“黑客帝国”调查报告——美国中央情报局（CIA）（之一）

美国中央情报局（Central Intelligence Agency，简称 CIA），一个比美国国家安全局（NSA）更为世人熟知的名字，它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，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。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”。

本系列报告从国家计算机病毒应急处理中心和 360 公司参

与调查的大量真实案例入手，揭秘其网络攻击武器的主要细节，披露部分发生在中国和其他国家的网络安全典型案事件的具体过程，全面深入分析美国中央情报局（CIA）的网络攻击窃密和相关现实危害活动，以及其对美国成为“黑客帝国”所做的贡献，为遍布全球的网络攻击受害者提供参考和建议。

1. 概述

从 20 世纪 80 年代国际社会主义阵营遭受冲击、90 年代初苏东剧变（“天鹅绒革命”）到 2003 年格鲁吉亚“玫瑰革命”，从 2004 年乌克兰“橙色革命”到 2005 年吉尔吉斯“郁金香革命”，从 2011 年西亚北非国家“阿拉伯之春”到 2014 年乌克兰“二次颜色革命”、中国台湾“太阳花革命”等，都被国际机构和世界各地学者认定为由美国情治机构主导的“颜色革命”典型案例。其他一些国

家中还发生过未遂的“颜色革命”事件，如 2005 年 3 月白俄罗斯“雪花革命”、2005 年 6 月阿塞拜疆“橙色风暴”、2005 年黎巴嫩“雪松革命”、2007 年缅甸“藏红花革命”、2009 年伊朗“绿色革命”等等。如果从冷战时期算起，带有“和平演变”和“颜色革命”色彩的政权更替事件更是不胜枚举。据统计，数十年来，美国中央情报局（CIA）至少推翻或试图推翻超过 50 个他国合法政府（而中央情报局只承认其中的 7 起），在相关国家引发动乱。

综合分析上述事件中的各类技术，信息通信和现场指挥成为影响事件成败的决定性因素。美国的这些技术在国际上处于领先地位，特别是 20 世纪 80 年代美国将互联网推向国际并得到世界各国的普遍接受，给美国情治部门对外发动“颜色革命”提供了前所未有的技术可能性。

美国前国务卿奥尔布赖特曾扬言：“有了互联网我们对中国就有了办法。”

此言不虚，多起“颜色革命”事件中都有西方大国借助互联网推波助澜的影子。西亚北非多国“阿拉伯之春”事件发生后，美国个别大型互联网跨国企业积极介入，向冲突各方投入大量人力、物力、财力，拉拢支持反对派，向与美国利益不符的他国合法政府公开发难，协助发布扩散虚假信息，推动民众抗议活动不断激化。

一是提供加密网络通信服务。为帮助中东地区部分国家的抗议者保持联络畅通，同时避免被跟踪和抓捕，美国公司（据称具有美国军方背景）研发出一种可以接入国际互联网又无法追踪的TOR技术（“洋葱头”路由技术，The Onion Router）。相关服务器对流经它们的所有信息进行加密，从而帮助特定用户实现匿名上网。该项目由美国企业推出后，立即向伊朗、突尼斯、埃及等国的反政府人员免费提供，确保那些“想动摇本国政府统治的异见青年”在参与活动时，能躲避当地合法政府的审查和监视。

二是提供断网通联服务。为确保突尼斯、埃及等国的反政府人员在断网情况下仍能与外界保持联系，美国《谷歌》《推特》公司迅速推出一款名为“Speak2Tweet”的专用服务，它允许用户免费拨号并上传语音留言，这些留言被自动转换成推文后再上传至因特网，《推特》等平台公开发布，完成了对事件现场的实时报道。

三是提供基于互联网和无线通讯的集会游行活动现场指挥工具。美国兰德公司花费数年研发出一款被称为“蜂拥”的非传统政权更迭技术，用于帮助通过互联网联接的大量年轻人加入“打一枪换一个地方”的流动性抗议活动，大大提升了活动现场指挥效率。

四是美国公司研发了一款名为“暴动”的软件，支持100%独

立的无线宽带网络、提供可变 WiFi 网络，不依赖任何传统物理接入方式，无须电话、电缆或卫星连接，能轻易躲过任何形式的政府监测。借助上述功能强大的网络技术和通讯技术手段，美国中央情报局（CIA）在全球各地策划组织实施了大量的“颜色革命”事件。

