美国情报机构网络攻击的历史回顾

——基于全球网络安全界披露信息分析

中国网络安全产业联盟

2023 年 4 月

版权声明

目　录

第一篇　网络战的开启——对“震网”事件的分析

20 世纪末期，信息技术迅猛发展，网络空间逐步成为人类社会的“第五空间”，与此同时，各国对网络空间军事化的担心也持续增加。2010 年“震网”病毒（Stuxnet）攻击伊朗核设施事件代表美国打开了“潘多拉魔盒”，人们对网络战的担心变成了现实。

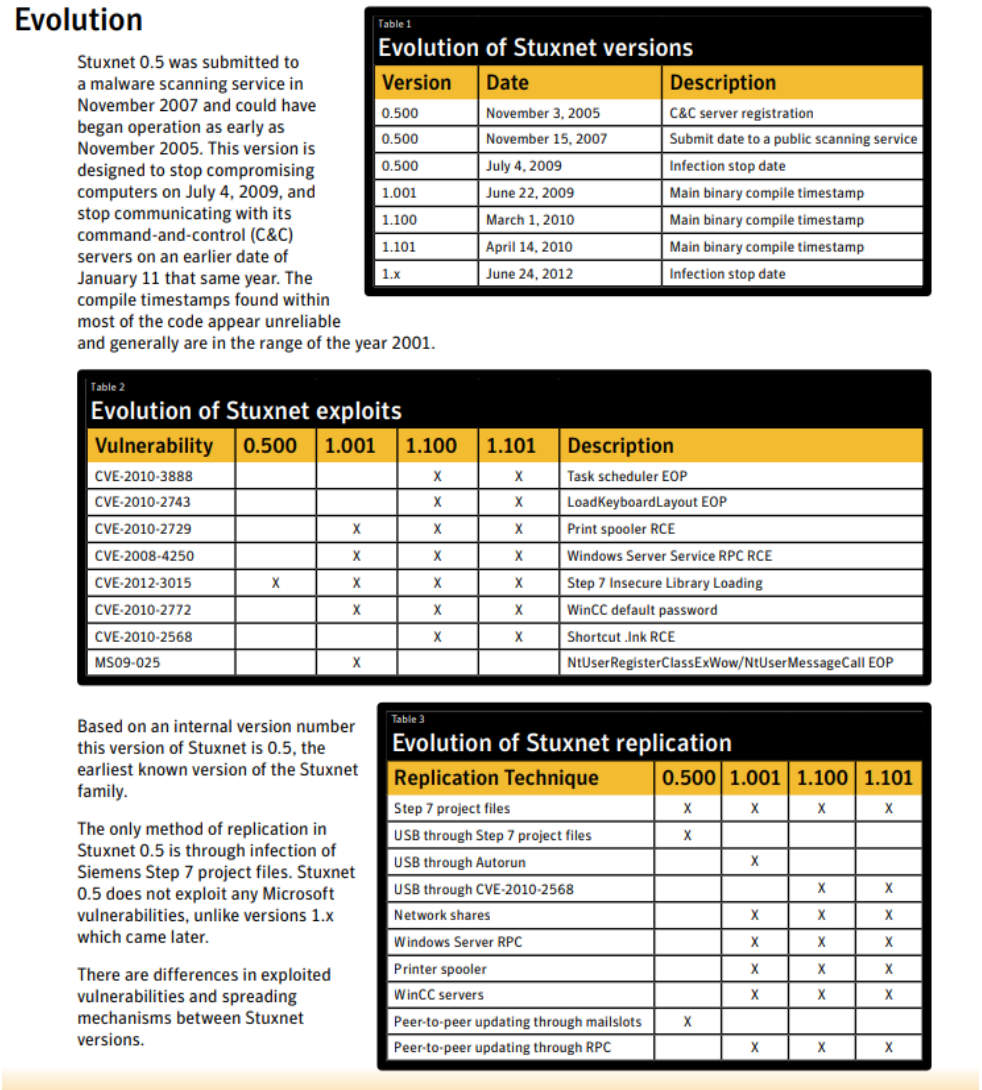
（一） 事件回顾

2010 年 11 月，伊朗政府公开承认该国纳坦兹核设施网络较早前遭受了病毒攻击。根据外界分析，攻击伊朗核设施的是“震网”病毒，毁坏了伊朗近 1/5（一说 2/3）的离心机，感染了 20 多万台计算机，导致近千台机器运行出现异常，使伊朗核计划倒退 2 年。“震网”病毒攻击事件后来被视为开启了网络战时代，拉开了网络病毒作为“超级破坏性武器”改变战争模式的序幕。

（二） 研究分析曝光经过

2010 年 6 月，**白俄罗斯网络安全公司 VirusBlokAda** 为伊朗客户调查电脑死机和重启问题，其技术人员在客户电脑中发现了一种新的蠕虫病毒。根据病毒代码中出现的特征字“stux”，新病毒被命名为“Stuxnet”。2010 年 8 月，**美国网络安全厂商赛门铁克**指出全球受该病毒感染计算机的约

60%均在伊朗境内。2010 年 9 月，赛门铁克再次披露了“震网”病毒的基本情况[1]、传播方法[2]、攻击目标，分析了其感染西门子 Step7 工程文件的方法、感染可编程控制器（PLC）的过程，并在随后的报告中披露“震网”病毒 0.5 版本与其他版本之间的演化过程（见图 1-1）[3]:



Evolution

Stuxnet 0.5 was submitted to a malware scanning service in November 2007 and could have began operation as early as November 2005. This version is designed to stop compromising computers on July 4, 2009, and stop communicating with its command-and-control (C&C) servers on an earlier date of January 11 that same year. The compile timestamps found within most of the code appear unreliable and generally are in the range of the year 2001.

Table 1
Evolution of Stuxnet versions

Version	Date	Description
0.500	November 3, 2005	C&C server registration
0.500	November 15, 2007	Submit date to a public scanning service
0.500	July 4, 2009	Infection stop date
1.001	June 22, 2009	Main binary compile timestamp
1.100	March 1, 2010	Main binary compile timestamp
1.101	April 14, 2010	Main binary compile timestamp
1.x	June 24, 2012	Infection stop date

Table 2
Evolution of Stuxnet exploits

Vulnerability	0.500	1.001	1.100	1.101	Description
CVE-2010-3888			X	X	Task scheduler EOP
CVE-2010-2743			X	X	LoadKeyboardLayout EOP
CVE-2010-2729		X	X	X	Print spooler RCE
CVE-2008-4250		X	X	X	Windows Server Service RPC RCE
CVE-2012-3015	X	X	X	X	Step 7 Insecure Library Loading
CVE-2010-2772		X	X	X	WinCC default password
CVE-2010-2568			X	X	Shortcut .lnk RCE
MS09-025		X			NtUserRegisterClassExWow/NtUserMessageCall EOP

Based on an internal version number this version of Stuxnet is 0.5, the earliest known version of the Stuxnet family.

The only method of replication in Stuxnet 0.5 is through infection of Siemens Step 7 project files. Stuxnet 0.5 does not exploit any Microsoft vulnerabilities, unlike versions 1.x which came later.

There are differences in exploited vulnerabilities and spreading mechanisms between Stuxnet versions.

Table 3
Evolution of Stuxnet replication

Replication Technique	0.500	1.001	1.100	1.101
Step 7 project files	X	X	X	X
USB through Step 7 project files	X			
USB through Autorun		X		
USB through CVE-2010-2568			X	X
Network shares		X	X	X
Windows Server RPC		X	X	X
Printer spooler		X	X	X
WinCC servers		X	X	X
Peer-to-peer updating through mailslots	X			
Peer-to-peer updating through RPC		X	X	X

图 1-1 “震网”病毒不同版本之间的演化过程

赛门铁克于 2010 年 11 月梳理了部分网络安全厂商发现、认识“震网”病毒的过程（见表 1-1）[4][5]:

表 1-1 赛门铁克对“震网”病毒的发现及认知

时间	事件
2008 年 11 月 20 日	Trojan.Zlob 变种被发现利用 LNK 漏洞，随后确认“震网”病毒正是利用了这一漏洞
2009年4月	安全杂志Hakin9公布了打印机后台处理程序服务中远程代码执行漏洞的细节，这一漏洞随后被确认为MS10-061
2009年6月	最早的“震网”样本被发现，没有利用MS10-046，也没有签名驱动文件
2010年1月25日	发现“震网”驱动文件的有效签名证书属于Realtek半导体公司
2010年3月	第一个利用MS10-046的“震网”变种被发现
2010年6月17日	Virusblokada 报道了 W32.Stuxnet 病毒（命名为 Rootkit.Tmphider），称它利用快捷方式（.lnk） 文件处理漏洞进行传播（随后被确认为MS10-046）
2010年7月13日	赛门铁克检测到W32.Temphid（之前认为是木马）
2010年7月16日	微软公布了安全公告“Windows Shell漏洞会导致远程代码执行（2286198）”，包括快捷方式（.lnk）文件处理漏洞 Verisign撤销Realtek半导体公司的证书
2010年7月17日	ESET确认了一个新的“震网”驱动文件，这次的签名证书则是来自JMicron科技公司
2010年7月19日	西门子发表调查报告“恶意代码感染西门子Win CC系统” 赛门铁克将之前检测到的W32.Temphid重命名为W32.Stuxnet
2010年7月20日	赛门铁克监控“震网”命令和控制流量
2010年7月22日	Verisign撤销了JMicron科技公司的证书
2010年8月2日	微软公布MS10-046，该补丁可以修复Windows Shell快捷方式漏洞
2010年8月6日	赛门铁克发表报告“Stuxnet如何通过注入PLC并隐藏代码来感染工业控制系统”[6]
2010年9月14日	微软发布了MS10-061，该补丁可以修复赛门铁克8月份发现的打印机后台处理程序漏洞

	微软公布了赛门铁克8月份确认的两个提权漏洞
2010年9月30日	赛门铁克在Virus Bulletin上公布了“震网”综合分析报告

俄罗斯网络安全厂商卡巴斯基是业内分析“震网”及其相关病毒报告最多、最完整的安全厂商，先后发表数十篇报告，从功能行为、攻击目标、漏洞利用、规避对抗、命令和控制服务器等多方面进行全面分析，尤其是讨论了“震网”病毒所利用的 LNK 漏洞和具有签名的驱动程序，并披露了“震网”病毒最早的五个受害者（见图 1-2）[7]。卡巴斯基分析后指出，如此复杂的攻击只能在“国家支持下”才可进行。

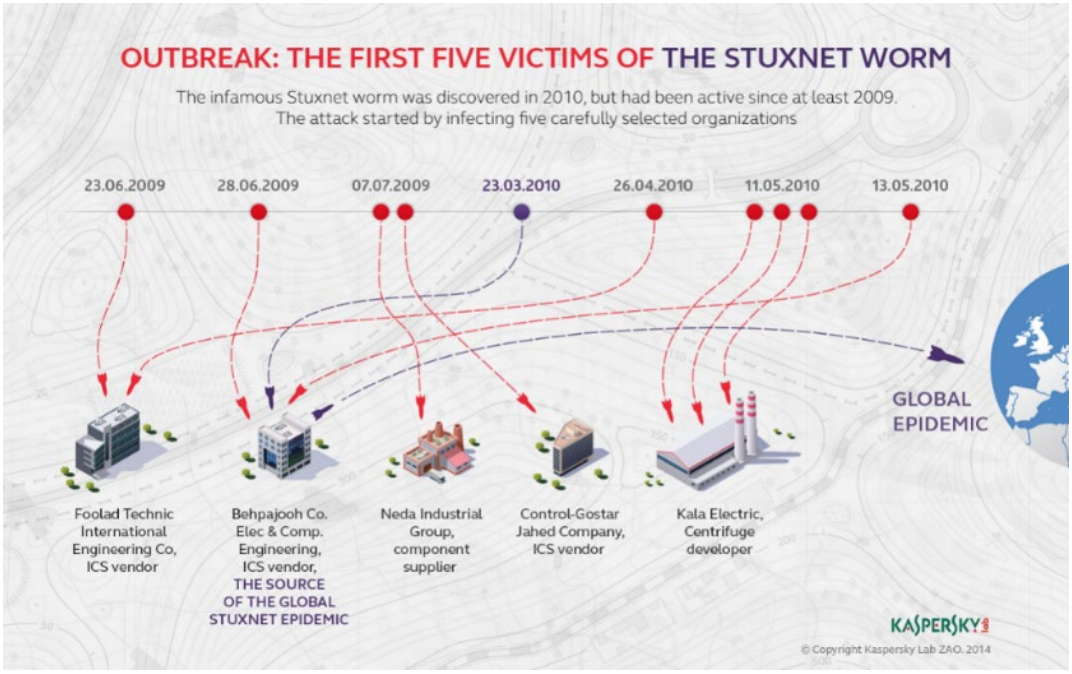


图 1-2 “震网”病毒最早攻击的五个受害者

中国网络安全厂商安天是中国最早分析“震网”及其相关病毒的厂商之一，在捕获样本后，搭建了模拟分析沙盘（见图 1-3）[8]。

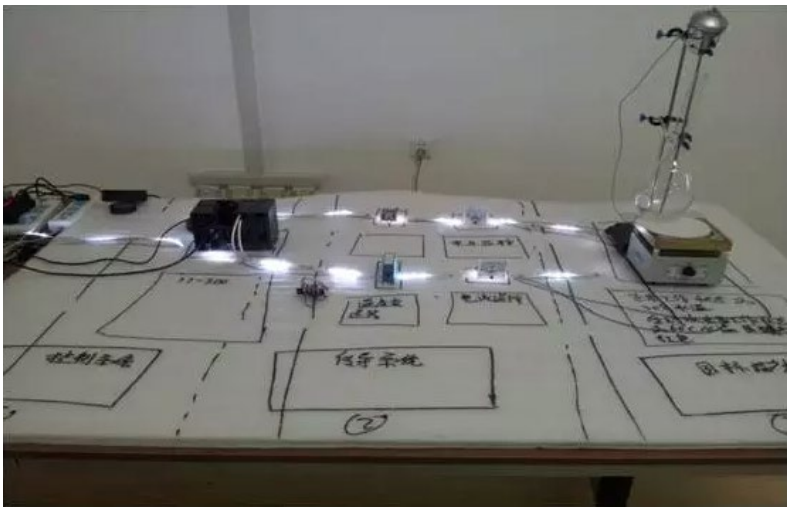


图 1-3 “震网”病毒模拟分析沙盘

2010 年 9 月 27 日，安天发布“对 Stuxnet 蠕虫攻击工业控制系统事件的综合报告”[9]，对“震网”病毒的攻击过程、传播方式、攻击意图、文件衍生关系和利用的多个零日漏洞进行分析，总结其攻击特点并给出解决方案（见图 1-4）[9]。

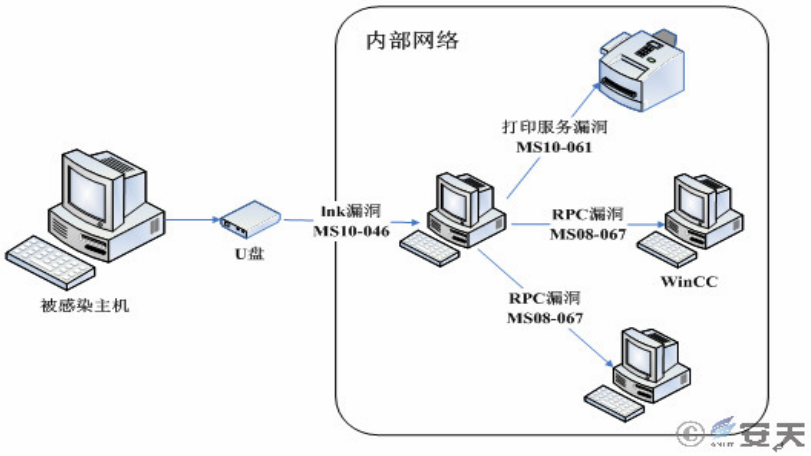


图 1-4 “震网”病毒突破物理隔离环境的传播方式

2010 年 10 月，针对“震网”USB 摆渡行为难以复现的问题，安天发布“对 Stuxnet 蠕虫的后续分析报告”，补充分

析“震网”病毒的 C2 地址、更新方式及 USB 摆渡传播条件的技术机理（见图 1-5）[10]。

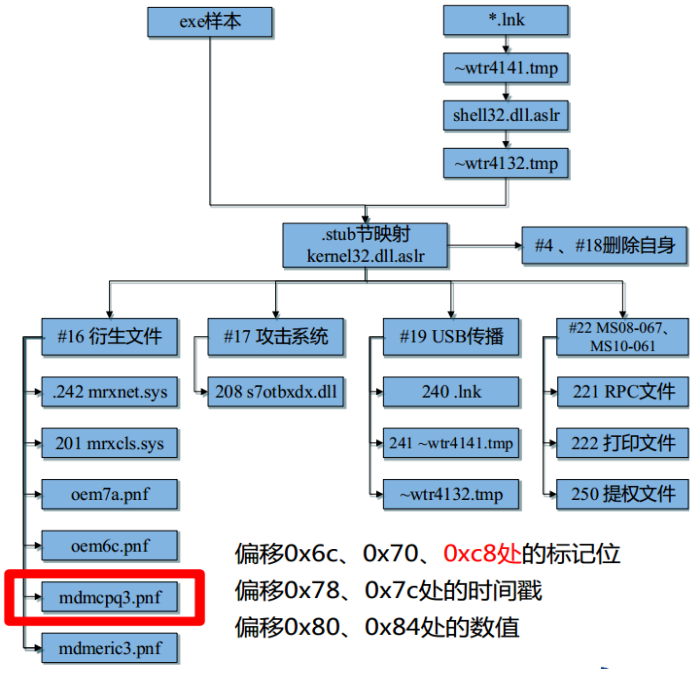


图 1-5 “震网”文件释放结构和 USB 传播逻辑图

2012 年 1 月，安天发布报告“WinCC 之后发生了什么”[11]，分析“震网”病毒攻击工业控制系统对现场设备的影响过程，并根据真实工业控制系统推测一个可能的攻击场景，搭建环境模拟了“震网”病毒对工控系统的攻击过程（见图 1-6）[11]。

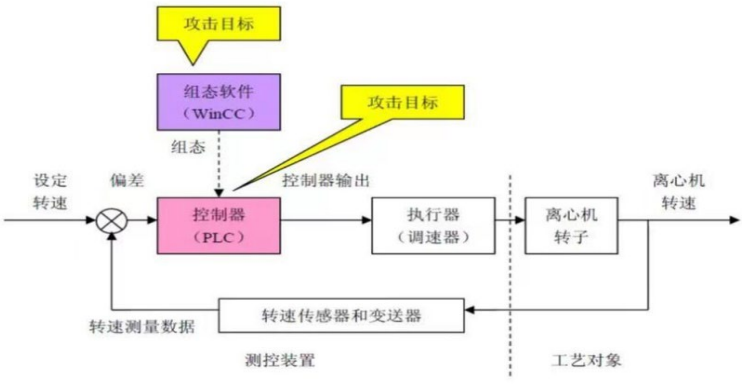


图 1-6 对转速干扰机理的分析推测

2013 年 11 月，**德国 IT 安全专家拉尔夫·朗纳（Ralph Langner）**先后发表两篇文章[12][13], 公布其三年来对“震网”这一“史上首次曝光的网络-物理（Cyber-Physical）战争武器”的跟踪和分析研究结果。他将“震网”事件称为**“网络战的教科书范例”**，基于对“震网”病毒两个版本及攻击事件的跟踪研究，概括性地勾画了“网络战产生物理性战果”的具体实现方法和作战流程。

（三） 小结

在网络安全厂商和安全专家的全面分析接力中，“震网”攻击事件的全貌和大量细节被呈现出来：这是一起经过长期规划准备和入侵潜伏的活动，借助高度复杂的恶意代码和多个零日漏洞作为攻击武器，以铀离心机为攻击目标，通过造成超压使离心机转数异常加速，导致 1000 多台离心机被摧毁，浓缩铀分离能力大幅降低。在信息技术发展历史上，出现过大量网络病毒和攻击事件，但“震网”被认为是第一个得到充分技术实证，对现实世界中的关键工业基础设施造成与传统物理毁伤等效的网络攻击行动，而且达到了预设的攻击目的。美国针对他国工业基础设施开展网络攻击，释放出“网络战”这个瓶子中的魔鬼。全球网络安全界的接力分析，对这次攻击行动进行了十分充分的画像[14]。遗憾的是，当时全球各国和网络安全界更多看到了攻击暴露的技术风险，却没有充分意识到事件背后美国所推动的网络空间军事化威

胁，在这些分析工作中，没有有效整合国家主权、安全视角，也缺少国际法等层面的联动思考。

参考资料

[1] Symantec. Stuxnet Introduces the First Known Rootkit for Industrial Control Systems. 2010. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=94b1015b-da22-499a-abff-7f263ee5e490&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[2] Symantec. Stuxnet P2P component. 2010. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=12adb5c4-1b6b-41dc-95a5-e6320371a847&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[3] Symantec. Stuxnet 0.5: The Missing Link. 2013. https://docs.broadcom.com/doc/stuxnet-missing-link-13-en

[4] Symantec. W32.Stuxnet Dossier. 2010. https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en

[5] Symantec. Stuxnet: A Breakthrough. 2010. https://community.broadcom.com/symantecenterprise/viewdocument/stuxnet-a-breakthrough?CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[6] Symantec. Exploring Stuxnet’ s PLC Infection Process. 2010. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ad4b3d10-b808-414c-b4c3-ae4a2ed85560&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[7] Kaspersky. Stuxnet: Zero victims. 2014.

https://securelist.com/stuxnet-zero-victims/67483/

[8] 安天. 安天研究人员在安全焦点峰会进行两场主题演讲. 2016.
https://www.antiy.cn/Market/Meeting/404.html

[9] 安天. 对 Stuxnet 蠕虫攻击工业控制系统事件的综合分析报告. 2010.
https://www.antiy.cn/research/notice&report/research_report/20100927.html

[10]安天. 对 Stuxnet 蠕虫的后续分析报告. 2010
https://www.antiy.cn/research/notice&report/research_report/20101011.html

[11]安天. WinCC 之后发生了什么？——浅析攻击工业控制系统对现场设备的影响过程.2012
https://www.antiy.cn/research/notice&report/research_report/20120117.html

[12]Ralph Langner. Stuxnet's Secret Twin. Foreign Policy. 2013.
https://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/

[13]Ralph Langner. To kill a centrifuge： A Technical Analysis of What Stuxnet's Creators Tried to Achieve. 2013.
https://www.langner.com/to-kill-a-centrifuge/

[14]肖新光. 请君入瓮一APT 攻防指南之兵不厌诈-序言. 2017.
https://blog.csdn.net/weixin_34403693/article/details/90540185

第二篇　“震网”之后的连锁反应——对“毒曲”“火焰”“高斯”的跟进分析

“震网”病毒还在全球肆虐，比其更加复杂的“毒曲”（Duqu）“火焰”（Flame）以及“高斯”(Gauss)等病毒又陆续闯入网络安全厂商的视野。经过深入的解构分析，业界专家逐步证实了这些病毒与“震网”同源，与“震网”同期甚至更早前就已经开始传播。

（一）事件回顾

2011 年 10 月 14 日，**匈牙利安全团队 CrySyS** 发现了一个与“震网”非常类似的病毒样本[1]，主要目的是为窃取秘密信息提供便利。因其创建文件都以“~DQ”作为前缀，故命名为 Duqu （“毒曲”）。

2012 年 4 月，伊朗石油部和伊朗国家石油公司都遭到了恶意软件攻击，后被证实为“火焰”病毒。该病毒当时已感染了伊朗、黎巴嫩、叙利亚、苏丹、其他中非和北非国家的相关计算机系统。安全厂商推测“火焰”病毒出现的最早时间可追溯到 2007 年，并可能于 2010 年 3 月就被攻击者放出（用于窃取伊朗石油部门的商业情报）。

2012 年 8 月，卡巴斯基发现中东地区出现一个专门收集财务信息的间谍软件“高斯”。这种新型网络监测病毒能监视银行交易并窃取网站登录信息，已有数千名中东银行的客户密码与重要数据被窃。在全球网络安全厂商随后的研究中，

“毒曲”“火焰”和“高斯”均被证实与“震网”病毒有相关性。

（二）研究分析曝光经过

1、“毒曲”

CrySyS 是最早发现“毒曲”病毒的研究机构。2011 年 10 月 14 日，**CrySyS** 发布了一份 60 页的报告“Duqu:发现一种类似“震网”的病毒”[1]，首次将该病毒命名为“毒曲”，称其在针对性攻击中被大量使用，并使用一个来自中国台湾科技公司的数字签名。CrySyS 对“毒曲”的主要功能做了分析，并与“震网”进行对比，确定二者之间极具相似性。

2011 年 10 月 18 日，**赛门铁克**发布分析报告，详细分析了“毒曲”病毒的全球感染情况、安装过程、加载逻辑，并指出“毒曲”的目的与“震网”不同，主要是用来收集目标的情报数据和资产，为类似“震网”病毒之类的攻击做准备（见图 2-1）[2]。

Feature	Stuxnet	Duqu
Modular malware	✓	✓
Kernel driver based rootkit	✓	✓ very similar
Valid digital signature on driver	Realtek, JMicron	C-Media
Injection based on A/V list	✓	✓ seems based on Stux.
Imports based on checksum	✓	✓ different alg.
3 Config files, all encrypted, etc.	✓	✓ almost the same
Keylogger module	?	✓
PLC functionality	✓	✗ (different goal)
Infection through local shares	✓	No proof, but seems so
Exploits	✓	?
0-day exploits	✓	?
DLL injection to system processes	✓	✓
DLL with modules as resources	✓ (many)	✓ (one)
RPC communication	✓	✓
RPC control in LAN	✓	?
RPC Based C&C	✓	?
Port 80/443, TLS based C&C	?	✓
Special "magic" keys, e.g. 790522, AE	✓	✓ lots of similar
Virtual file based access to modules	✓	✓
Usage of LZO lib	?	✓ multiple
Visual C++ payload	✓	✓
UPX compressed payload,	✓	✓
Careful error handling	✓	✓
Deactivation timer	✓	✓
Initial Delay	? Some	✓ 15 mins
Configurable starting in safe mode/dbg	✓	✓ (exactly same mech.)

