、意图并设计反制手段，在对手入侵之前拒止。即使对手成功入侵，也能通过阻断、修改 C2 指令等方法，缓解威胁。



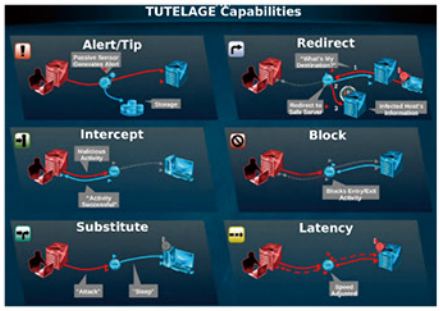
TUTELAGE 运行环境

系统通过部署在国防部（Department of Defense, DOD）非保密因特网协议路由器网（Non-secure Internet Protocol Router Network, NIPRNet）与互联网

（下转第二版）

（上接第一版）

连接的边界网关上的传感器发现恶意行为，并将这些行为报告给 TUTELAGE。TUTELAGE 使用深度包处理技术，通过内嵌的包处理器 (in-line packet processor) 透明地干预对手的行动，对双向的包进行检测和替换等，从而实现对恶意流量的拦截、替换、重定向、阻断等功能。



TUTELAGE 功能

通过商业科技和政府专业能力的深度融合，“爱因斯坦”系统允许国土安全部为联邦政府机构提供多种安全服务，包括入侵检测、入侵防御、解析和信息共享等。这些服务是以一系列专业的工程能力为基础的，如全网的信号情报获取能力、高效的深度包检测能力、从全流量数据中快速抽取特定信息的能力等。这些基础的专业工程能力是区别在国际网络空间对抗中取得实战效果的项目与实验室中的原型系统的关键。我国也可以利用军民融合的优势，依靠大规模工程建立超前部署的先进的网络空间安全防御基础平台，为前沿技术创新和探索打下基础，在此基础上，不断建设，叠加演进，最终形成一套完备有效的、具备全天候全方位感知能力的网络空间安全防御体系。

美国的网络空间安全主动防御体系借助商用技术和能力，将网络空间的威胁预警、入侵防御和安全响应能力相结合，创建跨领域的网络空间态势感知系统，为联邦政府网络基础设施提供安全保障。在后续的文章中，我们将关注美国在网络空间攻击方面的能力，介绍美国的网络攻击支持体系和装备体系，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 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	Trojan/Android.RedDawn.a[prv,exp] 2018-05-28	该应用程序运行会私自下载间谍程序动态加载，上传用户短信、联系人、照片等隐私信息，造成用户隐私泄露，请卸载。（威胁等级高）
		RiskWare/Android.jubaoqi.a[spr] 2018-05-29	该应用程序是非官方应用，诱导加 QQ 号、QQ 群，具有一定风险，请谨慎使用。（威胁等级低）
		AdWare/Android.njane.a[ads,exp] 2018-05-29	该应用程序包含 njane 广告插件，会加载广告子包，通过 banner、插屏等方式显示广告，可能会对手机的正常使用造成一定干扰和一定的流量消耗，建议谨慎使用。（威胁等级高）
		Trojan/Android.armaspy.a[prv,rmt,spy] 2018-05-30	该应用程序是一款间谍软件，安装无图标，后台接收远程控制命令，窃取用户短信、联系人、通话记录、浏览器记录，私自拍照、录音、录像、截屏、发送短信，并将用户隐私信息上传至远程服务器。造成用户隐私泄露，建议卸载。（威胁等级高）
		Trojan/Android.weixinghost.a[exp,rmt,rog] 2018-05-31	该应用程序包含恶意代码，运行后获取 root 权限，联网接收控制命令，调用按键精灵接口，模拟点击私自下载并静默安装未知软件，调用微信接口，扫描指定二维码添加微信账号、私自发送朋友圈、添加微信机器人、控制用户微信，篡改用户通讯录。警惕控制命令包含恶意刷量行为。造成用户流量消耗，影响用户手机正常使用，建议卸载。（威胁等级高）
		Trojan/Android.parallelspy.a[prv,spy] 2018-05-31	该应用程序是一款间谍软件，运行后隐藏图标，后台窃取用户短信、联系人、通话记录、地理位置、手机基本信息等隐私信息，私自拍照、录音、录像，发送短信，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）
		G-Ware/Android.CoinMiner.a[exp,rog] 2018-05-31	该应用程序伪装系统应用，运行诱导激活设备管理器，动态释放资源文件，提权静默安装，还会动态释放挖矿相关文件，需警惕该程序后台私自挖矿，影响用户正常使用，请卸载。（威胁等级中）
		G-Ware/Android.SexDowgin.a[exp,rog] 2018-06-01	该应用程序运行过程中频繁展示色情插屏广告，点击就会下载色情应用，造成用户流量消耗，影响用户身心健康，建议不要使用。（威胁等级中）
	较为活跃的样本	Trojan/Android.Reptilicus.b[rmt,prv,spy]	该应用程序是一款间谍软件，运行后隐藏图标，后台接收远程控制命令，窃取用户短信、联系人、通话记录、浏览器历史记录、安装信息、文件、社交应用记录等各种隐私信息，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	微软 Office 公式编辑器远程代码执行漏洞（CVE-2018-0802）	Microsoft Office 公式编辑器远程代码执行漏洞，编号 CVE-2018-0802，攻击者可以利用此问题，在当前登录用户的上下文中执行任意代码，失败的攻击尝试可能会引发 DoS 攻击，全部版本受影响。（威胁等级高）
	较为活跃样本	Trojan[DDoS]/Linux.Ddostf	此威胁是一类针对 Linux 平台的具有 DDoS 功能的木马家族。该家族样本运行后连接远程服务器，向其发送系统敏感信息。它可以接收远程服务器的命令并执行 DDoS 攻击，包括 TCP、UDP 及 HTTP 的洪水攻击。（威胁等级中）
		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，攻击者可以进行各种操作，收集用户的敏感信息。（威胁等级中）
		Trojan[Backdoor]/Linux.Gafgyt	此威胁是一种木马类后门程序，运行在 Linux 平台，主要功能为 DDoS 攻击、更新和下载等，通过扫描 SSH 弱口令进行传播。（威胁等级中）
		Trojan[Downloader]/Win32.Pfoenic	此威胁是木马类家族程序。这种程序的样本执行后进行文件下载并静默安装，同时在任务栏和桌面上创建游戏『超霸传奇』的快捷方式。（威胁等级中）

