美情报机构针对全球移动智能终端实施的监听窃密活动

中国网络安全产业联盟

2025 年 3 月

目 录

引 言

全球移动智能终端用户量巨大。2023 年 11 月国际电信联盟（ITU）发布的《2023 年事实与数据》报告显示，全球 10 岁及以上人口中手机拥有率为 78%，3G 及以上的移动宽带在全球总人口的覆盖率为 95%。智能手机不再局限于传统的运营商通讯功能，而是成为日常购物、娱乐、社交、学习、生活服务的基本入口，更是移动办公的节点，甚至成为接入各种政企内网的身份令牌。

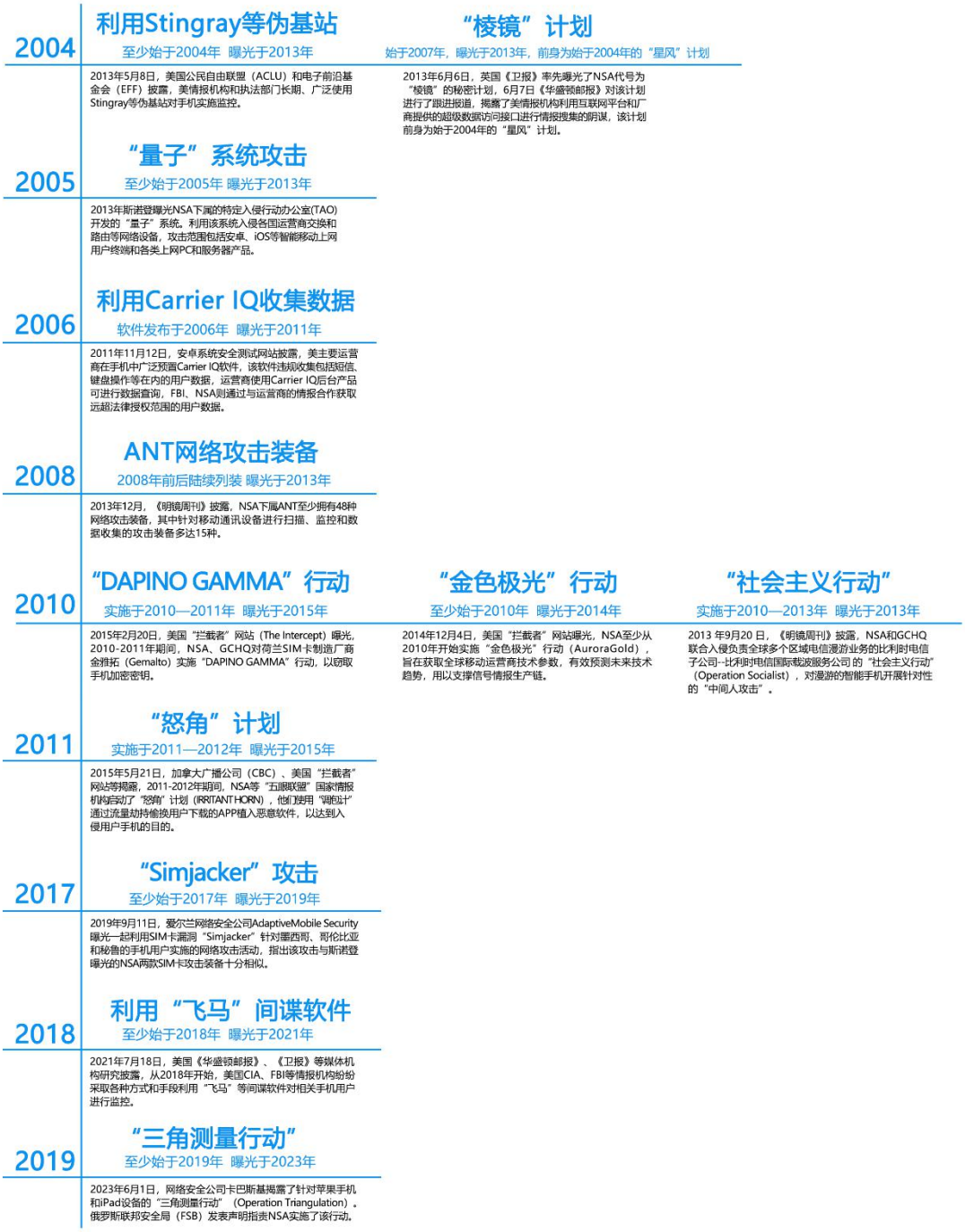
但同时，手机等移动智能终端也潜伏着巨大的网络安全隐患，较传统 PC 端具有更广泛的感知能力，配置高精度传感器，以及摄像头、麦克风等信号采集装置。通过对设备上的数据资产的收集和分析，能够对目标人员的工作生活轨迹、行为习惯、心理特点以及社会关系和周边环境，进行定向精准画像分析，甚至可以通过漏洞利用和恶意代码投放攻击控制手机，实现全方位监听监视。一部失陷手机就如同行走的窃听器、监视器，所到之处无密可保，全部透明于攻击者的“上帝视角”之下。而对于被引入作为移动办公环境的手机等智能终端设备而言，一旦失陷，不仅可能造成与目标相关的更高价值数据资产泄露，更可能成为攻击者入侵政企机构内网的突破口和跳板。

手机等移动智能终端因蕴藏着巨大数据资源价值，从出现开始，就为美国情报机构所觊觎。在过去二十多年的

时间里，全球关键信息基础设施运营者、安全厂商、研究者所面临的重大考验是，如何发现、分析和应对以美国国家安全局（NSA）、美国中央情报局（CIA）等为代表的美国情报机构发动的网络攻击活动。

相比传统 PC 端，手机等移动智能终端有更多的网络安全暴露面和可攻击面，包括涉及硬件、固件、系统和应用的终端设备层面，涉及数据接口、Wi-Fi、蓝牙、蜂窝网络、GPS 等地理定位在内的信息交互层面，同时手机系统的安全性与复杂的软硬件供应链体系相关、与 APP 应用的产业生态相关、与运营商的信号传输和大型互联网平台厂商数据存储汇聚相关，这些都是美方情报机构觊觎的环节和重点攻击的目标。

本报告梳理汇聚了大量业界和学界对美方情报机构针对移动智能终端开展的网络情报活动的披露分析（见下图），从终端设备、通信基础设施以及运营商和互联网厂商几个攻击目标层面对各方研究成果进行了分类整合，旨在对美方针对移动终端、移动产业链和供应链、运营商、大型互联网厂商的网络攻击活动和信息获取行为进行全局性认知和了解，以建立体系化防范能力，有效覆盖移动产业链和应用生态、关键信息基础设施和政企网络场景。



本报告第 1 篇至第 5 篇聚焦美方针对移动智能终端硬件、固件、系统和应用的攻击；第 6 篇至第 10 篇聚焦美方针对运营商基础设施和内部系统的攻击，其中后 2 篇为美方针对运营商及智能终端的组合攻击；第 11 篇重新解析“棱镜”

计划，揭露美情报机构通过互联网厂商的超级数据访问接口获取移动智能终端数据、进行大数据分析的情报活动。见下图：

全球各界披露的分析研究成果，共同揭露了美方针对全球移动智能终端开展的监听窃密行动，无孔不入、肆无忌惮、变本加厉。

第一篇　一条短信“接管”手机——针对 SIM 卡漏洞的高度复杂攻击

SIM 卡是移动通信系统的用户身份识别模块，用来登记用户身份识别数据和信息。利用 SIM 卡漏洞实施的攻击有一个明显的特点，即攻击不受硬件类型的限制。理论上，所有品牌和型号的手机，甚至带有 SIM 卡的物联网设备、可穿戴设备，无论安装有何种操作系统，只要插入的 SIM 卡中存在漏洞，即能够被攻击利用。2019 年 9 月，爱尔兰网络安全公司曝光一起利用 SIM 卡 S@T 浏览器中 Simjacker 漏洞，针对墨西哥、哥伦比亚和秘鲁的手机用户实施的网络攻击活动，指出该攻击与斯诺登曝光的 NSA 两款 SIM 卡攻击装备 MONKEYCALENDAR 和 GOPHERSET 十分相似。

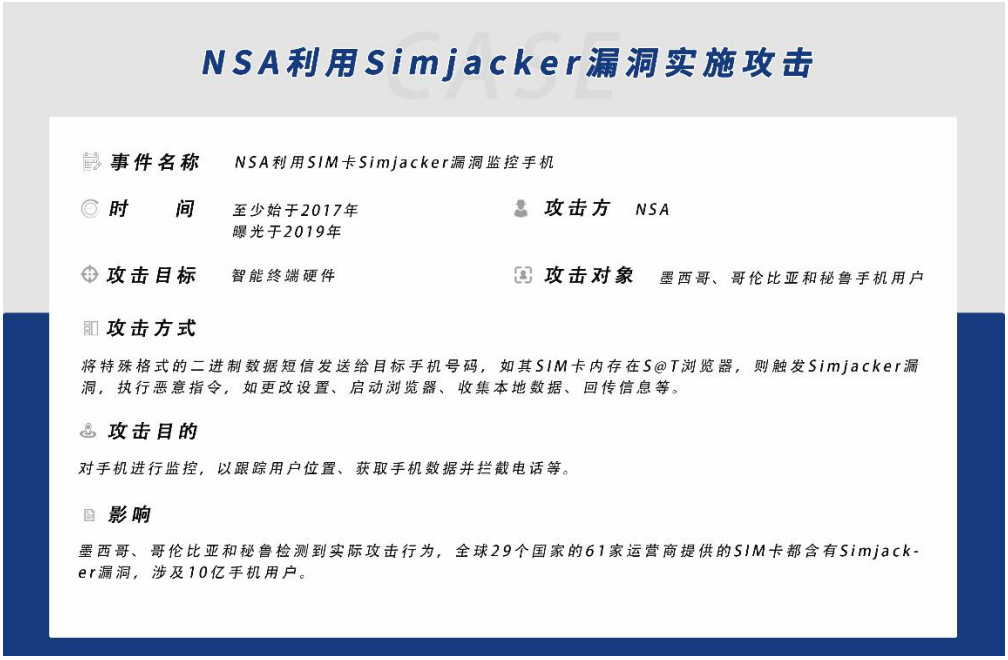


图 1-1 NSA 利用 Simjacker 漏洞实施攻击案例清单

（一）事件回顾

2019 年 9 月 11 日，总部位于爱尔兰都柏林的网络安全公司“自适应移动安全”（AdaptiveMobile Security）曝光了一起针对 SIM 卡 S@T 浏览器中 Simjacker 漏洞的攻击活动[1]。该攻击活动将特殊格式的二进制数据短信发送到手机，如 SIM 卡内存在 S@T 浏览器，则触发 Simjacker 漏洞，执行恶意指令，实现定位、窃密等恶意目的。

Simjacker 漏洞攻击只与 SIM 卡嵌入的功能组件有关，理论上插入含有该漏洞的 SIM 卡的所有品牌和型号的手机都可能受到攻击，甚至包括带有 SIM 卡的物联网设备和可穿戴设备。因此虽然“自适应移动安全”公司仅在墨西哥、哥伦比亚和秘鲁检测到实际的攻击行为，但当时全球 29 个国家的电信运营商提供的 SIM 卡都含有该漏洞，涉及 10 亿用户。

“自适应移动安全”公司指出，一方面 Simjacker 攻击与 4 个已曝光利用 SIM 卡漏洞的攻击十分相似，其中包括斯诺登曝光的 NSA 两款 SIM 卡攻击装备；另一方面实施者需要具有非常广泛技能、经验和资源，需要具备访问 SS7（7 号信令）网络的权限，对墨西哥等国移动用户有特定的兴趣，认为 NSA 是全球少数具备上述能力和特质的攻击实体。

（二）攻击方式

2019 年 10 月发布的《Simjacker 技术分析报告》[2]指出，Simjacker 攻击利用部分运营商发行的 SIM 卡中 S@T 浏览器对收到的消息有效性不做校验这个安全配置错误，实现对目标远程定位等攻击。

S@T 浏览器，全称为 SIMalliance Toolbox 浏览器，是 SIM 卡内置软件，其最初目的是启用诸如通过 SIM 卡获取用户账户余额等服务，因此并不广为人知。截至 2019 年，S@T 浏览器技术已有 10 年未更新，但当时该浏览器作为遗留技术被默认为许多品牌 SIM 卡的自带组件。

“自适应移动安全”公司分析了 Simjacker 的攻击步骤:

第一步：攻击者使用普通手机、GSM 调制解调器或者 A2P 短信服务，向攻击目标发送 SMS-PP（点对点）类型的短信，目标应用是 SIM 卡中的 S@T 浏览器;

第二步：攻击目标收到 SMS-PP 类型的短信后，手机上的逻辑被触发，S@T 浏览器成为 SIM 卡上的执行环境，SIM 卡“接管”手机，接收和执行敏感指令;

第三步：攻击代码一旦从手机检索到位置和特定设备信息（国际移动设备识别码 IMEI）等信息，就会对其进行整理，并再次触发手机上的逻辑，通过“数据消息”将合并后的信息发送到接收者号码。

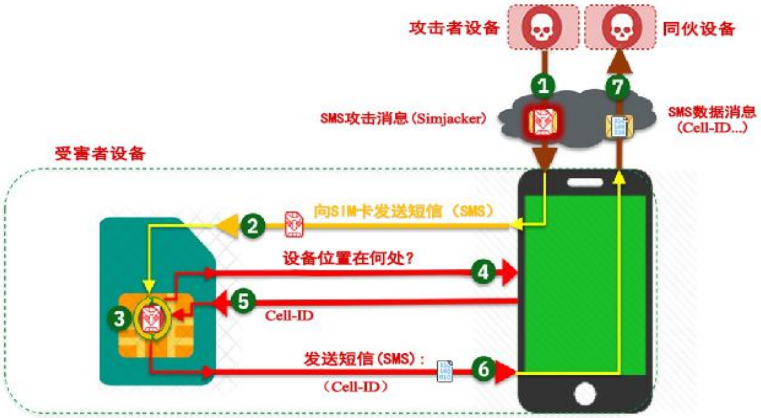


图 1-2 Simjacker 漏洞攻击技术流程

“自适应移动安全”公司认为，理论上 S@T 浏览器能够执行的命令包括获取设备当前位置、IMEI 信息、网络信息、语言信息、发送短信、播放音频、启动浏览器等，因此甚至能够强制手机发送虚假短信、拨打电话进行电信欺诈、打开恶意网站等。

“自适应移动安全”公司的首席技术官卡索·麦戴特（Cathal McDaid）表示[3]，Simjacker 漏洞攻击的特别之处一是受害者完全无感，收到的带有攻击消息的短信及发送的数据消息均未在短信记录中留痕。二是该攻击可能是“第一个真实存在的在短信中发送完整的恶意软件本身的案例”。以前通过短信发送的恶意软件仅发送其链接，需要用户点击链接下载。三是因为漏洞依赖于 SIM 卡上的软件而不是移动设备，所以各种类型手机均会遭受攻击。苹果、摩托罗拉、三星、谷歌、华为、中兴等几乎每个制造商的移动设备都被观察到遭受攻击，甚至还有带有 SIM 卡的物联网设备。

（三）溯源分析

2013 年 12 月，德国《明镜周刊》（Der Spiegel）披露了斯诺登曝光的 NSA 的 48 种 ANT 攻击装备[4]。“自适应移动安全”公司指出，Simjacker 攻击与其中两款针对 SIM 卡的攻击装备——MONKEYCALENDAR 和 GOPHERSET 颇具相似之处。GOPHERSET 利用 SIM 工具包（STK）的应用接口，向指定 SIM 卡发送 STK 指令搜集对方的呼叫记录、短信内容、联系人电话簿，并通过短信服务将提取到的数据发送到指定的号码。MONKEYCALENDAR 则是一种针对全球移动通信系统 GSM 用户 SIM 卡植入的间谍软件，该软件同样基于 SIM 工具包（STK），主要用于获取目标 SIM 卡的位置信息。

“自适应移动安全”公司分析认为，这三者的相似之处在于：一是攻击均利用了 STK 指令，二是攻击目的一致，均可获取位置信息、联系人电话簿、短信内容、呼叫日志等数据，三是均使用短信外发数据。