Table 1 – Comparing Duqu and Stuxnet at the first glance

图 2-1 "毒曲"和"震网"初步比较

卡巴斯基从 2011 年 10 月 20 日起，陆续发布了关于"毒曲"病毒的十篇分析报告[3-12]，认为"毒曲"是一个多功能框架，具有高度可定制性和通用性，可以与任意数量的任意模块组合工作，并公布了其与"震网"病毒的同源样本关联分析及时间戳关联分析。在后续的研究中，卡巴斯基披露了"毒曲"利用字体文件漏洞 MS11-077 投递文档文件发起攻击，分析"毒曲"命令与控制（C&C）以及第一层 C&C 和第二层 C&C 地址，指出"毒曲"2.0 的最大特点是恶意代码只驻留在被感染机器的内存里，不在物理硬盘留下痕迹。机器重启时恶意代码会被短暂清洗，但只要它连上内部网络，恶意代码就会从另一台感染机器传输过来。

值得一提的是，2015 年 6 月，卡巴斯基捕获到了“毒曲”病毒攻击，攻击者意图监控并窃取其源代码。卡巴斯基经过大量调查，发现这又是一次精心组织、精密实施的 APT 攻击，只有国家支持的团队才有能力做到，他们明确指认幕后黑手就是“毒曲”背后组织，因而将此次攻击样本命名为“Duqu 2.0”（见图 2-2）[13]。卡巴斯基联合创始人兼 CEO 尤金·卡巴斯基（Eugene Kaspersky）专门在“福布斯”网站上撰文“为什么攻击卡巴斯基实验室是一件愚蠢的事情”，对其进行了分析[13]。

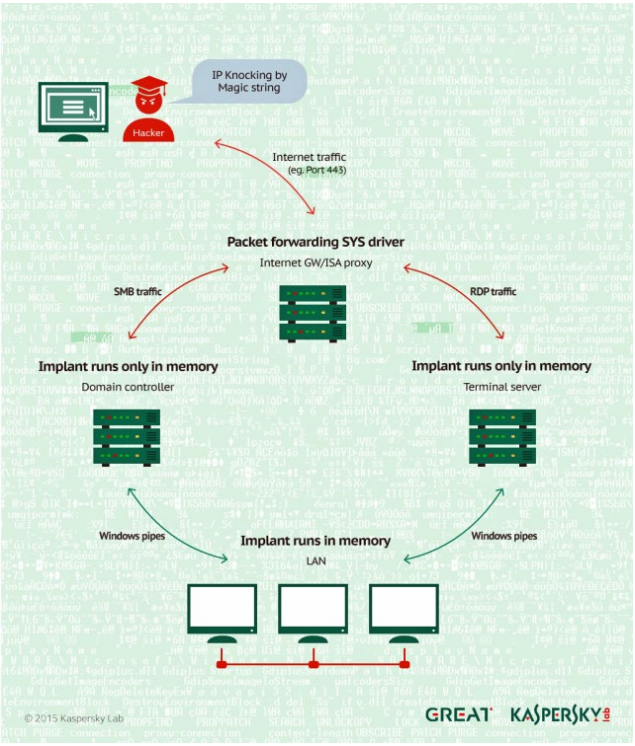


图 2-2 “毒曲”2.0 攻击过程图

2012 年 5 月，安天在《程序员》杂志上发表“探索 Duqu 木马身世之谜—— Duqu 和 Stuxnet 同源性分析”[14]，分析“毒曲”病毒的模块结构、编译器架构、关键功能，指出“毒

曲”与“震网”在结构和功能上具有一定的相似性。同时在分析“毒曲”的解密密钥、反跟踪手段、程序 BUG 时，研究人员发现“毒曲”与“震网”样本中出现相同的逻辑判断错误，根据编码心理学，判断两者具有同源性（见图 2-3）[14]。

比较项目	Duqu木马	Stuxnet蠕虫
功能模块化	是	
Ring0注入方式	PsSetLoadImageNotifyRoutine	
Ring3注入方式	Hook ntdll.dll	
注入系统进程	是	
资源嵌入DLL模块	一个	多个
利用微软漏洞	是	
使用数字签名	是	
包括RPC通讯模块	是	
配置文件解密密钥	0xae240682	0x01ae0000
注册表解密密钥	0xae240682	
Magic number	0x90,0x05,0x79,0xae	
运行模式判断代码存在Bug	是	
注册表操作代码存在Bug	是	
攻击工业控制系统	否	是
驱动程序编译环境	Microsoft Visual C++ 6.0	Microsoft Visual C++ 7.0

图 2-3 “毒曲”与“震网”同源关键代码基因对比

2、“火焰”

2012 年 4 月，伊朗石油部和伊朗国家石油公司遭到了恶意软件攻击，将“火焰”病毒带入了网络安全厂商的视野。**卡巴斯基**认为该病毒是当时攻击机制最复杂、威胁程度最高的计算机病毒之一[15]，结构复杂度是“震网”病毒的 20 倍。卡巴斯基首席安全专家亚历山大·戈斯捷夫(Alexander Gostev)表示，“火焰”病毒的编写和攻击机制都非常复杂。据相关线索分析，“火焰”的出现最早可追溯到 2007 年，可能已经以某种形式活跃了长达 5 至 8 年的时间，甚至更久。

卡巴斯基指出，一旦感染“火焰”病毒后，包括键盘、屏幕、麦克风、移动存储设备、网络、Wi-Fi、蓝牙、USB 和系统进程等信息都可能被收集，包括用户浏览网页、通讯通话、账号密码以至键盘输入等在内的记录信息，甚至通过蓝牙与被感染电脑相连的智能手机、平板电脑中的文件，全部可被发送给远程操控病毒的服务器（见图 2-4）[15]。一旦完成搜集数据任务，这些病毒还可自行毁灭，这也是其能够长期潜伏的原因之一。

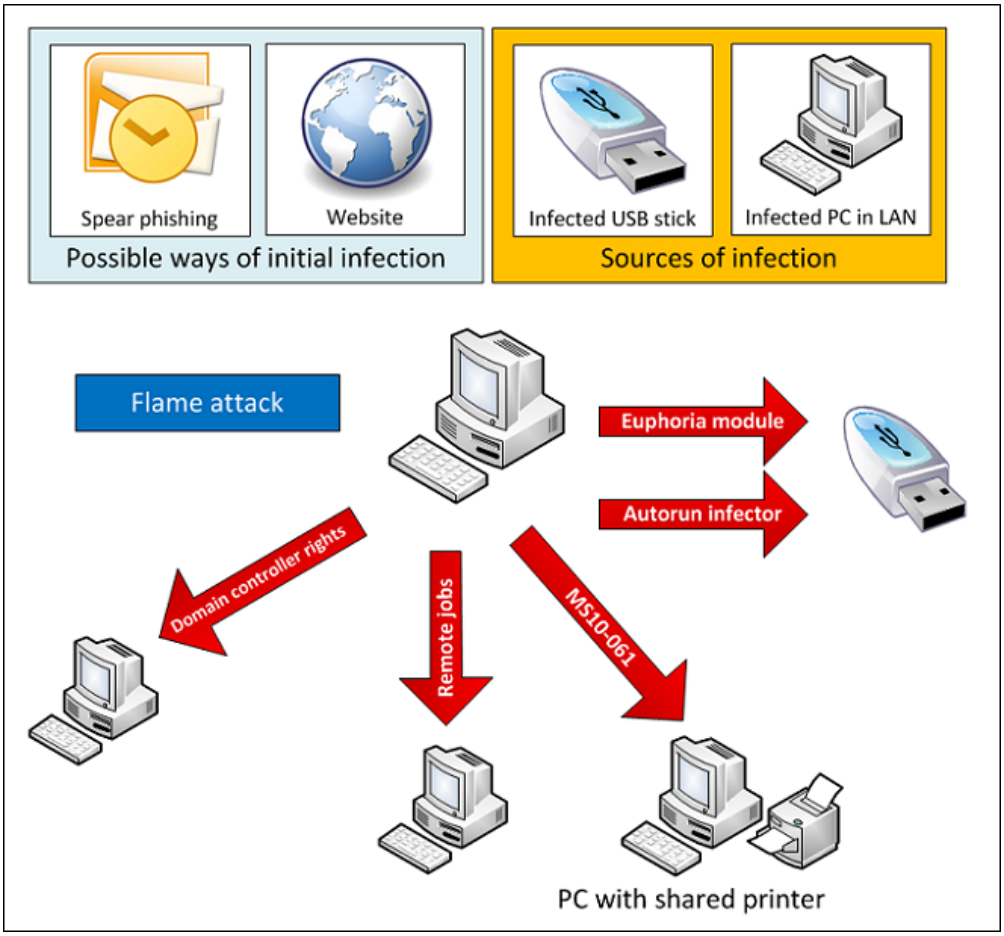


图 2-4 “火焰”可能的传播途径

卡巴斯基称，“火焰”病毒使用了中间人攻击技术，利用微软升级服务（Microsoft Windows Update）进行传播。“火

焰”病毒与“毒曲”的区别在于，“毒曲”和“震网”一样是基于 Tilded 框架，而“火焰”病毒则使用 Flamer 框架。与“震网”“毒曲”病毒相比，“火焰”病毒更为智能，其攻击目标和代码组成也有较大区别。卡巴斯基认为，两个框架背后的团队曾经共享过至少一个模块的源代码，表明他们至少有一次合作，属于同一机构的两个平行项目。“火焰”病毒的攻击机制更为复杂，且攻击目标针对特定地域，这或许表明，该病毒的幕后团队很可能由政府机构操纵。

尤金·卡巴斯基在一份声明中表示：“‘震网’和‘毒曲’病毒属于一系列攻击的组成部分，引起全球安全人士的警惕。而‘火焰’病毒的发现，意味着互联网安全大战进入新阶段。我们必须明白，诸如‘火焰’等病毒，是能够被轻松用来攻击任何国家。”

2012 年 5 月，**安天**发布报告，分析了“火焰”病毒的运行逻辑、传播机理和主要模块功能（见图 2-5）[16]，认为“火焰”是一个比“震网”具有更多模块的复杂组件化木马，其漏洞攻击模块中包含曾被“震网”病毒使用过的 USB 攻击模块，这可佐证两者的同源关系。

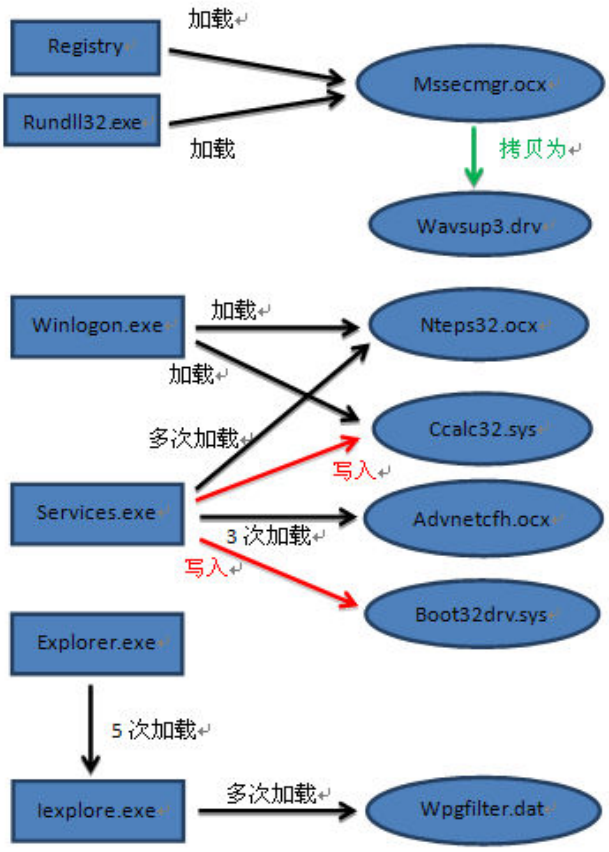


图 2-5 “火焰”病毒主模块启动加载顺序

2012 年 6 月，**微软**发布调查报告指出[17]，“火焰”病毒主要用于进行高度复杂且极具针对性的攻击，可从 PDF、电子表格和 Word 文档等文件中提取 1KB 样本，并压缩上传到命令控制服务器，然后攻击者发出指令抓取他们感兴趣的特定文档。“火焰”病毒攻击使用微软 Windows Update 的用户，通过设置伪造的服务器，绕过合法的 Windows Update 进行攻击。当电脑连接到网络上时，用户会看到伪装成正版的微软更新软件，而此时“火焰”病毒就从伪造的服务器传输到电脑里。该病毒使用的某些技术已被一些低级攻击者用于更广泛的攻击。

CrySyS 在其研究中将“火焰”病毒命名为 skyWIper，认为 skyWIper 是一种信息窃取恶意软件，其模块化结构结合了多种传播和攻击技术，可能已经活跃 5 到 8 年时间，甚至更久[18]。CrySyS 在报告中分析了其主要模块、存储格式、加密算法、注入机制和功能行为（见图 2-6）[18]，提出 skyWIper 可能由国家政府机构开发，具有大量预算和技术，并且可能与网络战活动有关。

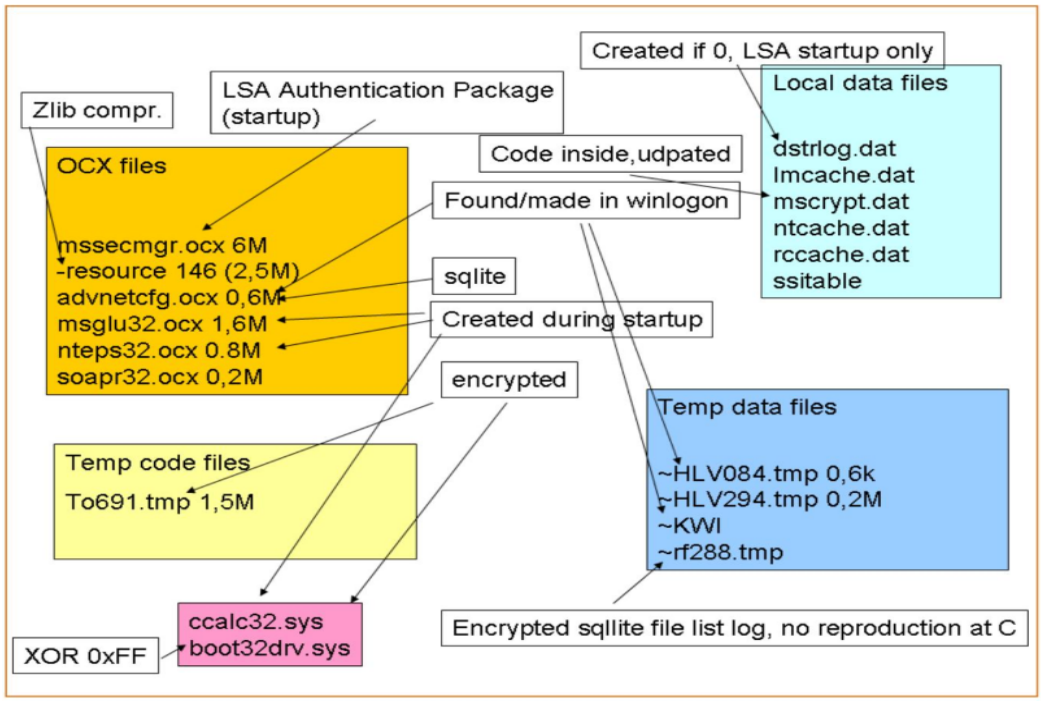


图 2-6 “火焰”相关文件

3、 “高斯”

2012 年 8 月，**卡巴斯基**发现“高斯”病毒，认为它是一个复杂的网络间谍工具包，由“火焰”病毒背后的参与者创建，具备高度模块化，能够支持新的功能，可以由攻击者以插件的形式进行远程部署（见图 2-7）[19]。

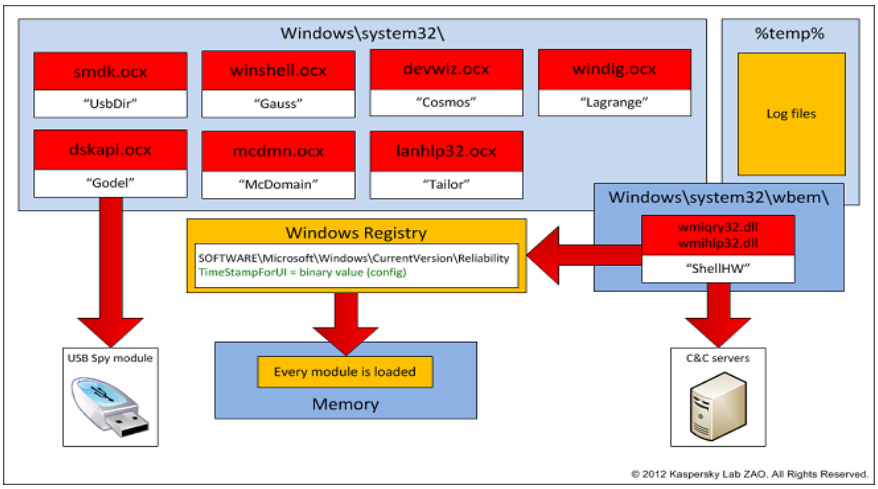


图 2-7 “高斯”架构图

卡巴斯基表示，有足够的证据表明“高斯”与“火焰”“震网”密切相关，由与“震网”“毒曲”“火焰”相关的组织创建，其中“震网”病毒攻击由国家发起。

由于“震网”事件规模比较庞大且版本比较多，在相当长的一段时间里，业界都没有获得“震网”的完整版本和样本集合，给“震网”留下了一些历史疑问，例如：为何一个具有高度定向性的攻击行动却呈现出发散性的传播效果，存在数以千计的样本。对于这些问题，安天通过持续的跟踪研究，在 2019 年发布“震网事件的九年再复盘与思考”[20]，分析了“震网”各个版本的特点、产生原因、作用机理、相关高级恶意代码工程框架，以及“震网”“毒曲”“火焰”“高斯”“方程式组织”所使用恶意代码间的关联，发现美国至少维护了 Tilded 和 Flamer 两个恶意代码框架和平行项目开发以上恶意代码，并且基于更多的线索，发现 Fanny 和 Flowershop 也与上述恶意代码串接到一起（见图 2-8）[20]。

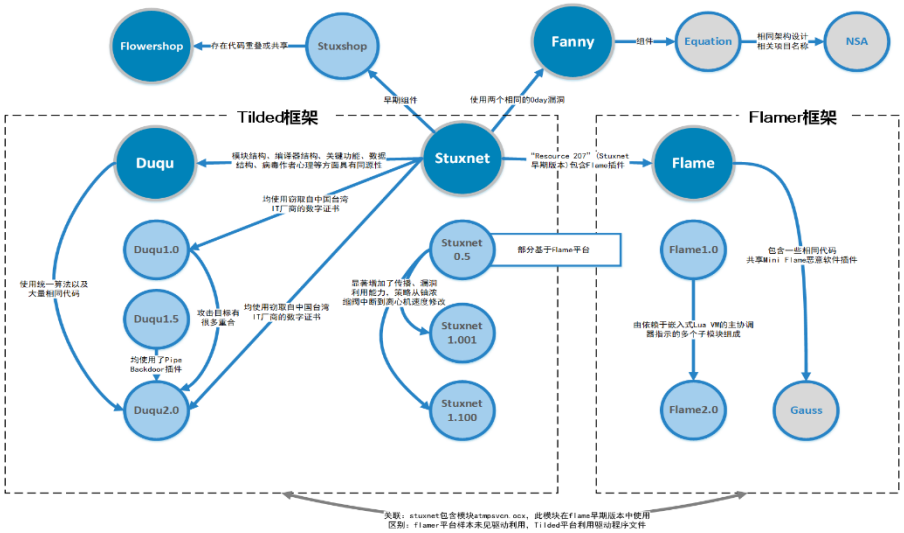


图 2-8“震网”和”毒曲””火焰””高斯”、Fanny、Flowershop 关系图

（三） 小结

“震网”病毒造成的巨大危害是建立在“火焰”“毒曲”恶意代码的长期运行和信息采集的基础之上。“震网”系列病毒攻击昭示了工业基础设施可能被全面入侵渗透乃至完成战场预置的风险和严重后果。多家厂商的样本研究已证实了“毒曲”“火焰”“高斯”与“震网”的关联性，并基本锁定其幕后黑手可能是美国。

对于“震网”及其同源病毒的发现与跟踪分析，全球网络安全厂商更多聚焦其复杂结构和精密设计，研究分析也基本建立在对所使用漏洞的原理分析、对样本的逆向分析，以及对样本作用机理的复盘之上，把攻击事件单纯当作安全威胁技术事件处理与防范，分析中始终缺乏从作业到作战视角的思考，没有从政治、外交、社会等层面对这些病毒攻击进行更深入的理解。

参考资料

[1] CrySyS. Duqu: A Stuxnet-like malware found in the wild. 2011. https://www.yumpu.com/en/document/view/17515556/duqu-a-stuxnet-like-malware-found-in-the-wild-crysys-lab

[2] Symantec. W32.Duqu: The Precursor to the Next Stuxnet. 2011. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=933c68f1-6ee7-473e-9eb6-6c8459f790f2&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[3] Kaspersky. The Mystery of Duqu: Part One. 2011. https://securelist.com/the-mystery-of-duqu-part-one/31177/

[4] Kaspersky. The Mystery of Duqu: Part Two. 2011. https://securelist.com/the-mystery-of-duqu-part-two/31445/

[5] Kaspersky. The Mystery of Duqu: Part Three. 2011. https://securelist.com/the-mystery-of-duqu-part-three/31486/

[6] Kaspersky. The Mystery of Duqu: Part Five. 2011. https://securelist.com/the-mystery-of-duqu-part-five-6/31208/

[7] Kaspersky. The Mystery of Duqu: Part Six (The Command and Control servers). 2011. https://securelist.com/the-mystery-of-duqu-part-six-the-command-and-control-servers-36/31863/

[8] Kaspersky. Stuxnet/Duqu: The Evolution of Drivers. 2011. https://securelist.com/stuxnetduqu-the-evolution-of-drivers/36462/

[9] Kaspersky. The Mystery of the Duqu Framework. 2012. https://securelist.com/the-mystery-of-the-duqu-framework-6/32086/

[10] Kaspersky. The mystery of Duqu Framework solved. 2012. https://securelist.com/the-mystery-of-duqu-framework-solved-7/32354/

[11] Kaspersky. The Mystery of Duqu: Part Ten. 2012. https://securelist.com/the-mystery-of-duqu-part-ten/32668/

[12] Kaspersky. The Mystery of Duqu 2.0: a sophisticated cyberespionage actor returns. 2015.

https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/

[13] Eugene Kaspersky. Why Hacking Kaspersky Lab Was A Silly Thing To Do. 2015 https://www.forbes.com/sites/eugenekaspersky/2015/06/10/why-hacking-us-was-a-silly-thing-to-do/

[14] 安天. 探索 Duqu 木马身世之谜一一 Duqu 和 Stuxnet 同源性分析. 2012. https://antiy.cn/research/notice&report/research_report/261.html

[15] Kaspersky. The Flame: Questions and Answers. 2012. https://securelist.com/the-flame-questions-and-answers/34344/

[16] 安天. Flame 蠕虫样本集分析报告. 2012. https://www.antiy.cn/research/notice&report/research_report/20120531.html

[17] Microsoft. Flame malware collision attack explained. 2012. https://msrc-blog.microsoft.com/2012/06/06/flame-malware-collision-attack-explained/

[18] CrySyS. skyWIper (Flame Virus)- Complex cyber-warfare targeted attacks. 2012. https://www.crysys.hu/publications/files/skywiper.pdf

[19] Kaspersky. Gauss: Nation-state cyber-surveillance meets banking Trojan. 2012. https://securelist.com/gauss-nation-state-cyber-surveillance-meets-banking-trojan-54/33854/

[20] 安天. 震网事件的九年再复盘与思考. 2019. https://www.antiy.com/response/20190930.html

[21] Trend Micro. DUQU Uses STUXNET-Like Techniques to Conduct Information Theft. 2011. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/90/duqu-uses-stuxnetlike-techniques-to-conduct-information-theft

[22] Kaspersky. The Roof Is on Fire: Tackling Flame's C&C Servers. 2012. https://securelist.com/the-roof-is-on-fire-tackling-flames-cc-servers/33033/

[23] Kaspersky. 'Gadget' in the middle: Flame malware spreading vector identified. 2012. https://securelist.com/gadget-in-the-middle-flame-malware-spreading-vector-identified/33081/

[24] Kaspersky.Flame: Replication via Windows Update MITM proxy server. 2012. https://securelist.com/flame-replication-via-windows-update-mitm-proxy-server/33002/

[25] Kaspersky. Back to Stuxnet: the missing link. 2012. https://securelist.com/back-to-stuxnet-the-missing-link/33174/

[26] Kaspersky. The Day The Stuxnet Died. 2012. https://securelist.com/the-day-the-stuxnet-died/33206/

[27] Kaspersky. Gauss: Abnormal Distribution. 2012. https://securelist.com/gauss-abnormal-distribution/36620/

[28] Kaspersky. The Mystery of the Encrypted Gauss Payload. 2012. https://securelist.com/the-mystery-of-the-encrypted-gauss-payload-5/33561/

[29] Kaspersky. What was that Wiper thing? 2012. https://securelist.com/what-was-that-wiper-thing-48/34088/

[30] Kaspersky. Full Analysis of Flame's Command & Control servers. 2012. https://securelist.com/full-analysis-of-flames-command-control-servers/34216/

[31] Kaspersky. Stuxnet: Zero victims. 2014. https://securelist.com/full-analysis-of-flames-command-control-servers/34216/

[32] Kaspersky. Duqu is back: Kaspersky Lab reveals cyberattack on its corporate network that also hit high profile victims in Western countries, the Middle East and Asia. 2015. https://www.kaspersky.com/about/press-releases/2015_duqu-is-back-kaspersky-lab-reveals-cyberattack-on-its-corporate-network-that-also-hit-high-profile-victims-in-western-countries-the-middle-east-and-asia

[33] Kaspersky. The Duqu 2.0 Technical Details. 2015. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

[34] Kaspersky. The Duqu 2.0 persistence module. 2015. https://securelist.com/the-duqu-2-0-persistence-module/70641/

第三篇　超级机器的全貌——斯诺登事件跟进分析

“震网”“毒曲”“火焰”揭开美国情报机构网络攻击能力的神秘面纱，但全球网络安全界对美国攻击能力的认知还停留在极度复杂的病毒木马和丰富的零日漏洞储备上。2013 年，斯诺登事件让大家看到，美国的网络情报攻击能力是一个“大到无形”的庞大体系。随着斯诺登泄露文件的逐步公开，全球网络安全厂商对于美国情报机构网络空间行动的相关工程体系、装备体系有了更多可以分析的文献资料，美国网络空间超级机器的全貌逐步显现。

（一） 事件回顾

2013 年 6 月 5 日，英国“卫报”曝光美国法院 2013 年 4 月 25 日秘密签发授权令，要求即日起至 7 月 19 日，美国电信巨头威瑞森公司（Verizon）须每日向美国国家安全局（NSA）上交数百万用户的通话记录，其中包括国际长途通话记录[1]。报道称，NSA 要求上交的具体数据包括通话次数、通话时长、通话时间等，通话内容不在其中，同时威瑞森公司必须全程严格保密。次日，爆料人美国中央情报局（CIA）情报职员斯诺登现身。斯诺登揭露了 NSA 一个代号为“棱镜”（PRISM）的秘密项目，曝光了包括微软、雅虎、谷歌、苹果等在内的 9 家国际网络巨头配合美国政府秘密监听通话记录、电子邮件、视频和照片等信息，甚至入侵包括德国、

韩国在内的多个国家的网络设备。后续系列公布文件共同揭露了美国政府长期以来实施的监听及网络入侵行动。

全球部分中立媒体不断跟进揭露美国情报机构的监听行动[2-4]。2013 年 10 月，英国“卫报”发表文章“攻击 Tor: NSA 如何获取用户的在线匿名信息”[2]，揭露了美国 NSA 应用漏洞开发技术和互联网监控技术，利用 Tor 用户 Firefox 浏览器漏洞对其发起网络攻击，以获取信息情报。具体操作是通过强大的网络监控能力识别出互联网上的 Tor 用户后，将其重定向到一组秘密网络服务器（代号为 FoxAcid），借此感染用户计算机。

2014 年 6 月，**英国科技媒体 The Register** 发布“NSA 与‘五只眼’吸血乌贼”评论文章，称斯诺登泄露文件显示 NSA 及“五眼联盟”在全球创建了秘密监视和控制网，范围覆盖全球通信及计算机安全组织和公司，互联网作为公共通信媒介的安全性已经完全被打破，对 IT 安全的伤害是蓄谋已久的、持续的[3]。

（二） 研究分析曝光经过

2013 年 7 月，安天技术负责人在中国《计算机学会通讯》撰文“斯诺登效应的前因解读”[5]，指出该事件并非简单的监控与隐私泄露问题，其影响纵深涉及到当前全球秩序、外交、情报与内政的诸多方面。安天分析斯诺登事件暴露的重点内容主要包括：一是“棱镜”项目作为 NSA 网络情报系统