RSA 首席技术官：技术的现代化成为滋生恶意行为的“催化剂”

Kelly Sheridan / 文　安天技术公益翻译组 / 译

RSA 首席技术官祖尔菲卡·拉姆詹（Zulfikar Ramzan）在 InteropITX 2018 主题演讲中预测了网络安全的未来、驱动因素以及企业 IT 部门如何作出反应。

在企业技术高管云集的会议室里，RSA 首席技术官祖尔菲卡·拉姆詹讨论了网络安全领域的现状以及 IT 企业在采用机器学习等新技术时应该高度重视的威胁。

“没有任何企业可以孤立存在。” 拉姆詹在主题演讲中表示，“随着技术以惊人的方式将我们联接起来，混乱的涟漪传播得越来越快、越来越广 ..... 在网络安全方面，这种情况非常普遍。”为了说明他的观点，他列举了最近发生的几起远超出攻击者预期的安全事件。大型连锁商 Target 遭遇了有史以来规模最大的攻击事件之一，攻击发生的原因是威胁源获取了访问第三方 HVAC 系统（Heating, Ventilation and Air Conditioning，供热、通风与空气调节系统）的口令。婴儿用摄像头的生产厂家成为了大规模 DDoS 攻击的“罪魁祸首”，并最终导致一些大型网站的下线。DNC（民主党全国委员会）攻击导致人们质疑民主的基础。

如今，网络事件导致一些董事会成员不得不引咎辞职。拉姆詹指出，在这样的世界里，我们需要更多地关注驱动因素而非安全趋势，这些驱动因素包括：技术的现代化、威胁源的恶意、迫使企业将其商业价值与安全态势联系起来的强制性要求。

“创新会引发漏洞，现代化会滋生恶意。”拉姆詹说。以勒索软件的演变为例。

勒索软件是随着支付技术的现代化而发展起来的一种相对较老的威胁。数字支付系统的出现使攻击者有办法从越来越多的受害者那里窃取资金。一些黑客还提供全天候的客户支持，帮助受害者付款。“当威胁源开始谈论客户支持时，安全的业态发生了重要变化。”拉姆詹解释说，他把这种观念模式称为“黑客工业复合体”。他指出，我们不仅要担心高级威胁源，还要担心那些乐意通过“小偷小摸”在短时间内窃取大量资金的普通攻击者。

拉姆詹还提到了人工智能和机器学习，这是 InteropITX 与会企业谈及的两个热门话题。人工智能已经存在并在安全领域中使用了很长一段时间，他解释说，用于对抗垃圾邮件、网络诈骗、恶意软件和恶意网络流量。“但是在 AI 能够做什么的研究方面，我们还处于起步阶段。”他继续说道。拉姆詹对人工智能和机器学习的担忧是：将所有数据放在一个地方，采用技术进行分析是否安全。他考虑的不是数据窃取，而是数据操纵。如果威胁源访问和修改企业的数据，很可能不会有人注意到。很少有人了解这些技术是如何运作的。

“机器学习不是为了对付威胁源而设计的，”他解释说，“但是如果你考虑普遍应用该技术，则必须考虑相关风险。”但是如何应对风险呢？拉姆詹警告说，在购买安全工具时采取“有病乱投医”策略是有危险的。该行业“亟待规范和理顺”，他说。在安全领域有大约 2000 家供应商，需要进行强强联合和创新。IT 专家应该确定哪些供应商能够提供最大的价值，并重点关注他们。