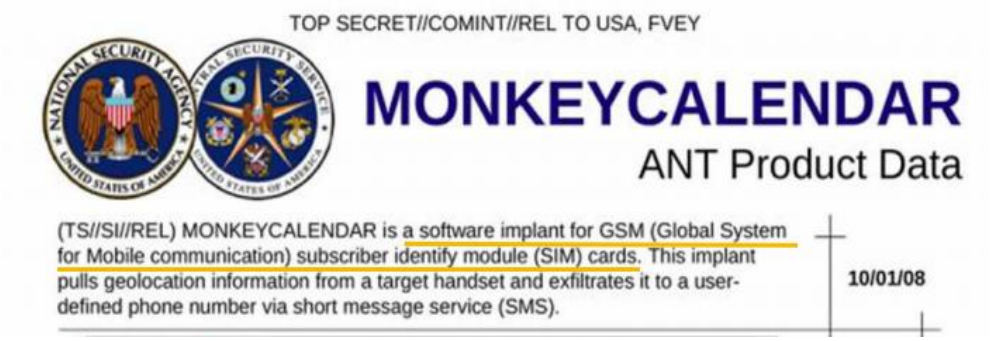


图 1-3 ANT 针对 SIM 卡的网络攻击装备 MONKEYCALENDAR

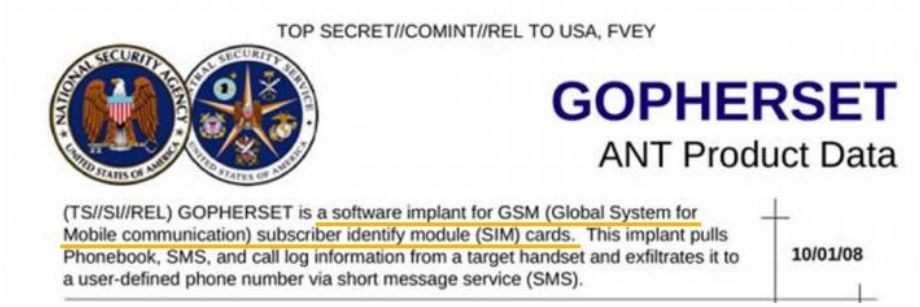


图 1-4 ANT 针对 SIM 卡的网络攻击装备 GOPHERSET

实施 Simjacker 攻击的组织还可以广泛访问 SS7 网络。“自适应移动安全”公司已经发现一些 Simjacker 受害者同时遭受了通过 SS7 进行的网络攻击，并认为该攻击方法被用作 Simjacker 漏洞攻击不成功时的后备方法。SS7 是通常用于局间的公共信道信令，叠加在运营者的交换网之上，是支撑网的重要组成部分。2019 年发布的《Sim 卡及移动端核弹漏洞密集爆发：近期网络战顶级数字武器解析》[5]报告指出，能登入 SS7 网络发起攻击的黑客，很大概率具备国家背景。

“自适应移动安全”公司仅在墨西哥、哥伦比亚和秘鲁检测到实际的攻击行为。早在 2013 年 7 月，英国路透社援引巴西知名报纸《环球报》报道称[6]，根据斯诺登曝光的资料，一些拉美国家已成为 NSA 监视的主要目标，尤其是哥伦比亚、委内瑞拉、巴西和墨西哥。该报道证实了 NSA 对墨西哥等国的移动用户有特定的兴趣。

因担心披露具体的溯源方法将有损其在全球范围内检测和阻止 Simjacker 攻击的能力，“自适应移动安全”公司

并未直接指出实施该攻击的组织名称。但是基于其对Simjacker攻击总体情况、技术特征、攻击武器、攻击路径、攻击对象等的分析，隐藏在Simjacker攻击后的“幕后黑手”NSA已浮出水面。

（四）延伸分析

根据斯诺登曝光资料，中国网络安全厂商安天梳理发现，NSA下属的ANT针对移动通讯设备进行扫描、监控和数据收集的攻击装备多达15种，约占全部已曝光的48种装备的三分之一。[7]

装备名称/代号	功能	装备名称/代号	功能
RAGEMASTER	视频数据监控	DROPOUTJEEP	手机数据收集
PICASSO	手机威胁监控	TOTECHASER	手机数据收集
GOPHERSET	手机威胁监控	TOTEGHOSTLY 2.0	手机数据收集
MONKEYCALENDAR	手机威胁监控	IRONCHEF	硬盘固件修改
GENESIS	手机扫描、信号伪装	WISTFULTOLL	注册表数据收集
CANDYGRAM	手机威胁监控	SPARROW II	无线数据收集
NEBULA	手机威胁监控	LOUDAUTO	雷达数据收集
WATERWITCH	手机威胁监控	CROSSBEAM	手机数据收集
TAWDRYYARD	雷达数据监控	CYCLONE Hx9	手机数据收集
SOUFFLETROUGH	硬盘固件	EBSR	手机数据收集
COTTONMOUTH-I	无线载荷攻击	ENTOURAGE	手机数据收集
COTTONMOUTH-III	物理隔离攻击	TYPHON HX	手机数据收集
DEITYBOUNCE	Dell漏洞利用	HEADWATER	持久化后门
GINSU	持久化代码	JETPLOW	持久化后门
IRATEMONK	硬盘固件	HALLUXWATER	持久化后门
SLICKERVICAR	硬盘固件	FEEDTROUGH	持久化后门
SWAP	硬盘固件	GOURMETTROUGH	持久化后门
SOMBERKNAVE	物理隔离攻击	CTX4000	电磁数据收集
ARKSTREAM	硬盘固件	PHOTOANGLO	电磁数据收集
NIGHTSTAND	物理隔离攻击	SCHOOLMONTANA	网络设备控制
HOWLERMONKEY (HM)	物理隔离攻击	SIERRAMONTANA	网络设备控制
SURLYSPAWN	按键记录收集	STUCCOMONTANA	网络设备控制
COTTONMOUTH-II	命令控制	NIGHTWATCH	视频信号处理
FIREWALK	流量监控	TRINITY	窃听芯片

图 1-5 ANT 网络攻击装备库

这些装备软件、硬件均有所涉及，装备形态包括恶意代码载荷、蜂窝塔、基站、信号收发器、手机等，可以组合使用，达成复杂攻击作业目标。

表 1-1 ANT 针对移动通讯设备的网络攻击装备

攻击装备名称	针对设备及功能	软件植入方式/硬件部署位置
DROPOUTJEEP	针对苹果 iPhone 操作系统的软件植入，能够从苹果设备远程推送/提取数据。能够收集的数据包括：短信、联系人电话簿、语音邮件、地理位置、热话筒、摄像头捕捉、蜂窝塔定位等，同时可以通过短信或 GPRS 数据连接进行命令、控制和数据过滤	首版通过近距离安装植入，未来版本将寻求远程安装
GOPHERSET	针对 GSM 系统中 SIM 卡的软件植入。能够收集手机中联系人电话簿、短信和通话记录等并通过短信将其发送给指定手机号码	通过 USB 智能卡读取器或空中编程（OTA）方式加载到 SIM 卡
MONKEYCALENDAR	针对 GSM 系统中 SIM 卡的软件植入。能够收集手机中的地理信息并通过短信将其发送给指定手机号码	通过 USB 智能卡读取器或空中编程方式加载到 SIM 卡
TOTECHASER	针对卫星、GSM 双模手机舒拉亚 2520（Thuraya 2520）中 Windows CE 操作系统的软件植入。能够收集舒拉亚 2520 手机中的 GPS 和 GSM 地理信息、通话记录、联系人电话簿和其他用户信息并通过短信将其发送给指定手机号码	现有版本需直接部署在舒拉亚 2520 手机上。正在研发可远程部署的版本
TOTEGHOSTLY 2.0	基于 StraitBizarre（一种可以实施量子注入攻击的跳板后门）的、针对 Windows Mobile 操作系统的软件植入，能够从 Windows 设备远程推送/提取数据。能够收集的数据包括：短信、联系人电话簿、语音邮件、地理位置、热话筒、摄像头捕捉、蜂窝塔定位等。通过短信或 GPRS 数据连接实现命令、控制和数据过滤功能	首版本通过近距离安装植入。未来版本将寻求远程安装
PICASSO	经过修改的 GSM 系统（目标）手机。用以收集通话记录、位置等数据，甚至可以打开手机麦克风来监听房间里的对话	以修改过的 GSM 手机替代目标手机
CROSSBEAM	一款可重复使用的符合 CHIMNEYPOOL 标准的 GSM 通信模块，能够收集和压缩语音数据。可以接收 GSM 语音，记录语音数据，并通过连接的模块或 4 种不同的 GSM 数据模式（GPRS、电路交换数据、语音数据和 DTMF）将接收到的信息发送回安全设施	GSM 通信模块，部署至手机上

CANDYGRAM	模拟目标网络的 GSM 蜂窝塔。每当目标手机进入 CANDYGRAM 基站的影响区域时，系统通过外部网络向注册的监测手机发送短信	GSM 蜂窝塔，部署至目标网络处
CYCLONE HX9	EGSM（900MGz）宏类（Macro-class）盒中网络（Network-in-a-box，NIB）系统。它使用现有的 Typhon GUI 并支持完整的 Typhon 功能库和应用程序	宏类盒中网络系统，部署至基站
EBSR	具有内部 802 .11 / GPS /手机功能的多用途，Pico 类三频有源 GSM 基站	GSM 基站，部署至目标网络处
ENTOURAGE	在 HOLLOWPOINT 平台上运行的测向应用，能够为 GSM/UMTS/CDMA2000/FRS 信号提供方位线（LOB）	测向应用，部署在 HOLLOWPOINT 平台
GENESIS	将一款商用 GSM 手机进行修改，增加软件无线电（SDR）及额外的系统内存。内部 SDR 允许有经验的用户在敌对环境中秘密执行网络调查，记录 RF 频谱或执行手机定位	手持式信号收发器，随身携带无需部署
NEBULA	多协议宏类盒中网络系统。它使用现有的 Typhon GUI 并支持 GSM、UMTS、CDMA2000 应用程序。支持 LTE 网络的能力正在开发中	宏类盒中网络系统，部署至基站
TYPHON HX	GSM 基站路由器，支持 GSM 频段 850/900/1800/1900 以及相关的完整 GSM 信令和呼叫控制	GSM 基站路由器，部署至基站网关
WATERWITCH	一种手持式精准定位工具，用于在现场对目标手机进行地理定位	手持式精准定位工具，随身携带无需部署

Simjacker 漏洞攻击的曝光是美方 ANT 攻击装备的应用案例，其所使用的技术、基础设施和方法证实美方网络攻击能力较之前有了巨大飞跃，最突出的一点是美方已无需近距离安装植入或 OTA 远程安装（此种方式攻击者需要掌握目标 SIM 卡的 OTA 密钥），仅通过短信即可启动监控，更具隐蔽性。“自适应移动安全”公司认为，攻击者已经利用 Simjacker 漏洞实施攻击至少两年、监控了数以万计的用

户才被其发现并曝光。

以 NSA 为代表的美国情报机构拥有一套完整的制式化移动攻击装备组合，能够进行严密的组织作业，且其作业过程高度隐蔽。

参考资料

[1] AdaptiveMobile Security. Simjacker Technical Paper. 2019. https://info.enea.com/Simjacker-Technical-Paper

[2] Simjacker 技术分析报告. 2019. https://mp.weixin.qq.com/s/hTgJEzbOxM5KMAIYK5ir3w

[3] Cathal McDaid. Simjacker Next Generation spying via SIM Card Vulnerability. 2019. https://www.enea.com/insights/simjacker-next-generation-spying-over-mobile/

[4] Jacob Appelbaum, Judith Horchert, Christian Stöcker. Catalog Advertises NSA Toolbox. 2013. https://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

[5] Sim 卡及移动端核弹漏洞密集爆发：近期网络战顶级数字武器解析.2019. https://www.secrss.com/articles/14161

[6] Anthony Boadle. NSA 'spied' on most Latin American nations: Brazil paper. 2013. https://www.reuters.com/article/us-usa-security-latinamerica-idUSBRE96816H20130709/

[7] 2023 网络安全威胁回顾与展望. 2024. https://www.antiy.cn/research/notice&report/research_report/2023_AnnualReport.html

第二篇　被偷走的“钥匙”——窃取手机 SIM 卡加密密钥

SIM 卡加密密钥是移动通信的重要组成部分，是保障通信安全的基础之一。在 SIM 卡加密密钥中鉴权密钥参与到移动设备入网合法性认证等工作中，为保障用户通信安全发挥着重要作用。该密钥在生产过程中由 SIM 卡制造商刻入 SIM 卡，并提供给网络运营商。而正是这把保障手机通信安全的“钥匙”却成为了美英情报机构的目标。2010 年至 2011 年间，美英情报机构对荷兰 SIM 卡制造厂商金雅拓（Gemalto）实施“DAPINO GAMMA”行动，以窃取手机加密密钥。

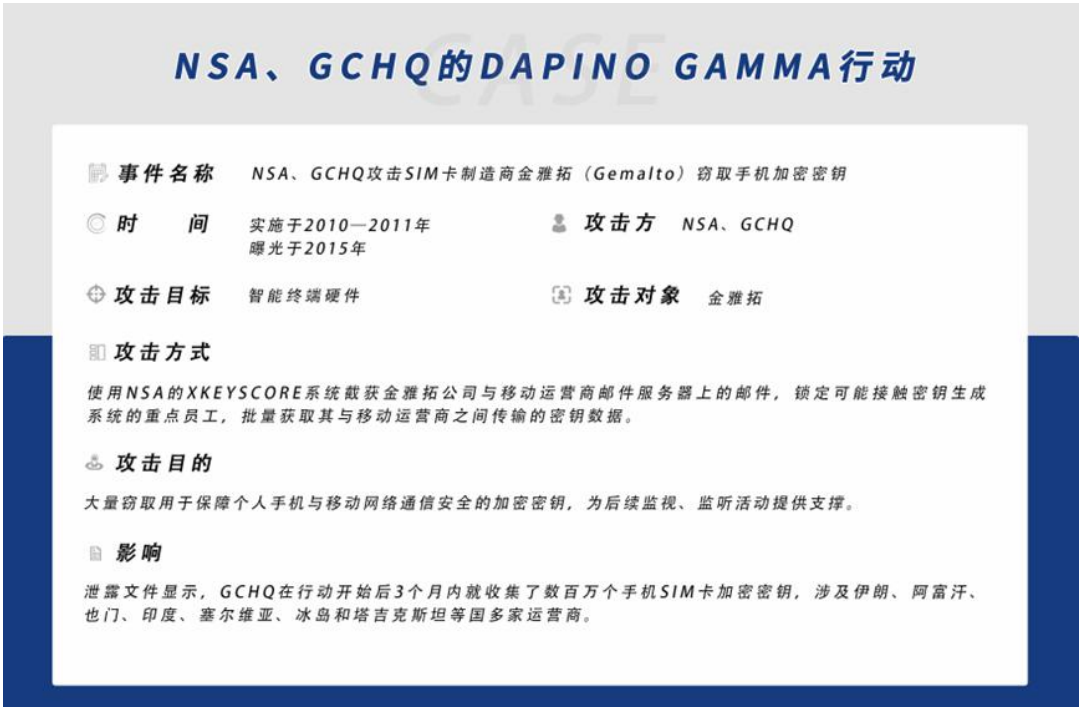


图 2-1 NSA、GCHQ 的 DAPINO GAMMA 行动案例清单

（一）事件回顾

2015 年 2 月 20 日，美国“拦截者”网站（The Intercept）依据斯诺登泄露的文件，发表名为“SIM 卡大劫案——间谍如何窃取加密城堡的钥匙”[1]的文章。披露在 2010 年至 2011 年间，由 NSA 和“五眼联盟”情报体系重要组织之一，英国政府通信总部（GCHQ）组成的“移动手机开发小组”（MHET）对 SIM 卡制造商金雅拓公司实施了名为“DAPINO GAMMA”的行动，旨在大量窃取用于保障个人手机与移动网络通信安全的鉴权密钥。美西方情报机构通过窃取手机 SIM 卡鉴权密钥，进而获取手机通信数据的行为被暴露无遗。

