美相关 APT 组织分析报告

360 数字安全集团 编制

目录

一、概述

“APT”（高级持续性攻击）是一种针对性、隐蔽性、持续性极强的网络攻击行为。现已发现的绝大多数 APT 组织都具有国家或政府背景，相关攻击行为通常由某个与特定国家政府关联的实体机构具体实施。APT 攻击的主要目标不是普通个体，而是特定的组织机构，包括政府、大学、医疗、企业、科研甚至重要信息基础设施运维单位等不同类型的重要机构。

过去数年，360 公司持续跟踪美国 APT 组织及其活动情况，发现美国顶尖 APT 组织对全球各国（包括美国盟友）的政府机构、重要组织和信息基础设施实施了复杂、精密、持续性的 APT 攻击行动。本报告针对美国代表性 APT 组织架构、攻击武器、实施过程等展开分析，并结合真实案例，全面印证了美 APT 组织凭借高度自动化、工程化的先进网络武器装备发起无差别网络攻击，给全球带来无穷的安全隐忧。

二、APT-C-16（索伦之眼）

索伦之眼（ProjectSauron）组织，又名 Strider、Sauron、APT-C-16、神行客，最早活跃于 2011 年，并一直活跃至 2016 年 8 月。

根据英国《每日邮报》媒体报道，该组织攻击过的目标包括中国、俄罗斯、比利时、伊朗、瑞典、卢旺达等 30 多个国家，以窃取敏感信息为主要目的。受该组织攻击的机构包括国防部门、大使馆、金融机构、政府部门、电信公司、军事和基础设施领域以及科技研究中心等。

1．组织归因分析

2016 年 8 月，赛门铁克公司披露了一个针对中国、俄罗斯等国家发动高级攻击的 APT 组织。随后，卡巴斯基也发布报告，针对该组织披露了更多详细分析资料。因在分析追踪文件时，发现其代码中带有 Sauron 字符，所以命名为索伦之眼（Project Sauron），其不仅是一个顶级黑客组织，而是一个拥有精密技术的顶级间谍模型平台。

经比对分析，确认该组织与 360 高级威胁情报中心独立截获的境外 APT 组织 APT-C-16 为同一组织。在 360 长期跟踪并对索伦之眼组织行动进行归属分析过程中，发现其与美国几大关联证据：

证据一、惯性语言的使用暴露所属国家：

索伦之眼组织攻击过程使用的语言、代码文本、关键模块输出均为英文。此外，索伦之眼在模块开发中使用“cruft”单词，该词语很少被非母语人士使用。其首次出现约在 1958 年，常被麻省理工学院（MIT）科技铁路模型俱乐部（TMRC）的学生们用在“垃圾”的意义上。

证据二、关键技术特征与美制造的恶意病毒存在相似：

索伦之眼组织攻击目标时使用了一种名为“Remsec”的高端恶意软件。而 Remsec 被发现与 2012 年 5 月卡巴斯基首次发现的超级电脑病毒 Flame 病毒(火焰病毒)存在诸多技术相似点。

Remsec 与 Flame 病毒的技术上的相似点包括：都采用 Lua 模块编写木马;盗取数据的方式多种多样;木马程序异常复杂;使用多种加密技术和数据传输技术;木马本身具有安全删除文件的能力;具备隔离网络文件窃取能力;受害者大多具有政治因素。

卡巴斯基、赛门铁克、360 公司相关技术报告研判的互相印证表明：Remsec 与 Flame 病毒疑似是师出同门，是由美国政府研发或资

助开发用于对伊朗等国家发起网络攻击的尖刀利器。

2．攻击武器

索伦之眼攻击目标所使用的 Remsec 恶意软件是一款技术含量很高的远程控制软件，主要用来暗中监视和控制目标。这种软件能够在受感染计算机上打开后门，记录用户点击的按键，并盗取相关文件。其攻击武器具备三大特征：

特征一：Remsec 恶意软件率先采用模块化设计，具备不同功能的模块之间作为一个框架整体协同工作，使攻击者能够完全控制受感染的计算机，从而允许他们跨网络移动、窃取数据并根据需要部署自定义模块。

特征二：Remsec 恶意软件具有强“隐身”性。它的几个组件采用可执行 blob（二进制大型对象）的形式，这对于传统防病毒软件来说更难以检测。除此之外，该恶意软件的大部分功能都是通过网络部署的，这意味着它仅驻留在计算机的内存中，并且从不存储在磁盘上，使得其更难以检测。索伦之眼整个攻击过程高度隐蔽，且针对性极强，对特定目标采用定制的恶意程序或通信设施，不会重复使用相关攻击资源。

特征三：索伦之眼武器工程化、复杂度、成熟性之高远非个体、游兵散将制造，背后需要大量人力、财力、技术资源投入开发，或为国家力量支持的高端网络武器开发使用项目。

总之，索伦之眼凭借超强恶意软件 Remsec，攻击方式、攻击效果和攻击隐蔽性等方面在当时具有领先能力，属于顶级 APT 组织。

3．攻击案例

2016 年 8 月，赛门铁克公司在报告中披露，自 2011 年起，索伦之眼攻击了中国、比利时、俄罗斯和瑞典的七个组织，包括位于俄罗斯的多个组织和个人、中国的一家航空公司、瑞典一个未公开的组织及比利时国内的一个大使馆。

2016 年 8 月，卡巴斯基公司在报告中披露，2015 年 9 月其反定向攻击技术遭遇了一次未知的攻击。可疑模块是一个可执行库，加载到 Windows 域控制器(DC)的内存中该库已注册为 Windows 密码过滤器，并且可以访问明文形式的敏感数据。经过研究发现索伦之眼大规模活动迹象，主要针对多国政府实体进行攻击行动。

三、APT-C-39（CIA）

美国中央情报局（Central Intelligence Agency，简称 CIA）是美国联邦政府主要情报机构之一，总部位于美国弗吉尼亚州兰利。

其主要业务范围涉及：收集外国政府、公司和公民情报信息；综合分析处理其他美国情报机构收集的情报信息；向美国高层决策者提供国家安全情报和安全风险评估意见；根据美国总统要求组织实施和指导监督跨境秘密活动等。长期以来，美国中央情报局（CIA）在世界各地秘密实施“和平演变”和“颜色革命”，持续进行间谍窃密活动。进入二十一世纪以来，互联网的快速发展给美国中央情报局（CIA）的渗透颠覆和捣乱破坏活动提供了新的机遇，全球各地使用美国互联网设备和软件产品的机构和个人成为美国中央情报局（CIA）的傀儡“特工”，帮助该机构迅速成为网络谍报战中的耀眼“明星”。