五是美国国务院将研发“反审查”信息系统作为重要任务，并为该项目注资超过 3000 万美元。

2. 美国中央情报局（CIA）的网络攻击武器系列

2017 年 3 月 7 日，《维基解密》网站披露了 8716 份据称是来自美国中央情报局（CIA）网络情报中心的秘密文件，内容涉及美国中央情报局（CIA）黑客团队的攻击手法、攻击行动项目代号、攻击工具技术规范和要求等，《维基解密》将相关文件称

为“Vault7”（穹顶 7），引发全球范围的高度关注。

2020 年，360 公司独立发现了一个从未被外界曝光的 APT 组织，专门针对中国及其友好国家实施网络攻击窃密活动，受害者遍布全球各地，我们将其单独编号为 APT-C-39。有证据表明，该组织使用与被曝“Vault7”（穹顶 7）资料相关联的网络武器工具（包括 Athena、Fluxwire，Grasshopper、AfterMidnight、HIVE、ChimayRed 等），针对中国和其他国家受害目标实施网络攻击，攻击活动最早可以追溯到 2011 年，相关攻击一直延续至今。被攻击目标涉及各国重要信息基础设施、航空航天、科研机构、石油石化、大型互联网公司以及政府机构等诸多方面。

在规模庞大的全球性网络攻击行动中，美国中央情报局（CIA）大量使用“零日”（0day）漏洞，其中包括一大批至今未被公开披露的后门和漏洞（部分功能已得到验证），在世界各地建立“僵尸”网络和攻击跳板网络，针对网络服务器、网络终端、交换机和路由器，以及数量众多的工业控制设备分阶段实施攻击入侵行动。在现已发现的专门针对中国境内目标实施的网络攻击行动中，我们成功提取了多个“Vault7”（穹顶 7）网络攻击武器样本，多个东南亚国家和欧洲的合作伙伴也提取到了几乎完全相同的样本，主要包括：

2.1 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。

2.2 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。

2.3 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。

2.4 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。

2.5 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。

2.6 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（https://www.cverc.org.cn/head/zhaiyao/news20220419-hive.htm）。

2.7 其他衍生工具

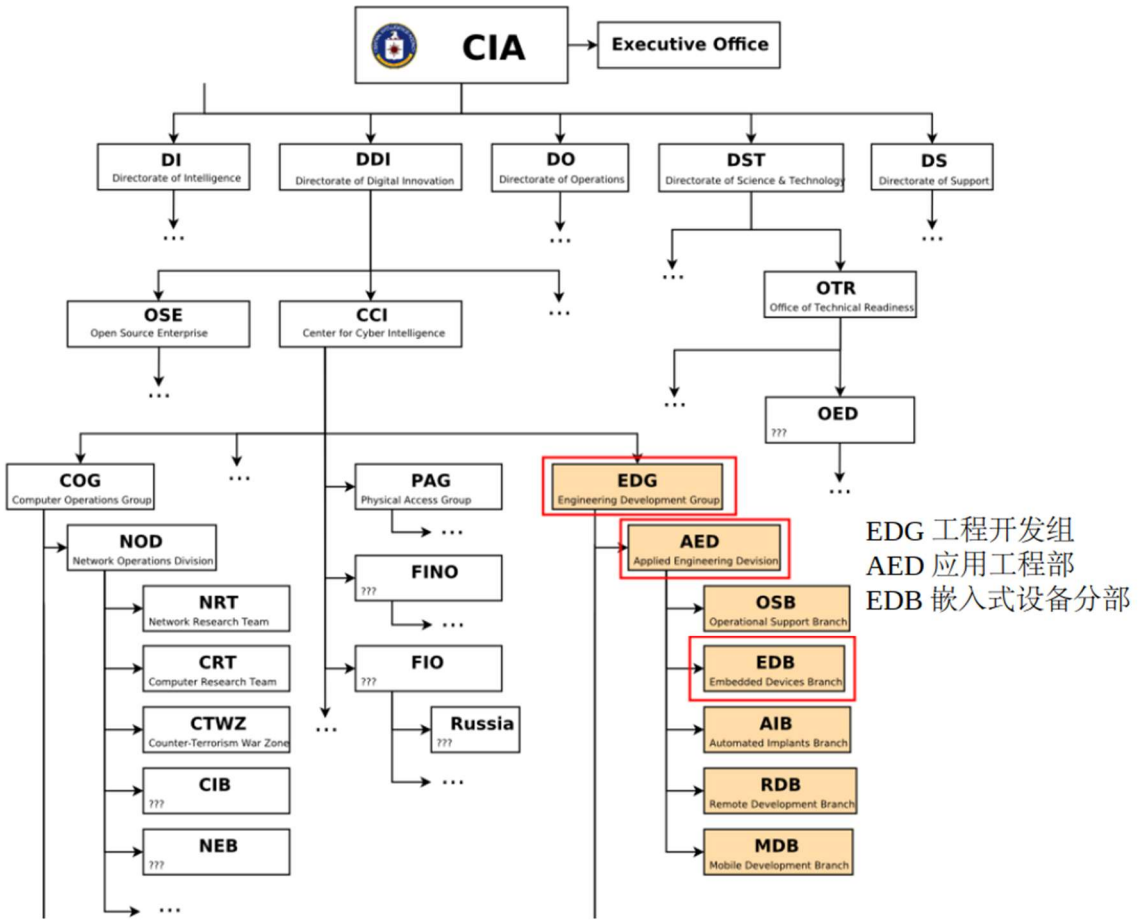
美国中央情报局（CIA）在通过上述“Vault7”（穹顶 7）网络武器实施攻击窃密过程中，还衍生和使用了大量“Vault7”（穹顶 7）资料之外的攻击样本，现已提取的样本中包括伪装的钓鱼软件安装包、键盘记录组件、系统信息收集组件、USB 文件窃取模块和不同的开源黑客工具等。