荷兰金雅拓公司是全球最大的 SIM 卡制造商之一，2019 年被法国军工企业泰雷兹集团（THALES）收购。2010 年前后其客户涉及全球 85 个国家的近 450 家移动运营商，每年生产约 20 亿张 SIM 卡[1]。斯诺登泄露的文件显示，仅在 3 个月的行动“测试”期间，GCHQ 就收集了数百万个手机 SIM 卡鉴权密钥，涉及伊朗、阿富汗、也门、印度、塞尔维亚、冰岛和塔吉克斯坦等国的多家移动运营商[2]，密钥窃取量可见一斑。此外，行动期间美英情报机构紧密配合，GCHQ 使用 NSA 的 XKEYSCORE 系统进行目标筛选与锁定，其获得的 SIM 卡密钥也与 NSA 情报共享。

（二）攻击方式

使用 NSA 的 XKEYSCORE 系统锁定目标：行动中 MHET 使用 NSA 的 XKEYSCORE 系统截获了金雅拓公司与移动运营商邮件服务器上的大量电子邮件，通过对邮件内容的分析找到可能有权访问金雅拓核心网络和密钥生成系统的重点人员或线索。

XKEYSCORE 是 NSA 用于检索和分析全球互联网数据的系统。XKEYSCORE 系统通过分布全球 150 个站点的服务器，实时拦截电子邮件、网络电话、网络聊天记录以及浏览历史等数据[3]。分析人员可以通过姓名、电话号码、IP 地址、浏览器等多种关键字来查找目标网络活动的内容数据和元数据。凭借该系统，NSA 可对互联网上特定目标的一举一动尽收眼底。XKEYSCORE 还具有良好的扩展性，可以与 NSA 的 TURBULENCE（湍流）网络攻击作业体系集成或交互，对其他渠道采集的网络信息进行自动分析，并触发任务逻辑；也可以接受来自其他项目任务的数据（如，外国卫星通信收集 SKIDROWE 项目的数据），并提供分析处理功能；XKEYSCORE 也为“五眼联盟”国家使用和共享情报提供支持[4]。

MHET 在邮件排查中发现，金雅拓公司采用电子邮件或 FTP 的方式，向其全球运营商客户批次发送 SIM 卡加密密钥。而在密钥文件的传输上，金雅拓仅采用易破解的简

单加密方式，有时甚至不对密钥文件进行加密就直接传输。这种粗放的传输方式为美英情报机构截获密钥文件创造了条件。

入侵金雅拓公司的内部网络：为了更方便、更准确的窃取 SIM 卡加密密钥，MHET 还入侵了金雅拓公司的内部网络，在多台内部计算机上植入恶意软件，为访问金雅拓公司内网提供权限，为截取密钥查找目标。斯诺登泄露文件显示，MHET 已经“成功地植入了金雅拓的多台机器，掌握了其整个网络，正在处理获取的数据”[5]。

开发程序批量窃取密钥：在前期侦察的基础上，MHET 成功截获了多个金雅拓个性化中心与移动运营商之间互联网通信数据，获取加密密钥。“拦截者”网站文章称，仅在 1 个月的时间内，MHET 就访问了与网络运营商或金雅拓有联系的 130 人的电子邮件，获取了近 8,000 个与 10 个国家特定手机相匹配的密钥，通过挖掘 6 个电子邮件，获取了 85,000 个加密密钥[1]。

为了进一步更大范围、更大量的窃取金雅拓与移动运营商之间传输的加密密钥，美英情报人员还专门开发了一种自动化拦截、采集密钥的程序。文件显示使用该程序“情报人员可以发现大量采用人工方式没有发现的密钥”[6]。不仅如此，2011 年 GCHQ 还发起了一项名为“HIGHLAND FLING”的行动，目标包括“攻击金雅拓位于法国的核心数

据存储库”、“渗透一个或多个将加密密钥写入 SIM 卡的金雅拓个性化中心”、以及“对德国 SIM 卡巨头捷德公司（Giesecke&Devrient）采取类似的密钥盗窃行动”[7]。

（三）延伸分析

SIM 卡加密密钥是手机与移动网络进行身份认证和信道加解密的重要工具。窃取 SIM 卡加密密钥可以为情报机构针对手机的抵近侦察提供技术支撑。如果拥有了目标手机的加密密钥，攻击者将更容易实现伪基站与目标手机的认证连接，特别是在安全性更高的 3G、4G 网络中。拥有了加密密钥将更容易破解通信加密，还原出明文通信内容。正如美国约翰·霍普金斯大学（Johns Hopkins University）密码破解专家马修·格林（Matthew Green）所说“对于 2G 网络来说还有其他方法可以侵入网络，但 3G、4G 网络并不容易破解，所以密钥就显得尤为重要”[1]。此外、美英情报机构窃取未启用的 SIM 卡加密密钥还可以建立手机 SIM 卡加密密钥数据库，为未来的信号情报（SIGINT）提供支撑。

提到信号情报获取，最为庞大的就是由美国主导的“梯队”（ECHELON）全球信号情报收集和分析系统。该系统由 NSA、GCHQ、加拿大通信安全局（CSEC）、澳大利亚信号局（ASD）和新西兰政府通讯安全局（GCSB）联合建立。系统最早成立于 20 世纪 70 年代，起初用于冷战期间监控苏联及其阵营之间的军事和外交通信，冷战结束后

转为截获全球范围内的商业和个人通信。“梯队”系统通过无区别地拦截通信数据，从海量数据中识别和提取有价值的信息。系统在世界各地建立了多套拦截设施并在“五眼联盟”国家设置了站点，执行远程情报收集和处理任务。

“梯队”系统的站点通过拦截卫星通信、交换电话网络和微波链路承载的通信数据，分析和处理全球范围内的电话呼叫、传真、电子邮件和其他流量数据。在系统中每个站点都会自动检索截获的数百万条消息并进行关键字匹配。系统的检索列表不仅包含站点所在国情报机构设置的关键词，还包含为五眼联盟其他机构设置的关键词。每当遇到包含某个情报机构关键词的数据时，它会自动挑选出该消息并将其直接发送到相关情报机构[8]。

不论是对手机 SIM 卡加密密钥的窃取，还是通过“梯队”系统对全球信号情报数据的收集，都反映出以美国为首的西方情报机构对全球信号情报数据持续的、大规模的疯狂搜集。无论是终端设备还是骨干线路，无论是政府官员、技术专家等高价值目标还是普通民众，都有可能成为美情报机构开展情报活动的目标。

参考资料

[1] Jeremy Scahill，Josh Begley. The Intercept. THE GREAT SIM HEIST. 2015. https://theintercept.com/2015/02/19/great-sim-heist/

[2] Grant Gross. Spy agencies hacked SIM card maker's encryption. 2015.

https://www.computerworld.com/article/2886738/spy-agencies-hacked-sim-card-makers-encryption.html

[3] Glenn Greenwald. The Guardian. XKeyscore: NSA tool collects nearly everything a user does on the internet. 2013. https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

[4] “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

[5] David Gilbert. International Business Times UK. US and UK spies hack SIM card encryption to monitor mobile phone conversations. 2015. https://www.ibtimes.co.uk/us-uk-spies-hack-sim-card-encryption-monitor-mobile-phone-conversations-1488759

[6] Snowden Archive. PCS Harvesting at Scale. 2015. https://grid.glendon.yorku.ca/items/show/269

[7] Snowden Archive. DAPINO GAMMA CNE Presence and IPT keys : Our workshops aims. 2015. https://grid.glendon.yorku.ca/items/show/333

[8] Nicky Hager. EXPOSING THE GLOBAL SURVEILLANCE SYSTEM. 2018. https://cryptome.org/echelon.htm

第三篇　悄无声息的入侵——针对苹果手机的“零点击”攻击

iOS 系统平台是由苹果公司开发的移动操作系统，用于 iPhone、iPad 和 iPod touch 等苹果移动设备。iOS 系统平台内置了一些苹果独有的功能，如 iMessage 就是苹果公司开发的即时通信服务，具有发送和接收短信、图像、视频和文档等多种功能，为苹果用户提供便捷的社交体验。而这类即时通信服务却成为了美情报机构利用的目标，美情报机构通过该类服务向苹果手机用户发送恶意代码或攻击载荷，以达到窃取手机数据的目的。2023 年 6 月俄罗斯联邦安全局（FSB）发表声明，指责 NSA 实施了针对苹果手机的“三角测量行动”（Operation Triangulation）。

图 3-1 NSA“三角测量行动”（Operation Triangulation）案例清单

（一）事件回顾

2023 年 6 月 1 日，网络安全公司卡巴斯基表示，其数十名高级员工的苹果手机遭受到入侵并发布名为《三角测量行动：iOS 设备被前所未知的恶意软件攻击》[1]的报告，揭露了一起最早可追溯到 2019 年的针对苹果手机和 iPad 设备的“零点击”攻击恶意行动。“零点击”攻击是指在整个攻击过程中无需手机用户进行任何交互操作，就可完成对目标移动设备的植入。由于攻击过程中使用了绘制并验证三角形来识别目标的技术，研究人员将这一系列攻击活动命名为“三角测量行动”[2]。随后，卡巴斯基陆续发布了共 6 份相关报告[3-6]。

同日，俄罗斯联邦安全局（FSB）发布声明指责美苹果公司与 NSA“密切合作”，通过复杂的恶意软件入侵了数千部苹果手机，目标主要为“驻俄罗斯和后苏联国家的外国外交人员，包括北约成员国、以色列、叙利亚和中国的外交人员以及部分俄罗斯当地用户”。FSB 称“苹果公司为美情报机构对俄开展情报监视活动提供了机会与条件，监视对象也包括美在反俄活动中的合作伙伴以及美国自己的公民”[7]。

（二）攻击方式

“三角测量行动”利用 iOS 系统内置的 iMessage 消息

服务和 iOS 系统 4 个零日漏洞，实现对苹果设备的“零点击”攻击。

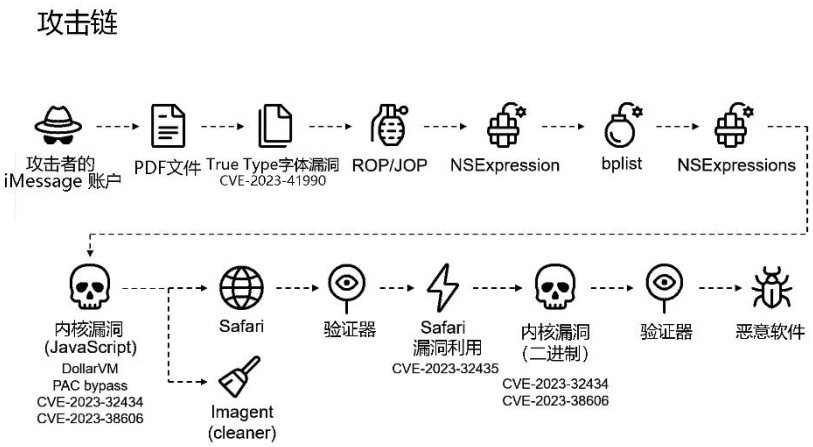


图 3-2 “三角测量行动”攻击链示意图[6]

攻击者首先通过 iMessage 服务器向目标 iOS 设备发送包含隐藏恶意附件的 iMessage 信息，设备在收到消息后，自动触发系统 4 个零日漏洞，自动完成后续恶意程序的植入。攻击者起初利用 WebKit 内存损坏和字体解析漏洞获取执行权限，随后利用整形溢出漏洞提升得到内核权限，再利用多个内存漏洞突破苹果硬件级的安全防御功能，在设备上执行并植入恶意程序。整个过程完全隐藏，不需要用户执行任何操作。恶意程序悄悄地将手机内的个人信息自动传输到设置好的远程服务器上。包括麦克风录音、即时通信的照片、地理位置以及设备的其他数据。

卡巴斯基针对主要的植入武器进行分析并将其命名为 TriangleDB。TriangleDB 在获取 iOS 系统内核 ROOT 权限后仅部署在手机内存中，手机重新启动后 TriangleDB 就会消

失，攻击者则须重新发送 iMessage 再次部署。如果在整个攻击过程中手机始终没有重启，TriangleDB 也将在 30 天后自行卸载消失，这一特性进一步增加了其隐蔽性[4]。

TriangleDB 在被部署前还有一个被称为“二进制验证器”的组件，该组件负责删除日志痕迹以及搜集命中设备的详细信息，并将这些信息发回 C2 服务器供攻击者判断设备价值，决定是否执行 TriangleDB 流程，若正常执行，TriangleDB 则从 C2 服务器加载调用多个子间谍模块，包括麦克风录音模块、KeyChain 凭证获取模块、SQLite 数据库窃密模块、GPS 定位模块、短信窃密模块等，支持攻击者开展平台级别的窃密操作活动，期间所有通信流量都经过对称（3DES）和非对称（RSA）算法加密并通过 HTTPS 协议进行交换。此外，攻击者还使用 WebGL 图形渲染程序进行画布指纹识别来验证目标。

2023 年 12 月 27 日，卡巴斯基发布《三角测量行动：最后一个（硬件）谜团》报告称，攻击者将数据写入特定的物理地址，同时通过将数据写入固件中未使用芯片的未知硬件寄存器来绕过基于硬件的内存保护，不知道攻击者是如何了解到并能使用这个未知硬件功能（unknown hardware feature）[6]。报告推测苹果公司可能与美情报机构合作。

（三）延伸分析

多数手机恶意软件在感染目标过程中依赖于用户的点击触发才能达成部署，对此用户可以通过提高自身安全意识来防范，而“零点击”攻击不需要用户对手机进行任何操作，不需要用户点击某个链接或打开某个文件，只要手机用户收到相关内容，恶意程序就能自动植入手机。大多数被攻击对象并不知道他们的手机已被植入恶意程序，很难保护个人手机与隐私安全。“零点击”攻击多利用系统未知或未被修复的漏洞，因此系统开发人员无法及时发现并修复。正如美国飞塔网络安全公司（Fortinet）研究员阿米尔·拉卡尼（Aamir Lakhani）所说，“即使是非常警惕和有意识的用户也无法避免零日漏洞攻击和‘零点击’攻击双重打击”[8]。

随着手机系统的日趋完善，能被发现和利用的“零点击”漏洞变得越来越少，“零点击”攻击成本变得越来越高。如以购买和销售漏洞为主要业务的美国 Zerodium 公司，就曾为获取“零点击”漏洞而公开出价 250 万美元[8]。这些都决定了像“三角测量行动”这样的攻击行为不可能大范围进行，攻击必然是针对高价值目标和小范围特定人群开展的。在“三角测量行动”攻击过程中，攻击者植入 TriangleDB 前进行了大量目标与设备信息的验证并删除部分

攻击痕迹，TriangleDB 仅存在于手机内存当中且具备自删除能力。这些都再次证明“三角测量行动”具有攻击手法高隐蔽性、攻击流程高复杂性、攻击目标高定向性的特点。根据这些特点有理由推断该行动是由具有国家背景的组织机构精心策划与实施的。

2024 年 1 月 16 日卡巴斯基发布报告称[9]，由于 iOS 系统特性，在 iOS 中发现恶意软件非常复杂且成本高昂，iOS 系统安全威胁往往不易被公众发现，其开发的轻量级检测工具，可检测出“飞马”间谍软件及其他 iOS 恶意软件。iOS 在各种手机系统中被认为体系结构设计相对更为合理，安全机制相对完备，但恰恰是美国情报机构自己的活动，严重影响全球用户对苹果手机的安全信任。

正如 2023 年 6 月 1 日俄外交部所说[10]，**“数十年来，美国情报机构一直在利用科技公司在互联网用户不知情的情况下大量收集用户数据”，“美国是一个将自己凌驾于法律之上的国家，任何国家都无权在访问智能手机用户个人数据等敏感领域滥用其技术能力。”**

参考资料

[1] Igor Kuznetsov.et al. Operation Triangulation: iOS devices targeted with previously unknown malware. 2023 https://securelist.com/operation-triangulation/109842/.