的一个组成部分，主要利用美国互联网企业所提供的接口进行数据检索、查询和收集工作；二是谷歌、微软、苹果、脸谱等美国大型互联网企业大多与此计划有关联；三是 NSA 下属的特定入侵行动办公室（TAO）对中国进行了长达 15 年的攻击，相关行动得到了思科的帮助（见图 3-1）[5]。

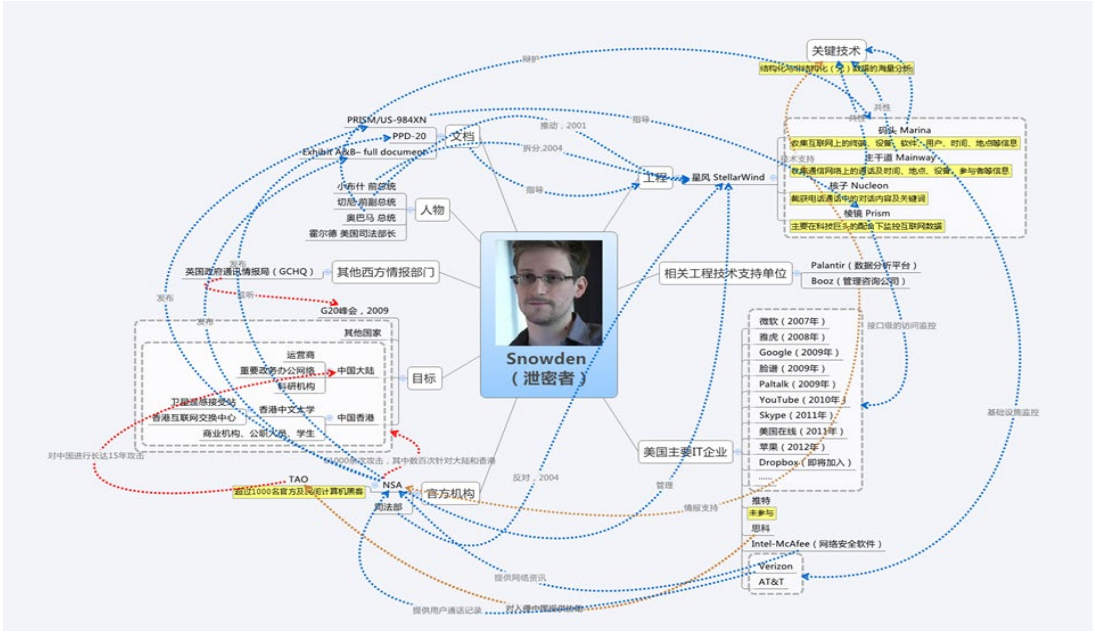


图 3-1 斯诺登事件相关信息关系图

斯诺登泄露文件披露，2004 年美国政府启动“星风”计划（STELLARWIND）进行大规模情报搜集、监听，后因法律等问题，将“星风”拆分为“棱镜”“主干道”“码头”“核子”等多个项目，并由 NSA 接管。安天 2017 年 12 月发布系列文章，深度解析斯诺登泄露文件中的“星风”计划等（见图 3-2）[6]。

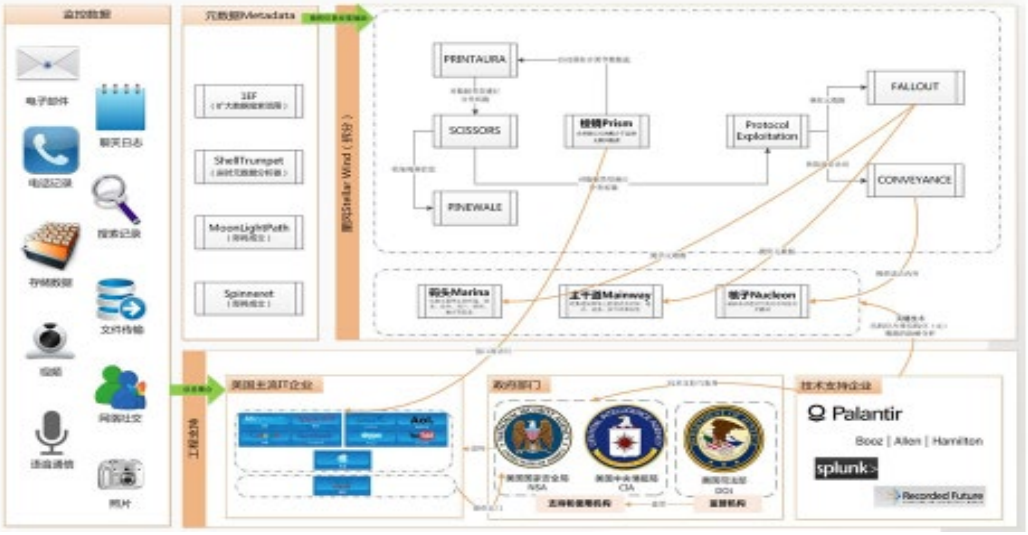


图 3-2 “星风”计划项目结构分析

文章指出，根据斯诺登泄露文件，美国开展了大量的网络情报窃听项目和计划，“棱镜”是其中典型代表。美国通过大型海底光缆监听、重点特殊区域监听、计算机网络利用（CNE）、卫星监听和第三方情报共享等方式，获取各类网络情报，实现对全球目标的完整画像，从而形成比较精准的目标定位能力，为美国获得网络空间防御与反制、威慑、攻击等全方位优势奠定了基础。

基于覆盖全球的情报获取能力，美国建立了以“湍流”（TURBULENCE）为代表的进攻性能力支撑体系，通过被动信号情报获取、主动信号情报获取、任务逻辑控制、情报扩散与聚合、定向定位等相关能力模块，实现完整的网络空间情报循环，并结合“监护”（TUTELAGE）、“量子”（QUANTUM）等网络空间攻防能力模块，进一步实现情报驱动的网络空间积极防御和进攻行动（见图 3-3、3-4）[6]。

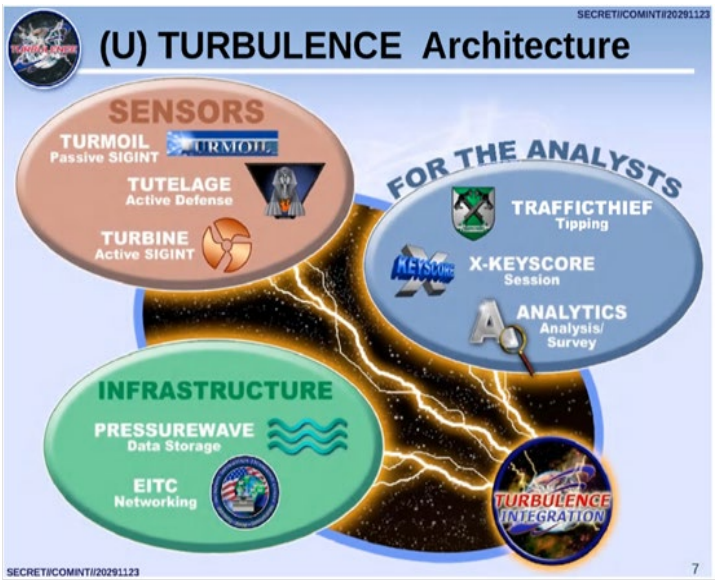


图 3-3 “湍流”架构

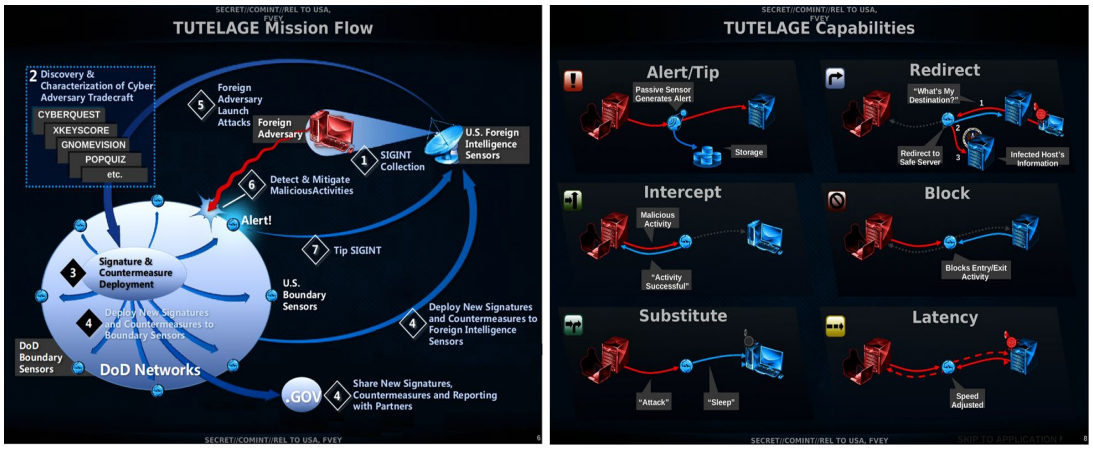


图 3-4 “监护”系统任务流程

2022 年，**中国网络安全厂商 360** 发布报告，披露 NSA 长达十余年对全球发起的无差别攻击，尤其对“量子”攻击系统、“酸狐狸”（FOXACID）零日漏洞攻击平台、“验证器”（VALIDATOR）和“联合耙”（UNITEDRAKE）后门进行分析，分析表明全球受害单位感染量或达百万级（见图 3-5）[7]。

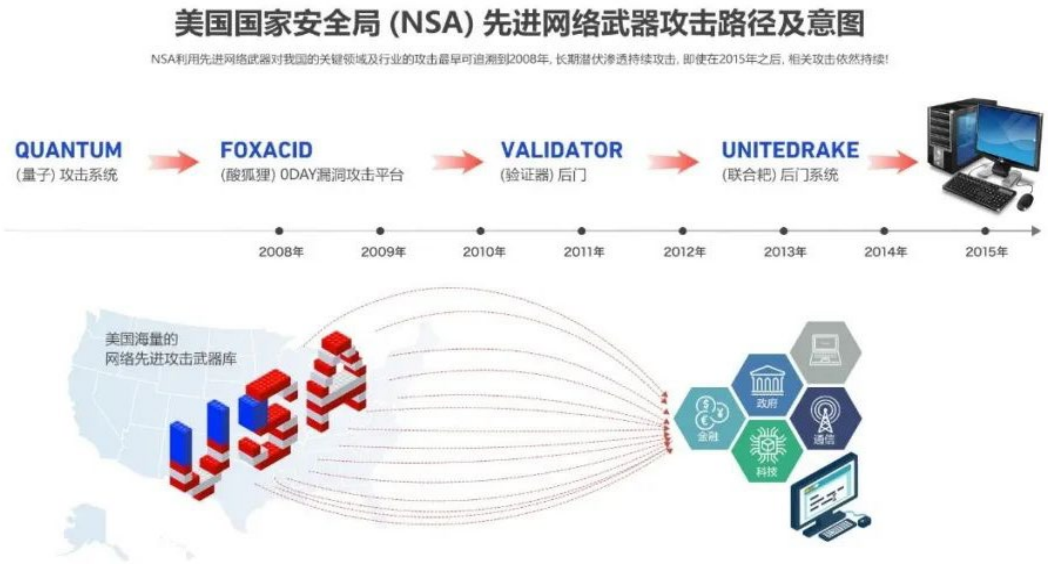


图 3-5 NSA 网络攻击武器路径及示意图

针对“量子”攻击系统，360 安全团队从攻击技术、攻击模块、应用场景和攻击实施过程进行了详细的技术分析（见图 3-6）[8]，结合发现的真实案例，全面印证 NSA 针对全球互联网用户实施大规模无差别网络攻击的详细情况。

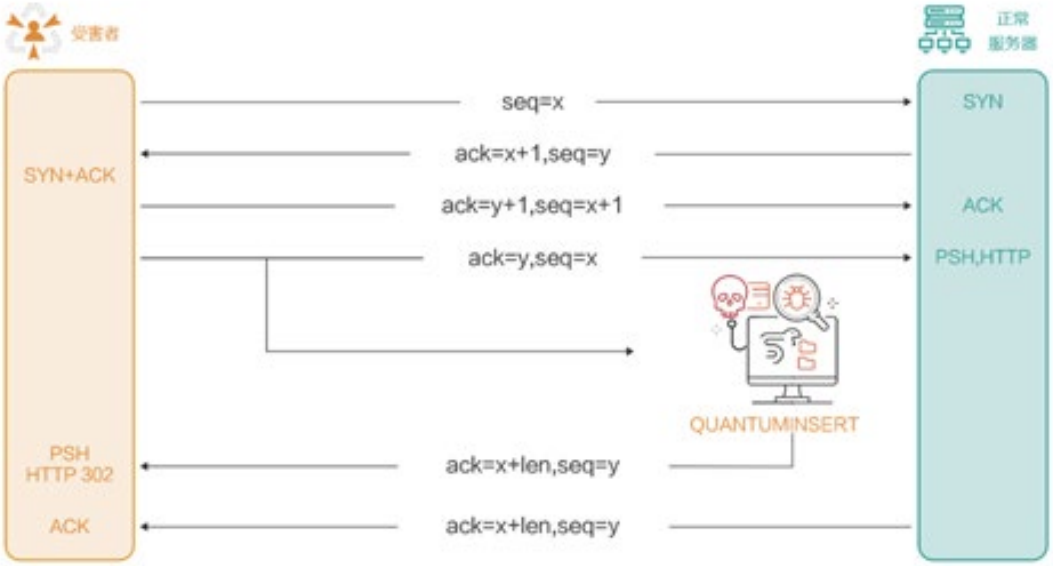


图 3-6 量子注入攻击过程

（三） 小结

通过斯诺登泄露文件，全球网络安全厂商逐步认识到了美国网络空间开展行动的能力体系。研究表明，基于复杂的组织体系、庞大的人员规模和充足的安全预算，通过一系列大型工程系统的建设，美国建立了支撑网络空间行动的完整工程体系，并以此为依托，将情报获取、积极防御、主动进攻及相关支撑环节等网络空间能力整合成整体的国家能力。

与此同时，美国具有国家安全至上的传统，随着国力发展，逐渐将全球无死角的监听与情报窃听能力视为其全球利益和霸权的基石，并利用获取的各类网络情报，形成网络空间行动的“先天优势”。特别是对于海底光缆和运营商的窃听，使美国在信号获取和情报收集方面具备了无与伦比的隐蔽性掩护和反溯源性优势。强大的作业体系化能力加之霸权化的隐蔽性和反溯源优势塑造了美国“大到无形”的网络空间威胁。

随着斯诺登泄露文件的公开，网络安全界的视角逐步从战术、技术、程序上升到战略层面，网络空间超级机器的全貌逐渐显露出来。

参考资料

[1] The Guardian. NSA collecting phone records of millions of Verizon customers daily. 2013.

https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[2] The Guardian. Attacking Tor: how the NSA targets users' online anonymity. 2013. https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

[3] The Register. NSA: Inside the FIVE-EYED VAMPIRE SQUID of the INTERNET. 2014. https://www.theregister.com/2014/06/05/how_the_interenet_was_broken/

[4] 明镜周刊. 斯诺登泄露 NSA 文档. 2013. https://www.spiegel.de/fotostrecke/qfire-die-vorwaertsverteidigng-der-nsa-fotostrecke-105358.html

[5] 肖新光. 斯诺登效应的前因解读. 中国计算机学会通讯. 2013（7）. https://www.antiy.cn/doc/market/201307.pdf

[6] 安天. “美国网络空间攻击与主动防御能力解析”系列文章 12 篇. 网信军民融合. 2017(12)-2018(11). https://mp.weixin.qq.com/s/PnaYXZ9snK6fv_lgCFszDw

[7] 360. 网络战序幕：美国国安局 NSA（APT-C-40）对全球发起长达十余年无差别攻击. 2022. https://mp.weixin.qq.com/s/jHjzky8xIaEuocHzbWjFSA

[8] 360. Quantum（量子）攻击系统–美国国家安全局“APT-C-40”黑客组织高端网络攻击武器技术分析报告（一）. 2022. https://mp.weixin.qq.com/s/lzf16Fchfv1fMG3IExq7XA

第四篇　后门的传言——对美国污染加密通讯标准的揭露

对于美国是否在基础 IT 产品中预埋后门，网络安全界一直存在广泛的质疑和猜测。1999 年 8 月，加拿大 Cryptonym 公司首席科学家安德鲁·费尔南德斯（Andrew Fernandes）发现 Windows 系统 CryptoAPI（加密接口）存在的一个名为“_NSAKey”的密钥，让人顿时联想到了简称为 NSA 的美国国家安全局。尽管微软对此进行解释，但其说法无法让网络安全界信服。全球网络安全界开始了寻找美国预留后门的努力。

2013 年 9 月初，美国和英国多家媒体报道了 NSA 在美国国家标准与技术研究院（NIST）发布的 SP 800-90A 标准中暗藏后门一事，证实了此前忧虑和怀疑已久的业界传闻。此后，在网络安全产业和学术界的持续努力下，这一怀疑逐渐得到证明，并且随着对斯诺登泄露文档的深入挖掘，还曝光了 NSA 对密码体系长期系统性的操控，以及利用加密标准漏洞对全球的监控，其行为破坏了全球对网络技术的信任，也对全球国际关系生态环境造成极大影响。

（一）事件回顾

2013 年 9 月初，美国《纽约时报》和非盈利在线新闻网站 Propublica，以及英国“卫报”分别报道了斯诺登泄露文件中有关 NSA 对加密技术的长期破坏活动，直接证实了安全

领域自 2007 年以来的一个猜测：美国 NIST 2006 年正式发布的特别出版物 SP 800-90（2012 年后改称为 SP 800-90A）“使用确定性随机位发生器的随机数产生算法推荐”中，推荐的 4 种“确定性随机位发生器”（DRBG）算法之一双椭圆曲线算法 Dual_EC_DRBG 确实存在后门；而令全球震惊和不安的是，这个计算效率低下（与其他三个相比）又带有漏洞的算法之所以能够成为标准，完全是 NSA 为达成监听全球的野心而精心安排的结果。

密码加密体系是基于一次一密的机制所设计，其中高质量随机数产生机制是现代加密技术的根基。如果随机数的产生机制被做了手脚，那么整个密码协议都极容易被攻破。

（二）来自学术界的质疑

2007 年，在国际密码学年会（Crypto 2007）上，**来自微软的密码学家 Niels Ferguson 和 Dan Shumow 从技术角度分析了 Dual_EC_DRBG 被植入后门的可能性**，其论证逻辑是：用于定义密码算法椭圆曲线的若干常数缺乏详细来源解释。如果这些常数经过特殊选择，且算法设计者掌握选择的相关细节和数据，则只需获得该算法生成随机序列的前 32 个字节，就可推断未来所有生成的“随机”序列（见图 4-1）[2]。

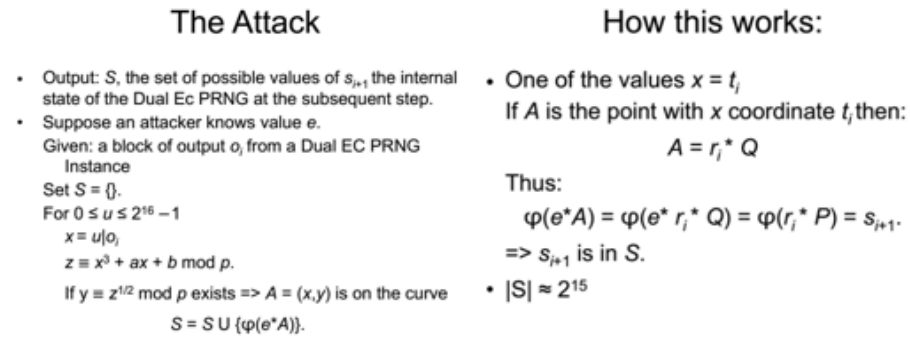


图 4-1 Dual_EC_DRBG 漏洞利用原理

但密码学家无法证明，算法设计者是否出于某些目的而保存了相关数据，因此对这一算法的讨论仅限于“漏洞”层面，直到 2013 年《纽约时报》等将这一猜测坐实。

（三） 证实

2013 年 9 月 6 日，美国**《纽约时报》**在 “NSA 能够骗过网上基本隐私保护”一文中报道[3]：“密码学家长久以来怀疑，NSA 在 2006 年 NIST 采纳的一个标准中植入了漏洞，该标准后来被已有 163 个成员国的国际标准化组织采纳。机密的 NSA 备忘录证实，两位微软密码学家 2007 年披露的致命弱点是由 NSA 设计的。NSA 编写了这一标准，并努力将其塞进国际组织，私下里称此为 ‘一个策略上的挑战’。”而这一活动只是“信号情报赋能计划”（SIGINT Enabling Project）的一部分，该计划每年获得 2.5-3 亿美元拨款，以便“积极参与美国和外国 IT 业界，隐蔽地影响和/或公开地利用商业产品的设计。”该机构 2013 年预算请求中的一个目标是“影响商业公钥技术的政策、标准和规范”（见图 4-2、4-3）[4]。

TOP SECRET//SI/TK//NOFORN

(U) COMPUTER NETWORK OPERATIONS
(U) SIGINT ENABLING

This Exhibit is SECRET//NOFORN									
	FY 2011[1] Actual	FY 2012 Enacted			FY 2013 Request			FY 2012 — FY 2013	
		Base	OCO	Total	Base	OCO	Total	Change	% Change
Funding ($M)	298.6	275.4	—	275.4	254.9	—	254.9	-20.4	-7
Civilian FTE	144	143	—	143	141	—	141	-2	-1
Civilian Positions	144	143	—	143	141	—	141	-2	-1
Military Positions	—	—	—	—	—	—	—	—	—
[1]Includes enacted OCO funding.							Totals may not add due to rounding.		

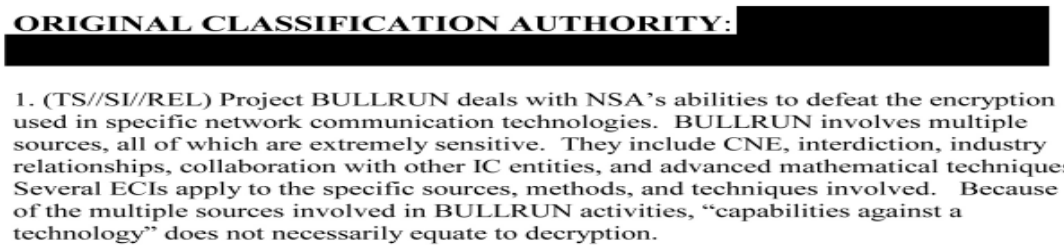
图 4-2 NSA“信号情报赋能计划”预算

(U) Project Description

(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this way, the SIGINT Enabling approach uses commercial technology and insight to manage the increasing cost and technical challenges of discovering and successfully exploiting systems of interest within the ever-more integrated and security-focused global communications environment.

图 4-3 NSA“信号情报赋能计划”计划描述

2013 年 9 月 5 日，**英国“卫报”**刊文“美英间谍机构如何打败互联网隐私和安全”[5]，报道了来自斯诺登泄密文档中有关 NSA 用来破解互联网加密技术的“奔牛”计划（BULLRUN）(见图 4-4)[4]，称“NSA 破解特定网络通信技术中加密功能的能力，涉及多个非常敏感的来源。”NSA 能够破解广泛使用的在线协议，包括 HTTPS，IP 语音和安全套接层（SSL）等。泄密文档还显示，NSA 的商业解决方案中心“利用与特定行业合作伙伴的敏感、合作关系”，在安全产品中植入漏洞。


ORIGINAL CLASSIFICATION AUTHORITY: [redacted]

1. (TS//SI//REL) Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple sources, all of which are extremely sensitive. They include CNE, interdiction, industry relationships, collaboration with other IC entities, and advanced mathematical techniques. Several ECIs apply to the specific sources, methods, and techniques involved. Because of the multiple sources involved in BULLRUN activities, "capabilities against a technology" does not necessarily equate to decryption.