1．组织架构

公开资料显示，CIA 下设情报处（DI）、秘密行动处（NCS） 、科技处（DS&T）、支援处（DS）四个部门。

情报处（DI）：

情报部是对情报信息的接收、诠释、分析和加工部门，主要任务是编写有关国际政治、经济、科技和军事方面的“动态情报”以及供总统和决策班子参考的文件，如供总统阅读的《每日要闻》、部级官员参考的《国家情报日报》、《国家情报简报》和一些专题性周刊；另一任务是对公开资料的研究，撰写定期的专题性研究报告。该部下设 8 个室及 2 个中心，有 3500 多名工作人员。

秘密行动处（NCS）：

是中情局内最大的情报搜集部门，主要负责向世界各地派遣间谍，参与、影响和颠覆外国政府的隐藏行动以及反间谍工作等，至少有 6000 多名工作人员，其中约有 4800 特工人员经常派驻国外，其中 2/3

人员从事谍报、反间谍和联络等情报工作，其余人员主要从事隐藏行动；大多数以国务院或国防部代表的官方合法身份作保护，从事联络、谍报及反谍报活动。

科技处（DS&T）：

该部成立于 1963 年，有工作人员 1300 多人。下设 6 个业务处（中心），即研究开发处、研究与工程设计处、外国广播收讯处、技术服务处和国家图像判读中心。部长由主管科技的副局长兼任。

该部的职责是进行基础研制工作，即对技术系统的研究、开发与使用业务（包括间谍卫星的操纵以及对尖端技术领域进行分析论证）编写科技情报。此外，它还负责中情局的大部分电子资料处理业务，并对各科学领域进行广泛的研究。

支援处（DS）

该部工作人员约 5000 人，部长由主管行动的副局长兼任。下设 8 个业务处，即卫生处（医务）、安全处（保卫）、训练与教育处、财务处、后勤处、人事处、信息处和通讯处。

该部是中情局的行政治理部门，主要是协助行动部进行隐藏行动，还为科学服务部和情报部提供各种形式的支援，并负责通讯、总务和训练等方面工作。

2．组织归因分析

2020 年 3 月，360 公司分析论证了一起美国中央情报局攻击组织(APT-C-39)对中国关键领域进行长达 11 年渗透的网络攻击事件。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多个单位均遭到不同程度的攻击，并主要集中在北京、广东、浙江等

省份。360 公司通过一系列证据，确认他们发现的 APT-C-39 网络攻击确系来自美国中央情报局 CIA。

具体关联证据如下：

证据一：APT-C-39 组织使用了大量 CIA"Vault7(穹窿 7)"项目中的专属网络武器。研究发现，APT-C-39 组织多次使用了 Fluxwire，Grasshopper 等 CIA 专属网络武器针对我国目标实施网络攻击。通过对比相关的样本代码、行为指纹等信息，可以确定该组织使用的网络武器即为“Vault7（穹窿 7）”项目中所描述的网络攻击武器。

证据二：APT-C-39 组织大部分样本的技术细节与“Vault7（穹窿 7）”文档中描叙的技术细节一致。360 安全云分析发现，大部分样本的技术细节与“Vault7（穹窿 7）”文档中描叙的技术细节一致，如控制命令、编译 pdb 路径、加密方案等。这些是规范化的攻击组织常会出现的规律性特征，也是分类它们的方法之一。所以，确定该组织隶属于 CIA 主导的国家级黑客组织。

证据三：早在“Vault7（穹窿 7）”网络武器被维基解密公开曝光前，APT-C-39 组织就已经针对中国目标使用了相关网络武器。2010 年初，APT-C-39 组织已对我国境内的网路攻击活动中，使用了“Vault7（穹窿 7）”网络武器中的 Fluxwire 系列后门。这远远早于 2017 年维基百科对“Vault7（穹窿 7）”网络武器的曝光。这也进一步印证了其网络武器的来源。在通过深入分析解密了“Vault7（穹窿 7）”网络武器中 Fluxwire 后门中的版本信息后，360 安全云将 APT-C-39 组织历年对我国境内目标攻击使用的版本、攻击时间和其本身捕获的样本数量

进行统计归类，如下表：

从表中可以看出，从 2010 年开始，APT-C-39 组织就一直在不断升级最新的网络武器，对我国境内目标频繁发起网络攻击。

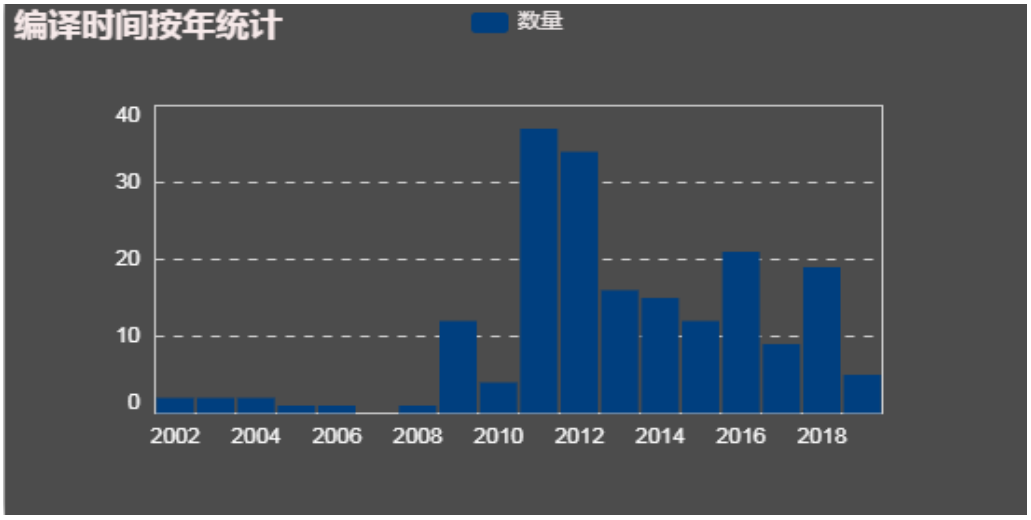
证据四：APT-C-39 组织使用的部分攻击武器同 NSA 存在关联。WISTFULTOLL 是 2014 年 NSA 泄露文档中的一款攻击插件。在 2011 年针对我国某大型互联网公司的一次攻击中，APT-C-39 组织使用了 WISTFULTOOL 插件对目标进行攻击。与此同时，在维基解密