[2] GEORGY KUCHERIN.et al. The outstanding stealth of Operation Triangulation. 2023.
https://securelist.com/triangulation-validators-modules/110847/

[3] Igor Kuznetsov. et al. In search of the Triangulation: triangle_check utility. 2023.
https://securelist.com/find-the-triangulation-utility/109867/

[4] Georgy Kucherin.et al. Dissecting TriangleDB.a Triangulation spyware implant. 2023.
https://securelist.com/triangledb-triangulation-implant/110050/

[5] Leonid Bezvershenko.et al. How to catch a wild triangle. 2023.
https://securelist.com/operation-triangulation-catching-wild-triangle/110916/

[6] Boris Larin.et al. Operation Triangulation: The last (hardware) mystery. 2023.
https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/

[7] FSB. ФСБ РОССИИ ВСКРЫТА РАЗВЕДЫВАТЕЛЬНАЯ АКЦИЯ АМЕРИКАНСКИХ СПЕЦСЛУЖБ С ИСПОЛЬЗОВАНИЕМ МОБИЛЬНЫХ УСТРОЙСТВ ФИРМЫ APPLE. 2023.
http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439739%40fsbMessage.html

[8] Andrada Fiscutean. CSO. Zero-click attacks explained, and why they are so dangerous. 2022.
https://www.csoonline.com/article/572727/zero-click-attacks-explained-and-why-they-are-so-dangerous.html

[9] Maher Yamout. A lightweight method to detect potential iOS malware. 2024.
https://securelist.com/shutdown-log-lightweight-ios-malware-detection-method/111734/

[10] The Ministry of Foreign Affairs of the Russian Federation. Press release on new facts of global surveillance by the United States. 2023.
https://www.mid.ru/cn/foreign_policy/news/1873533/

第四篇　“飞马”风波——对商用间谍软件的利用

“飞马”（Pegasus）间谍软件是以色列网络武器供应商NSO集团旗下的一款知名产品，该软件可以通过“零点击”方式感染目标手机，秘密地安装在运行iOS和安卓系统的手机（或其他移动智能终端）上，对目标手机进行长期监控。“飞马”软件可获取手机上的详细数据，包括电子邮件、照片、短信、通话记录等。除此之外，还能获取手机所处的地理位置，甚至能控制手机的摄像头与麦克风。从2018年开始，美国CIA、FBI等情报机构纷纷采取各种方式和手段利用“飞马”等间谍软件对相关手机用户进行监控。

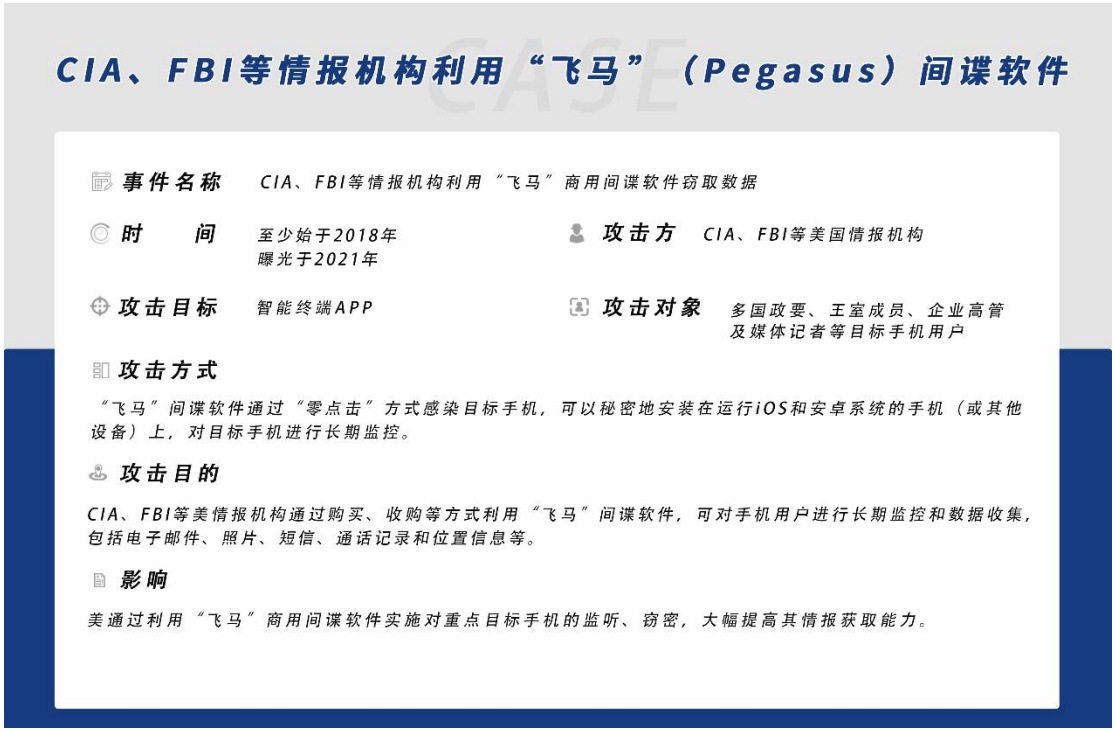


图 4-1 CIA、FBI 等情报机构利用“飞马”（Pegasus）间谍软件案例清单

（一）“飞马”间谍软件事件回顾

2021 年 7 月 18 日，《华盛顿邮报》、《卫报》等全球十余个国家的 17 家国际知名媒体机构[1]，在对以色列间谍软件“飞马”调查数月之后共同发表了一项调查报告，揭露了多个国家元首和政界要员受到了这款间谍软件的监听，包括法国总统马克龙、伊拉克总统萨利赫、南非总统拉马福萨、巴基斯坦总理伊姆兰·汗、埃及总理马德布利等，此外还有各国的众多王室成员、政府官员、企业高管、媒体记者等公众人物。“飞马”攻击事件经媒体曝光后，在国际社会引起轩然大波，这起事件让人们对商用间谍软件的超高攻击能力有了更深层的了解和认识。

（二）美情报机构对“飞马”等间谍软件的利用

“飞马”软件强大的攻击渗透和监控能力，吸引了全球的关注目光，也成为了有关国家政府和情报机构趋之若鹜的对象。美国对“飞马”软件青睐有加，美国缉毒署、特勤局和美军非洲司令部都与 NSO 集团进行过接触[2]，而 CIA 和 FBI 等情报机构也与 NSO 集团开展了深度合作。

1、 CIA 与“飞马”软件的技术渊源

据《纽约时报》2022 年 1 月报道[3]，早在 2018 年美国 CIA 就以反恐的名义购买了“飞马”软件，CIA 称其购买这款间谍软件的目的是为了支持吉布提政府的反恐行动。福

布斯网站 2017 年 3 月份发表的一份调查报告显示[4]，“据匿名安全研究人员称，CIA 入侵 iPhone 时使用的持久化技术与以色列网络武器供应商 NSO 集团的技术类似”，“它们都使用相同的漏洞，但实施方式略有不同”。由此可见，CIA 与 NSO 的技术渊源很深，他们之间或许存在着更深层次的合作关系。

2、 FBI 与 NSO 集团的深度合作

除 CIA 外，FBI 也是 NSO 集团的客户。《纽约时报》2022 年 1 月披露，“FBI 在 2018 年购买了‘飞马’软件，并在接下来的两年里在新泽西州的一个秘密设施测试了这款间谍软件”[3]。2019 年 6 月，3 名以色列 NSO 集团的工程师来到了位于美国新泽西州的 FBI 大楼，就“飞马”软件的功能和性能进行演示和测试。

NSO 工程师关于“飞马”间谍软件的功能演示引起了 FBI 的浓厚兴趣，但由于以色列政府的限制，普通版的“飞马”软件无法监视美国人的手机号码。为了解决这个问题，NSO 此后向 FBI 提供了一种名为“幻影”（Phantom）的新系统，该系统可以破解 FBI 瞄准的任何号码。以色列政府特意向 NSO 颁发了特殊许可证，允许美国政府机构客户使用该系统攻击美国号码。NSO 美国分支机构宣称，“‘幻影’系统允许美国执法和情报机构通过从移动设备提取和监控关键数据来获取情报。它是一个独立的解决方案，不需要

AT&T、Verizon、苹果或谷歌的合作。该系统将使目标的智能手机变成情报金矿”[2]。

3、 美政府通过影子公司购买 NSO 集团产品

据《纽约时报》2023 年 4 月报道[5]，一家美国政府影子公司 2021 年 11 月 8 日与以色列 NSO 集团的美国分支机构签订了一份秘密合同。根据协议安排，NSO 集团向美国政府提供地理定位工具“地标”（Landmark），该软件可以在用户不知情或不同意的情况下秘密跟踪手机位置。这笔交易的隐蔽性不同寻常，是由一位商人用假名代表影子公司签署的。而签署时恰值美商务部宣布制裁 NSO 集团几天后，这也充分显示了美国政府在网络武器扩散和公民隐私监控方面的两面性和虚伪面目。

4、 美情报机构授意国防承包商收购 NSO 集团

2022 年，美国知名国防承包商 L3 Harris 在美情报机构的授意下准备收购 NSO 集团[5]，意图全面控制 NSO。L3 Harris 与 NSO 达成的一项潜在协议，旨在购买 NSO 的黑客工具并接管其大部分员工。根据内部记录，尽管 NSO 被列入商务部黑名单，但 L3 Harris 高管与商务部官员就潜在交易进行了讨论，并已经制定了一份交易协议草案。尽管最终未能成功收购，该事件充分显示出美情报机构拟控制商业间谍软件实施情报活动的企图。

5、 持续利用其他以色列间谍软件

美国政府机构持续使用与“飞马”功能类似的间谍软件。媒体透露美国缉毒署（DEA）是以色列 Paragon 公司 Graphite 软件最大的客户之一。Paragon 公司吸取了 NSO 公司的教训，与美国政府建立密切的沟通渠道，包括：其客户清单寻求获得美国的许可；向两家美国风险投资公司 Battery Ventures 和 Red Dot 寻求资金，以获得美国的支持；聘请了一家美国政治咨询公司，就为赢得政府订单提供建议。通过这些措施，Paragon 公司实际上获得了美国政府的默许，美国政府间接获得了对 Paragon 公司很强的控制力[6]。

值得注意的是，DEA 虽然是打击非法毒品交易的执法机构，但其与美情报机构却有着千丝万缕的关系。DEA 经常利用其打击毒品交易的便利身份，为情报机构在境外开展活动提供帮助和掩护[7]。尽管美国政府禁用了“飞马”软件，但是仍在利用类似的间谍软件实施情报活动。

（三） 延伸分析

美表面上通过制裁 NSO 集团限制其他国家利用其软件，但背地里却通过影子公司购买其间谍软件，并授意国防承包商收购 NSO 集团。FBI 打着测试的幌子与 NSO 合作，开发了可攻击美国境内手机的“幻影”系统；FBI 还通过承包商 Riva 网络公司利用“地标”间谍软件在墨西哥实施长时

间的手机监控活动[8]。

美以之间的情报协同，历史上不仅有以方企业提供商业间谍工具给美方使用，也有以美为主研发攻击武器，双方联合运用，其中著名事件包括“震网”和入侵卡巴斯基的“毒曲 2”。**美情报机构通过利用和控制商业间谍软件，进一步强化了在移动网络领域的监控和情报获取能力。**

2022 年 4 月 5 日，美国《华盛顿邮报》报道称[9]，FBI 与 Babel Street 公司签订了高达 2700 万美元的创纪录软件服务合同，强化对社交媒体内容的搜索与追踪能力。FBI 招标条件明确要求软件“至少具备七种外语”的搜索及翻译能力，能实现对某一设定地理区域的搜索，可以对发帖人进行关联分析和情绪分析等，还要有表情分析、预测分析、机器探测等附加功能。透过这些令人不寒而栗的需求可以看到，**美情报机构通过对商用软件的利用将其已武装到牙齿的网络情报搜集能力发挥到极致。**

参考资料

[1] Takeaways from the Pegasus Project. 2021. https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/

[2] Ronen Bergman, Mark Mazzetti. The Battle for the World’s Most Powerful Cyberweapon. 2022. https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

[3] Mark Mazzetti , Ronen Bergman. F.B.I. Told Israel It Wanted Pegasus Hacking Tool for Investigations.2022.

https://www.nytimes.com/2022/05/12/us/politics/fbi-pegasus-spyware-israel.html

[4] Thomas Brewster. Wikileaks CIA Mega-Leak Implicates US And UK Spies In Deep iPhone Hacks.2017. https://www.forbes.com/sites/thomasbrewster/2017/03/07/iphone-wikileaks-cia-exploits-not-catastrophic/?sh=16846116650a

[5] Mark Mazzetti, Ronen Bergman. A Front Company and a Fake Identity: How the U.S. Came to Use Spyware It Was Trying to Kill. 2023. https://www.nytimes.com/2023/04/02/us/politics/nso-contract-us-spy.html

[6] Ben Lovejoy. US govt banned NSO's Pegasus, but said to buy rival spyware Paragon Graphite. 2023. https://9to5mac.com/2023/05/30/paragon-graphite/

[7] Ben Buchanan. The Hacker and The State. 2020. https://gerdab.ir/files/fa/news/1400/6/23/49615_176.pdf

[8] Mark Mazzetti. Who Paid for a Mysterious Spy Tool? The F.B.I., an F.B.I. Inquiry Found. 2023. https://www.nytimes.com/2023/07/31/us/politics/nso-spy-tool-landmark-fbi.html

[9] Aaron Schaffer. The FBI is Spending Millions on Social Media Tracking Software. 2022. https://www.washingtonpost.com/politics/2022/04/05/fbi-is-spending-millions-social-media-tracking-software/

第五篇　无法卸载的 APP——通过运营商广泛预置软件收集数据

安卓系统是全球最主要的手机操作系统之一。为追求更好的性能、用户界面和功能等目的，手机厂商多选择对原生的安卓系统进行深度定制。部分厂商会在只读存储器（ROM）中预装某些特定的应用程序，这些应用程序有可能成为美情报机构获取用户数据的工具。2011 年曝出美运营商 AT&T、Verizon、Sprint 和 T-mobile US 在手机中广泛预置 Carrier IQ 软件，该软件违规收集包括短信、键盘操作等在内的用户数据，运营商使用 Carrier IQ 后台产品可进行数据查询，FBI、NSA 则通过与运营商的情报合作获取远超法律授权范围的用户数据。

图 5-1 FBI、NSA 通过 Carrier IQ 软件收集用户数据案例清单

（一）事件回顾

Carrier IQ 成立于 2005 年，是一家美国的私营移动软件公司，其产品由移动设备上的嵌入式软件（IQ Agent）和服务器端分析应用程序组成，目的是使移动运营商能够详细了解移动服务和设备的各种性能和使用特征。IQ Agent 于 2006 年首次应用于智能手机上，随后应用于 USB 调制解调器和平板电脑等其他设备上。[1]

2011 年 11 月 12 日，美国白帽黑客特雷弗·埃克哈特（Trevor Eckhart）在安卓系统安全测试网站（androidsecuritytest.com）上发文称[2]，Carrier IQ 软件搜集与网络相关的信息，包括语音和数据服务；还搜集与网络无关的信息，包括设备类型、可用内存和电池电量、设备中软件的类型、设备的地理位置信息、设备用户的按键信息、设备的使用历史等，并回传服务器进行统计分析。Carrier IQ 提供的后台产品允许运营商等用户可以根据国际移动设备识别码 IMEI 或国际移动用户识别码 IMSI 对任何一个设备进行详细的历史记录查询，即用户的隐私被完全暴露给该公司及使用其服务的移动运营商。通常情况下，Carrier IQ 软件深度预装入 ROM。因此，要想彻底删除该软件，必须先 ROOT 手机后重新烧写（Flash）干净手机 ROM。普通用户一般难以操作。

2011 年 11 月 28 日，埃克哈特在 YouTube 发布视频，

展示 Carrier IQ 软件以明文形式记录各种击键的行为[3]，包括对安全网站密码的明文捕获，以及在禁用蜂窝网络时执行的活动。

2011 年 11 月，安天发布《对 Carrier IQ 木马的综合分析报告》[4]，证实 Carrier IQ 不仅主动捕获和读取用户手机的短信内容、监控用户的键盘操作和按键内容，甚至对获取的数据进行记录及传输。

（二）事件分析

美国四大电信运营商 AT&T、Verizon、Sprint 以及 T-Mobile US 均为 Carrier IQ 的用户，在其多款手机中预装了这一软件，涉及安卓、塞班、黑莓、iOS 等多个平台。相关报道称受影响设备数量达 1.41 亿[5]。黑莓、HTC、三星等多个品牌手机中均预装了 Carrier IQ 软件，手机厂商均表示是美国运营商强制要求在其设备上安装的。

2011 年 12 月，FBI 为拒绝按照《信息自由法》（FOI）要求公开 Carrier IQ 相关文件，被迫承认“为执法目的而编译的调查文件”中使用了 Carrier IQ 收集的数据[6]。

2013 年 6 月，彭博社发表文章《NSA 可以收集的远远超过你的电话记录》[7]指出，Carrier IQ 收集数据的情况曝光后，许多美国运营商和设备制造商从他们的手机中删除了 Carrier IQ 软件，但事实是运营商仍然在客户的手机上安装了隐藏的监控软件。对于 NSA 来说，从运营商网络中收