图 4-4 NSA“奔牛”计划描述

这些报道立刻引起全球安全领域的高度关注，对 NSA 操控密码及全球安全的行为展开各种研究和调查。2013 年 12 月 27 日，原“洋葱路由器”（Tor）项目核心程序员雅各·阿贝尔鲍姆（Jacob Appelbaum）在第 30 届混沌通信大会（30C3）上展示了一组泄露的 PPT 文档，其中包含 NSA 针对各种网络产品的可利用漏洞开发的程序与木马。产品覆盖服务器、路由器、防火墙和手机设备，囊括了从 DELL、HP、Juniper、CISCO 等通用品牌。阿贝尔鲍姆表示，他怀疑 NSA 与其中一些企业存在合作关系，披露这些内容的初衷是让相关企业在曝光的压力下，自己澄清是 NSA 的同谋还是受害者。

2013 年 9 月，美国密码学家马修·格林（Matthew Green）发表博文“对密码工程的几点思考”，指出“NSA 每年花费 2.5 亿美元，做了下面这样的事情[6]：

1. 篡改国家标准（特别是 NIST 标准）以削弱密码系统；

2. 对标准委员会施加影响，弱化协议；

3. 同软硬件开发商合作，弱化加密算法和随机数生成算法的强度；

4. 攻击下一代 4G 手机使用的加密系统；

……

所有这些程序都有不同的代号，但是 NSA 的解密程序都以 ‘BULLRUN’ 命名。”

马修·格林进一步概括了破解一套加密系统的三个途径：攻击加密算法、攻击加密算法的具体环境或者植入后门、直接入侵目标，并意味深长地指出，如果那些标准是可信的，那么更多的“破解”方法将是后两者。

2013 年 12 月 31 日，比利时自由安全顾问阿里斯（Aris）发布博文“Dual_EC_DRBG 后门：一个观点证明”[7]，结合斯诺登事件的背景，给出了明确的结论，“NSA 故意设置了这个漏洞，且方法非常巧妙，能够将整个内部状态以 32 个字节进行输出。它需要 32 个字节的输入作为种子，也让人印象深刻。NIST 的批准显然是完全疯狂的”。这是自 2006 年丹·舒穆（Dan Shumow）和尼奥斯·弗格森（Niels Ferguson）提出怀疑后，研究界对 NIST SP 800-90A 正式结论性的回应。该博文迅速被 ZDNet、Slashdot 等多个知名信息新闻网站转载和传播。

2014 年，美国**约翰·霍普金斯大学的斯蒂芬·查克威（Stephen Checkoway）等研究人员**从技术上实现了微软密码学家此前推测的漏洞利用[8]。他们对使用 Dual_EC_DRBG 的若干 TLS（安全传输层协议，用于在两个通信应用程序之间提供保密性和数据完整性）实现进行攻击和分析，包括

OpenSSL-FIPS、Windows SChannel（安全 TLS 通信子系统）以及 RSA BSafe 加密库，并将结果和分析发表在 USENIX 安全年会上（见图 4-5）[8]。其研究表明，利用单 CPU 或计算集群，花费数秒或数十秒，就可以获得通信密钥，论证了该标准的破坏性：由于漏洞的存在，各种使用 Dual_EC_DRBG 实现的 TLS 会话都是不安全的。

Attack	Intel Xeon Reference System			16-CPU AMD Cluster
	2^{22} Candidates (s)	Expected Runtime (min)	Expected Cost	Total Runtime (min)
BSAFE-C v1.1	–	0.26	16	0.04*
BSAFE-Java v1.1	75.08*	641	38,500	63.96*
SChannel I	72.58*	619	37,100	62.97*
SChannel II	62.79*	1,760	106,000	182.64*
OpenSSL-fixed I	–	0.04	3	0.02*
OpenSSL-fixed II	–	707	44,200	83.32*
OpenSSL-fixed III	–	$2^k \cdot 707$	$2^k \cdot 44{,}200$	$2^k \cdot 83.32$

图 4-5 查克威等利用 Dual_EC_DRBG 漏洞对不同 TLS 实现进行攻击的结果

斯蒂芬·查克威等人的研究，令人不安地联想起 2013 年 12 月 21 日**路透社**名为“连接 NSA 与安全产业先锋的秘密合同”的报道[9]，其中指出，NSA 通过高达 1000 万美元的协议，使加密技术公司 RSA 将 Dual_EC_DRBG 作为 BSafe 首选随机数据生成算法，辅助相关机构开展大规模监控。

（四） 余震延绵

正如英国**“卫报”**2013 年的报道所言：“NSA 的做法已经动摇了整个互联网的信任基础”。学术界和产业界对互联网通信安全的怀疑并没有随着时间而消减，而 NSA 果然“不负众望”，一再展示其对各类通信标准和应用的操控能力。

2015 年 5 月，美国**“连线”**（Wired）杂志发表“新的加密漏洞影响了成千上万的网站”一文[10]，称安全研究人员新发现一个自上世纪 90 年代已存在的关键漏洞“Logjam”，允许攻击者拦截解密全球用户和成千上万的网站/邮件服务器之间的安全通信。“仔细阅读泄露的 NSA 文件后，我们发现 NSA 对 VPN 的攻击与该漏洞一致”，研究人员在博客中写道。

2015 年，**荷兰埃因霍芬理工大学的丹尼尔·伯恩斯坦（Daniel Bernstein）等人**在欧洲委员会 ICT 计划、荷兰科学研究组织等多个资金资助下，对 NSA 系统化操控密码标准的体系方法进行了深度研究，并发表论文“Dual EC：一个标准化的后门”[11]。该论文梳理了携带后门的 Dual EC 算法进入 NIST 标准的过程，包括专业和学术意见是如何被系统性地忽略，阐述了这一后门在真实应用中的工作原理和破坏作用，并分析了美国标准化和专利生态系统是如何掩盖这一后门的。文章指出，**真正令人震惊的是 NSA 有组织地削弱加密标准的体系化方法，携带后门的 Dual EC 算法成为标准，仅仅是 NSA 系统化活动的冰山一角。**这一结论很快就被 Crypto AG 事件所证实。

2020 年 2 月 11 日，美国《华盛顿邮报》、德国电视二台（ZDF）和瑞士德语广播电视（SRF）发布联合调查报道，曝光总部位于瑞士的 Crypto AG 公司是如何被美、德两国情

报机构操控的。Crypto AG 依靠二战时期为美军生产密码编制设备起家。20 世纪 60 年代中期，CIA 和 NSA 抓住 Crypto AG 技术更新换代的契机，说服公司生产销售由 NSA 完全设计的全电子新型加密机。Crypto 公司在 1967 年推出了新一代电子加密机，其内部工作原理完全由 NSA 设计。自 20 世纪 70 年代以来，CIA 与德国联邦情报局（BND）共同持有 Crypto AG 的股权，暗中控制其销往超过 120 个国家的通讯加密设备的安全等级，通过拦截并解码加密程序以窃取各国政府及企业用户的加密通讯内容。

情报专家称，在 20 世纪 80 年代，美国情报官员处理的大约 40%的外国通信来自 Crypto AG 的密码系统。实际证明，在许多重大历史事件中，都有 Crypto AG 的身影（例如，英阿马岛之战中，CIA 使用 Crypto AG 获取阿根廷军队情报并提供给英国）。1993 年，在 BND 退出与美国在 Crypto AG 的合作伙伴关系后，美国收购了德方全部股份并继续把持 Crypto 公司。直到 2018 年左右，CIA 一直是 Crypto AG 公司的所有者。这一事件的曝光显示出美国情报获取的能力，也暴露出西方科技公司与美国情报机构之间存在千丝万缕的关系。

（五）小结

加密算法是现代网络安全技术的基石之一，合理的使用加密算法可以保证网络间通信的安全性。能够破解包括 VPN

和 HTTPS 在内的绝大多数互联网隐私保护和加密技术，表明大多数经过加密的个人和商业网络通讯数据、在线交易信息，对 NSA 来说都唾手可得。斯诺登泄露的 NSA 对各国的窃听、窃密活动，也引发全球对美国在政治、经济、外交等方面两面手法的重新认识和思考。

美国将全球无死角的信息情报获取能力视为支撑其全球利益的基础，在追求全球监听、全球控制的路上越走越远，既破坏了国家间的外交信任，也对自己造成难以弥补的“反噬”：2013 年 9 月 10 日，面对加密标准 SP 800-90A 的种种质疑，NIST 终于发表了声明：“我们想向 IT 网络安全界保证，严格审查标准的透明、公开的过程依旧存在。NIST 不会刻意削弱一项加密标准。我们将继续执行使命，与加密团体合作，为美国政府和大型工业创立最强大的加密标准。”NIST 同时重新开启了相关标准的审查期。2015 年，NIST 发布 SP 800-90A 修订版，去掉了其中的 Dual_EC_DRBG，然而产业和学术界对 NIST 的信任已经难以恢复，在 2015 年以来对多个加密标准及其实现进行了回溯和分析。而报道中涉及的硬件厂商也深受大众怀疑，每当阿贝尔鲍姆曝光文档中提及的服务器和交换机等产品被发现漏洞或缺陷时，人们往往首先想到的是被刻意植入了后门，而不是在开发中出现了弱点或缺陷。

参考资料

[1] Wired. MS Denies Windows “Spy Key”. 1999.
https://www.wired.com/1999/09/ms-denies-windows-spy-key/

[2] Microsoft. On the Possibility of a Back Door in the NIST SP 800-90 Dual Ec Prng. 2007.
http://rump2007.cr.yp.to/15-shumow.pdf

[3] The New York Times. NSA Able to Foil Basic Safeguards of Privacy on Web. 2013.
https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

[4] University of Auckland. CryptoWon't Save You Either. 2014.
https://www.cs.auckland.ac.nz/~pgut001/pubs/crypto_wont_help.pdf

[5] The Guardian. Revealed: how US and UK spy agencies defeat internet privacy and security. 2013.
https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[6] Matthew Green. A Few Thoughts on Cryptographic Engineering. 2013.
http://blog.cryptographyengineering.com/2013/09/on-nsa.html

[7] Aris. Dual_EC_DRBG Backdoor: a Proof of Concept. 2013.
https://blog.0xbadc0de.be/archives/155

[8] Johns Hopkins University. On the Practical Exploitability of Dual EC in TLS Implementations. 2014.
https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-checkoway.pdf

[9] Reuters. Secret contract tied NSA and security industry pioneer. 2013.
https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220

[10] Wired. New Critical Encryption Bug Affects Thousands of Sites. 2015.
https://www.wired.com/2015/05/new-critical-encryption-bug-affects-thousands-sites/

[11] Eindhoven University of Technology. Dual EC： A Standardized Backdoor. 2015.
https://pure.tue.nl/ws/files/3854147/588733604251427.pdf

第五篇　固件木马的实证——“方程式组织”正式浮出水面

固件是写入硬件的软件，其比操作系统更底层，甚至先于操作系统加载。如果把病毒写入固件中，就更隐蔽和难以发现。

2015 年 2 月 18 日，美国媒体“拦截者”（The Intercept）发布“研究人员发现了与 NSA 间谍活动有关的‘惊人的’恶意软件”文章[1]，披露了卡巴斯基的研究成果，证实了美国利用硬盘固件完成“持久化”的攻击活动，引发网络安全界震动。随着卡巴斯基系列报告从样本实证逐步曝光“方程式组织”，NSA 的底层“持久化”能力也越来越清晰地呈现出来。

（一）事件回顾

早在 2014 年 1 月，专注研究 BIOS 安全的网络安全专家达尔马万·萨利亨（Darmawan Salihun）开始在 InfoSec 研究所（InfoSec Institute）网站发表系列文章，分析曝光 NSA 的 BIOS 后门 DEITYBOUNCE、GODSURGE 等，并将这些恶意软件称为“上帝模式”[2]。

2015 年 2 月至 3 月期间，卡巴斯基发布系列报告[3-8]，揭露名为“方程式组织”（Equation Group）的 APT 组织，称其已活跃了近 20 年，是“震网”和“火焰”病毒的幕后操纵者，在攻击复杂性和攻击技巧方面超越了历史上所有的网

络攻击组织。在伊朗、俄罗斯、叙利亚、中国、英国、美国等全球超过 30 个国家感染了数千个，甚至上万个受害者。基于“方程式组织”所使用的恶意程序有自我毁灭机制，卡巴斯基推断受害者实际数目可能更多。

（二） 研究分析曝光经过

2015 年 2 月，**卡巴斯基**全球首次披露了“方程式组织”针对全球的网络间谍活动，称其为见过的最高级的威胁执行者。卡巴斯基先后发布多篇详细报告[3-8]，分析了“方程式组织”的诸多相关组件如：DoubleFantasy、EquationLaser、Fanny、EquationDrug、GrayFish、TripleFantasy，尤其提到了硬盘固件重写插件、EquationDrug、GrayFish 攻击平台，详解了各组件之间的协作关系（见图 5-1）[3]，并证明了“方程式组织”与“震网”之间的联系，指出 Fanny 使用的两个零日漏洞在 2009 年 6 月和 2010 年 3 月被“震网”使用。

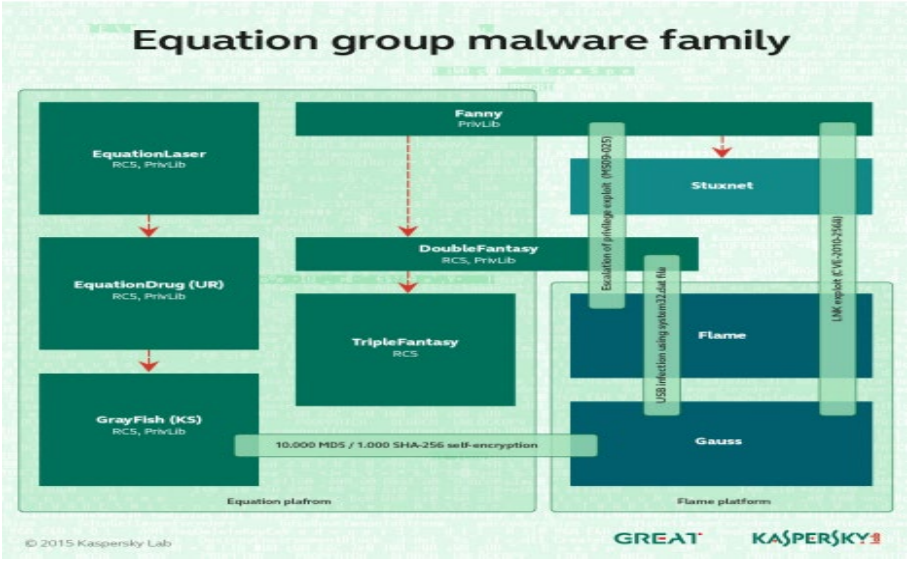


图 5-1 “方程式组织”相关组件

2016 年，卡巴斯基根据 RC 算法的常量值，验证了黑客组织“影子经纪人”（Shadow Brokers）泄露的 NSA 数据属于“方程式组织”[9]。

卡巴斯基指出，“方程式组织”在高价值目标中针对硬盘固件实现攻击持久化的植入。通过样本研究发现，数千个受害者中仅仅发现了数个被硬盘固件重编程模块感染的案例（见图 5-2）[3]，硬盘持久化率只有千分之二左右，由此可见“方程式组织”的固件木马是极具针对性和保密性的战术网络武器。

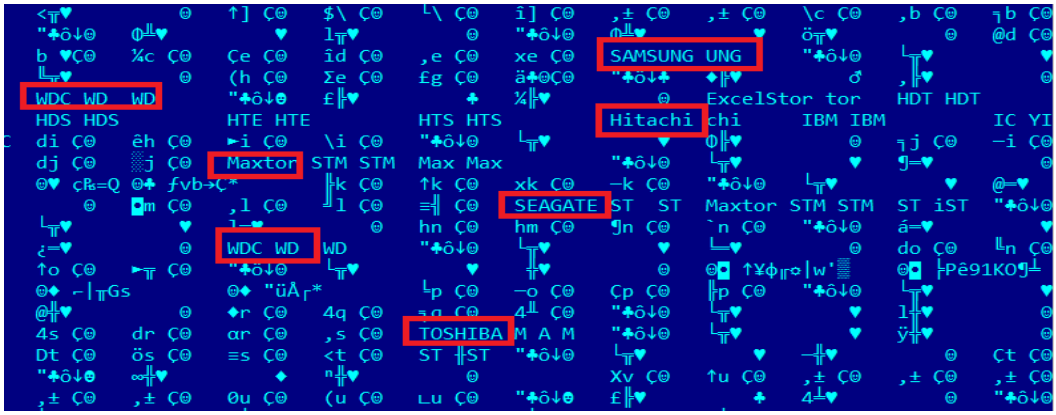


图 5-2 硬盘重编程插件感染能力

卡巴斯基披露“方程式组织”后，**安天**于 2015 年 3 月 5 日和 4 月 19 日分别公布了两篇“方程式组织”储备分析报告[10][11]。在“修改硬盘固件的木马——探索方程式（EQUATION）组织的攻击组件”报告中，分析了“方程式组织”主要攻击平台的组成结构、关联关系、回传信息、指令分支、C2 地址、插件功能，并解析了关键插件“硬盘重编程”模块的攻击技术原理（见图 5-3）[10]。

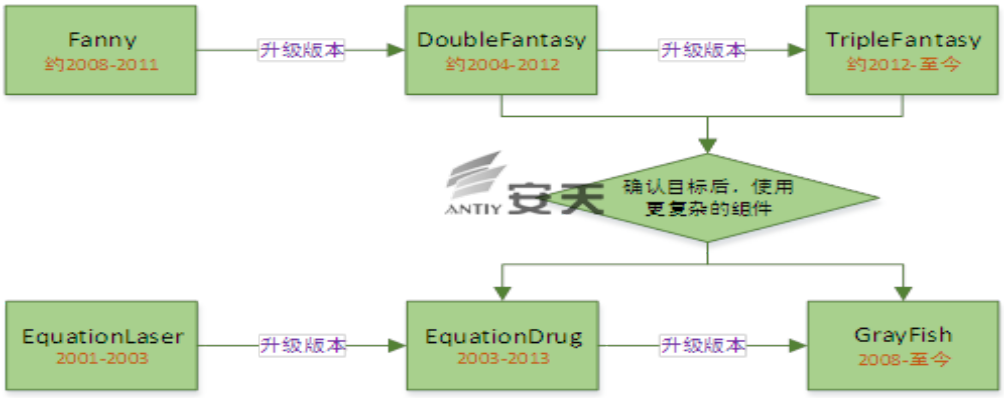


图 5-3 “方程式组织”各组件关系示意图

在“方程式(EQUATION)部分组件中的加密技巧分析”报告中，安天介绍了对该组织多个组件的本地配置和网络通讯加密算法和密钥的破解分析成果，并公布了密钥和密钥结构供业界研究参考（见图 5-4）[11]。

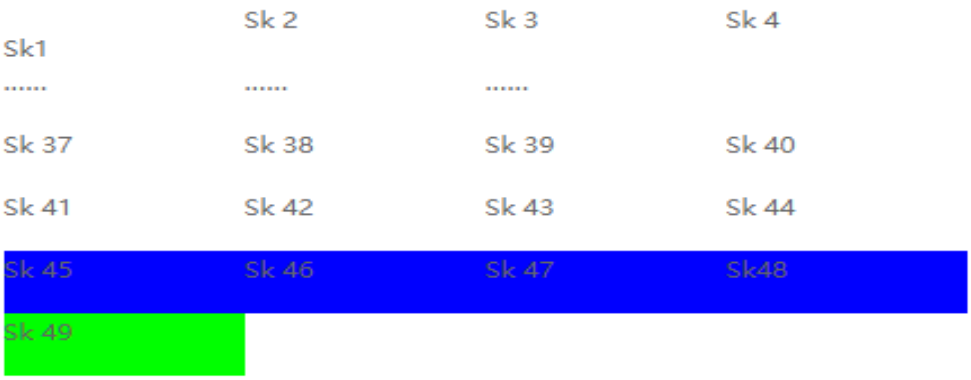


图 5-4 “方程式组织”加密算法密钥结构图

2022 年 2 月 23 日，**中国网络安全厂商**奇安信发布报告，披露美国 NSA “方程式组织”的顶级后门 Bvp47，并通过“影子经纪人”与斯诺登泄露的数据验证了 Bvp47 是属于“方程式组织”的黑客工具（见图 5-5）[12]。

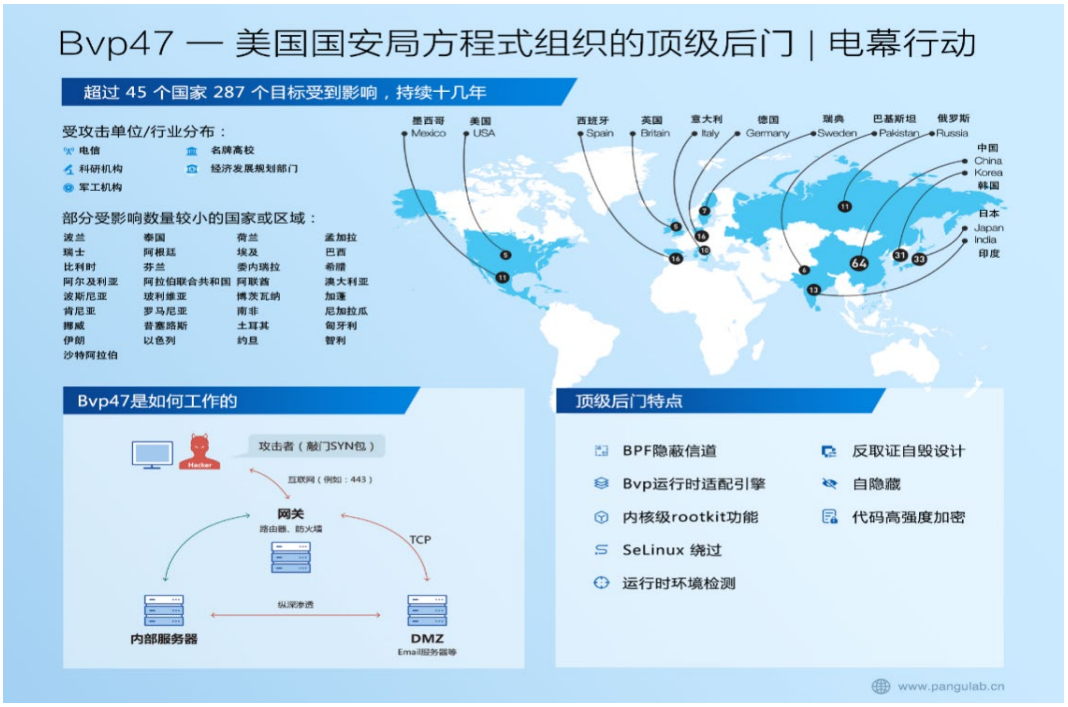


图 5-5 NSA“方程式组织”顶级后门 Bvp47

经过全面深入的技术模拟分析，奇安信还原了 Dewdrops、“饮茶”（Suctionchar_Agent）嗅探木马与 Bvp47 后门程序等其他组件配合实施联合攻击的场景（见图 5-6）[13]。

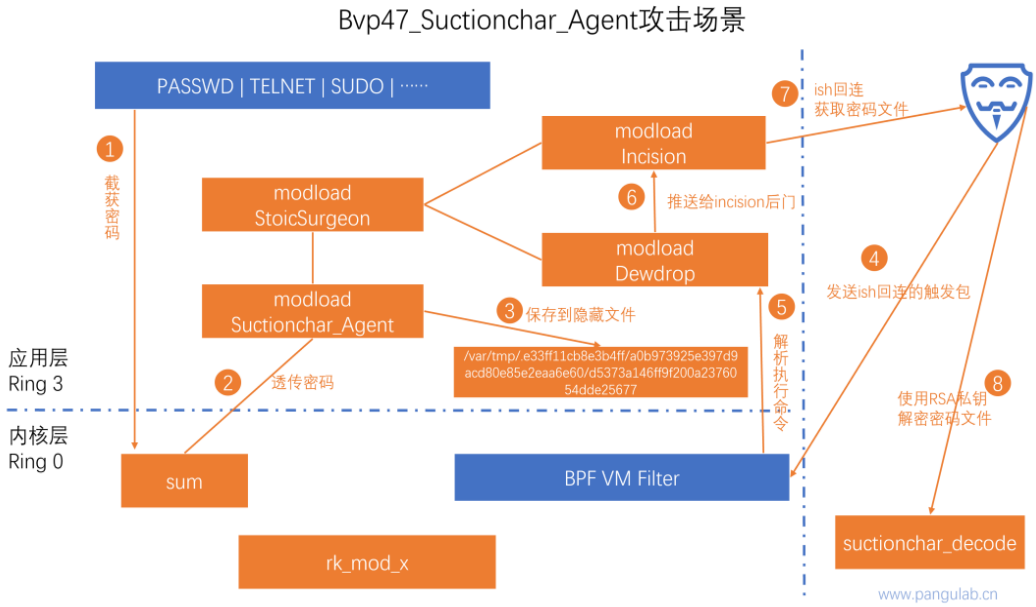


图 5-6 “饮茶”攻击场景

（三） 小结

APT（高级持续性威胁）的特点是更长的时间维系，更大的空间跨度，更广的资源调度能力，致使安全研究者更难接近其本质。以“方程式组织”为代表的美国顶级 APT 组织有一套完整、严密的作业框架与方法体系，拥有大规模支撑工程体系、制式化装备组合，能够进行严密的组织作业，高度追求作业过程的隐蔽性、反溯源性，使其攻击看似“弹道无痕”，其突破、存在、影响、持续直至安全撤出网络环境或系统的轨迹很难被察觉，导致防护者对其网络空间行动中实际的攻击战术、技术、程序以及相应轨迹知之甚少，无法在整个威胁框架视角进行全面的信息掌握和解读。

参考资料

[1] The Intercept. Researchers Find 'Astonishing' Malware Linked to NSA Spying. 2015. https://theintercept.com/2015/02/17/nsa-kaspersky-equation-group-malware/

[2] InfoSec Institute. NSA BIOS Backdoor a.k.a. God Mode Malware Part 1: DEITYBOUNCE. 2014. https://cysinfo.com/wp-content/uploads/2017/04/Shadow_release_updated.pdf

[3] Kaspersky. Equation Group: Questions and Answers. 2015. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf

[4] Kaspersky. Equation: The Death Star of Malware Galaxy. 2015. https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/

[5] Kaspersky. Equation Group: The Crown Creator of Cyber-Espionage. 2015.

https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage

[6] Kaspersky. A Fanny Equation: “I am your father, Stuxnet”. 2015. https://securelist.com/a-fanny-equation-i-am-your-father-stuxnet/68787/

[7] Kaspersky. Equation Group: from Houston with love. 2015. https://securelist.com/equation-group-from-houston-with-love/68877/

[8] Kaspersky. Inside the EquationDrug Espionage Platform. 2015. https://securelist.com/inside-the-equationdrug-espionage-platform/69203/

[9] Kaspersky. The Equation giveaway. 2016. http://securelist.com/the-equation-giveaway/75812/

[10]安天. 修改硬盘固件的木马 探索方程式(EQUATION)组织的攻击组件. 2015. https://www.antiy.com/response/EQUATION_ANTIY_REPORT.html

[11]安天. 方程式（EQUATION）部分组件中的加密技巧分析. 2015. https://www.antiy.com/response/Equation_part_of_the_component_analysis_of_cryptographic_techniques.html

[12]奇安信. Bvp47-美国 NSA 方程式组织的顶级后门. 2022. https://www.pangulab.cn/post/the_bvp47_a_top-tier_backdoor_of_us_nsa_equation_group/

[13]奇安信. “电幕行动”（Bvp47）技术细节报告（二）——关键组件深度揭秘. 2022. https://mp.weixin.qq.com/s/YN8AJOrQWcpleV0tqhRGQQ

第六篇　覆盖全平台的网络攻击——“方程式组织” Solaris 和 Linux 样本的曝光

2015 年初卡巴斯基通过样本实证，披露了美国情报机构 NSA “方程式组织” 的网络攻击行动，并猜测 “方程式组织” 可能具有攻击所有主流操作系统平台的能力。之后经过接力式的曝光，NSA 针对各种系统平台编写的病毒样本陆续被暴露在阳光之下。

（一） 事件回顾

2015 年卡巴斯基披露 NSA “方程式组织”，发布了系列分析报告，其中提到收集到的 “方程式组织” 恶意代码样本都是针对 Windows 系统的，但是有迹象表明非 Windows 恶意代码确实存在。

在 “影子经纪人” 2016 年 8 月所外泄的 “方程式组织” 针对多种防火墙和网络设备的攻击代码中[1]，公众第一次把 “方程式组织” 和名为 “ANT” 的攻击装备体系联系起来，并以此看到其针对 Cisco、Juniper、Fortinet 等防火墙产品实现注入和持久化的能力。2016 年 10 月 31 日，“黑客新闻”（The Hacker News）发布文章披露了 “影子经纪人” 公开的更多文件[2]，其中包括部分 “方程式组织” 入侵的其他国家服务器列表，文件显示，大部分被感染的服务器运行的是 Solaris 等版本的操作系统，有些运行的是 FreeBSD 或 Linux 系统。

（二）研究分析曝光经过

2015 年 2 月，**卡巴斯基**在一份关于“方程式组织”的问答中提到[3]，“方程式组织”可能具有多平台攻击能力。尽管收集到的样本都是针对 Windows 系统的，但是有迹象表明“方程式组织”使用的非 Windows 恶意代码确实存在。有实例证明，“方程式组织”恶意软件 DOUBLEFANTASY 存在 Mac OS X 版本。

2016 年 11 月 3 日，**安天**发布报告“从‘方程式’到‘方程组’——EQUATION 攻击组织的全平台载荷能力解析”[4]，分析了“方程式组织”针对多种架构和系统的攻击样本（见图 6-1），是全球首个通过真实样本曝光“方程式组织”针对 Solaris（SPARC 架构）、Linux 系统攻击能力的报告，安天的报告揭开了 NSA 全平台攻击覆盖能力的面纱，并总结梳理各方曝光其全平台攻击能力的信息。

信息	Windows	Linux	Solaris	Oracle-owned Unix	FreeBSD	Mac OS
安天：修改硬盘固件的木马 探索方程式（EQUATION）组织的攻击组件	分析样本载荷和硬盘持久化能力					
安天：方程式（EQUATION）部分组件中的加密技巧分析	分析加密算法					
安天：EQUATION攻击组织的全平台载荷能力解析（本报告）		曝光存在，分析相关载荷	分析相关载荷			
The Hacker News：《Shadow Brokers reveals list of Servers Hacked by the NSA》			曝光存在	曝光存在	曝光存在	
卡巴斯基：Equation:The Death Star of Malware Galaxy[8]	揭秘方程式攻击组织					
卡巴斯基：A Fanny Equation: "I am your father, Stuxnet"[9]	Fanny组件分析					
卡巴斯基：Equation Group: from Houston with love[[10]	Doublefantasy 分析					
卡巴斯基：《EQUATION GROUP: QUESTIONS AND ANSWERS》[11]	方程式组织问与答					根据网络特征提出猜测

图 6-1“方程式组织”全平台攻击能力

2017 年 1 月 25 日，基于“影子经纪人”泄露的“方程式组织”样本分析，安天发布“方程式组织 EQUATION DRUG 平台解析”报告[5]，绘制了“方程式组织”作业模块积木图（见图 6-2），揭示美国通过精细化模块实现前后场控制、按需投递恶意代码的作业方式。