Version	Samples	Capture time
Release 2.1.3 (April 15, 2011).	1	2011/5/25.
Release 2.2.0 (May 4, 2011).	5	2011/4/26-2011/10/25.
Release 2.2.1 (July 28, 2011).	20	2011/8/19-2012/2/27.
Release 2.2.3 (January 17, 2012).	16	2012/3/26-2012/6/4.
Release 2.3.0 (May 23, 2012).	4	2012/11/20-2013/4/9.
Release 2.4.1 (February 28, 2013).	1	2013/6/6.
Release 3.0.0 (August 23, 2013).	1	2013/10/21.
Release 3.1.0 (February 20, 2014).	1	2014/5/14.
Release 3.2.1 (August 18, 2014).	2	2015/3/20.
Release 3.3.0 (February 25, 2015).	3	2015/3/27-2015/4/21.
Release 3.3.1 (May 7, 2015).	2	2015/5/20-2015/8/4.
Release3.5.0(November13, 2015).	3	2016/9/16-2016/12/22.

泄露的 CIA 机密文档中，证实了 NSA 会协助 CIA 研发网络武器，这也从侧面证实了 APT-C-39 组织同美国情报机构的关联。

证据五：APT-C-39 组织的武器研发时间规律定位在美国时区。根据该组织的攻击样本编译时间统计，样本的开发编译时间符合北美洲的作息时间。

恶意软件的编译时间是对其进行规律研究、统计的一个常用方法，通过恶意程序的编译时间的研究，我们可以探知其作者的工作与作息规律，从而获知其大概所在的时区位置。下表就是 APT-C-39 组织的编译活动时间表（时间我们以东 8 时区为基准），可以看出该组织活动接近于美国东部时区的作息时间，符合 CIA 的定位。（位于美国弗吉尼亚州，使用美国东部时间。）



综合上述技术分析和数字证据，我们完全有理由相信：APT-C-39 组织隶属于美国，是由美国情报机构参与发起的攻击行为。

3．攻击武器

2017 年 3 月，“维基解密”曝光了“Vault7”秘密黑客项目，在一份被称为“Year Zero”的档案中，披露了 8716 份来自“美国中央情报局”（CIA）黑客部队的文件。这犹如一颗重磅炸弹，震惊世界。

据披露的文件显示，“Vault7”黑客工具是美国中央情报局（CIA）从事网络战的重要武器，能够结合多种计算机病毒、恶意软件、木马程序，对苹果、安卓手机系统、Windows 电脑操作系统进行攻击。

丢下这颗重磅炸弹的是美国中央情报局（CIA）的前雇员约书

亚·亚当·舒尔特(Joshua Adam Schulte)。

约书亚 1988 年 9 月出生于美国德克萨斯州拉伯克，毕业于德萨斯大学斯汀分校，曾作为实习生在美国国家安全局（NSA）工作过一段时间，于 2010 年加入美国中央情报局 CIA，在其秘密行动处（NCS）担任科技情报主管。

(国家秘密行动处(NCS)充当中央情报局秘密部门，是协调、去除冲突以及评估美国情报界秘密行动的国家主管部门。)

精通网络武器设计研发专业技术，又懂情报运作，约书亚成为 CIA 诸多重要黑客工具和网络空间武器主要参与设计研发者核心骨干之一。其中就包含“Vault7（穹窿 7）”CIA 这一关键网络武器。

2016 年，约书亚利用其在核心机房的管理员权限和设置的后门，拷走了“Vault7（穹窿 7）” 并“给到”维基解密组织，该组织于 2017 年将资料公布在其官方网站上。

2018 年，约书亚因泄露行为被美国司法部逮捕并起诉，2020 年 2 月 4 日，在联邦法庭的公开听证会上，检方公诉人认定，约书亚作为 CIA 网络武器的核心研发人员和拥有其内部武器库最高管理员权限的负责人，将网络武器交由维基解密公开，犯有“在中央情报局历史上最大的一次机密国防情报泄露事件”。

以上约书亚的个人经历和泄露的信息，为我们提供了重要线索，而其研发并由美国检方公诉人证实的核心网络武器“Vault7（穹窿 7）”，成为实锤 APT-C-39 隶属于美国中央情报局 CIA 的重要突破口。

据 360 跟踪发现，CIA 网络武器使用了极其严格的间谍技术规范，各种攻击手法前后呼应、环环相扣，现已覆盖全球几乎所有互联网和物联网资产，可以随时随地控制别国网络，盗取别国重要、敏感数据，而这无疑需要大量的财力、技术和人力资源支撑。其中代表性武器如下：

3.1 Fluxwire（磁通线）后门程序平台

一款支持 Windows、Unix、Linux、MacOS 等 9 种主流操作系统，和 6 种不同网络架构的复杂后门攻击行动管理平台，可将众多“肉鸡”节点组成完全自主运行的网状网络，支持自我修复、循环攻击和多路径路由。

3.2 Athena（雅典娜）程序

一款针对微软 Windows 操作系统的轻量级后门程序，由美国中央情报局（CIA）与美国 Siege Technologies 公司（2016 年被 Nehemiah

Security 收购）合作开发，可以通过远程安装、供应链攻击、中间人劫持攻击和物理接触安装等方式植入，以微软 Windows 服务方式驻留。所有攻击功能模块均以插件形式在内存中解密执行。

3.3 Grasshopper（蚱蜢）后门程序

一款针对微软 Windows 操作系统的高级可配置后门程序，可生成多种文件格式形式的（EXE，DLL，SYS，PIC）恶意荷载，支持多种执行方式，配以不同插件模块后，可隐蔽驻留并执行间谍功能。

3.4 AfterMidnight（午夜之后）后门程序

一款以微软 Windows 操作系统 DLL 服务形式运行的轻量级后门，它通过 HTTPS 协议动态传输、加载“Gremlins”模块，全程以加密方式执行恶意荷载。