集和汇总这些数据并不困难，就像它从谷歌获取大量数据一样。

（三）延伸分析

Carrier IQ 搜集数据情况曝光后，AT&T 承认自 2011 年 3 月开始在其设备上安装了该软件[8]。2015 年 12 月，AT&T 低调收购了 Carrier IQ，且未披露交易的相关细节。美各大运营商与情报机构合作由来已久。根据斯诺登曝光的信息，AT&T 公司与 NSA 开展了长达几十年的合作[9]，“棱镜”计划（PRISM）显示美情报机构对运营商和大型互联网厂商的数据进行深度挖掘和获取。2013 年 6 月 5 日，英国“卫报”网站报道称，NSA 曾要求 Verizon 公司提供数百万私人电话记录[10]。

美国各大运营商通过 Carrier IQ 软件获取了远超其流量优化所需的大量用户隐私数据，基于 AT&T 和 Verizon 等美国电信运营商与美情报机构的深度合作关系，**全球移动用户有理由怀疑，美情报机构通过美国境内的电信运营商，采取在用户手机中广泛预置 Carrier IQ 等网络诊断软件的方式，以极低的成本实现了对美国境内移动用户数据的采集，事实上已将移动运营商变为其情报资源**。

尽管美国国会 2015 年 6 月通过的《美国自由法案》（USA FREEDOM ACT）要求美情报机构在 6 个月之内停止原有的对电话数据进行大规模收集，之后需要向外国情

报监视法院（FISC）提出申请获得批准后，才可从电信公司调取特定对象的电话数据，但是美情报机构根本没有遵守该规定。美国《连线》杂志（WIRED）2023 年 11 月 20 日刊文《秘密的白宫监视计划使警察能够访问数万亿条美国电话记录》指出[11]，十多年来监控计划“数据分析服务”（DAS）允许美联邦、州和地方执法机构挖掘、分析美国用户的通话细节。DAS 计划的前身为“半球”计划（Hemisphere），允许美执法机构（包括警察、治安部门、美国海关、邮政检查员等）捕获和分析任何使用 AT&T 基础设施的全部通话记录。DAS 计划的曝光充分证明了**美情报机构的广泛监听活动无孔不入，即便是美国用户自身权益也无法得到保障。**

参考资料

[1] Wikipedia. Carrier IQ. 2024 https://en.wikipedia.org/wiki/Carrier_IQ#cite_note-21

[2] Trevor Eckhart. What is Carrier IQ?. 2011. https://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/

[3] Trevor Eckhart. Carrier IQ Part #2. 2011. https://www.youtube.com/watch?v=T17XQI_AYNo

[4] Antiy Labs. A Comprehensive Analysis on Carrier IQ. 2011. https://www.antiy.net/media/reports/carrieriq_analysis.pdf

[5] Dan Goodin. Carrier IQ VP: App on millions of phones not a privacy risk. 2011. https://www.theregister.com/2011/12/02/carrier_iq_interview/

[6] Andy Greenberg. FBI Says Carrier IQ May Be Used In 'Law Enforcement Proceedings'. 2011.

https://www.forbes.com/sites/andygreenberg/2011/12/12/fbi-says-carrieriq-may-be-used-in-law-enforcement-proceedings/

[7] Kevin Fitchard. The NSA Could Collect Far More Than Your Phone Records. 2013. https://www.bloomberg.com/news/articles/2013-06-12/the-nsa-could-collect-far-more-than-your-phone-records

[8] Brad Molen. Senator Al Franken asks about Carrier IQ, the companies answer: the complete breakdown. 2011. https://www.engadget.com/2011-12-17-senator-al-franken-asks-about-carrier-iq-the-companies-answer.html

[9] NSA Spying Relies on AT&T's 'Extreme Willingness to Help'. 2015. https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help

[10] Glenn Greenwald. 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

[11] Dell Cameron &Dhruv Mehrotra. Secretive White House Surveillance Program Gives Cops Access to Trillions of US Phone Records. 2023. https://www.wired.com/story/hemisphere-das-white-house-surveillance-trillions-us-call-records/

第六篇　窥探底数——获取全球移动运营商技术参数

自 20 世纪 70 年代美国贝尔实验室提出“蜂窝网络”概念以来，移动通信技术快速迭代更新。全球移动运营商的业务环境、运营模式等各不相同，因此其采用的网络制式、基础设施类型、加密方式、协议等技术参数也不尽相同。为获取全球移动运营商技术参数，以便挖掘漏洞针对性实施攻击，NSA 至少自 2010 年开始实施“金色极光”行动（AuroraGold），采取信号情报手段获取非公开数据——各移动运营商的国际漫游文件 IR.21，形成全球移动运营商技术参数数据情报库，支撑 NSA 信号情报生产链，对手机用户进行窃密及监听监控。

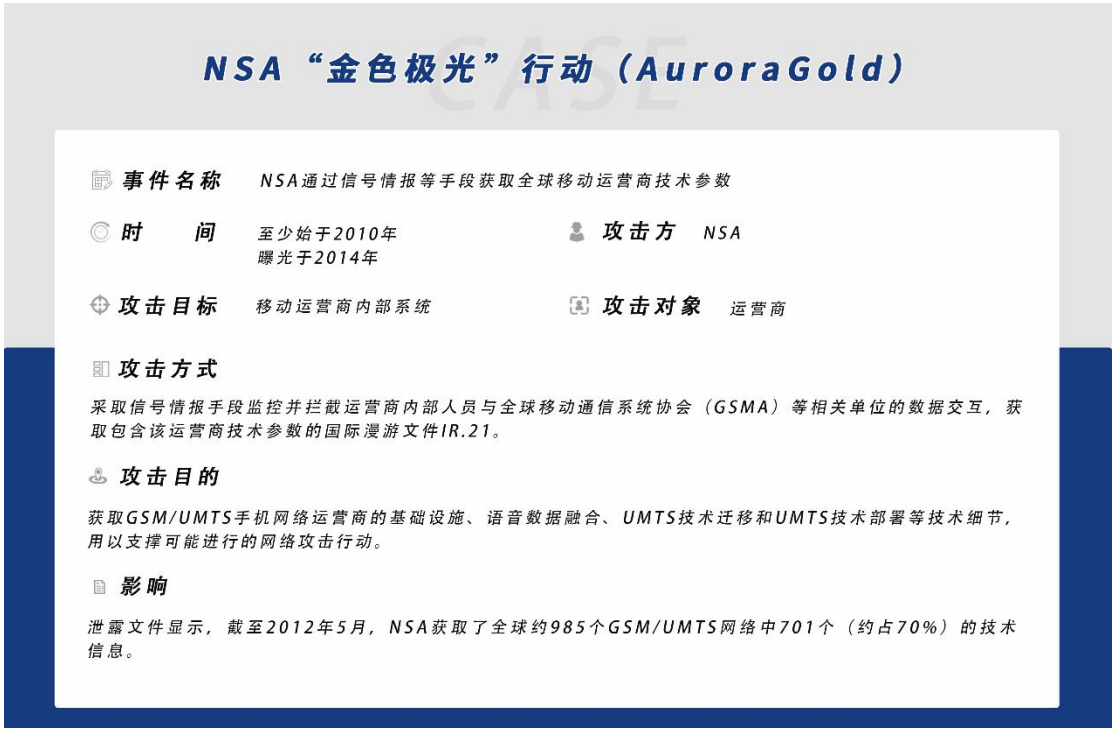


图 6-1 NSA“金色极光”行动（AuroraGold）案例清单

（一）事件回顾

2014 年 12 月 4 日，“拦截者”网站公布斯诺登泄露的相关文件显示，NSA 至少从 2010 年就开始“金色极光”行动[1]，旨在获取全球移动运营商技术参数，有效预测未来技术趋势，用以支撑信号情报生产链。“五眼联盟”情报机构均可共享“金色极光”数据情报库。

截至 2012 年 5 月，NSA 通过“金色极光”行动获取了全球约 985 个 GSM/UMTS 手机网络中 701 个（约占 70%）的技术信息，几乎覆盖了所有国家，包括英国、澳大利亚、新西兰、德国和法国等与美国关系密切的盟国。

（二）攻击方式

NSA 至少从 2010 年提出“信号情报规划循环”（SIGINT Planning Cycle）工程，旨在体系化地开展信号情报生产链工作，由 6 个环节组成，分别是：发现、区域&目标、技术趋势、漏洞、能力、交付。其中“金色极光”行动是“技术趋势”（Technology Trends）环节中的一部分。

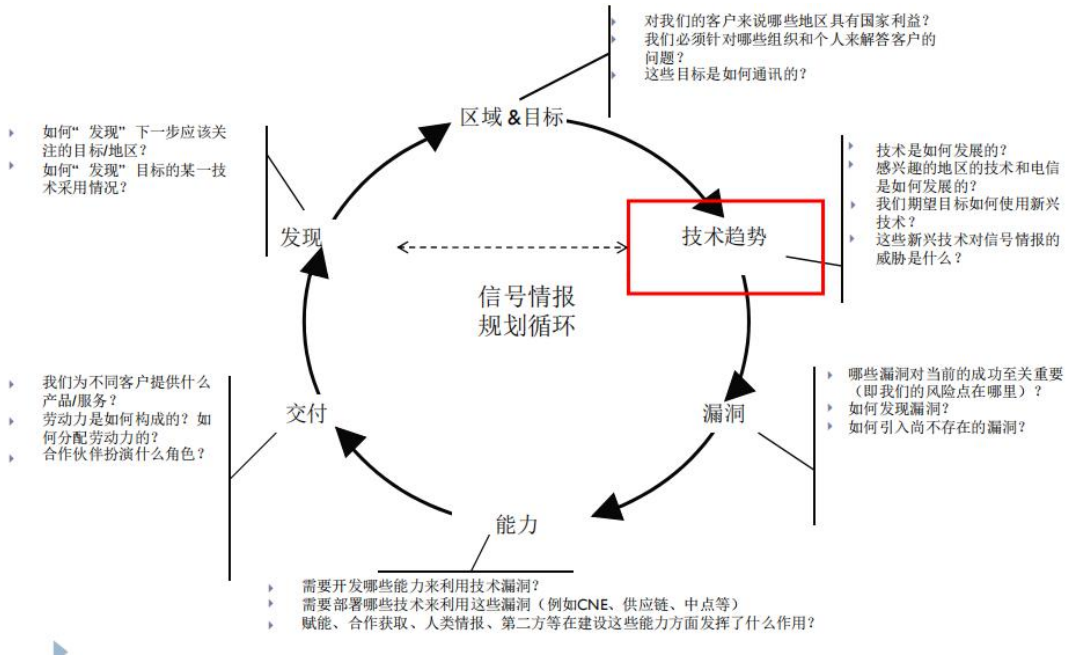


图 6-2 NSA“信号情报规划循环”示意图

在其后的“漏洞”环节，NSA 明确提出要利用“金色极光”行动提供的技术趋势数据，来识别其可以利用的漏洞，并引入尚不存在的漏洞，以在“能力”环节中利用这些漏洞。

德国安全研究员和密码学家卡尔斯滕·诺尔（Karsten Nohl）、芬兰网络安全公司 F-Secure 的高级研究员米克·海波宁（Mikko Hypponen）等多位网络安全专家均对 NSA 为达到间谍活动目的故意策划在全球通信系统中引入新漏洞的“金色极光”行动表示震惊。安全专家们指出[1]，一旦 NSA 引入了漏洞，那么就不仅仅是 NSA 可以利用它。这种有争议的策略可能会将普通民众暴露给黑客等犯罪分子。

NSA 文件显示，2011 年 3 月，在西方干预利比亚内乱两周前，美军非洲司令部利用“金色极光”行动的数据情

报库获取了利比亚全部移动运营商的短信网关域信息，并利用该信息入侵了利比亚的移动网络进行短信监控。

“金色极光”行动融合公开数据和非公开数据，经过数据解析和提取后构建了一个包含全球移动运营商技术参数及移动技术发展趋势的数据情报库，并以可视化方式输出。其中公开数据包括世界蜂窝信息服务（WCIS）可查询数据库的完整副本、国际电信联盟（ITU）运营公告及其他数据，非公开数据主要是“IR.21”。

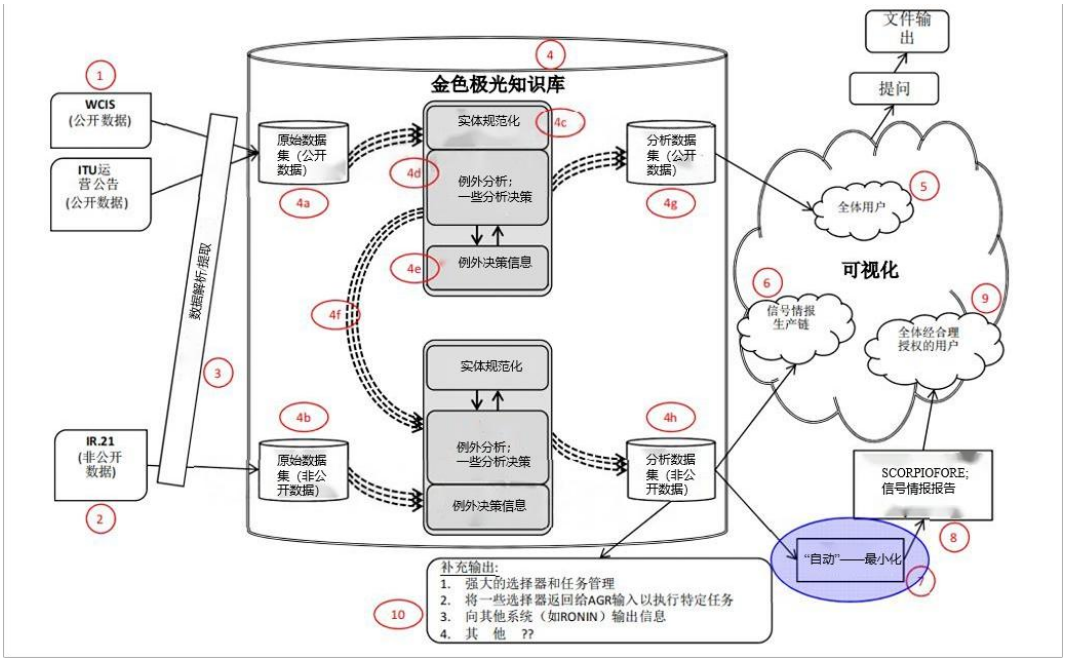


图 6-3 “金色极光”数据流与流程概述

IR.21 是国际漫游文件，是 GSM 国际漫游运营商间制作对方局数据的重要规范文件，以实现其客户在境外使用国际漫游服务。IR.21 文件标准格式由全球移动通信系统协会（GSMA）制定，GSMA 成立于 1995 年，是全球移动通信领域的行业组织，其成员包括 220 个国家和地区的近 800

家移动运营商以及230多家更为广泛的移动生态系统中的企业。

NSA评估认为IR.21包含了其“瞄准和利用所必需的信息”，可通过IR.21获取GSM/UMTS手机网络运营商的基础设施、语音数据融合、UMTS技术迁移和UMTS技术部署等技术细节，以支撑后续的情报工作。

表6-1 NSA评估IR.21文件的信号情报价值

IR.21字段	释义	利用价值
移动国家号（MCC） 移动网号（MNC）	唯一标识移动网络的十进制数字代码。所有用户的IMSI的前三位数字是用于标识国家的MCC，随后两位是用于标识该国家内网络的MNC	提供网络的唯一标识，以识别网络边界、接口、协议、软件、硬件等
移动用户国际号码（MSISDN）	在GSM或UMTS移动网络中移动用户的唯一标识号码（移动/蜂窝电话中SIM卡的电话号码）	允许识别所拨的真实电话号码
TADIG代码	GSMA分配的一个号码，用作文件内容和文件名中的主要标识符。也用作移动行业中更通用的实体标识符	识别用于计费目的的网络，并帮助确定目标
信令连接控制部分（SCCP）	一种网络层协议，用于在7号信令系统（SS7）电信网络中提供扩展的路由、流控制、分段、连接定向和纠错功能	在公共陆地移动网（PLMN）中提供路由信息，并提供对应用程序的访问，如800呼叫处理和电话卡处理，以识别目标和其他信息
用户身份验证	显示在GSM服务开始时是否对漫游用户执行身份认证以及A5加密算法的类型	还能展示新密码算法的出现，并支持目标分析、趋势和漏洞开发
移动应用部分（MAP）	一种SS7协议，它为GSM和UMTS移动核心网以及GPRS核心网中的各种节点提供了相互通信的应用层，以便向移动电话用户提供服务。MAP是用于访问归属位置寄存器、访问者位置寄存器、移动交换中心、设备标识寄	发布漫游协议信息时，可以更清楚地了解网络功能。提供关于用户、移动管理和应用程序的当前信息，这些信息可用于定位和目标开发