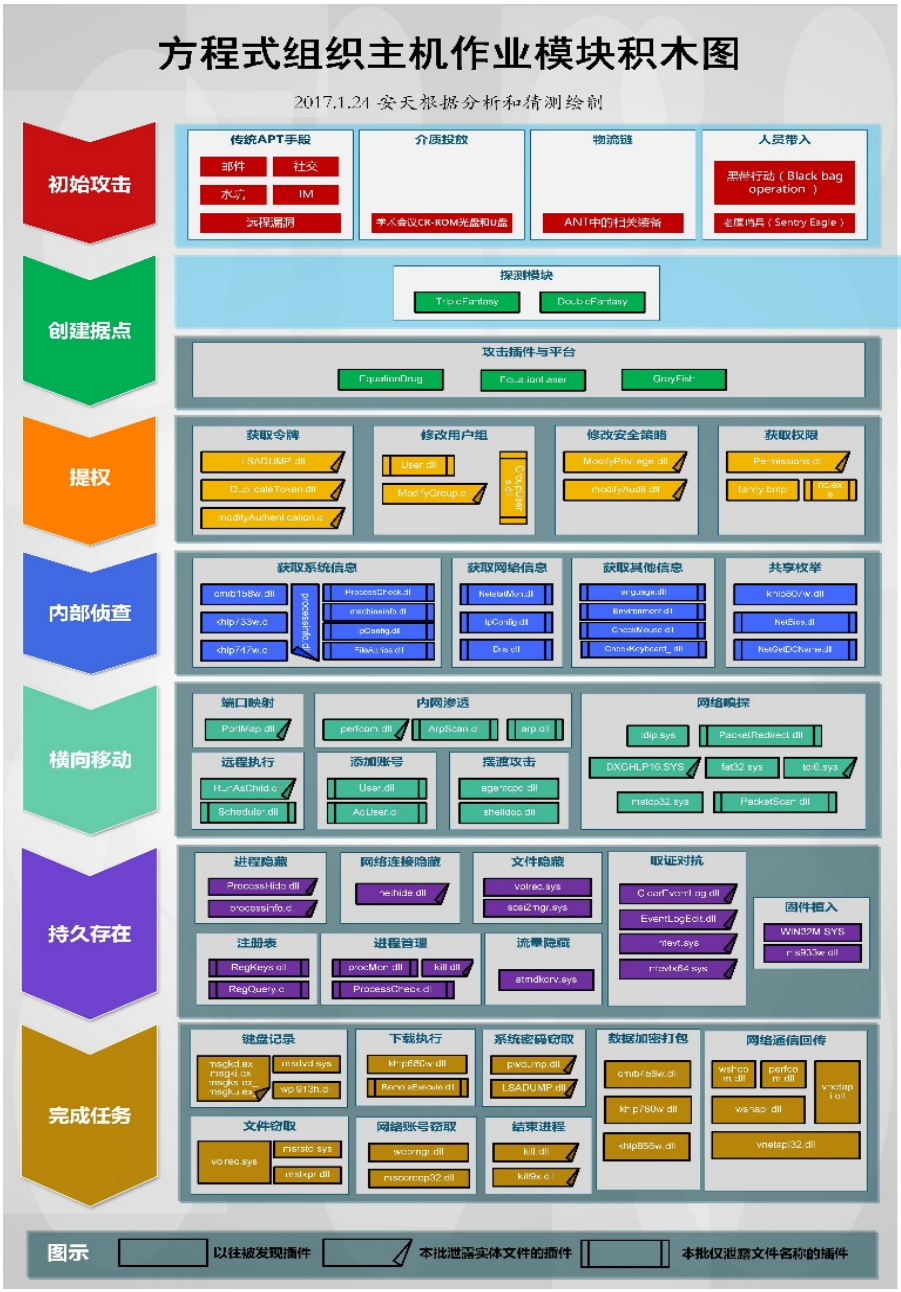


图 6-2 “方程式组织”主机作业模块积木图

可以看到，美国的作业模式往往先是由一个内存装载器（loader）搭载大量小型动态链接库（Dynamic Link Library, DLL）作为原子化攻击模块，通过加密信道传输至前场，由装载器进行加载，从而保证隐蔽性和可复用性。

（三） 小结

网络安全研究人员发现，超级攻击组织力图将其载荷能力扩展到一切可以达成入侵和持久化的场景。在这些场景中，各种服务器操作系统，如 Linux、Solaris、FreeBSD 等，更是其高度关注的目标。基于这样的研判，对于“方程式组织”这一超级 APT 攻击组织，网络安全厂商展开了细致深入的跟踪研究。“影子经纪人”的相关曝光文件印证了这一研判。安全厂商披露了“方程式组织”针对 Solaris 平台和 Linux 平台的部分样本分析，解析“方程式组织”覆盖全平台的攻击能力，对美国“大到无形”的网络空间作业能力的认识与了解更进了一步。

参考资料

[1] Cyber Security Review. Shadow Brokers reveals list of Servers Hacked by the NSA. 2016. https://www.cybersecurity-review.com/shadow-brokers-reveals-list-of-servers-hacked-by-the-nsa/

[2] Hacker News. Equation Group Cyber Weapons Auction. 2016. https://news.ycombinator.com/item?id=12290623

[3] Kaspersky. Equation Group: Questions and Answers. 2015. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf

[4] 安天. 从“方程式”到“方程组” EQUATION 攻击组织高级恶意代码的全平台能力解析. 2016. https://www.antiy.com/response/EQUATIONS/EQUATIONS.html

[5] 安天. 方程式组织 EQUATION DRUG 平台解析 —方程式组织系列分析报告之四. 2017. https://www.antiy.com/response/EQUATION_DRUG/EQUATION_DRUG.html

第七篇　泄露的军火——美国网络武器管理失控成为网络犯罪的工具

2017 年 4 月，“影子经纪人”事件分批曝光了 NSA 的网络武器装备，涉及大量系统级零日漏洞利用工具和先进的后门程序。美国未能实施有效管控，导致“军火级”网络攻击武器泄露，引发了全球用户的极大恐慌。在一个月后，WannaCry 勒索蠕虫仅利用美国 NSA 网络武器中的“永恒之蓝”（Eternalblue）漏洞，就制造了一场遍及全球的巨大网络灾难。

（一）　事件回顾

“永恒之蓝”漏洞被黑客利用实施勒索攻击：2017 年 5 月 12 日，黑客利用 NSA 泄露的“永恒之蓝”漏洞传播“蠕虫式”勒索软件 WannaCry，该蠕虫利用基于 445 端口的 SMB 漏洞 MS17-010 在全球范围感染了大量 Windows 系统计算机。受病毒侵害的电脑文件被加密，受害者向黑客支付赎金后才可获取密钥解锁恢复文件。WannaCry 勒索病毒造成了一场全球性互联网灾难，至少 150 个国家、30 万名用户中招，造成损失达 80 亿美元，影响到金融、能源、医疗等众多行业，造成严重的危机管理问题。微软在 2017 年 3 月份发布了该漏洞的补丁，“影子经纪人”在 2017 年 4 月 14 日公布的“方程式组织”使用的网络武器中包含了该漏洞的利用程

序，而黑客正是运用了这一网络武器，针对所有未及时打补丁的 Windows 系统电脑实施了此次全球性大规模攻击。

这是一起严重的因网络武器扩散导致的大规模网络安全事件[1]。超级大国无节制地发展网络军备，但又不严格履行保管义务，已经严重影响互联网的安全基础和信任。从此次事件也可以看出，高能力的网络武器一旦失控泄露，将快速转化为普遍性的攻击能力，从而引发雪崩式的社会风险。

（二） 各方反应

2017年4月16日，中国国家互联网应急中心（**CNCERT**）负责的中国国家信息安全漏洞共享平台（**CNVD**）发布“关于加强防范 Windows 操作系统和相关软件漏洞攻击风险的情况公告”[2]，对“影子经纪人”披露的多款涉及 Windows 操作系统 SMB 服务的漏洞攻击工具情况进行了通报（见表 7-1），并对有可能产生的大规模攻击进行了预警:

表 7-1 有可能通过 445 端口发起攻击的漏洞攻击工具

工具名称	**主要用途**
ETERNALROMANCE	SMB 和 NBT 漏洞，对应 MS17-010 漏洞，针对 139 和 445 端口发起攻击，影响范围:Windows XP、Windows 2003、Windows Vista、Windows 7、Windows 8、Windows 2008、Windows 2008 R2
EMERALDTHREAD	SMB 和 NETBIOS 漏洞，对应 MS10-061 漏洞，针对 139 和 445 端口，影响范围: Windows XP、Windows 2003

EDUCATEDSCHOLAR	SMB 服务漏洞，对应 MS09-050 漏洞，针对 445 端口
ERRATICGOPHER	SMBv1 服务漏洞，针对 445 端口，影响范围：Windows XP、 Windows server 2003，不影响 Windows Vista 及之后的操作系统
ETERNALBLUE	SMBv1、SMBv2 漏洞，对应 MS17-010，针对 445 端口，影响范围：较广，从 Windows XP 到 Windows 2012
ETERNALSYNERGY	SMBv3 漏洞，对应 MS17-010，针对 445 端口，影响范围：Windows8、Server2012
ETERNALCHAMPION	SMB v2 漏洞，针对 445 端口

事件爆发后，2017 年 5 月 13 日，CNVD 发布“关于重点防范 Windows 操作系统勒索软件攻击的情况公告”[3]，综合 360、安天等单位已获知的样本情况和分析结果，明确该勒索软件在传播时基于 445 端口并利用 SMB 服务漏洞（MS17-010），总体可以判断是由于此前“影子经纪人”披露漏洞攻击工具而导致的黑产攻击威胁。根据 CNVD 普查的结果，互联网上共有 900 余万台主机 IP 暴露 445 端口（端口开放），而中国大陆地区主机 IP 有 300 余万台。CNCERT 对勒索软件及相关网络攻击活动进行了监测，建议广大用户及时更新 Windows 已发布的安全补丁，同时做好网络边界、内部网络区域、主机资产、数据备份方面的防护工作。

卡巴斯基在 WannaCry 勒索软件攻击事件爆发后随即发布报告[4]，称这次网络攻击所用的黑客工具“永恒之蓝”，是由黑客组织“影子经纪人”此前在网上披露，来自 NSA 的

网络武器库。犯罪分子利用了微软 Windows 操作系统的一个弱点，对运行该系统的计算机开展广泛攻击。

安天曾在 2017 年 1 月发布的 2016 威胁年报中指出[5]，网络武器的扩散全面降低了威胁行为体的攻击成本，勒索模式带动的蠕虫回潮将不可避免。果然，在安天发布威胁年报 4 个月后，WannaCry 开始爆发并迅速进入全球性感染模式。安天对该勒索软件利用的 SMB 漏洞 MS17-010 进行了分析（见图 7-1）[6]，发布多份报告 [6][7]，并将其定性为“军火级攻击装备的非受控使用”。

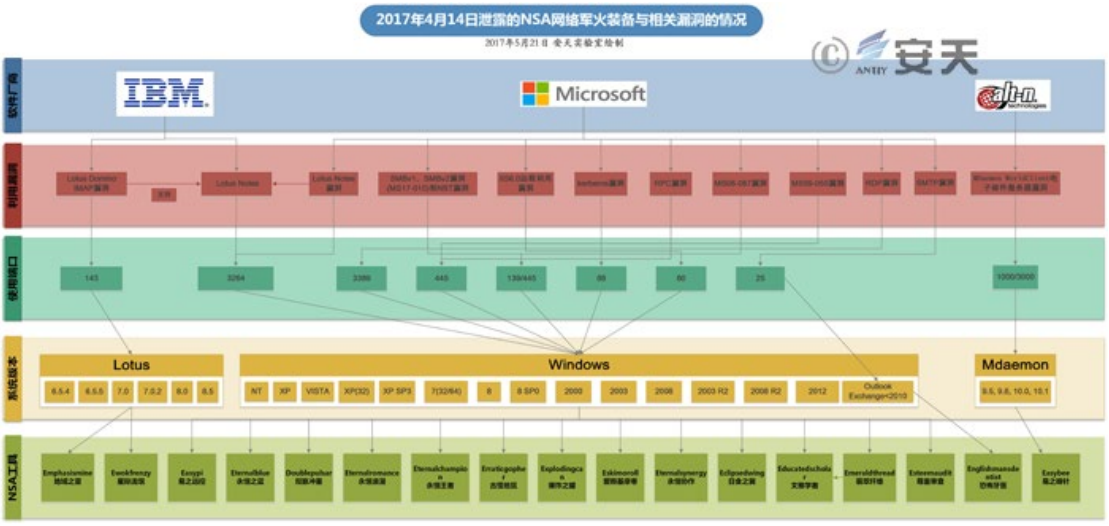


图 7-1 泄露的 NSA 网络武器与相关漏洞、系统版本关系图

鉴于 WannaCry 勒索软件仅利用了被曝光网络武器中的“永恒之蓝”漏洞，“影子经纪人”曝光的网络武器系列中还有其他漏洞及其利用工具需要关注和防范。2017 年 5 月 22 日，安天发布了“关于系统化应对 NSA 网络军火装备的操作手册”[6]，依托对 WannaCry 的分析和预判，为有效检测防御

目前样本和破坏机理并对后续勒索软件可能使用的技巧进行布防，提供了应对处置方案流程和相关应对举措，提醒使用者在日常的安全应用和维护中使用规范流程，整合安全设计、被动防御、积极防御和威胁情报，依托具有有效防护能力的安全产品来形成防御的纵深能力。

360 安全团队在 2017 年的 5 月 12 日检测到一款新型勒索病毒正在利用“永恒之蓝”漏洞武器迅猛传播，迅速发布警报呼吁民众及时安装系统补丁和安全软件。WannaCry 大规模爆发期间，360 获取到样本后，推出了系列解决方案[8]。

（三） 小结

超级大国储备有大量的网络武器，一旦被窃取泄露，可能造成的网络威胁及影响难以预料。“影子经纪人”的曝料让美国一批军火级网络攻击装备浮出水面，这些漏洞利用工具和恶意代码载荷的外泄，被低层级网络空间威胁行为体广泛利用，酿成了包括 WannaCry 大爆发等网络安全事件，由此深刻反映出美国网络攻击超级武器库的丰富储备和强大能力，以及因其未有效管控造成泄露被恶意使用而引发全球网络安全事故的极端严重性。WannaCry 利用的“永恒之蓝”漏洞只是网络武器中的沧海一粟，更多泄露的网络武器不会被无控制地传播和扩散，但可能会被有背景有纪律的网络攻击组织针对性地使用，其衍生的危害可能不低于“永恒之蓝”，

只是因为没有造成明显的大范围危害而尚未能引起足够的重视，但它们的存在和泄露才是更令人担忧的。

参考资料

[1] 新华社. 全球网络攻击波及中国 因美国网络武器库泄露. 2017. http://www.xinhuanet.com//world/2017-05/13/c_1120966771.htm

[2] 中国国家信息安全漏洞共享平台（CNVD）. 关于重点防范 Windows 操作系统勒索软件攻击的情况公告. 2017. https://www.cnvd.org.cn/webinfo/show/4139

[3] CNVD，关于重点防范 Windows 操作系统勒索软件攻击的情况公告. 2017. https://xjca.miit.gov.cn/zwgk/wlaq/art/2020/art_f77d00b8fb7e4d808f551e0179b9141a.html

[4] Kaspersky. What is WannaCry ransomware? 2017. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[5] 安天. 2016 网络安全威胁的回顾与展望. 2017. https://www.antiy.cn/research/notice&report/research_report/725.html

[6] 安天. 关于系统化应对 NSA 网络军火装备的操作手册. 2017. https://www.antiy.com/response/Antiy_Wannacry_NSA.html

[7] 安天. 安天针对勒索蠕虫“魔窟”（WannaCry）的深度分析报告. 2017. https://www.antiy.com/response/wannacry.html

[8] 360. WannaCry 爆发一周年 500 万台电脑惨遭勒索病毒攻击. 2018. https://www.360.cn/n/10169.html

第八篇　军备的扩散——美国渗透测试平台成为黑客普遍利用的工具

网络空间的“军备”，是指具有武器级水准的攻击平台、恶意代码、漏洞及其利用程序，以及其他用于助力达成攻击的工具或组件等。从当前现状来看，主要包括 NSA、CIA 等情报机构所研发的相关攻击工具和支撑体系，同时还包括部分商用工具，如美国的 Cobalt Strike 等商用攻击平台。近年来，由于美国对所销售的自动化渗透攻击测试平台的监管缺失，导致相关攻击平台全球泛滥，已成为了攻击组织的必备工具，被大规模用于实施内网渗透以及恶意网络攻击。

（一）问题概述

Cobalt Strike 是一款渗透测试工具，在 2012 年 6 月首次发布，其作者拉菲尔·穆奇（Raphael Mudge）曾是美国空军的安全研究员。Cobalt Strike 的商业版集成了服务扫描、自动化溢出、多模式端口监听、多种木马生成方式（DLL 木马、内存木马、Office 宏病毒和 Beacon 通信木马等）、钓鱼攻击、站点克隆、目标信息获取、浏览器自动攻击等功能，同时还能够调用 Mimikatz 等其他知名工具。作为一款渗透测试利器，Cobalt Strike 具备强大的功能和可扩展性，从前期载荷生成、诱饵捆绑、钓鱼攻击到载荷植入目标成功后的持续控制、后渗透阶段都可以很好支持，几乎覆盖攻击链的各个阶段。近年来，Cobalt Strike 因其易用性和可扩展性已经被黑客和

APT 组织利用实施真实的网络攻击，攻击者使用 Cobalt Strike 来托管其 C&C 服务器，然后通过它在受感染主机上部署恶意软件。美国科技安全公司 Proofpoint 2020 年的调查数据显示，在滥用 Cobalt Strike 实施的恶意攻击中有 15%与已知的黑客组织有关。

（二） 各方反应

2015 年 5 月 27 日，**安天**发现，在一例针对中国政府机构的准 APT 攻击事件中[1]，攻击者依托自动化攻击测试平台 Cobalt Strike 生成的、使用信标（Beacon）模式进行通信的 Shellcode，实现了对目标主机远程控制的能力。分析人员将样本模块与使用 Beacon 生成的载荷比较发现只有三处数据不同（见图 8-1）[1]，据此得出结论，样本模块是由 Beacon 生成。

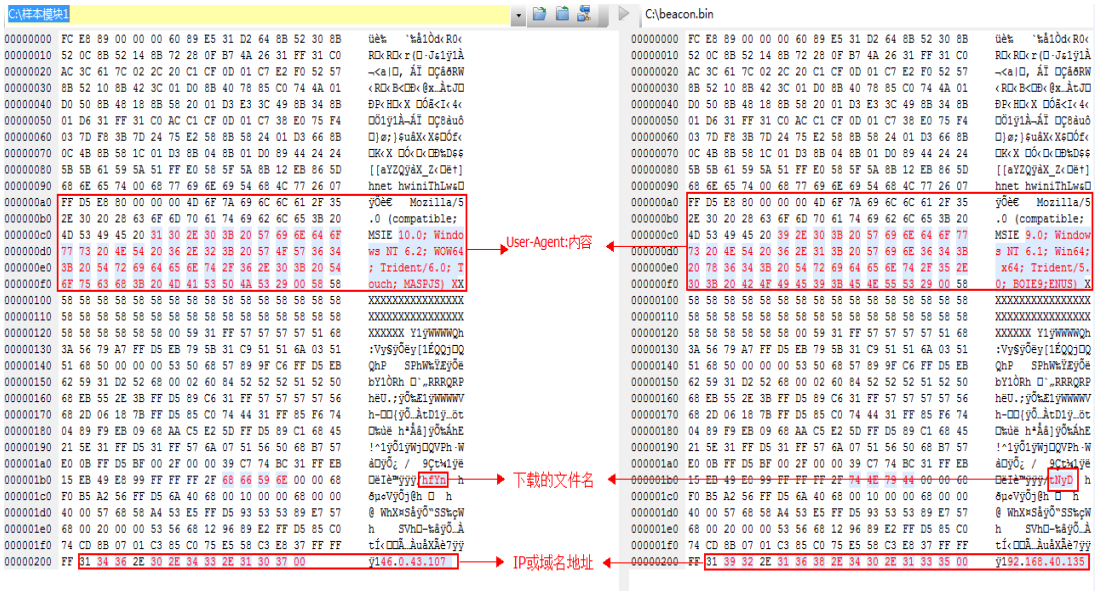


图 8-1 样本模块与 Beacon 生成载荷的对比分析图

2015 年的中国互联网安全大会（ISC 2015）上，安天作了题为“网络安全中的商业军火”的公开报告[2]，对 21 世纪初以来的 Regin、Cobalt Strike 等主要商业化网络武器进行了系统梳理，分析其与相关国家军事网络能力的渊源。以商业化攻击平台 Cobalt Strike 为例，其创始人拉菲尔·穆奇在美军现役和预备役网络部队的服役和研发背景（见图 8-2），清晰地反映了美军事网络技术和能力的外溢及其破坏性。

图 8-2 对 Cobalt Strike 创始人军事背景的分析

美国科技安全公司 Proofpoint2020 年的调查结果显示[3]，威胁行为体对 Cobalt Strike 渗透测试工具的运用较 2019 年增加了 161%。对于近几年 Cobalt Strike 被用于攻击的情况，Proofpoint 的数据图显示(见图 8-3) [3]：2016 年到 2017 年只有少量受害组织被发现攻击者使用了这款工具；2018 年开始显著增加，当年攻击者约在 1 千多家受害组织植入 Cobalt Strike；2019 年约有 5 千家受害组织出现了 Cobalt Strike；

2020 年则超过 9 千家；2021 年不到半年就有超过 8 千家组织成为该工具的受害者。Proofpoint 指出，自 2019 年至 2021 年，滥用 Cobalt Strike 的攻击中有 15%与已知的黑客组织有关。

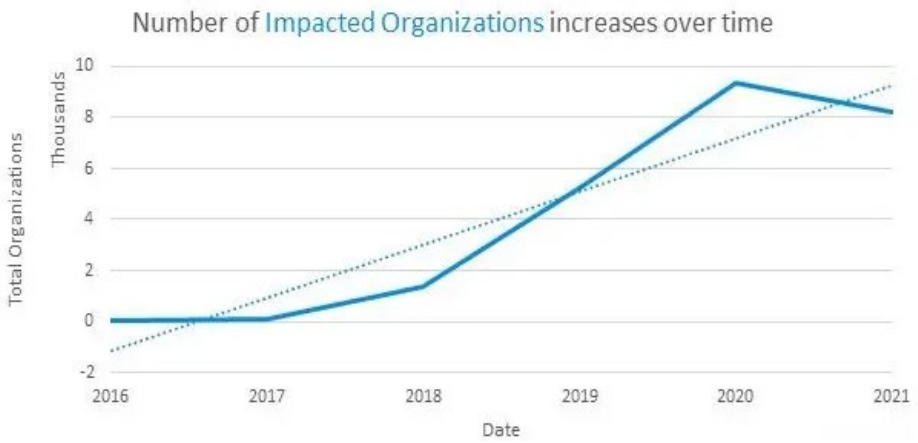


图 8-3 受影响机构数量增长趋势图

美国网络安全公司 Sentinelone 分析显示[4],作为自 2020 年 9 月中旬以来一直处于活跃状态的 Sekhmet 恶意软件家族的一个分支，Egregor 勒索软件的主要分发方式是 Cobalt Strike。攻击者通过各种手段（RDP 攻击、网络钓鱼）破坏目标环境，一旦 Cobalt Strike 信标有效载荷建立并持续存在，就可以利用它来交付和启动 Egregor 有效载荷。

奇安信监测发现[5]，威胁组织“Blue Mockingbird”利用 Telerik UI 漏洞（CVE-2019-18935）攻陷服务器，进而安装 Cobalt Strike 信标并劫持系统资源挖掘门罗币。分析指出，攻击活动中使用的载荷是 Cobalt Strike 信标，它是 Blue Mockingbird 滥用于执行已编码 PowerShell 命令的合法渗透

测试工具。脚本使用常见的 AMSI 绕过技术，逃避 Windows Defender 检测，下载并将 Cobalt Strike DLL 加载到内存中。

（三） 小结

技术可以实现能力的传播，计算机技术使攻击行为和攻击能力变得自动化，而高度自动化的商业攻击平台使这种能力扩散速度远远超出了我们的预测。当前在攻防两端均拥有全球最顶级能力的超级大国，对于有效控制这种武器级攻击手段的扩散，应该负起更多的责任。但现实中拥有最强网络科技能力的美国并未实践其所标榜“实力越强，责任越大”的救世情怀，反而基于自身强大的防御能力，未对诸如 Cobalt Strike 这种自动化攻击平台进行有效约束管控，而是放任其进行商业销售，这不仅给网络空间埋下了安全隐患，而且对他国安全造成了无法预估的潜在影响。

单向威慑的本质就是“讹诈”，一个和平稳定的世界不应基于简单的“赢者通吃”模式。作为超级大国，美国的自信不应只来自“能够绝对打赢网络战争”，更应来自“对他国有效释放安全保证、对自己进行能力约束”[6]。

参考资料

[1] 安天. 一例针对中国政府机构的准 APT 攻击中所使用的样本分析. 2015. https://www.antiy.com/response/APT-TOCS.html

[2] 安天. 网络安全中的商业军火. 中国互联网安全大会（ISC 2015）. 2015. https://www.antiy.com/presentation/20150929-ISC.pdf

[3] Proofpoint. Cobalt Strike: Favorite Tool from APT to Crimeware. 2022. https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware

[4] Sentinel Labs. Egregor RaaS Continues the Chaos with Cobalt Strike and Rclone. 2022. https://www.sentinelone.com/labs/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone/

[5] 奇安信. 黑客利用已存在三年之久的 Telerik 漏洞部署 Cobalt Strike. 2022. https://blog.csdn.net/smellycat000/article/details/125342296

[6] 新华网. 肖新光：美国凭什么能开启“上帝模式”. 2015. http://www.xinhuanet.com/world/2015-09/19/c_128246851.htm

第九篇　“拱形”计划的曝光——应对美国对网络安全厂商的监控

面对美国具备极高水平的攻击能力，全球网络安全界一直通过分析、曝光样本，提升和改进产品能力等方式，与隐藏在幕后的美国情报机构的攻击活动“隔空较量”。在2015年6月，全球多家媒体同时曝光斯诺登泄露的NSA“拱形”计划（CamberDADA），将美国情报监控并构造反病毒厂商“黑名单”的恶行昭然天下，形成了一场舆论的较量。

（一）事件回顾

2015年6月22日，“自由斯诺登”网站曝光了一份标有“绝密”（top secret）字样的NSA文档“轻松获胜：利用信号情报来了解新病毒”（An Easy Win: Using SIGINT to Learn about New Viruses）（见图9-1）[1]，披露了美国、英国有关情报机构实施的“拱形”计划。该计划主要利用美国入侵全球运营商的流量获取能力，对卡巴斯基等反病毒厂商和用户间通讯进行监控，以获取新的病毒样本及其他信息。根据文档封面内容，该计划可能始于2007年，由NSA下设机构信息保障局（IAD）和威胁行动中心（NTOC）参与。