3.5 ChimayRed（智美红帽）漏洞利用工具

一款针对 MikroTik 等品牌路由器的漏洞利用工具套件，配合漏洞利用可植入“TinyShell”等轻量级网络设备后门程序。

3.6 HIVE（蜂巢）网络攻击平台

“蜂巢”网络攻击平台由美国中央情报局（CIA）下属部门和美国著名军工企业诺斯罗普·格鲁曼（NOC）旗下公司联合研发，它为美国中央情报局（CIA）网络攻击团队提供一种结构复杂的持续性攻击窃密手段。它管理利用全球范围内数量庞大的失陷资产，组成多层动态跳板和秘密数据传输通道，7×24 小时向美国中央情报局（CIA）上传用户账户、密码和隐私数据。

CIA“Vault7（穹窿 7）”武器从侧面显示美国打造了全球最大网络武器库，而这不仅给全球网络安全带来了严重威胁，更是展示出该 APT 组织高超的技术能力和专业化水准。

4．攻击案例

间谍行动——CIA 长期秘密打造人工间谍和间谍武器

2014 年 12 月 21 日，“维基解密”网站发布两份美国中情局机密文件。这两份文件为在国外执行任务的特工“出谋划策”，教他们如何持假身份证件顺利入境。

2017 年 11 月，维基揭秘最新曝光的中情局网络间谍活动的秘密文件代号为“8 号保险库”。文件内容包括：为了隐瞒电脑病毒的来源，中情局研制出一款名叫“蜂巢”的非法源代码，可以将病毒伪装成其它组织和公司的恶意软件，从电脑中窃取机密。

窃听事件——CIA 秘密窃听全球 120 国

2020 年 2 月 11 日，《华盛顿邮报》和德国公共广播公司的联合调查，从上世纪 70 年代开始，美国中央情报局（CIA）和德国联邦情报局秘密收购了瑞士一家加密公司，利用其设备窃听了全球 120 个国家。对此，瑞士表示已经展开调查。

攻击渗透——CIA 对中国关键领域发起长达 11 年网络攻击渗透

2021 年 7 月 20 日，中国国家互联网应急中心数据显示，2020 年位于境外的约 5.2 万个计算机恶意程序控制服务器，控制了中国境内约 531 万台主机，就控制中国境内主机数量来看，美国及其北约盟国分列前三位。美国中央情报局的网络攻击组织 APT-C-39，曾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进行了长达 11 年的网络渗透攻击。

四、APT-C-40（NSA）

从 2008 年开始，360 安全云整合海量安全大数据，独立捕获了大量异常复杂的网络黑客攻击程序样本，经过长期分析跟踪并从多个受害单位实地取证，结合关联全球各国发布的威胁情报，以及对斯诺登事件、“影子经纪人”曝光事件的综合研究，确认这些黑客攻击程序样本属于美国国家安全局（NSA），进而证实 NSA 长期对我国开展了极为隐蔽的无差别黑客攻击行动，**最终将实施攻击行动的这些带有 NSA 背景的黑客组织单独编号为 APT-C-40。**

据“斯诺登”、“影子经纪人”披露，泄露的一系列 NSA 网络武器被他国特别是“五眼联盟”国家黑客广泛利用，造成了全球性的网络安全灾难。如“永恒之蓝”被“WannaCry”蠕虫病毒利用，在 2017 年攻击了中国和全球多个国家地区，给各国信息网络造成了严重危害。而 APT-C-40 组织则针对中国各行业龙头企业，政府、大学、医疗机构、科研机构，甚至关乎国计民生的重要信息基础设施运维单位等机构实施了长达十余年时间的秘密黑客攻击活动，窃取了海量重要数据，造成的潜在威胁难以评估。

1．组织架构

NSA 是完全隶属于美国军方的组织，它专注于电子情报和网络战。2013 年，前情报员斯诺登爆料了 NSA 的“棱镜计划”，揭示了 NSA 在全球范围内进行的大规模网络监听活动，包括对中国的监控。

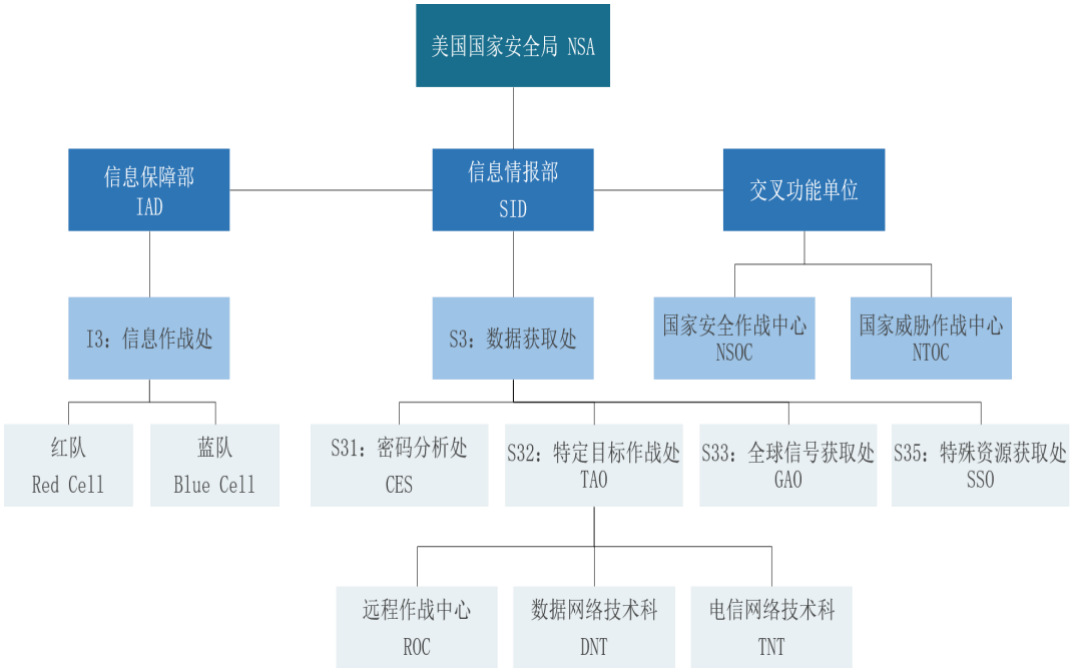
2016 至 2017 年间，“影子经纪人”（The Shadow Broker）公开揭露了属于 NSA 的大量网络攻击武器和机密办公文档。美国“The Intercept”网站结合爱德华·斯诺登（Edward Snowden，前 CIA 技术分