	存器、认证中心、短消息服务中心和服务 GPRS 支持节点（SGSN）的应用层协议	
网元信息	特定网络组件、制造商、软件和硬件版本等	这些特定信息对于定位和利用是必要的。包括核心和无线电接口信息
网络封包数据服务	用于识别受影响的 GPRS 网络。此信息中还包括一个接入点名称（APN）。APN 可以识别由 GPRS 网络提供给移动用户的服务类型。APN 还有助于识别 IR.21 中涉及的网络和运营商的封包网络，并可用于定位	提供关于正在接入的 WAP 网关和多媒体消息服务网关 IP 地址的信息，有助于目标开发。还提供了对网络中使用的 GPRS 隧道协议版本的深入了解。涵盖 GPRS、EDGE（增强型数据速率 GSM 演进技术）和 HSPA（高速分组接入）

为获取各运营商的 IR.21 文件，“金色极光”行动使用信号情报手段监控并拦截了运营商漫游协调员与 GSMA 工作组等相关单位的数据交互，以及相关的 1,200 多个电子邮箱信息。

除获取 IR.21 文件外，“金色极光”行动持续监视 GSMA、ITU 等行业组织，以尽早获取新的技术标准、全球移动通信新技术及其发展趋势等信息，支撑 NSA“信号情报规划循环”其他环节。

（三）延伸分析

“金色极光”行动中，NSA 将攻击目标锁定全球移动运营商，通过获取技术趋势等数据情报针对性地构建其网空攻击能力。2015 年 6 月斯诺登曝光的 NSA“拱形”计划（CamberDADA）反映出的美情报活动策略与此如出一辙。在“拱形”计划中[2]，NSA 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信进行监控，获取新的病毒样本，以协助其策划能够绕过检测的网络攻击行动，以及研发可利用的攻击武器。该计划后续目标还包括中国网络安全公司安天在内的 16 个国家 23 家全球重点网络安全厂商。

在“金色极光”行动中，NSA 极力收集的运营商 IR.21 文件包含通讯加密的详细信息，可用来破解加密和窃听对话。英国科技媒体 The Register 刊文分析“金色极光”事件时指出，NSA 的目标技术趋势中心（TTTC）在 GSMA 等标准机构内开展间谍行动，以获取包括加密标准在内的新安全协议的高级副本，以便能够在部署之前研究出如何破解它们[3]。事实上，NSA 一直觊觎密码体系。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[4][5]，证实了此前忧虑和怀疑已久的业界传闻。**NSA 长期对密码体系进行系统性操控，利用加密标准漏洞对全球实施监控，破坏了全球对网络技术的信任，也对全球网络安全生态造成极大损害。**

参考资料

[1] Ryan Gallagher. The Intercept. OPERATION AURORAGOLD：How the NSA Hacks Cellphone Networks Worldwide. 2014. https://theintercept.com/2014/12/04/nsa-auroragold-hack-cellphones/

[2] 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.2023.
http://www.china-cia.org.cn/AQLMWebManage/Resources/kindeditor/attached/file/20230411/20230411161510_6312.pdf

[3] Iain Thomson. The Register. Snowden files show NSA's AURORAGOLD pwned 70% of world's mobe networks. 2014.
https://www.theregister.com/2014/12/04/snowden_files_show_nsas_auroragold_pwned_70_of_worlds_mobile_networks/

[4] Nicole Perlroth, Jeff Larson, Scott Shane. 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

[5] James Ball, Julian Borger, Glenn Greenwald. 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

第七篇　伪装的基站——广泛使用伪基站监控手机

国际移动用户识别码 IMSI 用于识别移动电话用户在全球范围内的身份。IMSI 位于手机 SIM 卡当中，由 15 位数字组成，包含国家代码、移动网络代码和用户识别码等信息。手机在与移动网络建立连接时，使用 IMSI 完成认证后，合法接入网络。攻击者使用伪基站设备，强制手机与其连接，获取手机 IMSI、仿冒身份认证、建立网络与手机的中转连接，从而窃取通信数据。美情报机构和执法部门长期、广泛使用 Stingray 等伪基站对手机实施监控。

图 7-1 FBI、NSA、DHS 等使用伪基站设备案例清单

（一） 美情报机构和执法部门广泛使用伪基站

2013 年 5 月 8 日，美国公民自由联盟（ACLU）和电子前沿基金会（EFF）公开了一份简报[1]，披露美 FBI 使用侵入性监视技术和设备进行手机信息收集，其中所涉及的设备为美国防承包商 Harris 公司开发的伪基站 Stingray。

Stingray 是一款 IMSI 捕获器[2]，采取“中间人”攻击的方式开展工作，对于基站它是伪装的手机，对于手机它是伪装的基站。

图 7-2 Stingray 伪基站

连接建立后，Stingray 就具备了截获通信数据的能力，不仅可以收集手机的 IMSI 和位置信息，还可以窃取通话、短信和网络浏览信息。当用户使用 3G 及以上移动网络时，Stingray 还会迫使手机降级到 2G 网络，并要求手机采用不加密或可以破解的弱加密技术进行数据传输，以此来实现监控目的[3]。Stingray 系列设备可以在车辆、飞机、直升机和无人机上安装使用。手持版 Stingray 设备名为 KingFish，可随身携带使用。

2020 年 7 月 31 日美国“拦截者”网站发布文章[3]，披露美执法部门使用 Stingray 定位手机，获取短信、电子邮件和语音通话等信息，并通过情报合作在运营商的协助下掌握手机持有人的身份和住址信息，获取通联关系。Stingray 设备可以将目标精准定位在米级范围内，通过测量手机与 Stingray 设备的信号强弱锁定目标。

2014 年 11 月 13 日《华尔街日报》披露[4]，从 2007 年开始，美国法警局就在小型通用飞机上安装了名为“脏盒”（Dirtbox）的伪基站。该设备由美国防承包商波音公司旗下的数字接收器技术公司（DRT）制造，用于大范围收集手机用户的个人和位置信息[5]。“脏盒”单次飞行就能收集数万部手机的 IMSI 号码和位置信息，在飞机上就能将目标手机精确定位到大约 3 米的范围。与地面上的 Stingray 相比，空中的“脏盒”能够收集更多的数据，更方便、快速地在广阔的区域移动。

图 7-3 Dirtbox（DRT 2101A）伪基站

随着移动网络技术的发展，美情报机构和执法部门不断的更新采购该类设备。Harris 公司为其研发了多款针对

3G、4G 网络的伪基站。加拿大 Octasic 公司生产的伪基站也成为美情报机构和执法部门的采购目标，Octasic 的设备能够同时对包括 2G、3G、4G 在内的 8 个频段开展工作[6]。

伪基站被美政府部门和军队大量使用。根据美国公民自由联盟披露的信息[7]，Stingray 这类 IMSI 捕获器被美陆军、美海军、美海军陆战队、FBI、美国土安全部、美法警局等多个政府机构和军队单位使用。一名 FBI 人员在接受媒体采访时称[8]，其在 10 年间使用 Stingray 超过 300 次，美警察、特勤局以及其他联邦机构每天都在使用这一技术。美国公民自由联盟和美媒体披露数据显示，美国土安全部在 2013 年到 2017 年间，共使用 Stingray 设备 1885 次[9]，2017 年到 2019 年间至少使用 466 次[10]。美众议院监督委员会报告显示，美司法部拥有 310 套伪基站，美国土安全部拥有 124 套伪基站。2010 至 2014 财年，美司法部在伪基站技术上的支出超过 7100 万美元，美国土安全部在伪基站技术上的支出超过 2400 万美元[11]。

（二）伪基站成为监视和网络攻击的途径

伪基站将手机变成监视工具。2013 年 7 月 22 日《华盛顿邮报》发表的文章称，NSA 早在 2004 年就开发出了一项即使在手机关机的情况下也能定位的技术，美军称其为“The Find”，在伊拉克这项技术为他们提供了数千个新目标[12]。2014 年 6 月 6 日 CNN 网站发表《NSA 如何远程“打

开”你的手机》文章称[13]，NSA 通过伪基站向手机基带芯片发送命令，使手机无法真正关机，此时“关机”的手机或可开启麦克风用于环境监听，或可发送位置信息用于定位。

伪基站成为网络攻击的途径。“拦截者”网站文章称[3]，美军使用的伪基站可以发送钓鱼短信，还可以使手机通过军方控制的服务器而不是移动运营商的服务器收发短信，从而达到监控的目的。美情报机构使用的伪基站可以将恶意软件注入目标手机。如果手机浏览器存在漏洞，情报机构可以将手机浏览器定向到恶意网站，再将恶意软件下载到手机。

美 CIA 前任局长迈克尔·海登（Michael Hayden）坦言，NSA 监控计划并没对反恐起到作用，却可以让情报分析员跟踪民众的网络行为[14]。**美情报机构及执法部门滥用伪基站对个人手机实施的规模化、无差别监控，不择手段，极大侵害全球公民的通信权益，严重威胁他国国家安全。**

参考资料

[1] Linda Lye. ACLU. Court Ruling Gives FBI Too Much Leeway on Surveillance Technology. 2013. https://www.aclu.org/news/national-security/court-ruling-gives-fbi-too-much-leeway-surveillance

[2] Columns, Michael A. Miller. Long Island Weekly. Time For Cops To Come Clean On ‘Stingray’. 2014.

https://longislandweekly.com/time-for-cops-to-come-clean-on-stingray/

[3] Kim Zetter. The Intercept. How Cops Can Secretly Track Your Phone. 2020. https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/

[4] Devlin Barrett. The Wall Street Journal. Americans' Cellphones Targeted in Secret U.S. Spy Program. 2014. http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533

[5] Electrospaces. DRTBOX and the DRT surveillance systems. 2018. https://www.electrospaces.net/2013/11/drtbox-and-drt-surveillance-systems.html

[6] Dell Cameron.Dhruv Mehrotra. GIZMODO. Cops Turn to Canadian Phone-Tracking Firm After Infamous 'Stingrays' Become 'Obsolete'. 2020. https://gizmodo.com/american-cops-turns-to-canadian-phone-tracking-firm-aft-1845442778

[7] Wikipedia stingray phone tracker https://en.wikipedia.org/wiki/Stingray_phone_tracker

[8] K. Zetter. WIRED. Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight. 2013. http://www.wired.com/2013/04/verizon-rigmaiden-aircard/

[9] Adolfo Flores. BuzzFeed News. DHS Has Used A Controversial Cell Phone–Tracking Device More Than 1,800 Times. 2017. https://www.buzzfeednews.com/article/adolfoflores/this-is-how-many-times-the-department-of-homeland-security

[10] Alexia Ramirez. ACLU. ICE Records Confirm that Immigration Enforcement Agencies are Using Invasive Cell Phone Surveillance Devices. 2020. https://www.aclu.org/news/immigrants-rights/ice-records-confirm-that-immigration-enforcement-agencies-are-using-invasive-cell-phone-surveillance-devices

[11] House Committee on Oversight and Government Reform. Publicintelligence. House Oversight Committee Report on Law Enforcement Use of Cell-Site Simulation Technologies. 2016.
https://publicintelligence.net/us-cell-site-simulator-privacy/

[12] D.Priest. The Washington Post. NSA growth fueled by need to target terrorists. 2013.
https://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html

[13] Jose Pagliery. CNN. How the NSA can ‘turn on’ your phone remotely. 2014.
https://money.cnn.com/2014/06/06/technology/security/nsa-turn-on-phone

[14] 环球网. 盘点！美国操纵网络霸权的四大罪状. 2022.
https://opinion.huanqiu.com/article/49qsYllip9g

第八篇　入侵运营商内网——利用 Regin 软件攻击移动网络

Regin 是由美国 NSA 开发并与“五眼联盟”合作伙伴共享的一款功能特别强大的恶意软件，其技术先进、结构复杂、“隐身”能力强，可以根据不同目标定制功能，针对性部署，进行远程监控和情报收集。2010 至 2013 年期间，NSA 和 GCHQ 利用 Regin 联合攻击了比利时电信及其子公司国际载波服务公司的内部网络，入侵了提供跨国漫游服务的 GRX 路由器系统，对漫游的智能手机开展针对性的“中间人攻击”。

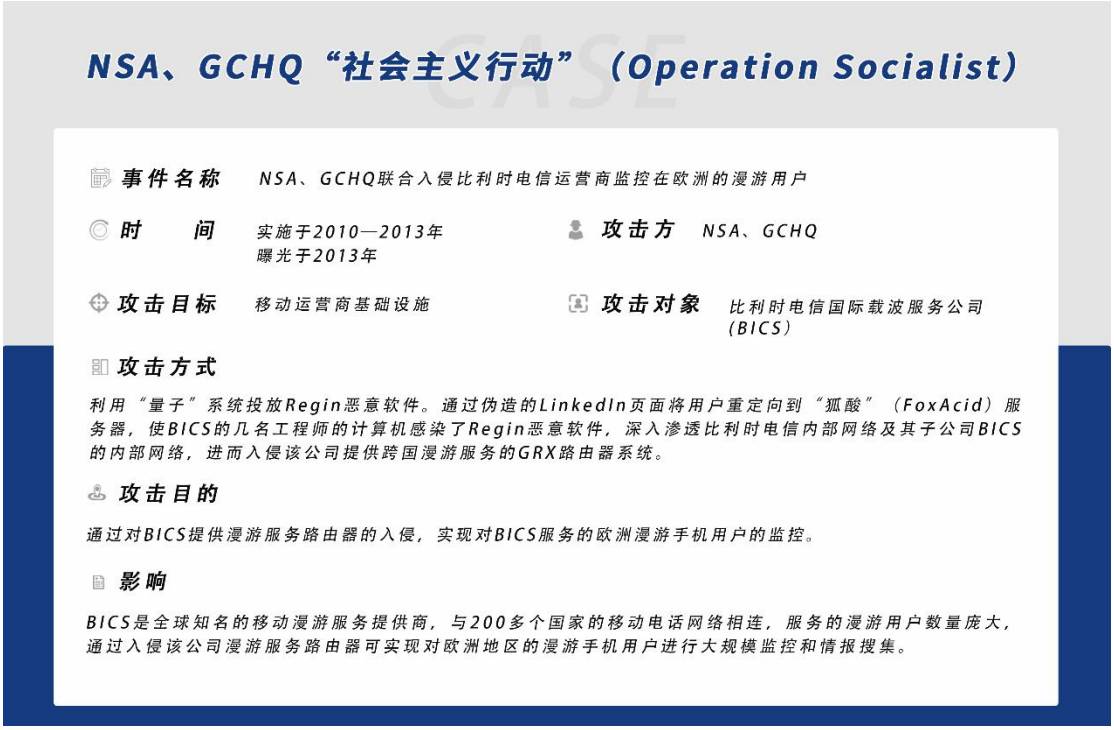


图 8-1 NSA、GCHQ“社会主义行动”（Operation Socialist）案例清单

（一）事件回顾

2013年9月20日和11月11日，《明镜周刊》陆续披露，NSA和GCHQ从2010年开始联合开展“社会主义行动”（Operation Socialist）[1]，入侵比利时电信子公司——比利时电信国际载波服务公司（Belgacom International Carrier Services，BICS）提供跨国漫游服务的GRX路由器系统，对漫游的智能手机开展针对性的“中间人攻击”。事件引发全球广泛关注，因为这是首次披露的发生在欧盟国家之间的网络攻击。

2014年12月13日，“拦截者”网站进一步报道“社会主义行动”称[2]，比利时电信公司从2012年夏天开始发现网络异常，2013年6月才确认其计算机系统感染了高度复杂的恶意软件，该恶意软件“伪装成合法的微软软件”，悄悄窃取数据。Regin网络攻击平台正是“社会主义行动”中所使用的恶意工具。斯诺登泄露的档案表明GCHQ和NSA是Regin平台的研发运营者。在2010年至2013年期间，GCHQ利用Regin平台入侵了比利时电信公司。该公司作为欧洲最大的漫游服务运营商之一，当外国游客入境欧洲时大多会连接比利时电信提供的国际漫游网络。Regin由此进入公众的视野，成为了网络安全领域持续关注的恶意软件。