最后，他解释了安全事件发生时应如何应对。“提前规划你无法控制的混乱情况，”他指出，即规划事件响应的“三点”。

第一点是可用性。在制定事件响应计划时，你应使用企业已有的资源。“事件响应计划并不是一个愿望清单，”拉姆詹说，“就像不要在每个走廊放置空的灭火器一样，要确保企业资源的即时可用性。”

第二点是预算。他指出，安全漏洞会带来意想不到的成本。例如，你可能需要法律帮助，如果你没有内部团队，则需要聘请外部律师事务所。拉姆詹说：“响应计划必须具有预算权力。没有预算，它就只是一个童话故事。”

第三点是协作。在事件发生期间，企业的大部分部门都会不可避免地受到波及。在安全团队忙于确定、分析威胁源头时，IT 团队则忙于给系统打补丁并隔离受影响网络来止损。如果客户受到影响，则销售团队将会参与其中；如果涉及到销售，那么营销团队也可能会参与其中。

他总结说，网络安全的成功取决于企业评估未来风险的能力。“我们应快速适应并采用技术来促进创新。”

原文名称	RSA CTO: 'Modernization Can Breed Malice'
作者简介	Kelly Sheridan。Kelly Sheridan 是 Dark Reading 的编辑。
原文信息	2018 年 5 月 3 日发布于 Dark Reading 原文地址 https://www.darkreading.com/threat-intelligence/rsa-cto-modernization-can-breed-malice/d/d-id/1331721
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《Tofsee 僵尸网络分析报告》

近日，波兰 CERT 发现一个活跃的僵尸网络：Tofsee，又名 Gheg。它作为一种多功能的僵尸网络恶意软件，可用于挖比特币、发送邮件、窃取凭证、实施 DDoS 攻击等。安天捕风小组发现该僵尸网络发送的所有电子邮件都是随机的，一些简单的垃圾邮件过滤器可能无法过滤这些消息，从而使电脑感染 Tofsee 恶意软件，使人防不胜防。

Tofsee 使用基于 TCP 的非标准协议与被控端通信，建立连接后的第一条消息（大小总是 200 字节）总是由服务器发送，其包含的最重要内容是一个随机的 128 字节的密钥，用于加密进一步的通信，在每个发送或接收字节之后，密钥都会被修改。第一条消息中还包含一个C2 IP地址列表，但有趣的是，这个列表中可能不包含自身的 IP，这样的话连接很快就会终止，并从新接收的列表中选择一个随机服务器作为通信伙伴。随机服务器能有效的充当指向实际服务器的“指针”。

由于 Tofsee 的模块化设计，该僵尸网络的功能多样，且相对独立，只要获取到相应的模块，就可以实现相应功能，适应性极强，通过对其插件进行分析，Tofsee 整体可实现的功能如下：1）可下载、安装恶意程序，实施非常复杂的 DDoS 攻击，例如 HTTP Flood 或常规的 SYN Flood。2）可嗅探、替换通讯，监听 0.0.0.0:1080 上的 TCP 连接并提供多线程 SOCKS 代理服务器，将其他恶意软件从受害者计算机中移除。3）可检测肉鸡是否被列入垃圾邮件程序或被拉入黑名单，窃取微软 Outlook 的网络凭证，从 C2 下载邮件模板后生成并发送垃圾邮件，同时添加恶意程序附件到邮件上。4）通过社交媒体，如 Facebook，Twitter 与 Skype 等通讯软件进行传播。5）辅助货币加密挖矿程序进行挖矿。

安天捕风小组提醒广大互联网用户安全、健康上网，安装杀毒、防毒软件并及时升级系统和修补设备漏洞。

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、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 BD 静态分析鉴定器、动态行为鉴定器、静态分析鉴定器、安全云鉴定器将文件判定为木马程序。

概要信息

文件名	ae0d32e51f36ce6e6e8c5ccdc3d253a0
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	180 KB
MD5	AE0D32E51F36CE6E6E8C5CCDC3D253A0
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.TSGeneric
判定依据	安全云

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
删除自身	★★★★
其他进程写入可疑数据	★★★
延时	★★★

常见行为

查找指定内核模块	★
创建特定窗体	★
打开自身进程文件	★
读取自身文件	★★
设置文件属性为隐藏	★★
隐藏文件	★★
释放 PE 文件	★
增加 run 自启动项	★
获取驱动器类型	★
获取计算机名称	★
请求加载驱动的权限	★
获取主机用户名称	★
创建挂起的进程	★★
访问其他进程内存	★
独占打开文件	★
获取系统内存	★★
访问 dns	★
连接网络	★
自启动	★

进程监控

PID	创建	命令行
1668	yyhhvgtt.exe	"C:\Documents and Settings\Administrator\yyhhvgtt.exe"
1712	svchost.exe	svchost.exe
1780	cmd.exe	"C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\3033.bat"