析员和美国国家安全局 NSA 承包商雇员）揭露的美国国家安全局（NSA）内幕情报，确认了斯诺登曝光的网络攻击武器确属美国国家安全局（NSA）。

2013 年至 2017 年间，中立网络权威人士、中立新闻媒体和坚定捍卫公民隐私权利的中立机构相继发布解读分析报告，确认网络上披露的所谓“NSA 网络武器和机密文档”全部属于 NSA。

根据爱德华·斯诺登（Edward Snowden）披露的内幕情报，仅在 2011 年，美国国家安全局（NSA）就组织实施了至少 231 次网络攻击行动，攻击行动的主要目标包括中国、俄罗斯、伊朗和朝鲜等国家。2013 年，美国投入全球情报搜集计划的预算高达 526 亿美元，其中涉及网络安全行动的预算，只有三分之一被用于网络安全防御，其它资金均被用于网络攻击。显然，对于美国国家安全局（NSA）而言，最好的防守就是进攻。

根据公开资料显示，美国国家安全局（NSA）下属包括 16 个单位，具体如下图所示（至今 NSA 已更新组织架构）：



其中作为美国国家安全局（NSA）针对全球开展情报窃取活动的“尖兵利器”是其信号情报局下面最大的部门——接入技术行动处（TAO、Tailored Access Operations)。

根据维基百科记录，该部门早在 1998 年就开始在网上活跃，主要职责是为美国情治机构提供针对美国本土和其他国家高级目标的通讯监控、情报获取，甚至远程破坏（摧毁）行动。

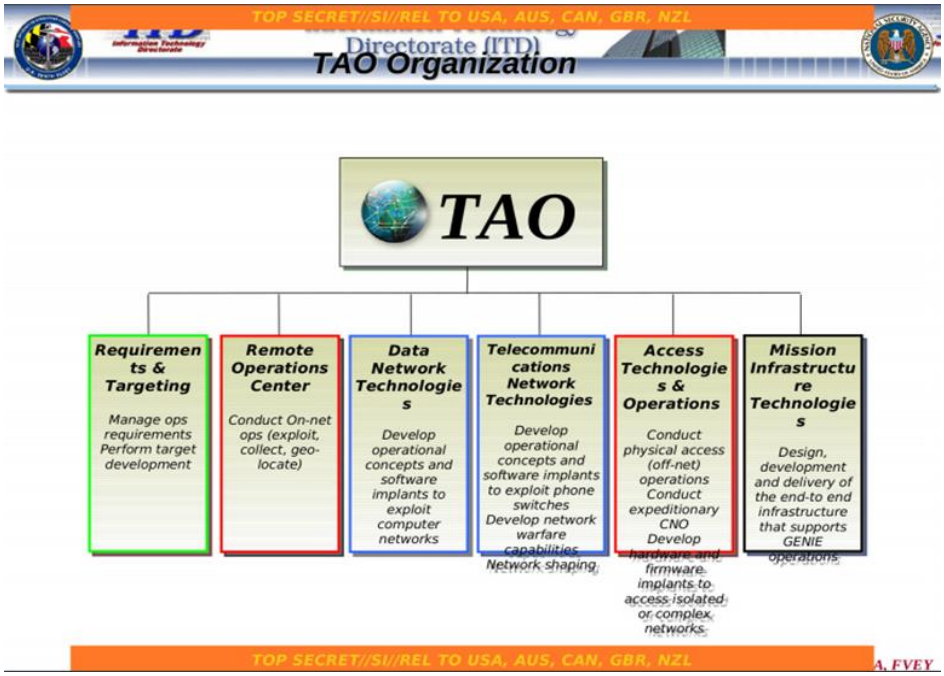
具体包括秘密侵入目标国家的关键信息基础设施和重要互联网信息系统、破解窃取账号密码、突破或破坏对手计算机安全防护系统、监听网络流量、窃取隐私和敏感数据，获取通话内容、电子邮件、网络通信内容和手机短信等。

据了解，接入技术行动处（TAO）还承担负一项重要职责，即当美国总统命令对他国通讯或网络信息系统实施瘫痪或摧毁行动时，由接入技术行动处（TAO）将相关网络攻击武器提供给到美国网络战司令部（U.S. Cyber Command），由该司令部具体组织实施网络攻击行动。

公开信息显示，TAO 组织成员由超过 1000 名现役军人、网络黑客、情报分析师、专家学者、计算机软硬设计师，以及电子工程师等人员组成。根据其工作性质，TAO 的下属网络攻击实施部门被称为远程作战中心(ROC，Remote Operations Center)，办公地点位于美国国家安全局（NSA）马里兰州总部的米德堡内。据分析，接入技术行动处（TAO）的办公和网络攻击据点还广泛分布于美国国家安全局（NSA）位于夏威夷瓦希瓦和瓦胡岛、佐治亚州戈登堡、德克萨斯州圣安东尼奥，以及科罗拉多州的巴克利太空部队基地等地。

美国国家安全局（NSA）总部，马里兰州米德堡

根据公开披露信息，美国国家安全局（NSA）接入技术行动处（TAO）的组织代号及架构示意图如下：



- S321-总部，远程作战中心（ROC，Remote Operations Center），雇员超过 600 人，负责日常接收、整理、汇总从世界各地被 TAO 远程控制的信息系统中窃取的账号密码和重要敏感信息。

- S323-数据网络技术分部(DNT)：负责开发网络攻击和网络间谍

活动武器，其中：

◆ S3231-访问权限部门（ACD，Access Division）。

◆ S3232-网络安全技术部门（CNT）。

◆ S3233-未知。

◆ S3234-计算机技术部门（CTD）。

◆ S3235-网络技术部 门(NTD)。

● S324-电信网络技术分部(TNT，Telecommunication Network Technologies)：负责组织研发针对电信网络进行黑客攻击的方法和相关技术。

● S325-任务基础设施分部(MIT，Mission Infrastructure Technologies)：负责对 TAO 建设运营的全球化网络攻击基础设施进行维护和配置，确保其能够可靠运行 TAO 所有的各种网络攻击武器和间谍软件。