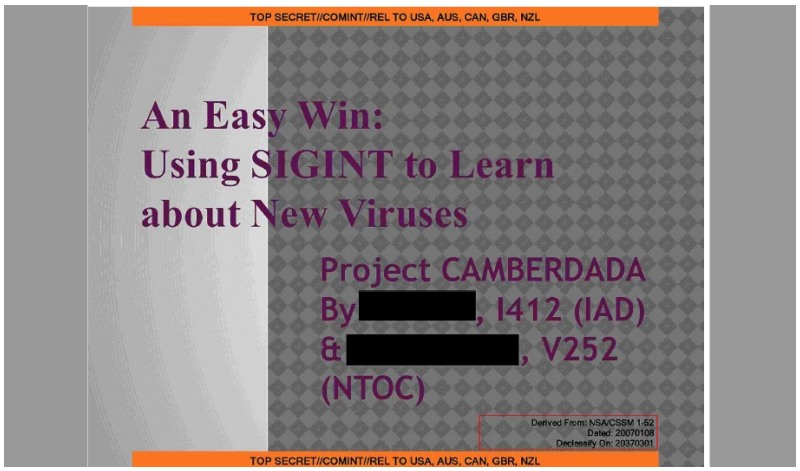


图 9-1 “拱形”计划文件封面

该计划后续目标包括欧洲和亚洲 16 个国家的 23 家全球重点网络安全厂商，其中中国安全厂商包括安天（Antiy）（见图 9-2）[1]。

图 9-2 “拱形”计划所列除卡巴斯基外更多的监控目标厂商

（二） 各方反应

6 月 22 日，斯诺登曝光“拱形”计划当天，部分西方媒体同步报道该事件[2-5]。

美国媒体“拦截者”网站刊文称[2]，“拱形”计划显示自 2008 年开始 NSA 就针对卡巴斯基和其他反病毒厂商的软件

展开了系统性的间谍活动。NSA 充分利用美国针对全球网络的监听能力，以卡巴斯基等网络安全厂商为主要目标，监听、获取全球用户发送给反病毒厂商的邮件，提取其中的病毒样本和其他信息，并意图对这些样本进行分析、遏制、利用等操作，分析安全厂商是否已发现、掌握其网络攻击武器。

美国“连线”网站刊文“美英情报机构瞄准反病毒厂商”[3]，称“拱形”计划描绘了一个系统性的软件“逆向工程”活动，通过监控安全厂商发现软件漏洞，以便帮助情报机构绕过这些软件。斯诺登泄露文件指出，NSA 的信号情报中心每天从发送至卡巴斯基的数十万个恶意文件中筛选出 10 个进行分析。之后，NSA 分析人员检查卡巴斯基杀毒软件对这些恶意文件的响应，以确保它们尚未被纳入检测，之后，NSA 黑客“改造恶意软件”供自己使用，并定期检查卡巴斯基是否将其纳入了病毒库。

美国“福布斯”副主编也于 6 月 22 日在该杂志撰文“NSA 监视非美国反病毒公司”[4]。报道称，英国和美国情报机构对反病毒公司进行间谍活动，并调查了公司反病毒软件弱点，以期增强他们的攻击性监视技术。文章指出，鉴于先前有关英国情报机构 GCHQ 和 NSA 超强黑客能力的披露，这是可以预见的。反病毒软件在电脑上被赋予了很高的权限，因而成为了一个很好的目标，情报机构也正努力破解它们。报道专门指出，美国反病毒领导企业迈克菲（McAfee）和赛门铁

克，以及英国最著名的反病毒厂商守护士（Sophos）均不在名单之上。这三家公司有许多前政府雇员，并与政府的情报和执法机构有着密切的工作关系。显然这份名单是美国情报机构对美国主导五眼情报联盟（美、英、加、澳、新）以外，有能力发现和遏制美国情报活动安全厂商的“黑名单”。

根据中国**新华社**的采访报道，被列入监控范围的反病毒企业纷纷对美国媒体表示，相关报道令人不安[6]。

斯洛伐克安全企业 ESET 表示，信息安全产业的所有企业都应该联合起来，共同反对削弱安全产品的任何企图。“我们的第一要务始终是保护我们的用户，保护我们的产品和我们的系统不受任何入侵，不管这种入侵来自何方”。

卡巴斯基发言人表示，安全企业应该共同努力，捍卫用户隐私以及互联网隐私等权利，挫败大规模监听行动，让世界变得更加安全。

捷克 AVG 技术公司表示，美国 2015 年 6 月刚刚通过的《自由法案》对国家监控行为加以新的限制，这是确保用户安全和安心的积极行动，但在数字生态系统重建信心需要长期努力。

上述企业均称对其安全产品有信心，没有发现它们的产品受到削弱。

被列入目标的中国安全厂商**安天**发布“对相关媒体报道‘中企曾被美国情报机构攻击’涉及我司的两点声明”[7]，

指出泄密文档中所披露的手段主要是相关情报机构在公网信道监听获取用户上报给厂商的邮件，并非是对安全厂商自身的网络系统和产品进行的攻击。更为重要的是，这份监控“目标名单”的出台，将使本已出现裂痕与猜忌的全球安全产业更趋割裂。

（三）小结

美国通过间谍行动直接利用全球网络安全厂商助力其网络空间作业能力。卡巴斯基曾在其报告中分析对其的入侵行动“意图在于学习反病毒软件”[8]。

“拱形”计划通过对全球网络安全厂商的监控，获取大量病毒样本，而用户人工提交给厂商的样本往往是能够绕过厂商检测的样本，NSA 获取这些样本后交由 TAO 再利用，包括对样本配置进行修改，转化为可利用的攻击武器。同时 NSA 通过相关样本的提交时间与厂商后续的响应情况，来判定厂商的处理能力，以便更好地策划行动，绕过检测[9][10]。

“拱形”计划的目的：一是捕获全球用户向反病毒厂商上报的样本，二是为 TAO 提供可重用样本资源，三是监测反病毒厂商的处理能力及是否放行某些恶意代码样本。

美国情报机构把自身所在国家以外的国际反病毒和安全厂商视为自己全球攻击、监听活动的绊脚石，同时又与自己国家的安全厂商微妙互动，强行在反病毒和安全厂商中划分出阵营。目标除了俄罗斯的卡巴斯基外，后续目标还锁定

了包括了罗马尼亚的比特梵德（Bitdefender）、德国的小红伞（Avira）、中国的安天（Antiy）等在内的目标，但美国、英国等五眼情报联盟国家的主要反病毒厂商赛门铁克、迈克菲、趋势（Trend Micro）、守护士等均不包括在名单之内。可能说明英国、美国相关情报机构与所在国安全厂商有直接的互动方式和沟通渠道，而无需借助监听的方式。

美国情报机构这一行动是强行在反病毒和安全厂商中划分出阵营，必将导致各国艰难形成的安全产业协作和应急协同机制荡然无存，也将显著伤害全球其他国家用户对美国有关安全厂商的基本信任。

参考资料

[1] Edward Snowden. An Easy Win: Using SIGINT to Learn about New Viruses. 2015. https://edwardsnowden.com/wp-content/uploads/2015/06/project-camberdada.pdf

[2] The Intercept. Project CAMBERDADA-NSA. 2015. https://theintercept.com/document/2015/06/22/project-camberdada-nsa/

[3] Wired. US and British Spies Targeted Antivirus Companies. 2015. https://www.wired.com/2015/06/us-british-spies-targeted-antivirus-companies/

[4] Forbes. NSA Spied On Non-American Anti-Virus Companies.2015. https://www.forbes.com/sites/thomasbrewster/2015/06/22/foreign-av-companies-targeted-by-nsa/?sh=3b7081495b8c

[5] RT. NSA, GCHQ targeted Kaspersky, other cybersecurity companies–Snowden docs.2015. https://www.rt.com/usa/268891-nsa-gchq-software-kaspersky/

[6] 新华社. 综述：多国网络安全厂商抨击美英监听计划. 2015.
http://news.xinhuanet.com/world/2015-06/25/c_1115727217.htm
[7] 安天. 对相关媒体报道“中企曾被美国情报机构攻击”涉及我司的两点声明. 2015.
https://www.antiy.com/press/20150625.html
[8] Eugene Kaspersky. Why Hacking Kaspersky Lab Was A Silly Thing To Do. 2015
https://www.forbes.com/sites/eugenekaspersky/2015/06/10/why-hacking-us-was-a-silly-thing-to-do/
[9] 至顶网.“棱镜”无死角美监视计划涵盖全球反病毒厂商.2015.
http://security.zhiding.cn/security_zone/2015/0624/3055909.shtml
[10]安全牛. NSA 监控全球反病毒厂商 英美除外. 2015.
https://www.aqniu.com/vendor/8284.html

第十篇　破窗效应——对“影子经纪人”和维基解密泄露数据进行迭代分析

斯诺登“棱镜门”事件首次让世人看到美国庞大的网络情报体系和能力，2016 年至 2017 年期间，“影子经纪人”和维基解密事件则进一步揭开美国 NSA 和 CIA 两大情报机构网络军火库的面纱。通过这几次网络事件，网络安全界大概了解美国在网络空间的体系化能力和全方位布局，而不是像此前那样，只是通过具体事件和样本代码获得战术层面的认识。在最初的两年中，网络安全界通过对曝光文件的系统分析，逐渐了解美国网络攻击能力框架，并为其规模之全面、覆盖之广泛所震惊；此后，全球网络安全界不断在真实网络攻击事件中发现并重新认识美国攻击武器和系统，对美国网络攻击体系的认识逐步深入和全面。

（一） 事件回顾

2016 年 8 月至 2017 年 4 月，**“影子经纪人”**分批曝光了 NSA 针对网络安全设备的攻击装备、针对全球服务器攻击列表清单、入侵 SWIFT 机构资料、FuzzBunch（FB）漏洞攻击平台和 DanderSpritz（DSZ）远控平台等网络武器装备，并称这些攻击装备与“方程式组织”有关。根据相关分析和资料显示，这些攻击装备是美国若干年前开发的，涉及大量系统级零日漏洞利用工具和先进的后门程序，暴露了美国的漏洞储备能力和攻击技术水平。

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，其中包含 7818 个网页和 943 份附件。泄露的文件包含庞大攻击装备库的文档信息，其平台面覆盖非常广泛，不仅包括 Windows、Linux、iOS、Android 等常见的操作系统，也包括智能电视、车载智能系统、路由器等网络节点单元和智能设备。

（二）研究分析曝光经过

2016-2018 年，全球网络安全学术界和产业界在震惊之余，纷纷开始对泄露的资料进行整理和分析，针对“影子经纪人”曝光的材料，梳理出了 NSA 网络作业体系中以 FB、Operation Center（OC）和 DSZ 为代表的三大核心模块；而维基解密曝光的“七号军火库”（Vault 7）包含的 CIA 网络作业 15 个工具(集)和 5 个框架，也得到较为全面的整理。

2017 年 4 月，CysInfo 对“影子经纪人”泄露的文件进行了分析。FB 是模块化的漏洞利用框架（见图 10-1）[1]，其核心是分成五类的众多插件，尤其令人关注的是其“Special”和“Exploit”类别之下的 17 个零日漏洞利用，其中多数与 Windows 操作系统的 SMB 零日漏洞相关，这些漏洞在 2017 年 3 月才由微软修复；此外还有一些是针对 IBM Lotus Domino 平台、Microsoft IIS、IMAP、RDP 等的漏洞利用。

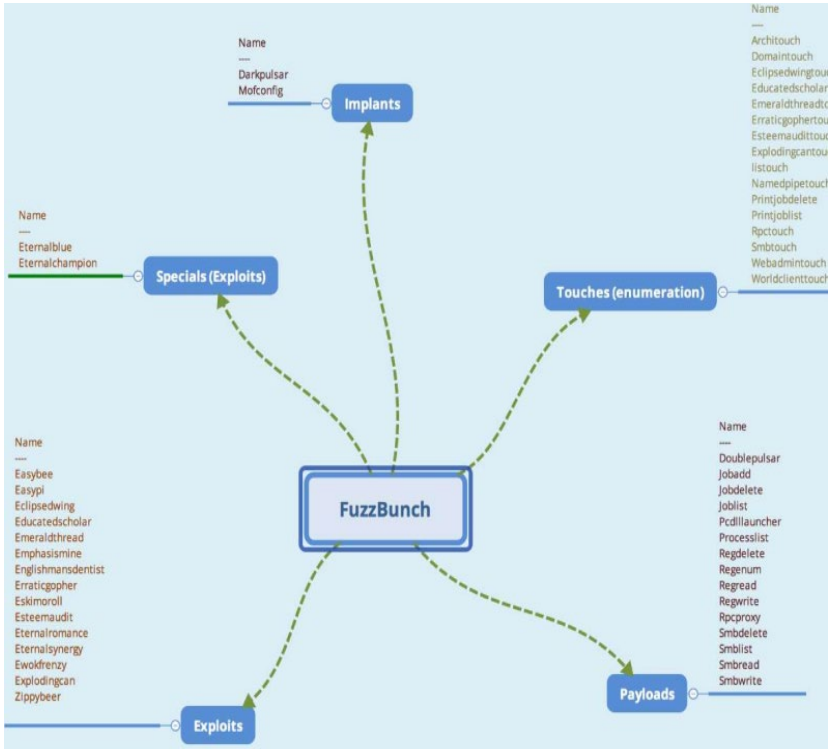


图 10-1 FuzzBunch 框架结构

CysInfo 称，OC 是一个充分武器化的一站式工具框架（见图 10-2）[1]，用于控制受害机器，可向受害机器部署多种不同的远程监视工具、网络包操纵和重定向，收集用户敏感信息，关闭安全产品；OC 中的核心插件是 PeddleCheap，为攻击者提供灵活的用户界面，加载 DSZ 等攻击载荷。

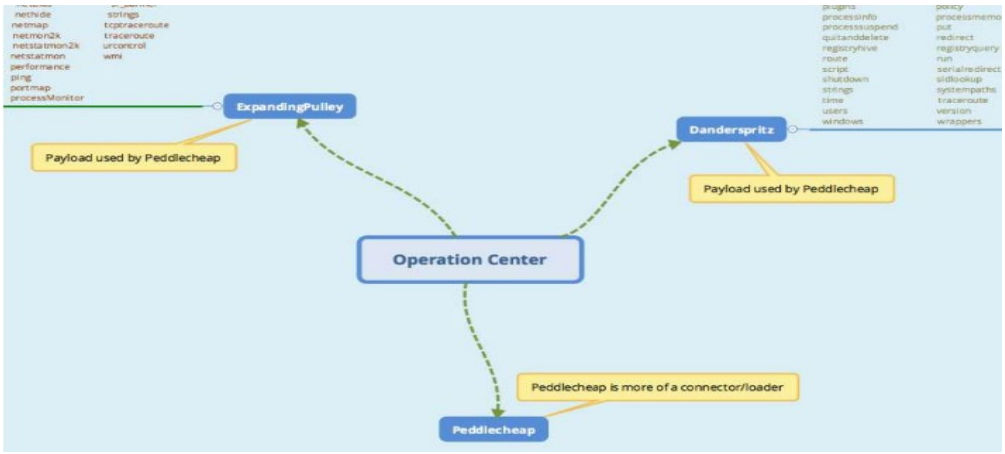


图 10-2 Operation Center 框架结构

OC 的复杂程度表明，其开发持续多年，并有强大的资源投入。代码中的注释显示，OC 的开发最早可追溯到 2006 年左右；而 OC 的载荷之一，clocksvc.exe，回传的 IP 地址属于北美顶尖大学纽约州立大学石溪分校（见图 10-3）[1]，是其开发得到学术资源支持的明证。

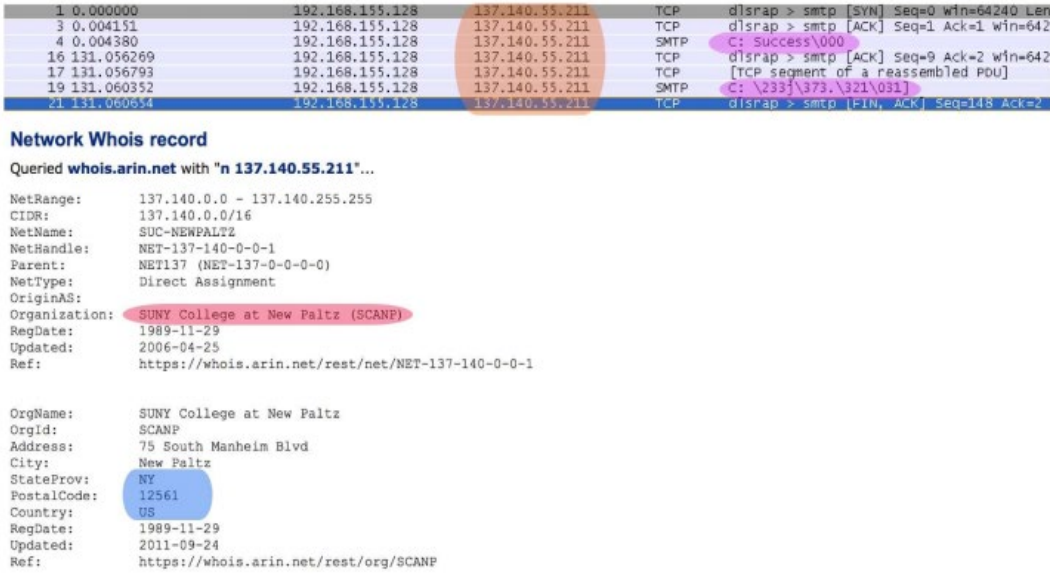


图 10-3 Clocksvc.exe 的 IP 分析

更令人惊讶的是，根据趋势科技的分析[2]，clocksvc.exe（趋势科技称其为 Tildeb）是一个攻击 Windows NT 4.0 和 Microsoft Exchange Server 的内存植入程序（见图 10-4），历史甚至远早于 2006 年：编译时间戳是 2000 年 10 月 3 日！

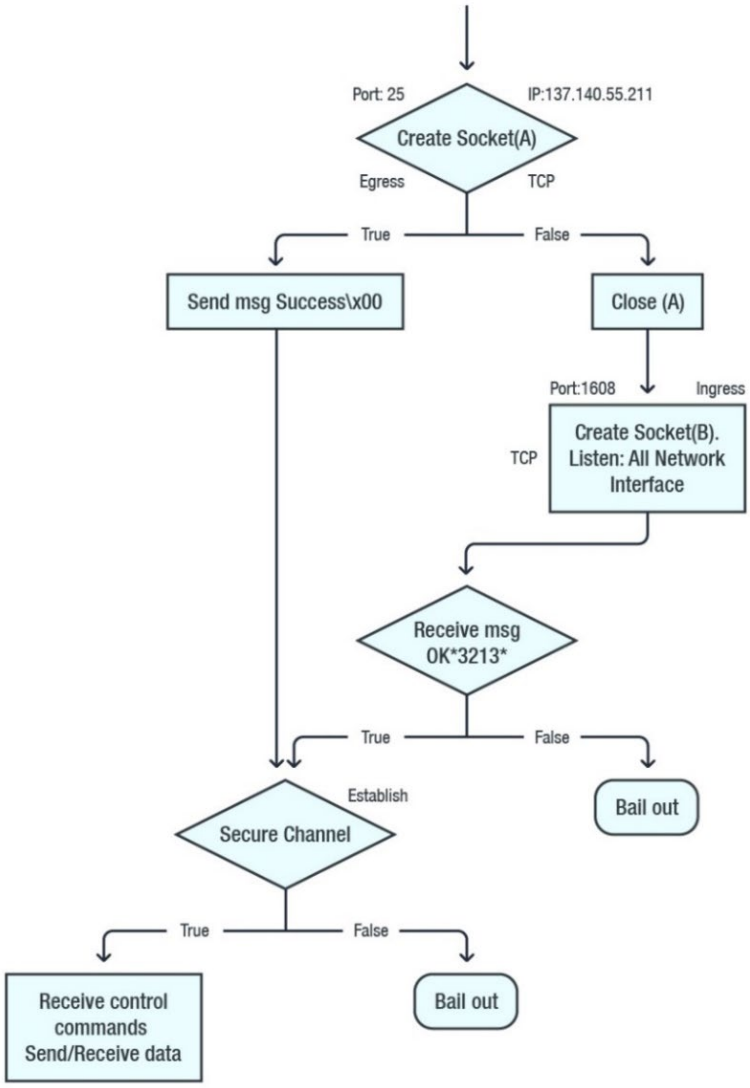


图 10-4 Tildeb(clocksvc)建立连接过程

2017-2018 年，安天对斯诺登、“影子经纪人”和“维基解密”泄露的攻击装备和文档进行了深入系统的分析，并自 2017 年 12 月起，在《网信军民融合》杂志连载 12 期“美国网络空间攻击与主动防御能力解析”系列报告[3]，从情报循环、进攻性能力支撑、攻击装备和积极防御等多角度对美国网络空间攻防能力进行了系统化梳理，清晰地展现美国在网络空间安全领域的能力体系。

安天在系列报告中指出，美国构建了制式化、全平台、全能力的网络空间攻击装备体系，攻击目标覆盖个人主机、服务器、网络设备、安全设备、移动智能设备等各类 IT 设备，包括 Windows、Linux、MacOS、Android 等各类操作系统，从功能上涵盖侦察、物理隔离突破、内网横向移动、持久化潜伏驻留、供应链与物流链渗透、远程控制等各个环节。

2018 年 10 月，**卡巴斯基**对框架 DSZ 中 DarkPulsar 后门进行了深度分析[4]。DSZ 由多种插件组成，可由 OC 中的 PeddleCheap 加载，用于控制受感染机器，进行情报收集、漏洞利用和监测。通过分析管理模块和用于加密 C&C 和植入程序之间流量的几个常量，发现了神秘的 DarkPulsar 后门，包括 32 位和 64 位版本，感染 Windows 2003/2008 Server。卡巴斯基在俄罗斯、伊朗和埃及追踪到约 50 名受害者，涉及核能、电信、IT、航空航天等多个领域。从 DarkPulsar 的持久性和潜伏能力（例如将其流量封装到合法协议中并绕过密码保护以通过身份验证）可以看出，背后的开发者非常专业。DarkPulsar 的开发人员在开发持久性机制时毫不吝啬资源，包括禁用 NTLM 协议安全性的功能，以绕过在身份验证期间输入有效用户名和密码的要求，表明 DarkPulsar 针对的是具有长期监视和控制价值的目标。

2021 年，**以色列安全厂商 Checkpoint** 发布报告[5]，对 DSZ 中的 Double Feature 组件进行了深度分析。DSZ 高度模

块化，包含用于持久性、侦察、横向移动、绕过防病毒引擎和其他可疑活动的各种工具。DoubleFeature 可以有效地充当受害机器的诊断工具，评估 DSZ 中哪些工具可以在受害机器上部署使用。对于部署的工具，如针对 Windows 系统的远程访问工具 UnitedRake (UR)，DoubleFeature 进行监视和日志记录。UR 是卡巴斯基在其原始报告中称为“EquationDrug”的工具，由此也表明，DSZ（以及 FB 和 OC）都是“方程式组织”庞大的工具集。

2022 年 3 月，**360 安全团队**发布了关于 NSA 攻击组织 APT-C-40 的分析报告[6]。报告称，对取证数据的分析表明，该组织早在 2010 年就开始了针对中国系列行业龙头公司的攻击，涉及众多关键网络管理服务器和终端，该攻击活动与 NSA 的某网络战计划实施时间前后衔接。报告指出，美国网络攻击属于无差别攻击，可以劫持全世界任意地区任意上网用户的正常网页浏览流量，中国境内的政府、金融、科研院所、运营商、教育、军工、航空航天、医疗等行业以及重要敏感单位及组织机构均为其主要目标。

2017 年 4 月，**赛门铁克**分析了维基解密泄露的“七号军火库”资料后指出[7]，其中描述的间谍工具和装备可以将一个名为“长角牛”（Longhorn）的威胁组织与近期在欧洲、亚洲和非洲的 16 个国家发生的至少 40 起网络攻击事件关联起来，因为该组织“使用的工具与维基解密披露的工具开发

时间线及技术特征高度相关”。分析称，“长牛角”至少自2011年起已活跃，是一个非常复杂精密的组织，使用大量零日漏洞利用和复杂的恶意软件对金融、能源、电信、教育以及航天等所有关键行业进行定向攻击。

2020年，**360安全团队**披露了CIA攻击组织（APT-C-39）对中国航空航天、科研机构、石油行业、大型互联网公司以及政府机构等关键领域长达十一年的网络渗透攻击[8]。据360报道称，通过对维基解密泄露的“七号军火库“网络武器资料研究，发现了与之关联的一系列针对中国关键领域的长期定向攻击活动。这些攻击活动最早可以追溯到2008年9月，并一直持续到2019年6月左右，主要集中在北京、广东、浙江等地。360安全团队深入分析了五大关联证据（例如APT-C-39组织多次使用了Fluxwire，Grasshopper等CIA专属网络武器针对中国目标实施网络攻击等），可靠地证明APT-C-39组织隶属于CIA。对APT-C-39的活动分析表明，CIA的网络武器给全球网络安全带来了严重威胁。

2022年3月，中国国家计算机病毒应急处理中心（CVERC）正式公开发布了对NSA使用“NOPEN”木马的分析报告[9]。该木马一旦被植入受害者计算机，就会成为“潜伏者”，随时向攻击者敞开“金库大门”，各种机密数据、敏感信息一览无余。有证据显示，该木马已经控制全球海量的互联网设备，窃取了规模庞大的用户隐私数据。

（三） 小结

“影子经纪人”的文档揭示受害范围超过45个国家287个目标，包括俄罗斯、日本、西班牙、德国、意大利等，持续十几年时间。2022年9月曝光的针对中国西北工业大学攻击中，NSA使用了多达41种网络武器，其中就有“影子经纪人”泄露过的NOPEN[10]。时隔7年，NSA和CIA巨大的网络军火冰山，仍然有待安全领域不断发现和认识。

参考资料

[1] InfoSec Institute. NSA BIOS Backdoor a.k.a. God Mode Malware Part 1: DEITYBOUNCE. 2014. https://cysinfo.com/wp-content/uploads/2017/04/Shadow_release_updated.pdf

[2] Trend Micro. Tildeb: Analyzing the 18-year-old Implant from the Shadow Brokers' Leak.2017. https://documents.trendmicro.com/assets/tech-brief-tildeb-analyzing-the-18-year-old-implant-from-the-shadow-brokers-leak.pdf

[3] 安天. “美国网络空间攻击与主动防御能力解析”系列文章12篇. 网信军民融合. 2017(12)-2018(11). https://mp.weixin.qq.com/s/PnaYXZ9snK6fv_lgCFszDw

[4] Kaspersky. DarkPulsar. 2018. https://securelist.com/darkpulsar/88199/

[5] Check Point. A Deep Dive into DoubleFeature, Equation Group's Post-Exploitation Dashboard. 2021. https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/

[6] 360. 网络战序幕：美国国安局 NSA（APT-C-40）对全球发起长达十余年无差别攻击. 2022.
https://mp.weixin.qq.com/s/jHjzky8xIaEuocHzbWjFSA

[7] Symantec. Longhorn Tools Used Cyberespionage Group Linked Vault 7. 2017.
https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7

[8] 360. 披露美国中央情报局 CIA 攻击组织（APT-C-39）对中国关键领域长达十一年的网络渗透攻击. 2020.
https://mp.weixin.qq.com/s/IfnVrmcUInr0OBF7I1m4Wg

[9] CVERC. “NOPEN”远控木马分析报告. 2022.
https://www.cverc.org.cn/head/zhaiyao/news20220314-nopen.htm

[10]安天. 从“NOPEN”远控木马浮出水面看美国网络攻击装备体系. 2022.
https://mp.weixin.qq.com/s/J2L-Czapzi3Vj5dzOpGzjA

第十一篇　首次完整的溯源——复盘“方程式组织”攻击中东技术设施的完整过程

2017 年之前，尽管全球网络安全界对美国网络攻击活动有一些分析，但除“震网”事件因美国主动暴露而有一些机理过程分析外，都停留在样本分析层面。2017 年“影子经纪人”的曝料让网络安全界得以把分析成果串接起来。安天等厂商将曝光的各种信息线索进行组合复盘，结合长期积累的研究成果，得以初步还原美国“方程式组织”的一起网络攻击过程。