3. 美国中央情报局（CIA）网络攻击武器样本功能分析

在针对中国境内多起典型网络攻击事件的调查过程中，360 公司从受害单位信息网络中捕获并成功提取了一大批与网曝美

国中央情报局（CIA）“Vault7”（穹顶 7）资料紧密关联的木马程序、功能插件和攻击平台样本。深入分析发现，相关程序样本大都遵循了“Vault7”（穹顶 7）资料中的《Network Operations Division In-memory Code Execution Specification》、《Network Operations Division Cryptographic Requirements》和《Network Operations Division Persisted DLL Specification》等美国中央情报局（CIA）恶意软件开发标准和技术规范。这些标准和规范分别对应网络攻击窃密活动中恶意代码的加载执行、数据加密和持久化行为，相关网络武器进行了极其严格的规范化、流程化和专业化的软件工程管理。据悉，目前只有美国中央情报局（CIA）严格遵守这些标准和规范开发网络攻击武器。

据“Vault7”（穹顶 7）资料显示，上述网络攻击武器归属于美国中央情报局（CIA）的 EDG（工程开发组），由其下属的 AED（应用工程部）和 EDB（嵌入式设备分部）等多个分部独立或联合研发。这些网络武器大都诞生于一个名为“devlan.net”的美国中央情报局（CIA）最高机密内部网络中。“devlan.net”是美国中央情报局（CIA）工程开发部（EDG）建立的庞大的网络武器开发测试基础设施。另据“devlan.net”的开发日志数据显示，仅“HIVE”（蜂巢）一个项目就至少投入 EDG 两百余名工程师参与研发。



进一步技术分析发现，美国中央情报局（CIA）的后门程序和攻击组件大都以无实体文件的内存驻留执行的方式运行，这使得对相关样本的发现和取证难度极大。即使这样，联合技术团队还是成功找到了解决取证难题的有效方法。为后续描述和分析问题方便，我们暂且将美国中央情报局（CIA）的攻击武器分为 9 个类别：

3.1 框架平台类。我们发现并捕获了 Fluxwire（磁通线）、Grasshopper（蚱蜢）、Athena（雅典娜）的攻击样本和攻击活动，经过实地检测，这些样本的功能、攻击特征和网络行为均可与“Vault7”（穹顶 7）资料中的描叙一一印证。

3.2 攻击模块投递类。美国中央情报局（CIA）使用了大量功能简单的小型恶意代码下载器，用于加载执行更多的恶意代码及模块，相关样本无特别的恶意功能及特征，但在与框架平台等攻击武器配合时却可展现出强大的窃密功能，极难将其归因溯源。