● S328–远程访问行动分部（ATO，Access Technologies Operations）：由美国中央情报局（CIA）和联邦调查局（FBI）雇员组成，负责执行所谓“离网行动”，即由中央情报局（CIA）或联邦调查局（FBI）特工实际进行他国互联网和电信网络秘密植入流量监听和网络窃密设备，窃取系统账号密码使美国国家安全局（NSA）接入技术行动处（TAO）的网络攻击实施者可以从米德堡远程“合法”访问这些网络设备。**据悉，美国国家安全局（NSA）装备的特殊任务潜艇-吉米卡特号，就被用于对全球范围的光纤和电缆进行窃听。**

吉米卡特号（USS Jimmy Carter）

◆S3283-远程访问权限行动部门（EAO）

◆S3285-持久化部门

相关资料显示，NSA 窃密期间的 TAO 负责人是罗伯特·乔伊斯（Robert Edward Joyce）。

此人 1967 年 9 月 13 日出生，曾就读于汉尼拔高中，1989 年毕业于克拉克森大学，获学士学位，1993 年毕业于约翰·霍普金斯大学，获硕士学位。1989 年进入美国国家安全局工作。曾经担任过 TAO 副主任，2013 年至 2017 年担任 TAO 主任，他主持实施了对中国和世

界其他国家的网络攻击和间谍窃密行动。

2017 年 10 月 13 日，罗伯特•乔伊斯受命担任美国国土安全顾问。

2018 年 4 月 10 日至 2018 年 5 月 31 日，罗伯特•乔伊斯担任时任美国总统唐纳德·特朗普的白宫国土安全顾问。

2018 年 5 月，罗伯特•乔伊斯担任美国国家安全局（NSA）的网络安全战略高级顾问。

2021 年 1 月 15 日-至今，美国国家安全局（NSA）宣布，罗伯特•乔伊斯担任该局的网络安全主管。

2．组织归因分析

2022 年 6 月 22 日，西北工业大学发布《公开声明》称遭受境外网络攻击。国家计算机病毒应急处理中心和 360 公司联合组成技术团队开展技术分析工作，判明相关攻击活动源自美国 NSA 下属 TAO。相关证据如下：

证据一：攻击时间完全吻合美国工作作息时间规律

根据对相关网络攻击行为的大数据分析，对西北工业大学的网络攻击行动 98%集中在北京时间 21 时至凌晨 4 时之间，该时段对应着美国东部时间 9 时至 16 时，属于美国国内的工作时间段。其次，美国时间的全部周六、周日中，均未发生对西北工业大学的网络攻击行动。第三，分析美国特有的节假日，发现美国的阵亡将士纪念日放假 3 天，美国“独立日”放假 1 天，在这四天中攻击方没有实施任何攻击窃密行动。依据上述工作时间和节假日安排进行判断，针对西北工业大学的攻击窃密者都是按照美国国内工作日的时间安排进行活动的。

证据二：武器操作失误暴露工作路径

20XX 年 5 月 16 日 5 时 36 分（北京时间），攻击方一次失误操作暴露出攻击者上网终端的工作目录和相应的文件名，从中可知木马控制端的系统环境为 Linux 系统，且相应目录名（\Linux\etc\autoutils）系美国国家安全局“特定入侵行动办公室”（TAO）网络攻击武器的专用名称（autoutils）。

证据三：大量武器与遭曝光的 NSA 武器基因高度同源

被捕获的对西北工业大学攻击窃密中所用的 41 款不同的网络攻击武器工具中，有 16 款工具与“影子经济人”曝光的美国国家安全局“特定入侵行动办公室”（TAO）武器完全一致；有 23 款工具虽然与“影子经济人”曝光的工具不完全相同，但其基因相似度高达 97%，属于同一类武器，只是相关配置不相同；有两款工具无法与“影子经济人”曝光工具进行对应，但这两款工具需要与美国国家安全局“特定入侵行动办公室”（TAO）的其它网络攻击武器工具配合使用，因此这批武器工具明显具有同源性，都属于美国国家安全局“特定入侵行动办公室”（TAO）。

3．组织代表武器

据公开信息显示，高级网络技术分部（ANT，Advanced Network Technology Division)是接入技术行动处（TAO）负责网络监控的主要部门。根据爱德华·斯诺登披露的内部信息，高级网络技术分部（ANT）日常负责对全球互联网实施大规模流量监控和攻击窃密活动。

2014 年，高级网络技术分部（ANT）通过设立新的研究项目，将美国国家安全局（NSA）的网络监控能力延伸到开源网络软硬件产品上。据公开资料显示，大多数新开发的此类网络攻击武器均已交由美

国及其他“五眼联盟”国家使用。

NSA 针对全球发起网络攻击事件中使用的武器类别主要分为五大类，分别是：

a) 漏洞攻击突破类武器

(1)“剃须刀”

此武器用于对跳板机的攻击，可针对开放了指定 RPC 服务的 X86 和 SPARC 架构的 Solaris 系统实施远程溢出攻击，攻击时可自动探知目标系统服务开放情况并智能化选择合适版本的漏洞利用代码，直接获取对目标主机的完整控制权。

(2)“孤岛”

此武器同样可针对开放了制定 RPC 服务的 Solaris 系统实施远程溢出攻击，直接获取对目标主机的完整控制权。与“剃须刀”工具不同之处在于此工具不具备自主探测目标服务开放情况的能力，需由使用者手动选择欲打击的目标服务。

（3）“酸狐狸”武器平台

此武器平台部署在哥伦比亚，可结合“二次约会”中间人攻击武器使用，可智能化配置漏洞载荷针对 IE、FireFox、Safari、Android Webkit 等多平台上的主流浏览器开展远程溢出攻击，获取目标系统的控制权。

（4）Validator 验证器

另外，名为“验证器”Validator（Validator 验证器）的木马程序是 NSA 在网络攻击活动中最先植入目标的轻量级后门，主要功能是对攻击目标的网络系统环境进行探查，被认为是 NSA 专门开展的“木马尖兵”为目的的轻量级后门。

“验证器”木马具备对攻击目标开展系统环境信息收集的能力，同

时也为更为复杂的木马程序的安装（植入）提供条件。该款木马可以通过网络远程和物理接触两种方式进行安装，具有 7X24 小时在线运行能力，使 NSA 的系统操控者和数据窃密者可以上传下载文件、远程运行程序、获取系统信息、伪造 ID，并在特定情况下紧急自毁。

b) 持久化控制类武器

依托此类武器对目标网络进行隐蔽持久控制，可通过加密通道发送控制指令操作此类武器实施对西北工业大学网络的渗透、控制、窃密等行为。

（1）“二次约会”