（一）事件回顾

2017 年 4 月 14 日，“影子经纪人”曝光的美国网络攻击相关数据中包含一个名为 SWIFT 的文件夹，完整详细曝光了“方程式组织”针对 SWIFT 金融服务提供商及合作伙伴的两起网络攻击行动“JEEPFLEA_MARKET”和“JEEPFLEA_POWDER”[1][2]。其中，“JEEPFLEA_MARKET”是 2012 年 7 月至 2013 年 9 月期间，针对中东地区最大的 SWIFT 服务提供商 EastNets 发起的攻击行动。该行动成功窃取了 EastNets 在比利时、约旦、埃及和阿联酋的上千个雇员账户、主机信息、登录凭证及管理员账号；“JEEPFLEA_POWDER”攻击行动主要针对 EastNets 在拉美和加勒比海地区的合作伙伴 BCG（Business Computer Group），但此项行动并未成功。

（二） 研究分析曝光经过

2019 年 6 月，安天发布“‘方程式组织’攻击 SWIFT 服务提供商 EastNets 事件复盘分析报告”[3][4]。在该报告中，安天基于“影子经纪人”泄露资料与历史捕获分析成果进行关联分析，完整复盘了“方程式组织”攻击中东最大 SWIFT 金融服务提供商 EastNets 事件，还原了美国攻击跳板、作业路径、装备运用、战术过程、场景环境和作业后果。报告详细分析了被攻击目标资产信息，如网络设备和网络安全设备信息、管理服务器信息、应用服务器信息和 SWIFT 业务服务器信息，绘制了网络拓扑结构图（见图 11-1）[3]，并梳理了各个资产的品牌型号信息和安全漏洞信息及对应攻击者使用的攻击武器名称。

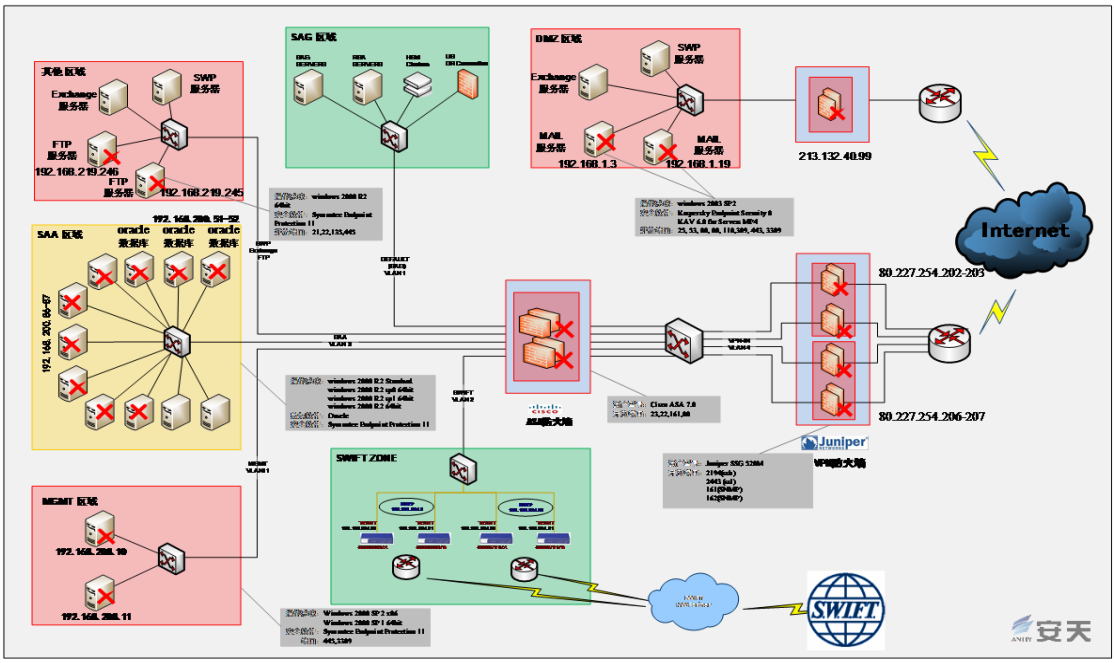


图 11-1 EastNets 被攻击资产简况拓扑图

报告总结了美国此次作业使用的攻击装备信息，根据功能目的将其分为漏洞利用工具和平台类、持久化植入武器类、控制后门类，并对武器功能、适用场景和关联漏洞进行描述（见图 11-2）[3]，指出美国拥有覆盖全平台全系统的攻击能力和大量的零日漏洞储备。

攻击装备名称	漏洞编号	针对设备及功能
未知装备 A	CVE-2015-7755	未知装备 A 是针对 Juniper ScreenOS（Juniper SSG 及 NetScreen 防火墙产品使用的操作系统）的漏洞攻击装备，在通过 SSH 与 Telnet 登录 Juniper 防火墙时存在身份认证绕过漏洞；
EPICBANANA	CVE-2016-6367	EPICBANANA 是针对 Cisco ASA and PIX 设备中 command-line interface (CLI) 解析器的漏洞攻击装备；
EXTRABACON	CVE-2016-6366	EXTRABACON 针对 Cisco ASA 设备的 SNMP 服务（端口 161、162）漏洞攻击装备；
ENTERNALCHAMPION	CVE-2017-0146	ENTERNALCHAMPION（永恒冠军）是针对 Windows Server 2008 SP1 x86 等的“永恒”系列漏洞攻击装备，利用 Windows 的 SMBv1 远程代码执行漏洞；
ETERNALSYNERGY	CVE-2017-0146	ETERNALSYNERGY（永恒协作）是针对 Windows 8 等的“永恒”系列漏洞攻击装备，利用 Windows 的 SMBv1 远程代码执行漏洞；
ETERNALBLUE	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148	ETERNALBLUE（永恒之蓝）是针对 Windows 7/8/XP 等的“永恒”系列漏洞攻击装备，利用 Windows 的 SMBv1 远程代码执行漏洞；
ETERNALROMANCE	CVE-2017-0143	ETERNALROMANCE（永恒浪漫）是针对 Windows XP、Vista 7、Windows Server 2003/2008/2008 R2 等的“永恒”系列漏洞攻击装备，利用 Windows 全平台的 SMBv1 远程代码执行漏洞；
EXPLODINGCAN	CVE-2017-7269	EXPLODINGCAN（爆炸之罐）是利用 IIS6.0 webDAV 漏洞的攻击装备；

图 11-2 “方程式组织”攻击 EastNets 所使用的漏洞利用工具列表

该报告还对攻击路径给出了推测（见图 11-3）[3]：攻击者从互联网四个跳板发起攻击，先后击穿了两层防火墙（VPN 防火墙、ASA 防火墙），并且在防火墙上预制了 Rootkit；之后又通过多个零日漏洞穿梭进内网体系，获取多台业务服务器的控制权；最后通过相关的 SQL 语句，从 Oracle 服务器上获得了攻击方感兴趣的账户名、密码和交易轨迹等相关信息。

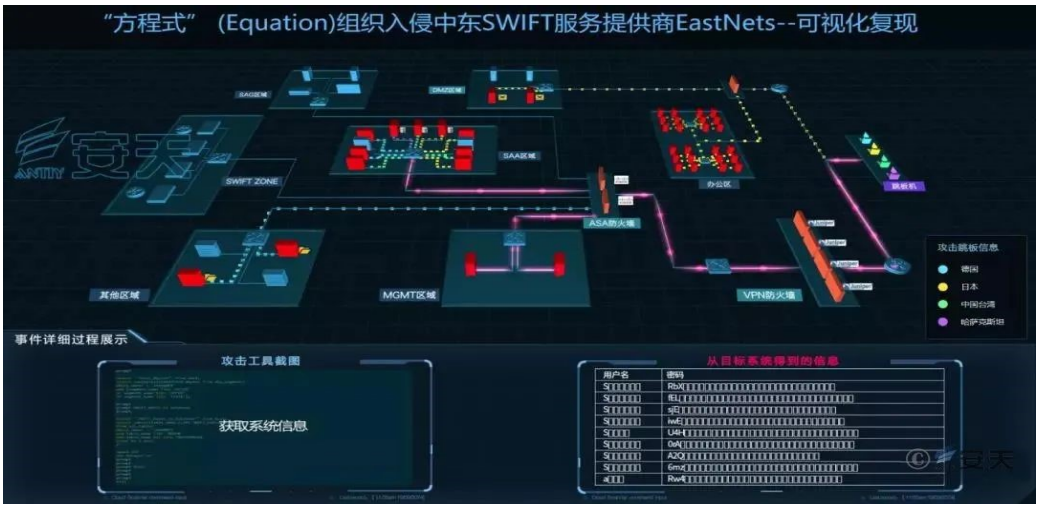


图 11-3 “方程式组织”入侵 EastNets 可视化复现

安天在此报告中提到了美国 NSA 制式化网络攻击装备“NOPEN”木马。在 2022 年中国西北工业大学网络攻击事件中，NSA 正是使用该木马攻击控制了西工大的边界服务器。

（三） 小结

面对美国“大到无形”的超强网络作业能力压迫，安全厂商通过多年坚持不懈的跟踪与积累，并结合“影子经纪人”的爆料文件，已经初步实现了完整复盘美国“方程式组织”攻击事件，在与美国的对抗过程中，全球网络安全厂商也在不断地成长。

“影子经纪人”的爆料让美国的一批攻击装备浮出水面。一方面，这些漏洞利用工具和恶意代码载荷的外泄，被其他低层级的网络空间威胁行为体广泛利用，酿成了 WannaCry 大爆发等网络安全事件；另一方面，这些信息也成为了安全

研究者极为宝贵的研究资源，帮助他们能够从完整的威胁框架角度去分析顶级 APT 组织的攻击活动全貌。

参考资料

[1] Bleeping Computer. Shadow Brokers Release New Files Revealing Windows Exploits, SWIFT Attacks. 2017.
https://www.bleepingcomputer.com/news/security/shadow-brokers-release-new-files-revealing-windows-exploits-swift-attacks/

[2] The Times of Israel. Hacked files suggest NSA penetrated SWIFT, Mideast banks. 2017.
https://www.timesofisrael.com/hacked-files-suggest-nsa-penetrated-swift-mideast-banks/

[3] 安天. “方程式组织”攻击 SWIFT 服务提供商 EastNets 事件复盘分析报告. 2019.
https://www.antiy.com/response/20190601.html

[4] 新华社. 对美国网络攻击目标泛化的隐忧. 2019.
https://baijiahao.baidu.com/s?id=1636198876284800319&wfr=spider&for=pc

第十二篇　国际论坛上的斗争——揭露美国对网络空间安全的操控

自从2010年的“震网”事件开始，网络安全界就越来越多地认识到美国对网络安全的肆意操纵和破坏，并通过国际会议、论坛等交流活动，揭露美国网络行为、意图和活动。而美国作为具有网络安全技术优势的国家，不但没有承担大国应有的责任，反而利用其在网络空间的话语权，通过突然撤稿等手段干扰和打压正常国际交流，阻挠信息的传播和共享。

（一）突然撤稿

2014年，“黑帽”（Black Hat）会议突然撤回美国卡内基梅隆大学网络安全研究人员亚历山大·沃洛金（Alexander Volynkin）的报告“破解Tor并不需要成为美国国家安全局：对用户进行去匿名化的简单方法”。这一不同寻常的撤稿事件（见图12-1），立即引起广泛的讨论和质疑，认为大会是在美国政府的压力下撤回报告[1]。

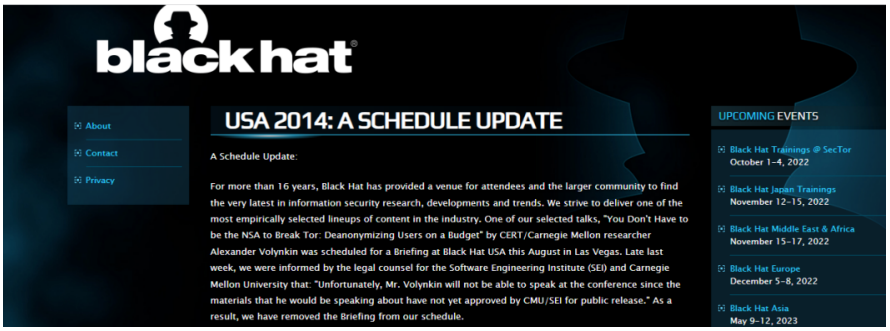


图 12-1 Black Hat USA 2014 的临时撤回报告说明

尽管美国政府采取各种手段干扰网络安全领域的合作和交流，但具有合作和共享精神的全球网络安全企业界和学术界仍致力于共享和开放，推动全球网络空间的安全发展。

（二） 全球安全厂商在国际会议和论坛上的努力

2012 年，赛门铁克副总裁、首席架构师凯里·纳成贝格（Carey Nachenberg）在美国斯坦福大学 CSIAC 科学论坛作了题为“一个计算机病毒如何摧毁伊朗核项目”的报告，披露了“震网”令人惊叹的传播、逃杀等技术手段及其强大的破坏力。在传播机制分析中指出，为了实现“震网”病毒在网络中的扩散，使用了 7 个不同的软件漏洞（后门），其中有 6 种是此前未知的（见图 12-2）[2]。

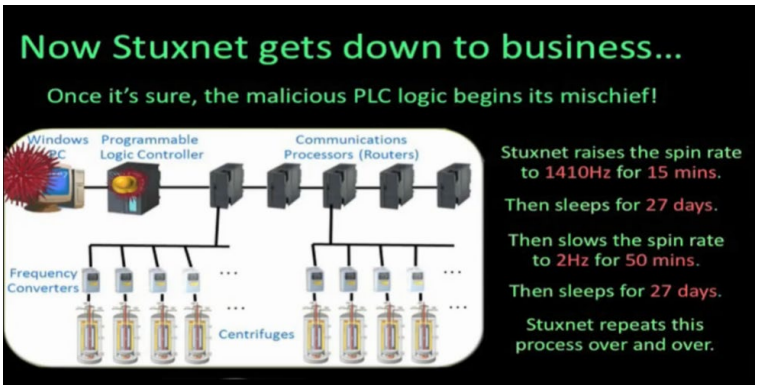


图 12-2 纳成贝格分析“震网”的破坏过程

2013 年 12 月 27 日，原 Tor 项目核心程序员雅各·阿贝尔鲍姆（Jacob Appelbaum）在第 30 届混沌通信大会（30C3）上展示了一组泄露的 PPT 文档，其中包含了针对服务器、路由器、防火墙和手机设备的可利用漏洞以及对应的利用程序与木马（见图 12-3）[3]，所涉及产品包括 DELL 服务器、HP

服务器、Juniper Netcreen 和 SSG 防火墙、华为 Eudemon 防火墙、华为路由器、Cisco 防火墙、iPhone 和 Windows mobile。其中也包括了一些通用木马程序与专用硬件：包括通过 BOOTKIT 执行的硬盘固件木马、BIOSKIT、USB 注入+无线网桥设备、针如对 XP 系统的无线软件植入工具、伪 GSM 基站、SIM 卡短信植入工具、针对 iphone 的植入工具、针对 Windows mobile 的植入工具、采集信息的间谍手机等等。

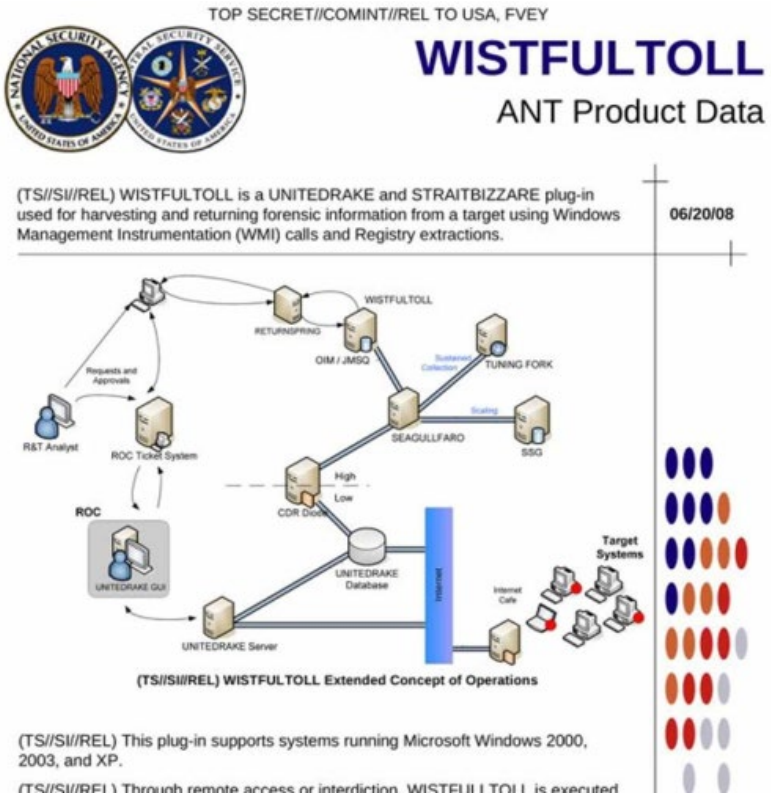


图 12-3 阿贝尔鲍姆曝光的 NSA 网络工具 WISTFULTOLL

2014 年，美国媒体“拦截者”网站披露了斯诺登泄露的多份英国通信总部（GCHQ）与 NSA、“五眼联盟”其他国家相关机构分享的有关“线上隐秘行动”文档，说明这些机构是如何操控和歪曲网络内容，破坏互联网的完整性。卡巴

斯基研究人员布莱恩·巴塞洛缪（Brian Bartholomew）等人在 2016 年的 Virus Bulletin 年会（VB 2016）上发布“挥舞假旗！定向攻击中搅混水的欺骗策略”报告，进一步分析了美国网络行动中的多种欺骗手段[4]。

2015 年，德国《明镜周刊》披露了斯诺登泄露的 NSA 在网络空间的“第四方情报收集”（The Fourth Party）手法和项目，即通过侵入（并利用）第三方网络基础设施，更加隐蔽地获取情报或实施网络攻击。以此情报为基础，结合自己对多个网络安全事件的深入分析，卡巴斯基公司的胡安·安德烈斯·格雷罗-萨德（Juan Andres Guerrero-Sannde）等研究人员在 2017 年的 Virus Bulletin 年度会议（VB 2017）上发布报告“行走在敌人的阴影中：当第四方收集成为溯源的地狱”[5]，系统地分析了这一攻击手法的隐蔽性和高度复杂性。例如，一个未知的 APT 组织（卡巴斯基将其命名为 ScarCruft）利用被已知 APT 组织 DarkHotel 侵入的网站，采用与 DarkHotel 类似的战术、技术、程序，对俄罗斯、中国以及韩语国家的公司和个人进行定向攻击（见图 12-4）[5]。报告指出，这种只有全源情报机构才能开展的行动，不仅超出传统网络安全厂商的威胁情报能力，更破坏了威胁情报的生态。

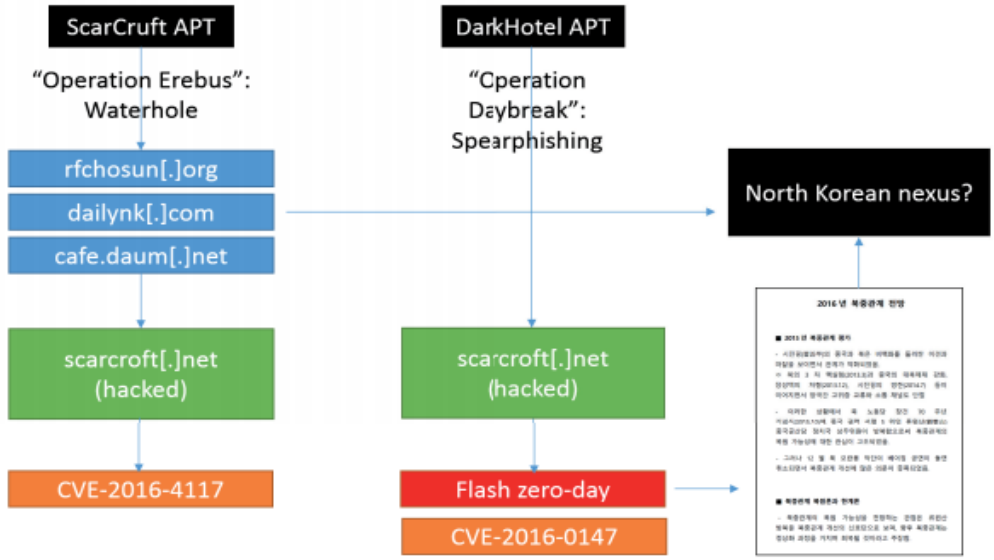


图 12-4 对 APT ScarCruft 利用 DarkHotel 活动隐藏自己活动的分析

2016 年，美国哥伦比亚大学国际与公共事务学院的高级研究人员杰森·希利（Jason Healey）在《国际事务杂志》发表“美国政府与零日漏洞”一文，深入分析了美国漏洞公平裁决程序（VEP）自 2008 到 2016 年的发展历程，并对当前（2016 年）美国可能囤积的零日漏洞军火数量进行了谨慎的估算（见图 12-5）[6]。

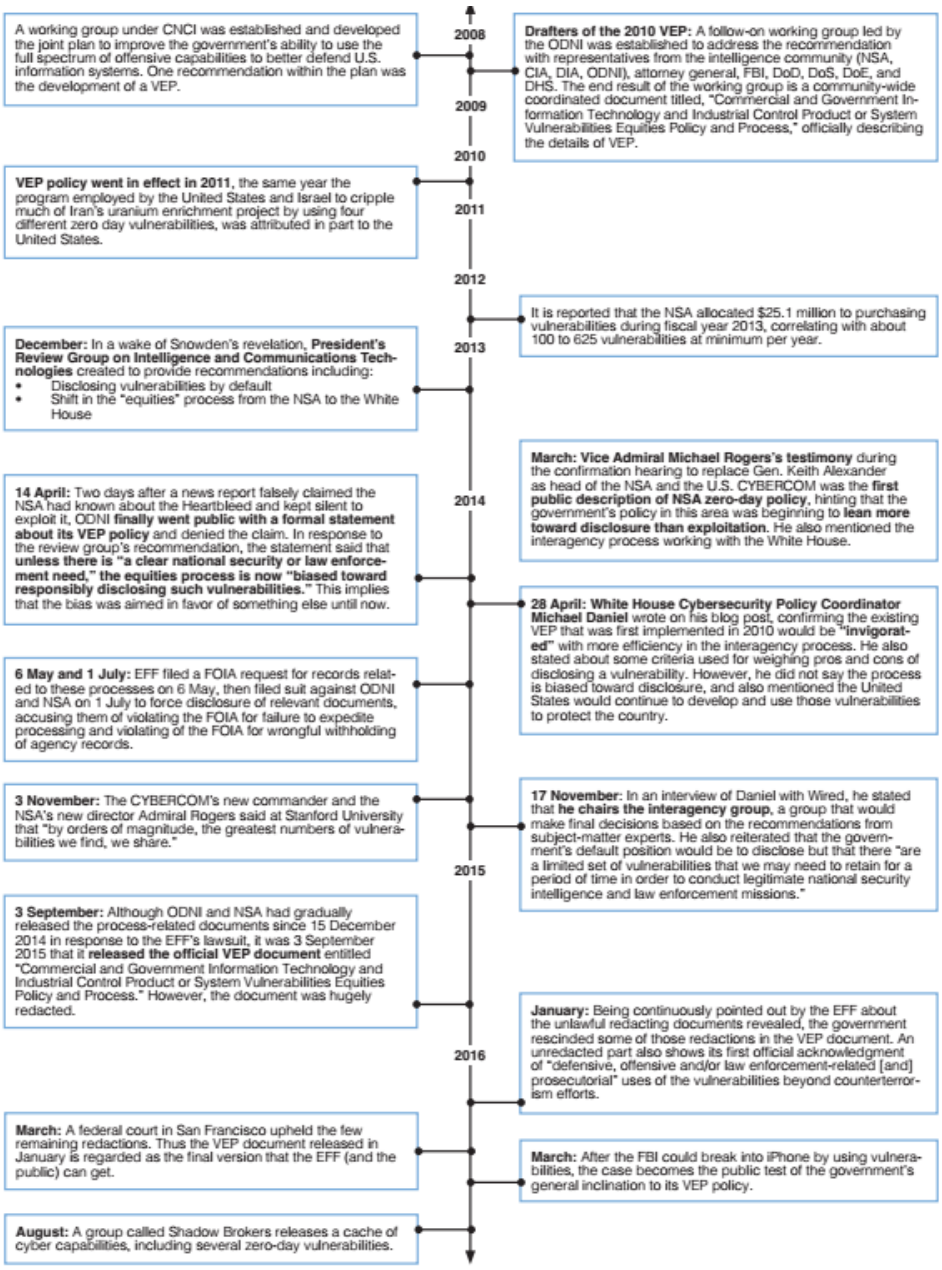


图 12-5 希利梳理的美国 VEP 政策发展过程

中国网络安全专家和安全厂商一直积极地探讨国家级网络威胁对网络安全秩序的破坏。

2013 年 6 月 11 日，在“新时代网络威胁之路”研讨会上，中国复旦大学国际关系与公共事务学院的沈逸教授作了题为“从三叶草到棱镜门——监控与美国网络安全战略”的

报告[7]，对美国国家监控行为进行了历史梳理，通过对美国从 20 世纪 40 年代以来的代表性情报监听案例“三叶草”行动（1945-1975）到 21 世纪初的“棱镜”项目的系统剖析，总结了美国监控背后的复杂因素及其对全球网络安全的影响和危害。

2015 年 6 月，中国反病毒大会在天津召开，安天发布大会报告“A^2PT 与‘准 APT’事件中的攻击武器”，报告首次将美国所发动的网络攻击称为 A^2PT 攻击（即高级的高级持续性威胁攻击）（见图 12-6）[8]。

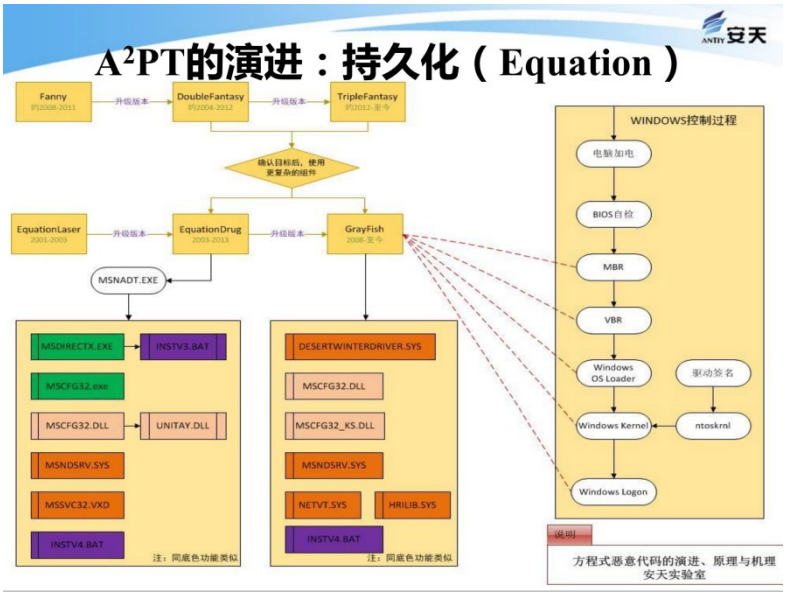


图 12-6 中国反病毒大会报告揭露方程式组织高级木马的原理结构

2016 年，安天在“中俄网络空间发展与安全论坛”作了名为“熊猫的伤痕”报告，分析中国遭到的多起高级持续威胁，特别披露了美国“方程式组织”对中国重点基础工业企业的攻击，并总结了其特点和能力（见图 12-7）[9]。

图 12-7 2016 年“中俄网络空间发展与安全论坛”技术报告“熊猫的伤痕”

2019 年，中国台湾安全公司 DevCore 的研究人员奥林奇·柴（Orange Tsia）和迈赫·常（Meh Chang）在黑帽大会发布“像 NSA 那样渗透进入公司内网”报告，展示了如何采用已曝光 NSA 手法（如“方程式组织”使用的），对 Fortinet 和 Pulse Secure 的 SSL VPN 进行未授权远程代码执行漏洞利用，（相对）轻松地攻入内网（见图 12-8）[10]。

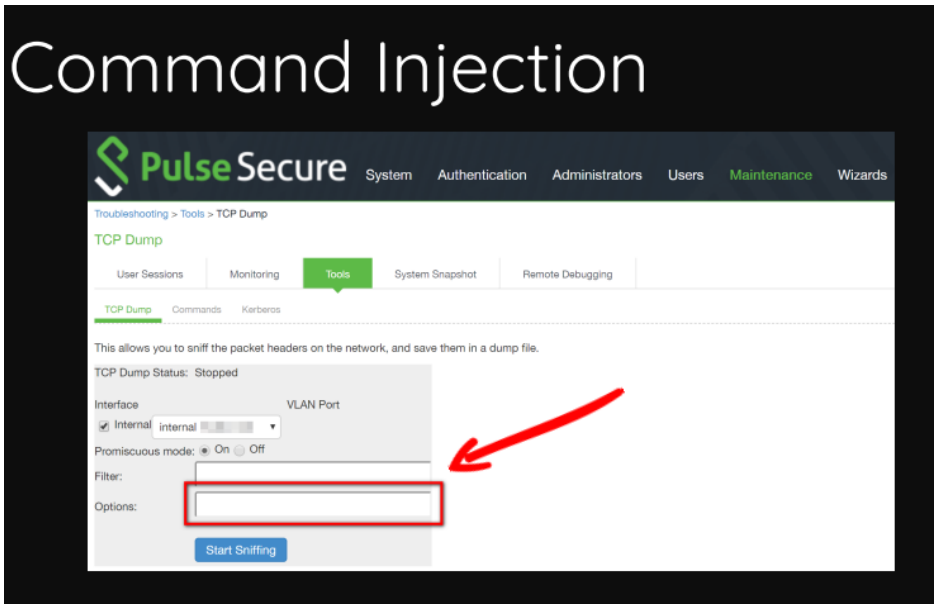


图 12-8 奥林奇·柴等展示的 Pulse Secure 漏洞利用后的命令注入

报告指出，SSL VPN 是各种规模的公司都广泛使用的内网与公网连接方式，而市场 VPN 厂商相对集中，NSA 早已热衷于发现并利用其中的漏洞。

（三） 小结

全球性网络安全挑战日益严峻，只有各国秉持开放合作的精神才能共建共享安全的网络空间，而国际论坛正是企业、学术交流的重要空间。过去十年来，通过广大安全厂商和学术人员在各种国际论坛上的不懈努力，美国利用技术优势操控和干预网络安全的野心和行为已越来越多地被暴露、被认识，并激励更多厂商和学术界的进一步研究和探索。

参考资料

[1] BlackHat. A Schedule Update. 2014. https://www.blackhat.com/latestintel/07212014-a-schedule-update.html

[2] Symantec. How a Computer Virus Foiled Iran’s Nuclear Program. 2012. https://cisac.fsi.stanford.edu/multimedia/forensic-dissection-stuxnet.