3.3 远程控制类。现已提取多款远程控制插件，大都属于框架平台类攻击武器衍生出的攻击模块组件，二者之间相互配合。

3.4 横向移动类。提取到的大量恶意程序样本中，包含多款通过系统管理员凭据使用 Windows 远程服务安装植入的后门程

序。除此之外，美国中央情报局（CIA）还劫持多种安全产品内网的升级程序，通过内网升级服务器的升级功能下发安装后门程序，实施内网中的横向移动攻击。

3.5 信息收集窃取类。联合技术团队偶然提取到美国中央情报局（CIA）使用的一款信息窃取工具，它属于网曝美国国家安全局（NSA）机密文档《ANT catalog》48 种先进网络武器中的一个，是美国国家安全局（NSA）的专用信息窃取工具。这种情况说明美国中央情报局（CIA）和美国国家安全局（NSA）会联合攻击同一个受害目标，或相互共享网络攻击武器，或提供相关技术或人力支持。这为对 APT-C-39 攻击者身份的归因溯源补充了新的重要证据。

3.6 漏洞利用类。调查中发现，至少从 2015 年开始，美国中央情报局（CIA）就在世界各地建立了庞大的网络攻击跳板资源，利用“零日”（0day）漏洞对全球范围 IOT（物联网）设备和网络服务器无差别攻击，并将其中的大量失陷设备转换为跳板“肉鸡”，或隐藏自身攻击行为，或将网络攻击嫁祸给其他国家。例如，美国中央情报局（CIA）使用代号为“ChimayRed”（智美红帽）的漏洞攻击套件定向攻击多个型号的 MikroTik 品牌路由器，其中包括中国境内大量使用这种路由器的网络设备。攻击过程中，美国中央情报局（CIA）首先会恶意修改路由器启动脚本，使路由器

重启后仍执行后门程序；然后，美国中央情报局（CIA）再修改路由器的 CGI 程序堵住被美国中央情报局（CIA）自身利用的漏洞，防止其他攻击者再次入侵造成权限丢失；最终，美国中央情报局（CIA）会向路由器植入“蜂巢”（HIVE）或“TinyShell”等只有美国中央情报局（CIA）可以使用的专属后门程序。

3.7 伪装正常软件类。美国中央情报局（CIA）针对攻击目标的网络环境，将后门程序定制伪装为目标使用的用户量较少的冷门软件安装包，针对目标实施精准的社会工程学攻击。

3.8 安全软件攻防类。美国中央情报局（CIA）掌握了专门用于攻击商业杀毒软件的攻击工具，可以通过这些专用工具远程关闭和杀死指定杀毒软件的进程，使相关杀毒软件对美国中央情报局（CIA）的攻击行为或攻击武器失效。

3.9 第三方开源工具类。美国中央情报局（CIA）也会经常使用现成的开源黑客工具进行攻击活动。美国中央情报局（CIA）网路攻击行动的初始攻击一般会针对受害者的网络设备或服务器实施，也会进行社会工程学攻击。在获得目标权限之后，其会进一步探索目标机构的网络拓扑结构，在内网中向其它联网设备进行横向移动，以窃取更多敏感信息和数据。被美国中央情报局（CIA）控制的目标计算机，会被进行 24 小时的实时监控，受害者的所有键盘击键都会被记录，剪切板复制粘贴信息会被窃取，

USB 设备（主要以移动硬盘、U 盘等）的插入状态也会被实时监控，一旦有 USB 设备接入，受害者 USB 设备内的私有文件都会被自动窃取。条件允许时，用户终端上的摄像头、麦克风和 GPS 定位设备都会被远程控制和访问。

4. 小结

美国操纵的网络霸权发端于网络空间，笼罩世界，波及全球，而作为美国三大情报搜集机构之一，美国中央情报局（CIA）针对全球发起的网络攻击行为早已呈现出自动化、体系化和智能化的特征。仅仅在《维基解密》网站中泄露出来的 8716 份文件中，就包含了美国情治部门诸多重要黑客工具和网络攻击武器，表明美国已经打造了全球最大的网络武器库。通过实证分析，我们发现其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，美国式的网络霸权可见一斑，“黑客帝国”实至名归。

本系列报告尝试披露美国中央情报局（CIA）长期针对中国境内网络目标进行攻击窃密的各类活动，初步探索这些网络攻击和数据窃密活动。

针对美国中央情报局（CIA）对我国发起的高度体系化、智

能化、隐蔽化的网络攻击，境内政府机构、科研院校、工业企业和商业机构如何快速“看见”并第一时间进行“处置”尤为重要。为有效应对迫在眉睫的网络和现实威胁，我们在采用自主可控国产化设备的同时，应尽快组织开展 APT 攻击的自检自查工作，并逐步建立起长效的防御体系，实现全面系统化防治，抵御高级威胁攻击。