此武器长期驻留在网关服务器、边界路由器等网络边界设备及服务器上，可针对海量数据流量进行精准过滤与自动化劫持，实现中间人攻击功能。

（2）“NOPEN”木马

此武器是一种支持多种操作系统和不同体系架构的控守型木马，可通过加密隧道接收指令执行文件管理、进程管理、系统命令执行等多种操作，并且本身具备权限提升和持久化能力。

（3）“怒火喷射”

此武器是一款基于 Windows 系统的支持多种操作系统和不同体系架构的控守型木马，可根据目标系统环境定制化生成不同类型的木马服务端，服务端本身具备极强的抗分析、反调试能力。

（4）“狡诈异端犯”

此武器是一款轻量级的后门植入工具，运行后即自删除，具备提权功能，持久驻留于目标设备上并可随系统启动。

（5）“坚忍外科医生”

此武器是一款针对 Linux、Solaris、JunOS、FreeBSD 等 4 种类型操作系统的后门，该武器可持久化运行于目标设备上，根据指令对目标设备上的指定文件、目录、进程等进行隐藏。

c) 嗅探窃密类武器

依托此类武器嗅探目标工作人员运维网络时使用的账号口令、生成的操作记录，窃取目标网络内部的敏感信息和运维数据等。

（1）“饮茶”

此武器可长期驻留在 32 位或 64 位的 Solaris 系统中，通过嗅探进程间通信的方式获取 ssh、telnet、rlogin 等多种远程登录方式下暴露的账号口令、操作记录、日志文件等。

（2）“敌后行动”系列武器

此系列武器是专门针对运营商特定业务系统使用的工具，根据被控业务设备的不同类型，“敌后行动”会与不同的解析工具配合使用。

d) 隐蔽消痕类武器

依托此类武器消除攻击在目标网络内部的行为痕迹，隐藏、掩饰其恶意操作和窃密行为，同时为上述三类武器提供保护。

（1）“吐司面包”

此武器可用于查看、修改 utmp、wtmp、lastlog 等日志文件以清除操作痕迹。

e) 攻击平台类武器

根据可考的美国国家安全局（NSA）机密文档显示，NSA 的实战化网络攻击武器体系极其复杂，配套可以根据不同的攻击任务配置多种攻击武器和攻击方式组织，在攻击过程中会植入的不同阶段会针对特定目标植入不同和类型的后门木马程序。

其中，APT-C-40 组织针对中国境内目标的网络攻击中所使用的最具代表性模块化武器平台是 Quantum（量子）攻击系统。

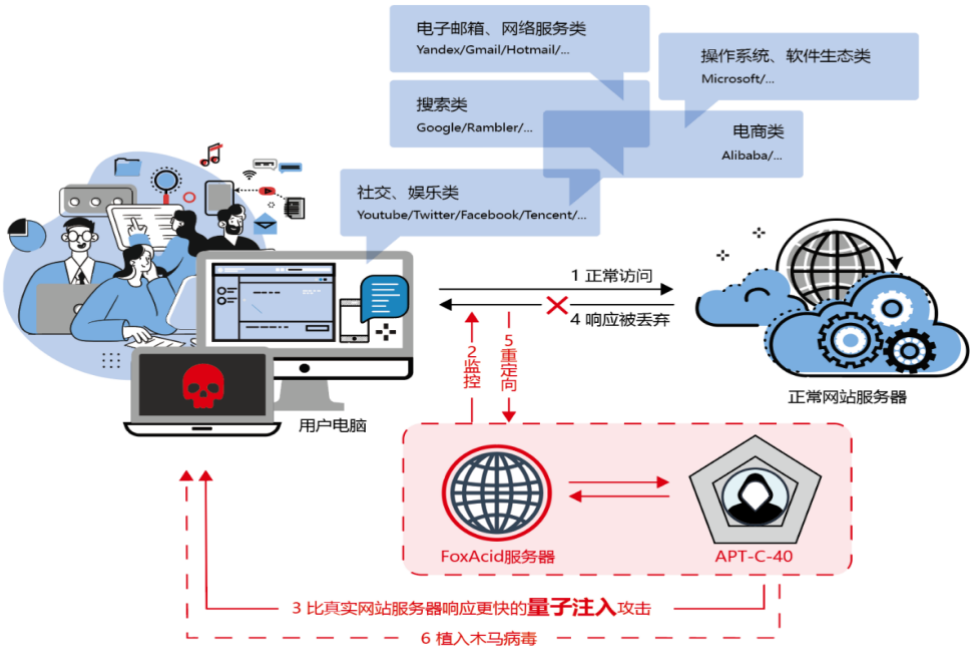
其作为美国国家安全局（NSA）针对国家级互联网专门设计的一种先进的网络流量劫持攻击技术，主要针对国家级网络通信进行中间劫持，以实施漏洞利用、通信操控、情报窃取等一系列复杂网络攻击。

据 NSA 官方机密文档《Quantum Insert Diagrams》内容显示，Quantum（量子）攻击可以劫持全世界任意地区任意网上用户的正常网页浏览流量，进行 0day（零日）漏洞利用攻击并远程植入后门程序。受所处地域和传输距离等因素影响，从美国国家安全局（NSA）各个办公地点发起的“量子”（QUANTUM）攻击，对于特定的攻击目标和软硬件组合来讲可能速度过慢，不足以完成相关攻击任务。从本质上看，这些远程攻击是利用联网设备响应时间（速度）等竞争性条件，使美国国家安全局（NSA）的攻击服务器可以早于合法服务器抢先做出应答，骗取攻击目标信任，接管后续通讯进程，进而达成攻击意图。

为解决此类问题，美国国家安全局（NSA）从 2011 年中期开始，设计开发了一套代号为“量子射击”（QFIRE）的功能原型，可根据具体任务需要将美国国家安全局（NSA）的漏洞分发服务器部署到更靠近攻击目标的托管服务器（运行在 VMware ESX 上的虚拟机）中，建成了名为“特殊收集站点”（SCS）的全球化网络攻击任务运行网络。“量子射击”（QFIRE）的部署目的是降低美国国家安全局（NSA）攻击武器发出欺骗应答的延迟时间，从而提高远程网络攻击的成功率。