[3] ZDNET. Top NSA hacks of our computers. 2014. https://www.zdnet.com/pictures/top-nsa-hacks-of-our-computers/

[4] Kaspersky. Wave Your False Flags! Decption Tactics Muddying Attribution in Targeted Attacks. 2016. https://www.virusbulletin.com/virusbulletin/2016/11/vb2016-paper-wave-your-false-flags-deception-tactics-muddying-attribution-targeted-attacks

[5] Kaspersky. Walking in Your Enemy’s Shadow: When Fourth-Party Collection Becomes Attribution Hell. 2017.

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170728/Guerrero-Saade-Raiu-VB2017.pdf

[6] Columbia University. The U.S. Government and Zero-Day Vulnerabilities. 2016. https://jia.sipa.columia.edu/sites/default/files/attachments/Healey%20VEP.pdf

[7] 沈逸.从三叶草到棱镜门——监控与美国网络安全战略.新时代网络威胁之路研讨会.2013.

[8] 安天. A^2PT 与“准 APT”事件中的攻击武器. 中国反病毒大会. 2015.

[9] Antiy. The Panda’s Scar—The APT Attacks against China. 2016. https://www.antiy.com/response/20200304.html

[10] DevCore. Infiltrating Corporate Intranet Like NSA. 2019. https://i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-Like-NSA.pdf

第十三篇　限制和打压——美国泛化安全概念制裁他国网络安全厂商

近年来，为了维护其政治霸权、经济利益以及军事技术和能力优势，同时制裁具备技术竞争力的他国知名网络安全企业，美国泛化“国家安全”概念，将其作为遏制对手的万能牌，在任何需要的时机肆意打出，甚至不顾破坏国际秩序和市场规则，不惜损害包括美国在内的全球消费者利益。

（一）禁用卡巴斯基的软件产品

知名网络安全公司卡巴斯基是美国重点全方位打压的对象，其不仅是 NSA 制定“拱形”计划的头号目标，更成为产品被禁用的厂商。2017 年 9 月 13 日，美国国土安全部以卡巴斯基可能威胁美国联邦信息系统安全为由，要求所有联邦机构 30 天内查明其信息系统内所使用的卡巴斯基软件产品，90 天内卸载相关产品。美国百思买（Best Buy）等零售商也下架了卡巴斯基产品。特朗普政府时期曾授权允许商务部约束美国企业，禁止或限制他们与“外国对手”国家开展互联网、电信和科技等业务往来。具体到卡巴斯基公司，美国商务部有权禁止美国公民使用或购买其软件，或通过“联邦公报”中的规定禁止用户下载软件更新。2022 年美国政府进一步加强对卡巴斯基软件产品的国家安全审查力度，构陷卡巴斯基，称其反病毒软件具有计算机系统访问权限，可能会被用于从美国计算机中窃取敏感信息甚至篡改内容。

（二）运用实体清单制约中企发展

随着中国互联网科技的高速发展，更多中国公司在全球市场表现出强劲的竞争实力，对美国长期以来的网络霸权地位构成挑战。自奥巴马执政以来，美国政府对网络安全的重要性日渐重视，以“国家安全”“经济安全”等为名所采取的保护主义措施也日渐强硬。众所周知被美国商务部屡屡使用的“阳谋”手段，就是不断把具有自主创新技术实力的中国互联网科技企业纳入制裁“实体清单”。

美国商务部的“实体清单”就是一份制约对手涉美国贸易的黑名单，被列入清单是因为美国认为对方所掌握的技术、所拥有的能力已对美国海外利益和国家利益产生了足够威胁。自 2018 年中兴被制裁开始，维护“国家安全”成为美国把多个中国科技企业加入“实体清单”的理由。在 2020 年 5 月 22 日被美国商务部列入“实体清单”的中国公司及机构名单中，首次出现了网络安全企业——奇虎 360，理由是“具有采购相关物项用于中国军事最终用途的风险”[1]。2022 年 10 月 5 日，美国国防部根据《2021 财年国防授权法案》第 1260H 条公布了第二批“在美国经营的中国涉军公司”（Chinese Military Companies，CMC）实体清单，中国网络安全企业北京知道创宇信息技术股份有限公司与奇虎 360 上榜[2]。被列入 CMC 清单的公司暂无具体制裁措施，但根据美国

财政部规定，CMC 清单属于“禁投清单”，即禁止或限制投资清单。

（三）施压曝光美国攻击的他国网络安全企业

2015 年 6 月，自由斯诺登网（Edwardsnowden.com）披露了一份内部文件“轻松获胜: 利用信号情报来了解新病毒”（An Easy Win: Using SIGINT to Learn about New Viruses）[3], 介绍了美国、英国有关情报机构自 2007 年开始执行的“拱形”计划，主要对以卡巴斯基公司等全球知名反病毒公司与用户间的通讯为主要目标进行监控，以获取新的病毒样本及其他信息。文档还列举了计划展开监控的更多目标（“More Targets”），涵盖 23 家反病毒厂商，其中包括中国安全厂商安天。

2016 年 12 月 22 日，主要从事网络监控和管理的美国 NetScout 公司发文对中国网络空间安全协会进行歪曲和抹黑，认为安天如同卡巴斯基一样发布“方程式组织”分析报告，揭露 APT 活动，是“中国反 APT”代言人（见图 13-1）[4]。


Non-Government Organization in Support of Government Hopes

By Neal Dennis on 12/22/2016.
Posted in advanced persistent threats, analysis, Interesting Research, Malware, threat analysis.

Red Team analysis is the process of viewing a situation from the perspective of an adversary thus providing insights beyond those that might otherwise be limited by normative biases. This blog provides an assessment of one company's foray into the popular APT outing trend in the context of China's cyber buildup and what that could mean for future U.S. cyber espionage endeavors.

Antiy Labs – A New Mouthpiece?

Until recently, U.S. companies and Russian Kaspersky Labs have mostly led the charge in exposing APT related activities with a few other, predominately European, companies following suit. A Chinese anti-virus company, Antiy Labs, has now joined the party. They recently published a purported Equation Group APT related disclosure. Antiy Labs has published a limited amount of APT related research articles over the past three years but have not received the level of international press coverage that their western counterparts have.

图 13-1 美国 NetScout 公司对安天等中国企业的分析

2022 年 2 月 17 日，美国国会“美中经济与安全审查委员会”（USCC）召开 2022 年年度报告周期第二次听证会[5]，主题为“中国的网络空间能力：网络战、间谍活动以及对美国影响”，研讨重点聚焦网络安全领域，专题评估中国的网络能力及其对美国安全和利益的影响。与会网络安全专家认为，中国拥有成熟的大规模防御能力，能够探测到美西方的网络空间行动。听证会特别点名了两家中国网络安全公司：安天和奇虎 360，因其公开发表了对 NSA 和 CIA 网络空间行动的分析。美国专家指出，安天和奇虎 360 是中国最资深的两家反病毒公司，他们发布的信息能够让民众更加信服（见图 13-2）[5]。由此可见，美国对中国能力型网络安全企业有清晰的认识，而且始终在关注并分析其可能对美国产生的威胁以及美国可能面临的挑战。未来，或将会有更多的制约手段针对类似企业。

Two Chinese cyber security firms in particular: Antiy Labs[59] and Qihoo360[60], have openly published analyses of NSA and CIA cyber operations. While these reports are heavily bolstered by the Shadowbrokers and Vault7 leaks respectively and do not provide enough information for independent researchers to validate their claims, Antiy and Qihoo are two of the oldest antivirus companies in China and therefore likely have the data visibility that would make these claims credible. **Chinese MSS contractors have also been able to observe and recreate U.S. made cyberweapons**: one contractor was found using NSA hacking tools a full year before the tools were made public via the Shadowbrokers leak, suggesting that the contractor observed the hacking tools being used against Chinese targets and recreated the tool from those observations.[61]

图 13-2 美国会听证会点名关注安天和奇虎 360

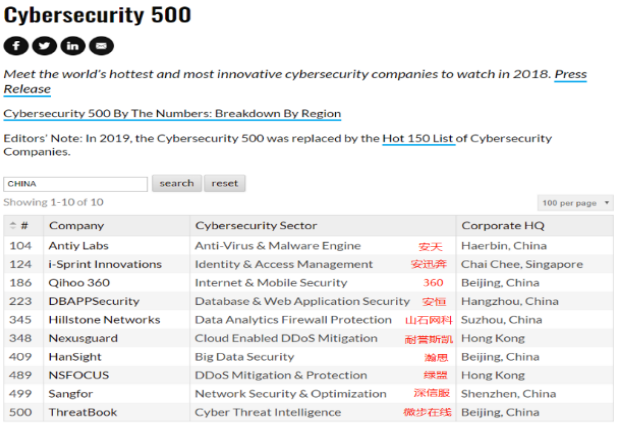
（四）对中国网络安全企业另册排名并据此打压

随着中国互联网科技企业的技术发展，部分中国网络安全厂商的国际知名度和影响力也在逐渐扩大。Cybersecurity

Ventures 是全球知名投资咨询机构，主要从事网络安全市场调研和信息搜集，专注于网络安全行业的初创公司和新兴公司。Cybersecurity Ventures 对网络安全创新 500 强榜单的排名，是对全球数千家网络安全厂商进行独立评估，其声称上榜的都是“最热门、最具创新力”的企业[6]。2019 年之前，Cybersecurity Ventures 发布的网络安全 500 强名单中，安天（Antiy Labs）、山石网科（Hillstone Networks）、安恒（DBAppSecurity）、奇虎 360（Qihoo 360）等中国网络安全企业都曾上榜（见图 13-3[6]、13-4[7]）。但榜单上美国企业近 300 家，而中国企业一直不超过十家，不能真实体现中国网络安全产业的能力。

vendor		specialty
95. Antiy Labs	安天	anti-virus engine & solution
142. Hillstone Networks	山石网科	data analytics firewall protection
314. DBAppSecurity	安恒	web application & database security
412. Vkansee	印象认知	fingerprint sensors for mobile security

图 13-3 2015 年 Cybersecurity Ventures 500 强上榜的中国厂商（部分）



Cybersecurity 500

Meet the world's hottest and most innovative cybersecurity companies to watch in 2018. Press Release

Cybersecurity 500 By The Numbers: Breakdown By Region

Editors' Note: In 2019, the Cybersecurity 500 was replaced by the Hot 150 List of Cybersecurity Companies.

CHINA search reset

Showing 1-10 of 10 100 per page

#	Company	Cybersecurity Sector		Corporate HQ
104	Antiy Labs	Anti-Virus & Malware Engine	安天	Haerbin, China
124	i-Sprint Innovations	Identity & Access Management	安讯奔	Chai Chee, Singapore
186	Qihoo 360	Internet & Mobile Security	360	Beijing, China
223	DBAPPSecurity	Database & Web Application Security	安恒	Hangzhou, China
345	Hillstone Networks	Data Analytics Firewall Protection	山石网科	Suzhou, China
348	Nexusguard	Cloud Enabled DDoS Mitigation	耐赛斯凯	Hong Kong
409	HanSight	Big Data Security	瀚思	Beijing, China
489	NSFOCUS	DDoS Mitigation & Protection	绿盟	Hong Kong
499	Sangfor	Network Security & Optimization	深信服	Shenzhen, China
500	ThreatBook	Cyber Threat Intelligence	微步在线	Beijing, China

图 13-4 2018 年 Cybersecurity Ventures 500 强上榜的中国厂商（部分）

自 2019 年起，Cybersecurity Ventures 的“网络安全 500 强”名单被“网络安全公司热门 150 强名单”所取代，但其中全部为欧美厂商，中国网络安全企业被其另外单独排名[8]。2020 年 9 月，Cybersecurity Ventures 则发布中国最热门、最具创新性的“中国网络安全公司”名单，包括安天、奇虎 360、奇安信、山石网科、安恒、深信服、微步在线等 20 家企业 [9]。在 2022 年 2 月 17 日美国会“美中经济与安全审查委员会”（USCC）举行的“中国的网络空间能力：网络战、间谍活动以及对美国影响”听证会中[5]，与会专家称“中国的民间商业实体大量参与了中国的网络运营”，明确建议“国会可以不只是点名羞辱，而是要求商务部或财政部分别将与网络运营有关的中国机构列入实体名单和制裁名单，以此提高这些中国网络空间威胁组织实施网络攻击的成本”。听证会专家对中国网络安全产业情况的注解，则正是依据 Cybersecurity Ventures 发布的中国最热门、最具创新力的“中国网络安全公司”名单[10]。

（五）小结

近年来，美国凭借自身技术实力和市场能力建立起来的霸权和优势受到了严峻挑战。为尽快全面遏制对手，美国政府选择运用“国家安全”这一“万能胶”来加固各种壁垒，通过打击并遏制竞争对手，巩固其在全球互联网市场的领导地位。同时，美国将网络安全与经济、贸易、科技、意识形

态等议题挂钩，作为其发起贸易战、科技战的有利借口，并使得网络安全议题空前泛化和政治化。以安全议题为掩护实施保护主义战略，对美国和五眼联盟以外的安全企业进行打压遏制，或许能够暂时维持美国的霸权和利益，但其推行“美国优先”的单边主义行为，必将最终损害其国家信誉和长远发展。

参考资料

[1] Department of Commerce. Commerce Department to Add Two Dozen Chinese Companies with Ties to WMD and Military Activities to the Entity List. 2020. https://2017-2021.commerce.gov/news/press-releases/2020/05/commerce-department-add-two-dozen-chinese-companies-ties-wmd-and.html

[2] DoD. DoD Releases List of Peoples Republic of China Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021. 2022. https://www.defense.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/

[3] Edward Snowden. An Easy Win: Using SIGINT to Learn about New Viruses. 2015. https://edwardsnowden.com/wp-content/uploads/2015/06/project-camberdada.pdf

[4] NETSCOUT ASERT Team. Non-Government Organization in Support of Government Hopes. 2016. https://www.netscout.com/blog/asert/non-government-organization-support-government-hopes

[5] USCC. China’s Cyber Capabilities: Warfare, Espionage, and Implicaitons for the United States. 2022. https://www.uscc.gov/sites/default/files/2022-2/February_17_2022_Hearing_Transcript.pdf

[6] CRN. The full Cybersecurity 500 list. 2015
https://www.crn.com.au/news/the-full-cybersecurity-500-list-401442

[7] Cyber security ventures. Cybersecurity 500 by the Numbers: Breakdown by Region. 2018.
https://cybersecurityventures.com/cybersecurity-500-by-the-numbers-breakdown-by-region/

[8] Cybercrime Magazine. China Cybersecurity Companies. 2018.
https://cybersecurityventures.com/china-cybersecurity-companies/

[9] Cybersecurity Ventures. China Cybersecurity Companies. 2020.
https://cybersecurityventures.com/china-cybersecurity-companies/

[10] Cybersecurity Ventures. The Hot 150 Cybersecurity Companies To Watch In 2021. 2021.
https://cybersecurityventures.com/cybersecurity-500/

结束语

美国以 NSA、CIA 等为代表的情报机构和以网络空间司令部为统领的网络空间作战力量，拥有全球最大规模的网络攻击团队、最庞大的支撑工程体系与制式化的攻击装备库、最强大的漏洞采集和分析挖掘能力以及关联资源储备，支撑进行最危险和最活跃的全球网络行动。美国建设了包括“湍流”等在内的数十个大型情报作业工程体系，涵盖了数据获取体系和网络入侵攻击两大能力集合。数据获取和攻击能力覆盖全球，其中包括：借助“码头”“主干道”等系统获取网络运营商和全球海底光缆等的数据；凭借“棱镜”作为超级接口，对美国主要互联网和 IT 厂商数据全量检索查询；结合其他美方窃取的各类信息，构成了全球的目标画像和网络地形绘制能力。同时，利用标准和供应链顶层优势，还在加密标准中植入后门，对密码体系进行长期系统性的操控和利用。这些手段的组合运用堪称开启了情报活动的上帝模式。

“大到无形”，美国的作业行动具有装备体系覆盖全场景、漏洞利用工具和恶意代码载荷覆盖全平台、持久化能力覆盖全环节的特点，已经成为了全球网络安全的最严重威胁。美国把自身霸权凌驾于他国主权安全之上，肆意发动网络攻击，严重威胁了他国安全，破坏了人们对网络技术的信任，更对全球政治、外交生态环境造成极大影响和破坏。这些信息的曝光，同时也重挫了世界各国对美国产品及服务的信任。

全球各国今天能完整看到这些，不只是依靠斯诺登、“影子经纪人”等的爆料，更是全球网络安全界包括企业、高校、研究组织和个人长期跟踪分析的结果。过去十余年，这段分析、曝光揭露美国情报机构活动的历史是一个复杂漫长的过程。

起初，大家只是从魔鬼的脚印看到脚趾。全球网络安全厂商对“震网”“毒曲”“火焰”等病毒的分析，都基本建立在漏洞原理分析、样本逆向分析，以及样本作用机理复盘之上，逐渐解析出这些病毒的同源相关性，以及相同的幕后黑手——美国情报机构。但是，分析中缺乏更深远的体系化思考，仍把 APT 攻击甚至 A^2PT 攻击，作为一种技术意义威胁类型来进行对抗。

随着斯诺登事件、“影子经纪人”和维基解密事件陆续将美国情报机构监听全球、无差别网络攻击以及污染加密通讯标准等恶行曝光，基于这些珍贵的资料线索，在全球网络安全界的逐步跟进研究下，美国超强的网络空间作业能力体系彻底浮出水面。

为了撰写这份报告，中国网络安全产业联盟（CCIA）累计整理了来自数十家安全企业、高校和个人的近千份研究成果。我们深深感到，正是如此多的机构、如此多的人、如此大量的努力，才能让人类看到这个“大到无形”魔鬼的全貌。我们想起了鲁迅先生的名言，“人类血战前行的历史，正如

煤的形成，当时用大量的木材，结果却只是一小块”。每一个在这个过程中做出了努力的组织、机构和个体，都值得给与尊重和敬意。

而在这一漫长而艰辛的研究分析过程中，全球网络安全产业的态度也发生了巨变。曾在“震网”事件中充分深度分析的赛门铁克、迈克菲等美国安全厂商如今对美国的网络攻击闭口不言；欧洲曾非常繁荣的反病毒产业体系，多年来在美国资本不断渗透控股并购下，本地规模性标志企业逐渐凋零。只有卡巴斯基，在多年打压下仍倔强而孤独地支撑着欧洲网络安全厂商的荣光。而中国网络安全企业和产业在这个斗争过程中，尽管也面临着巨大的压力，但正在不断做大做强。

全球网络空间处在一个战略性的十字路口。受困于一个黑暗的单极世界，还是参与构建光明的人类网络空间命运共同体，这对全球网络安全界是一个历史性的选择。

附录：相关大事记

【2007 年】

8 月，美国网络安全研究人员 Dan Shumow 和 Niels Ferguson 发布“NIST SP 800-90 双椭圆曲线 DRBG 中有可能存在一个后门”。

【2010 年】

8 月，美国赛门铁克发布“Stuxnet 第一个已知的工业控制系统 Rootkit”。

9 月，中国安天发布“对 Stuxnet 蠕虫攻击工业控制系统事件的综合分析报告”。

10 月，美国赛门铁克发布“W32.Stuxnet 档案”。

【2011 年】

10 月，匈牙利 CrySyS 发布“Duqu：发现类似 Stuxnet 的恶意软件”。

【2012 年】

5 月，俄罗斯卡巴斯基发布“The Flame:问与答”。

5 月，匈牙利 CrySyS 发布“sKyWIper：针对目标攻击的复杂恶意软件”。

8 月，俄罗斯卡巴斯基发布“Gauss：异常分布”。

【2013 年】

6 月 5 日，英国《卫报》揭露 NSA 监听事件。

6 月 6 日，斯诺登曝光 NSA“棱镜”项目。

9 月 5 日，英国《卫报》报道“美英间谍机构如何打败互联网隐私和安全”。

9 月 6 日，美国《纽约时报》报道“NSA 能够骗过网上基本隐私保护”。

9 月 10 日，美国国家标准与技术研究院重启 SP 800-90A 标准的审查期。

11 月，美国政府禁止网络安全专家赴华参加信息安全论坛（ISF2013）。

11 月，德国 IT 专家 Ralph Langner 在《外交政策》上发布“‘震网’病毒的秘密双胞胎”。

11 月，德国 IT 专家 Ralph Langner 发布“技术分析：‘震网’病毒的制造者想要得到什么”。

12 月 21 日，英国路透社报道“连接美国国家安全局和安全产业先锋的秘密合同”。

12 月 27 日，前 Tor 核心程序员 Jacob Appelbaum 在第 30 届混沌通信大会曝光 NSA 的部分“间谍工具库”。

【2014 年】

1 月，InfoSec 发布“被称为上帝模式恶意软件的美国国家安全局 BIOS 后门第一部分：DEITYBOUNCE”。

【2015 年】

2 月，维基解密发布“方程式组织是如何作恶的？我们如何避免被攻击？”。

2 月，俄罗斯卡巴斯基发布“方程式组织：问与答”“方程式组织：恶意软件银河的死星”。

3 月，中国安天发布“修改硬盘固件的木马 探索方程式（EQUATION）组织的攻击组件”。

4 月，中国安天发布“方程式（EQUATION）部分组件中的加密技巧分析”。

6 月，斯诺登披露美国国家安全局内部文件“轻松的胜利：利用 SIGINT 来了解新病毒”。

6 月，俄罗斯卡巴斯基发布“DUQU 2.0 的技术细节”。

6 月 22 日，美国媒体“拦截者”“连线”“福布斯”同时曝光 NSA 的“拱形”计划。

6 月 24 日，NIST 发布修订的 SP 800-90A，去掉了其中的 Dual_EC_DRBG。

7 月，荷兰埃因霍芬理工大学发布“Dual EC：标准化后门”。

【2016 年】

8 月，“影子经纪人”曝光 NSA“方程式组织”网络攻击装备。

8 月，“黑客新闻”报道“方程式组织网络武器拍卖”。

11 月，中国安天发布“从“方程式”到“方程组” EQUATION 攻击组织高级恶意代码的全平台能力解析”。

10 月，Cybersecurity Review 发布“影子经纪人揭示了被美国国家安全局黑客攻击的服务器列表”。

【2017 年】

3 月 7 日，维基解密开始发布“七号军火库”，披露 CIA 网络攻击武器的秘密文件。

4 月 14 日，“影子经纪人”发布“方程式组织”的部分工具文件。

4 月 16 日，中国国家信息安全漏洞共享平台（CNVD）发布“关于加强防范 Windows 操作系统和相关软件漏洞攻击风险的情况公告”。

9 月，美国国土安全部要求所有联邦机构信息系统禁用卡巴斯基软件产品。

【2018 年】

2017 年 12 月至 2018 年 11 月，中国安天在《网信军民融合》杂志连载 12 篇“美国网络空间攻击与主动防御能力解析”系列文章。

10 月，俄罗斯卡巴斯基对框架 DanderSpritz 中的 DarkPulsar 进行了深度分析。

【2019 年】

6 月，中国安天发布“‘方程式组织’攻击 SWIFT 服务提供商 EastNets 事件复盘分析报告”。

9 月，中国安天发布“‘震网’事件的九年再复盘与思考”。

【2020 年】

2 月 11 日，美国《华盛顿邮报》等多家媒体曝光瑞士加密设备厂商 Crypto AG 公司被美国德国情报机构操控。

5 月 22 日，美国商务部将包括中国网络安全厂商 360 在内的 24 家中国公司列入实体清单。

【2022 年】

2 月 17 日，美国参议院召开关于“中国的网络能力：战争、间谍活动和对美国的影响”的听证会，点名两家中国网络安全厂商：“安天实验室”与“奇虎 360”。

2 月 23 日，中国奇安信发布“Bvp47-美国 NSA 方程式的顶级后门”。

3 月 2 日，中国 360 发布“网络战序幕：美国国安局 NSA（APT-C-40）对全球发起长达十余年无差别攻击”。

3 月 15 日，中国安天发布“从‘NOPEN’远控木马浮出水面看美国网络攻击装备体系”。

9 月 5 日，中国国家计算机病毒应急处理中心发布“西北工业大学遭美国 NSA 网络攻击事件调查报告（之一）”。

9 月 27 日，中国国家计算机病毒应急处理中心发布“西北工业大学遭美国 NSA 网络攻击事件调查报告（之二）”。

10 月 5 日，美国国防部公布第二批“在美国经营的中国涉军公司”（CMC）实体清单，“北京知道创宇信息技术股份有限公司”与“奇虎 360”被列入清单。