2019年6月，路透社独家报道了“西方情报机构黑客2018年底入侵俄罗斯搜索引擎Yandex”的事件[3]，称黑客

在俄罗斯搜索引擎 Yandex 植入一种罕见的恶意软件 Regin，以刺探 Yandex 用户的账户情况。美网络安全公司赛门铁克（Symantec）安全响应中心技术总监维克拉姆·塔库尔（Vikram Thakur）称，“Regin 是用于间谍活动的攻击框架皇冠上的明珠，它的架构、复杂性和功能都处于领先地位”[3]。这一事件证明了 Regin 软件此后数年一直在活跃之中。

（二）溯源分析

2014 年 11 月 23 日，赛门铁克发布的分析报告《Regin: 顶级间谍工具可以实现隐形监视》称[4]，Regin 是一个极其复杂的软件，可以定制各种不同的功能，可以根据不同目标进行部署，采用了隐蔽并能够维持长期情报收集行动的框架。它不遗余力地隐藏自己及其在被攻击计算机上的活动，其隐身行动采用了许多最先进技术。

赛门铁克报告称，Regin 的主要目的是情报收集，它涉及针对政府组织、基础设施运营商、企业、学者和私人的数据收集行动。Regin 是一个多阶段、模块化的威胁，具有灵活性，在需要时可加载针对单个目标定制的功能。这种模块化方法已经在其他复杂的恶意软件家族中发现，如“火焰”（Flamer）和“面具”（Weevil），而 Regin 的多级加载体系结构与“毒曲/震网”（Duqu/Stuxnet）威胁家族中看到的类似。Regin 能够安装大量额外的有效载荷，有些是为目标计算机高度定制的。赛门铁克在调查中也发现了更

先进的针对某些特定目标的载荷模块。

2014 年 11 月 24 日，也就是赛门铁克发布报告的次日，卡巴斯基发布了更详细的 Regin 技术分析报告《针对 GSM 网络的国家级攻击平台 Regin》[5]。卡巴斯基在这份报告中称，“Regin 本质上是一个网络攻击平台，攻击者将其部署在受害者网络中，以便在所有层面进行全面远程控制”。卡巴斯基发现“关于 Regin 的最有趣的方面涉及大型 GSM 运营商的感染”。

卡巴斯基的报告称，Regin 是第一个已知除了执行其他“标准”间谍任务外还能够渗透和监控 GSM 网络的攻击平台。该平台背后的攻击者已经破坏了全球至少 14 个国家的计算机网络。其背后组织的主要攻击对象包括电信运营商、政府、金融机构、研究组织、跨国政治机构和参与高级数学/密码研究的个人。

2015 年 1 月 17 日，《明镜周刊》根据斯诺登曝光信息公布了“五眼联盟”代号为 QWERTY 的恶意程序副本。QWERTY 旨在偷偷记录 Windows 电脑的所有键盘敲击。卡巴斯基对其进行分析，认为这些代码与 Regin 有关联。通过仔细对比，卡巴斯基分析人员认定 QWERTY 恶意软件在功能上与 Regin 50251 插件是等同的[6]。卡巴斯基从技术上证明了 Regin 与 NSA 的另一个间谍模块 QWERTY 的同源关系[7]。卡巴斯基得出的结论是，“QWERTY 恶意软件开发人

员和 Regin 开发人员是同一组人或在一起工作”。

（三）延伸分析

据《明镜周刊》报道[8]，美西方情报机构在针对比利时电信的攻击行动中，投放 Regin 利用的是“量子”系统（Quantum），通过伪造的 LinkedIn 页面将用户重定向到“狐酸”（FoxAcid）服务器，使 BICS 的几名工程师的计算机感染了 Regin 恶意软件，使得 GCHQ 间谍能够深入渗透比利时电信内部网络及其子公司 BICS 的内部网络，入侵提供跨国漫游服务的 GRX 路由器系统，对漫游的智能手机开展针对性的“中间人攻击”。报道称**攻击行动可获取目标手机的所有互联网通信流量、跟踪位置或植入间谍软件，从而实现对漫游移动用户的大规模监控。**

卡巴斯基表示，Regin 渗透和监控 GSM 网络的能力可能是这些行动中最不寻常和最有趣的方面。在当今世界，人们已经变得过于依赖使用老式通信协议的手机网络，而最终用户几乎没有或根本没有安全性保障。尽管所有 GSM 网络都嵌入了允许执法机构跟踪嫌疑人的机制，但是还有其他实体也可以获得这种能力，然后滥用它来对移动用户发起其他类型的攻击。

事实上，NSA 对电信运营商的攻击由来已久。安天发布的《方程式组织 CDR 解析器样本分析报告》[9]，基于“影子经纪人”2016 年披露信息，详细分析了“方程式组

织”针对电信通话数据呼叫详细记录（Call Detail Record，CDR）的解析提取工具。由电话交换机类电信设备生成的CDR数据，包含呼叫时间、时长、完成状态、源号码和目的地号码等各种通话属性，“方程式组织”的CDR解析器能够按照指定的匹配条件（如时间范围等）对CDR文件进行搜集，随后根据加密的参数文件内容（如位置区域码，电话号码等）对搜集到的CDR文件数据进行解析。安天报告指出，该工具仅负责数据筛选和获取并加密存储，并不负责回传，这一作业方式符合美方模块化的作业和严格加密的习惯和特点。攻击者可以在入侵之后通过参数构建各种条件规则进行针对性的数据获取，并搭配数据解密、数据回传工具进行完整的入侵窃密攻击。

运营商作为一个数据通讯、数据汇聚的枢纽节点，在美方情报机构眼中有巨大的战略价值，是美方情报机构长期窥伺的目标。据斯诺登曝光的资料显示，“星风”计划中的“主干道”与“核子”就是专门针对全球电信通话数据的收集和监听计划，“主干道”通过与运营商建立合作关系获得相关数据，“核子”则截获电话通话中的对话内容及关键词获得指定数据。**美方情报机构通过攻击运营商，实现其在通信领域的全方位大纵深网络情报活动。**

参考资料

[1] Britain's GCHQ Hacked Belgian Telecoms Firm. 2013.

https://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

[2] Ryan Gallagher. The Inside Story of How British Spies Hacked Belgium's Largest Telco. 2014. https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

[3] Christopher Bing, Jack Stubbs, Joseph Menn. Exclusive: Western intelligence hacked 'Russia's Google' Yandex to spy on accounts 2019. https://www.reuters.com/article/us-usa-cyber-yandex-exclusive-idUSKCN1TS2SX/

[4] Symantec. Regin: Top-tier espionage tool enables stealthy surveillance. 2014. https://docs.broadcom.com/doc/regin-top-tier-espionage-tool-15-en

[5] Kaspersky. The Regin Platform Nation-State Ownage of GSM Networks. 2014. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08070305/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf

[6] Costin Raiu, Igor Kuznetsov. Comparing the Regin module 50251 and the "Qwerty" keylogger. 2015. https://securelist.com/comparing-the-regin-module-50251-and-the-qwerty-keylogger/68525/

[7] Pierluigi Paganini. Regin and Qwerty Keylogger Are Linked With Five Eyes Intelligence. 2015. https://securityaffairs.com/32818/intelligence/regin-qwerty-keylogger-fiveeyes.html

[8] GCHQ Used Fake LinkedIn Pages to Target Engineers. 2013. https://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html

[9] 方程式组织 CDR 解析器样本分析报告. 2024. https://www.antiy.cn/research/notice&report/research_report/Equation_CDR.html

第九篇　基于运营商攻击上网终端——“量子”系统对手机和上网 PC 的攻击能力

所有手机等移动终端和各类上网终端都依赖于运营商体系访问网络和各种应用，而美国情报机构通过“量子”系统入侵各国运营商交换和路由等网络设备，把全球运营体系改造为可用于攻击上网用户的投放体系，攻击范围包括安卓、iOS 等智能移动终端和各类上网 PC 和服务器产品。“量子”系统于 2013 年首次被斯诺登曝光，由 NSA 下属的特定入侵行动办公室（TAO）开发并负责使用，是一套用于对高价值目标实施网络攻击的工程体系和入侵工具集。

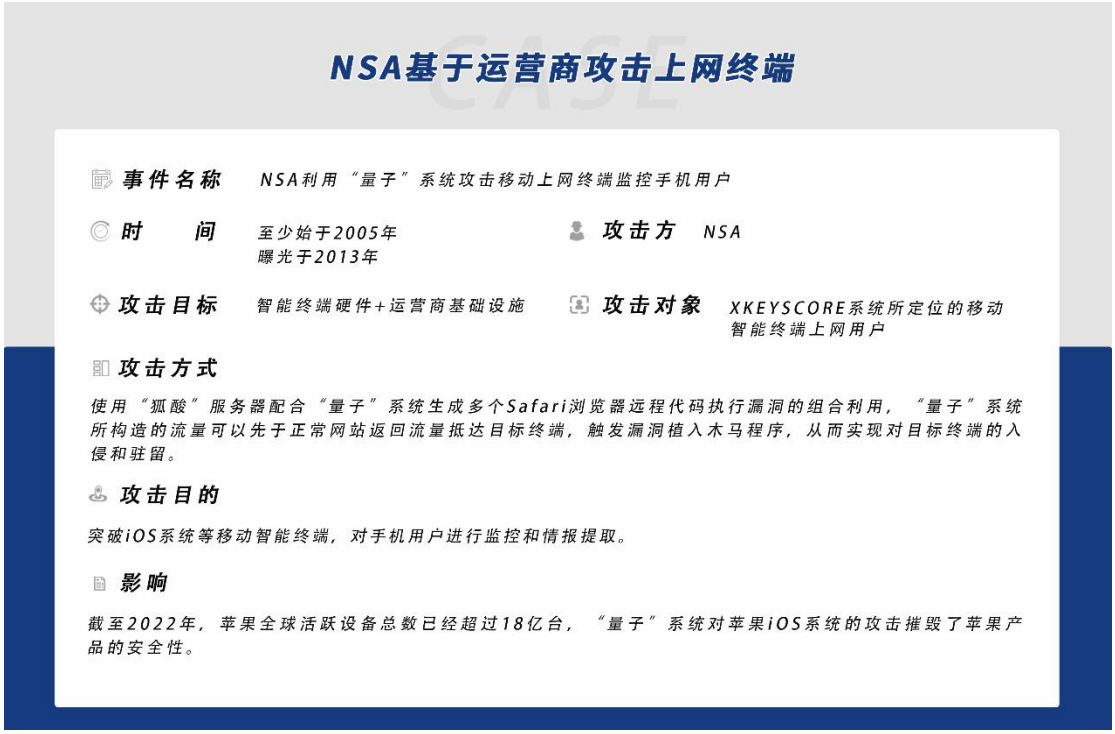


图 9-1 NSA 基于运营商攻击上网终端案例清单

（一）事件回顾

2023年6月9日，安天发布《“量子”系统击穿苹果手机——方程式组织攻击iOS系统的历史样本分析》[1]，披露NSA下属“方程式组织”早年基于“量子”系统在网络侧针对iOS系统上网终端发起攻击，利用浏览器漏洞投放后门程序的渗透活动。此前，卡巴斯基发布了分析报告《三角测量行动：iOS设备被前所未知的恶意软件攻击》[2]，指出恶意软件通过“零点击”方式对iOS设备进行了攻击。

安天报告所披露“量子”系统对iOS系统的攻击和卡巴斯基所曝光的“三角测量行动”攻击同样来自“方程式组织”，但两篇报告所揭示的攻击路径和样本是完全不同的，是两种不同的攻击方式。卡巴斯基所曝光的攻击是依托iMessage漏洞投放样本；安天发现的“方程式组织”针对iOS平台的攻击行为可能出现在2013年或更早，攻击样本通过“量子”系统进行投放。

（二）溯源分析

安天报告分析的iOS攻击样本并不是常规的iOS APP应用安装包，而是针对iOS底层的木马。木马主体伪装成名为regquerystr.exe的PE格式文件进行投放，其真实格式是ARM架构的Mach-O可执行程序，利用漏洞或通过沙盒逃逸完成后门程序的释放和执行。木马程序首先检测内核

版本和用户权限，然后释放后门程序 mvld，主要用于收集设备信息以及与远程服务器通信，程序运行后会生成日志文件并删除自身文件。

攻击样本有 13 个指令代码，其功能与安天曝光过的“方程式组织”Windows 和 Solaris 木马 DoubleFantasy 系列指令十分相似[3]。此外，mvld 木马内部解密出信息 FAID，其中 ace02468bdf13579 与之前曝光的 NSA 作业所需强制性的唯一标识代码一致，该标识也存在于“影子经纪人”泄露的方程式武器库中的 SecondDate 武器中，种种信息都指向：该木马来自美方情报机构 NSA 下属的“方程式组织”。

安天报告称，将该 iOS 木马与方程式组织的 DoubleFantasy 木马装备序列进行对比分析，可以得出如下结果：在功能、行为、算法、信息收集和指令控制集合上几乎相同；木马使用方程式组织加密算法中最常使用的数值 0x47，收集终端信息格式与 DoubleFantasy 一致，控制指令代码结构与 DoubleFantasy 基本一致，这些充分证明了 iOS 木马与 NSA“方程式组织”的关联。

（三）“量子”系统揭秘

“量子”系统项目于 2013 年首次被斯诺登曝光，由 NSA 发起，并与 GCHQ 和瑞典国防无线局（FRA）联合执行，用于开发和运营承载实施网络攻击的工程体系和入侵工具集，以实现对网络空间中网络状态的干预和控制，由

NSA 下属的 TAO 开发并负责使用。

据“连线”网站 2015 年 4 月报道[4]，被称为“量子注入”的黑客技术自 2005 年以来一直被 NSA 及其合作伙伴 GCHQ 使用，以侵入高价值、难以到达的系统并植入恶意软件。“量子注入”工作原理是在目标浏览器尝试访问网页时劫持浏览器，并迫使其访问恶意网页。这项“非常成功”的技术让 NSA 在 2010 年通过劫持至恶意网页方式在全球计算机上植入了 300 个恶意软件。

“量子注入”技术要求在相对靠近目标机器的地方拥有快速反应的服务器，能够快速拦截目标浏览器流量，以便在合法网页到达之前将恶意网页发送到目标计算机。为了实现这一目标，NSA 使用了代号为“狐酸”（FoxAcid）的服务器，以及放置在互联网关键节点的称为“射手”（Shooter）的特种高速服务器[4]。流量嗅探和“射手”机器距离目标越近，“狐酸”就越有可能“赢得”快速到达受害者机器的竞争。

“量子”系统的运行支点，是对网络通信基础设施的关键路由和网关等设备的入侵和劫持，从而具备获取分析和劫持攻击目标上网过程的能力。其首先基于上网设备的相关 IP、码号、链路、身份账号或其他标识依托 XKEYSCORE 系统进行识别，看是否符合攻击目标定义，以及是否为已经攻击成功设备，如果是待攻击目标，则进

一步判断是否存在可用漏洞，然后选用相应的工具执行秘密入侵。安天公司在其报告中绘制了“量子”系统的攻击能力频谱猜想图，认为“量子”攻击能力完全覆盖了全球所有主要上网终端，包括各类 PC、服务器和移动智能终端设备和相关浏览器[1]。

图 9-2 安天绘制的量子系统可攻击场景图谱化分析

（四） 延伸分析

“量子”系统的作业能力一方面来自其掌控的大量未公开漏洞资源和漏洞利用工具储备，另一方面来自于“方程式组织”对全球关键网络通信设备的攻击控制程度。例如，为了诱骗目标访问“狐酸”服务器，NSA 依靠其与美国电信公司的秘密合作关系，在互联网骨干网的关键位置部署“射手”服务器[5]。可见，**美情报机构与电信基础设施**

所有者之间的密切合作是其网络攻击行动取得成功的关键。这也是美方对全球网空战场预置的重要环节，通过对全球运营商入侵和劫持实现前出性预置，为后续的网络攻击行动塑造网络空间环境。