在“量子”（Quantum）攻击平台的功能套件中，“量子饼干”（QUANTUMCOOKIE）代表着一种更加复杂的网络攻击形式，可用于攻击“暗网”（Tor）用户。还有一个名为“量子松鼠”

（QUANTUMSQUIRREL）的网络攻击武器，可以被伪装成任何可路由的 IPv4 或 IPv6 主机，使美国国家安全局（NSA）的网络攻击实施者能够在通过“量子松鼠”（QUANTUMSQUIRREL）作为跳板访问互联网时，随时生成虚假的地理位置信息和个人身份凭证。



美国国家安全局（NSA）“量子松鼠”（QUANTUMSQUIRREL）网络武器 PPT 演示，解释了“量子松鼠”（QUANTUMSQUIRREL）伪造 IP 的欺骗能力

4. 攻击案例

据公开资料显示，美国国家安全局（NSA）接入技术行动处（TAO）的攻击目标，包括但不限于中国、石油输出国组织（阿尔及利亚、安哥拉、赤道几内亚、加蓬、伊朗、伊拉克、科威特、利比亚、尼日利亚、刚果共和国、沙特阿拉伯、阿拉伯联合酋长国和委内瑞拉等）、墨西哥公共安全秘书处等国家和国际组织。

截至目前，接入技术行动处（TAO）已有超过500个网络攻击和数据窃密行动代号被公开披露。通过对这些被披露的行动代号及其概要的综合研判分析，可以整体上了解美国国家安全局（NSA）在全球范围发动无差别网络攻击的方向、范围、规模、数量等情况。

网络监听相关案例：

2013年，美国前防务承包商雇员爱德华&斯诺登向媒体曝光美方代号“棱镜”的大规模秘密监听项目，监听对象不仅覆盖美国公民，也包括法国、德国等欧洲国家政要和民众。

2021年5月，欧洲媒体爆料，美国在丹麦情报部门帮助下，监听德国、法国、瑞典、挪威等欧洲国家领导人。

2023年4月，“泄密门”事件闹得沸沸扬扬。一批疑似美军秘密文件被泄露到社交媒体上，其内容显示，美国监听乌克兰总统泽连斯基与乌官员的内部对话，并获取了韩国和以色列等盟国内部沟通情况。美媒指出，有关信息是美方通过所谓“信号情报”获取，而“信号情报”是情报界专用术语，意味着美国政府持续监听这些国家。

网络攻击相关案例：

2010年，美国通过间谍活动将“震网”病毒植入伊朗纳坦兹核设施内部网络，导致大批铀浓缩离心机瘫痪。

俄外交部国际信息安全司司长安德烈&克鲁茨基赫公开表示，截至2022年5月，来自美国等国的6.5万多名黑客定期参与针对俄方关键信息基础设施的攻击。

据香港《大公报》报道，美国前中央情报局雇员斯诺登跟香港英文报章披露，美国国家安全局(NSA)自 2009 年起即入侵香港及中国内地的计算机，目标包括香港中文大学、公职官员、企业及学生电脑。

2014 年 1 月 14 日，《纽约时报》报道美国国家安全局在全球近10万台电脑中植入软件，可以监控这些电脑的活动或发起网络攻击。国安局在 2014 年之前就启用一项技术，借助无线电波获取一些已经采取保护措施或没有接入互联网的电脑中的数据。

国安局通过“间谍、电脑生产商或不知情使用者”等渠道，把带有这种软件的微型电路板或 USB 存储卡安装进目标电脑，再通过接收这些设备发出的无线电波，获取电脑中的数据。这种软件还可以用来针对目标电脑发起网络攻击。

国安局的说法是，这项技术意在“积极防御”，针对一些国家的军队、贩毒集团、欧盟内部贸易组织，以及沙特阿拉伯、印度、巴基斯坦等美国反恐伙伴的电脑。这一技术并没有在美国本土使用。上述电脑入侵项目部分内容在“棱镜”情报监控丑闻曝光者爱德华·斯诺登先前披露的秘密文件中曾被提及。

2022 年 4 月，中国西北工业大学信息系统发现遭受网络攻击判明相关攻击活动源自美国国家安全局的“特定入侵行动办公室”。过程中，成功提取了名为“二次约会”的间谍软件多个样本。根据黑客组织“影子经纪人”泄露的美国国家安全局内部文件，该恶意软件为美国国家安全局开发的网络“间谍”武器。它主要部署在目标网络边界设备（网关、防火墙、边界路由器等），隐蔽监控网络流量，并根据需要精准选择特定网络会话进行重定向、劫持、篡改。

五、总结

美国 APT 组织全球化无差别黑客入侵行径，引发了我们的进一步思考：

一、美国 APT 组织网络武器攻击已完全实现了工程化、自动化。

网络战时代到来，网络武器的自动化、智能化优势成为超越信息优势的“进阶优势”，其自动化的“思考”速度和质量，极大提高了美国自主作战系统实现制胜目标的优势，也为全球网络安全带来无穷隐忧。

二、为实施并制胜网络战，美国政府充分利用一切先进技术和网络资源。美国有着全球最先进的互联网技术，这是尽人皆知的，但为了掌握网络战主导权，美国将诸如 QUANTUM（量子）攻击系统等大量顶级技术手段、高端人才、情报力量纳入作战序列，由此可见，美国对发展网络作战力量的重视程度，并不计成本地投入资源、增加筹码。

三、美国 APT 组织的网络攻击属于无差别攻击，目标是全球范围，甚至包括美国盟友。由上述分析可见，美国针对各类电子邮箱、社交网络、搜索引擎、视频网站等几乎所有互联网用户发起无差别的网络攻击，美国的网络战略打击是全球性的、无节制的，在美国网络攻击的镰刀之下，没有哪一国能独善其身。

四、美国的网络战战略，或不仅限于网络窃密。通过公开的资料已知，美国已经完成了其网络战战略目标第一步——网络窃密，像斯诺登还有维基百科爆料的“棱镜”计划都属于这一范畴，但不排除美国的下一步目标野心将更大。一旦 APT 组织通过在对手的电脑网络中安插硬件或软件后门，实现关键目标远程操控，包括军事系统、国家公共安全领域的服务器、民航公路铁路交通系统的主机、银行金融系统的服务器等，如果美国更大的战略目标实现，其对手将毫无谈判余地。