“量子”的攻击机理不仅对手机等上网终端造成危害，实际上已经变成了美方网络军事行动的体系化布置的重要手段。通过“量子”系统，美方恶意代码可以在跨网入侵后部署在关键目标网内的交换机和路由器，包括防火墙等网络设备，从而在内网构建入侵桥头堡。以此提高网络部队的机动能力，使其能进入关键地形并在必要时控制关键地形，**保证美军能在必要时开展远征网空作战行动，无需在外国领土建立实体存在的情况下进行力量投送。**

总之，“量子”投放体系、面向浏览器和网络客户端的漏洞库，加上 A^{2}PT 组织的能力体系，不仅为美方在网络空间的军事行动提供了支撑保障，也**使得所有 PC 和移动设备都面临被美情报机构攻击渗透的风险，从而将全球手机用户和网民都置于“量子”高悬的达摩克利斯之剑下。**

参考资料

[1] “量子”系统击穿苹果手机——方程式组织攻击 iOS 系统的历史样本分析. 2023. https://www.antiy.cn/research/notice%26report/research_report/EQUATION_iOS_Malware_Analysis.html

[2] IGOR KUZNETSOV. Operation Triangulation: iOS devices targeted with previously unknown malware. 2023. https://securelist.com/operation-triangulation/109842/

[3] 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

[4] Kim Zetter. How to Detect Sneaky NSA 'Quantum Insert' Attacks. 2015. https://www.wired.com/2015/04/researchers-uncover-method-detect-nsa-quantum-insert-hacks/

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

第十篇　APP“调包计”——“怒角”计划的植入式攻击

在移动互联网时代，手机等移动智能终端的丰富功能来自各种应用程序（APP）的支持。手机厂商和操作系统供应商官方 APP 商店为用户提供了安全便利的下载渠道。但是，这一可直达用户手机的巨大可信资源也成为网络攻击者觊觎的目标。泄露信息显示，2011 年至 2012 年期间，NSA 等“五眼联盟”国家情报机构启动了“怒角”计划（IRRITANT HORN），他们使用“调包计”，通过流量劫持偷换用户下载的 APP 植入恶意软件，以达到入侵用户手机的目的。

图 10-1 NSA 等情报机构“怒角”计划（IRRITANT HORN）案例清单

（一）事件回顾

2015 年 5 月 21 日，加拿大广播公司（CBC）、美国“拦截者”网站等西方媒体及相关机构刊文[1]，揭露 NSA 与“五眼联盟”国家情报机构实施“怒角”计划，称“NSA 计划劫持谷歌应用商店来攻击智能手机”。“怒角”计划的泄露，揭开了以美国为首的“五眼联盟”国家情报机构长期对移动用户手机进行攻击和监控的黑幕。

斯诺登泄露的绝密文件显示[2]，“怒角”计划由 NSA 和其他“五眼联盟”国家情报部门联合发起。通过劫持谷歌和三星应用商店的下载链接，情报机构在用户下载或更新应用程序时，修改目标智能手机和应用程序服务器之间传递的数据包的内容，然后发送给手机，骗取用户安装已植入间谍软件的“调包”APP，利用手机 APP 漏洞，从而对目标手机进行严密监控，收集海量用户信息，进行情报提取作业。

此前，斯诺登泄露的文件已显示，“五眼联盟”国家情报机构为苹果和安卓智能手机设计了间谍软件，感染目标手机后可获取电子邮件、短信、网络历史记录、通话记录、视频、照片及所存储的其他文件。但“五眼联盟”情报机构是通过什么方法将其开发的间谍软件感染到目标手机并不为外界所知。显然，此次曝光的“怒角”计划让外界得以了解“五眼联盟”国家情报机构的“中间人攻击”活动[1]。

（二）“怒角”计划揭秘

为了实施“怒角”计划，以美国为首的“五眼联盟”情报机构成立了“网络情报技术推进小组”（Network Tradecraft Advancement Team，NTAT），成员包括美国、加拿大、英国、新西兰和澳大利亚等国的情报人员。2011 年 11 月至 2012 年 2 月期间，NTAT 先后在澳大利亚和加拿大举行了一系列秘密技术研讨会，旨在寻找利用智能手机技术对移动用户进行监控的新方法，计划劫持谷歌和三星应用商店的数据链，使用间谍软件感染智能手机。

NTAT 使用 XKEYSCORE 系统来识别通过互联网电缆传输的智能手机流量，然后追踪智能手机与三星和谷歌运营的应用程序服务器的链接，并攻击和劫持用户与应用商店的链接，向目标手机发送已植入恶意软件的 APP 骗取用户安装，这些植入的间谍软件可以用来收集手机上的数据，而手机用户毫不知情。

为了遵守互不监视对方公民的协议，“五眼联盟”情报机构将注意力集中在非“五眼联盟”国家的 APP 服务器上，包括法国、瑞士、荷兰、古巴、摩洛哥、巴哈马和俄罗斯等。这些情报机构还试图将目标的智能手机设备与他们的在线活动相匹配，使用“五眼联盟”强大的 XKEYSCORE 系统中保存的电子邮件、聊天和浏览历史记录数据库来帮助建立他们正在跟踪的人员的档案[3]。

NTAT 在寻找进入移动应用商店服务器的方法时，还发现了中国广泛使用的 UC 浏览器中的安全漏洞，UC 浏览器应用程序将用户的电话号码、SIM 卡号和设备详细信息泄露给中国的服务器，为“怒角”计划窃取中国用户信息提供了便利[1]。加拿大公民实验室（Citizen Lab）分析对应的安卓版 UC 浏览器后发现了“重大安全和隐私问题”，指出其可泄露多种数据，包括一些用户的搜索查询、SIM 卡号和可用于跟踪人员的唯一设备识别码。公民实验室分析报告证实了“五眼联盟”发现的 UC 浏览器中的隐私漏洞的真实性[4]。

“五眼联盟”情报机构想要做的不仅仅是使用 APP 商店作为用间谍软件感染手机的跳板，他们还热衷于寻找劫持它们的方法，以便选择性地向目标手机发送虚假信息，用于宣传或误导对手，进行认知作战[1]。

（三）延伸分析

“怒角”计划依托 NSA 的绝密监控项目 XKEYSCORE 进行流量分析，筛选目标，选择攻击路径，并建立跟踪人员档案，便于情报机构更全面更具体地了解监控对象，更加有的放矢的开展情报搜集行动。XKEYSCORE 计划为“怒角”计划的目标筛选和持续监控提供了有力的数据支撑，充分体现了美情报机构强大的体系化监控与攻击能力。另外，基于“怒角”计划的流量劫持和“中间人攻击”模

式与“量子”系统类似，有理由怀疑“怒角”计划在流量侧的劫持与投放的体系可能是“量子”系统，其功能的实现可能通过“量子”系统来承载。

美西方情报机构通过“怒角”计划植入恶意代码控制目标手机终端，实施长期监控窃密，与此同时，还可以通过植入的恶意代码有针对性地向用户发送误导信息，将情报获取与认知作战相结合，以获取更大的情报综合效益。“怒角”计划是美方庞大的网络情报作业体系工程中的一环，支撑其针对全球移动智能终端的窃密监听活动。

参考资料

[1] Ryan Gallagher. NSA PLANNED TO HIJACK GOOGLE APP STORE TO HACK SMARTPHONES. 2015. https://theintercept.com/2015/05/21/nsa-five-eyes-google-samsung-app-stores-spyware/

[2] Five Eyes Presentation: Synergising Network Analysis Tradecraft. https://www.documentcloud.org/documents/2083944-uc-web-report-final-for-dc.html

[3] Amber Hildebrandt, Dave Seglins. Spy agencies target mobile phones, app stores to implant spyware. 2015. https://www.cbc.ca/news/canada/spy-agencies-target-mobile-phones-app-stores-to-implant-spyware-1.3076546

[4] Citizen Lab. Privacy and Security Issues with UC Browser. 2015. https://citizenlab.ca/2015/05/a-chatty-squirrel-privacy-and-security-issues-with-uc-browser/

第十一篇　“棱镜”背后的阴谋——构建超级数据访问接口

无论是谷歌、脸书等大型互联网厂商，还是苹果等智能手机厂商，或是微软等基础 IT 厂商等，都以手机 APP 作为主要服务形式，为用户提供服务。APP 具有采集用户基本信息、操作行为等数据的能力，这些采集到的数据会汇聚到提供服务的厂商数据中心。依托各种丰富的 APP 应用与用户交互，大型互联网平台厂商把 APP 数据存储在其平台，而“棱镜”计划正是构建了访问这些数据的超级接口。斯诺登披露的“棱镜”计划，揭露了美情报机构利用互联网平台和厂商提供的超级数据访问接口进行情报搜集的阴谋。

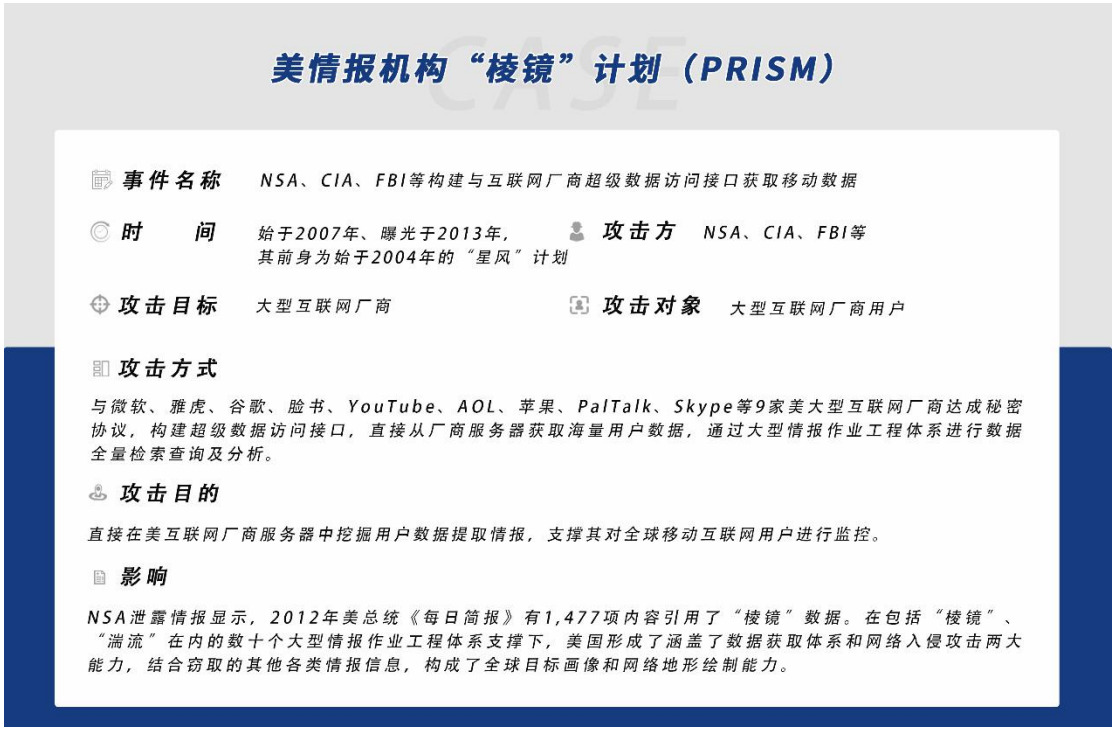


图 11-1 美情报机构“棱镜”计划（PRISM）案例清单

（一）“棱镜”事件回顾

2013 年 6 月，斯诺登将两份绝密资料交给英国《卫报》和美国《华盛顿邮报》，并与媒体约定了发表时间。2013 年 6 月 6 日，英国《卫报》率先曝光了 NSA 代号为“棱镜”的秘密计划[1]，揭露美国情报机构通过美科技公司秘密对全球用户进行监控的内幕，引起了国际社会的强烈反响。《华盛顿邮报》于 6 月 7 日对美“棱镜”计划进行了跟进报道[2]，称 NSA 和 FBI 于 2007 年启动了一个代号为“棱镜”的秘密监控计划，直接进入美国大型科技公司的中心服务器里挖掘数据、收集情报，包括微软、雅虎、谷歌、脸书、YouTube、AOL、苹果、PalTalk、Skype 等在内的 9 家国际网络巨头皆参与其中。《华盛顿邮报》获得的绝密文件显示，NSA 和 FBI 直接利用美国 9 家领先互联网公司的中央服务器，提取音频和视频聊天、照片、电子邮件、文件和访问记录，使分析人员能够跟踪全球目标。

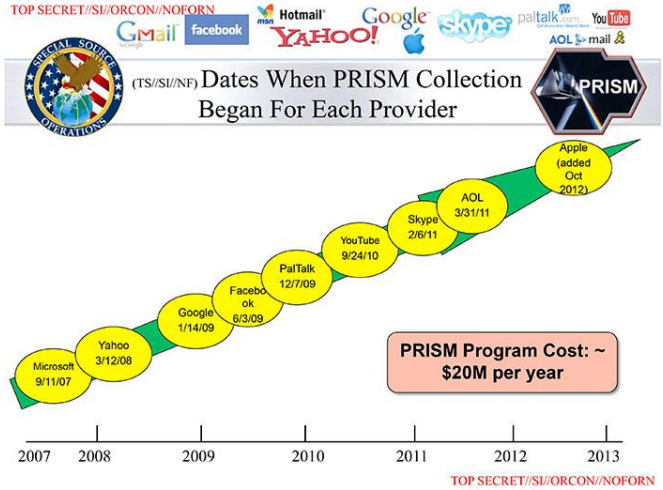


图 11-2 参与“棱镜”计划的美国大型科技公司

据《华盛顿邮报》报道[2]，NSA 将参与“棱镜”计划的合作伙伴的身份视为“棱镜”计划最敏感的秘密，担心这些公司一旦暴露就会退出该计划，“98%的‘棱镜’产品基于雅虎、谷歌和微软，我们需要确保不损害这些来源”。NSA 的内部演示文稿“将这一新工具描述为总统《每日简报》最多产的贡献者，该简报在 2012 年有 1,477 项内容引用了‘棱镜’数据”。《华盛顿邮报》获得的文件显示，“NSA 的报告越来越依赖‘棱镜’作为其主要素材来源，占情报报告的近七分之一”。《华盛顿邮报》2013 年 12 月 4 日报道[3]，NSA 在全球范围内收集手机位置信息，每天收集世界各地手机的位置信息将近 50 亿条，“分析人员可以在世界任何地方找到手机，追踪它们的行踪并揭露使用它们的人之间隐藏的关系”。显然，NSA 强大的数据收集和情报挖掘能力与“棱镜”计划密不可分。

表 11-1 美科技公司参与“棱镜”计划详细情况

厂商名称	参与“棱镜”计划时间	可能被访问的数据资源
微软	2007 年 9 月 11 日	电子邮件、用户数据、文件
雅虎	2008 年 3 月 12 日	搜索词、电子邮件、用户数据、文件
谷歌	2009 年 1 月 14 日	搜索词、电子邮件、短信、通话记录、联系人信息、用户密码、文件、用户数据等
脸书	2009 年 6 月 3 日	用户数据、联系人、照片、位置信息
PalTalk	2009 年 12 月 7 日	视频/语音聊天

YouTube	2010 年 9 月 24 日	视频
Skype	2011 年 2 月 6 日	视频/语音聊天
AOL	2011 年 3 月 31 日	电子邮件、用户数据、文件
苹果公司	2012 年 10 月	电子邮件、短信、通话记录、联系人信息、用户数据、文件、用户密码，位置信息、聊天记录等

（二）“棱镜”计划的运作

据斯诺登泄露的文件披露，2004 年美国政府启动“星风”计划（STELLARWIND）进行大规模监听和情报搜集活动，后将“星风”拆分为“棱镜”（PRISM）、“主干道”（MAINWAY）、“码头”（MARINA）以及“核子”（NUCLEON）等 4 个项目，并由 NSA 负责实施。“棱镜”计划是一个自 2007 年开始实施的绝密级情报收集行动，主要方式是利用美国主要互联网企业所提供的数据接口进行情报作业。“主干道”和“码头”项目分别对通信和互联网上数以亿兆计的“元数据”进行存储和分析。“核子”项目负责截获电话通话者对话内容及关键词，相比于“主干道”和“码头”，“核子”项目更加聚焦于内容信息的获取，通过拦截通话以及通话者所提及的地点，来实现日常的监控。“棱镜”与这些情报收集项目一起构成了体系化的情报作业能力，使美情报机构可以实现对全球互联网人员目标、信道目标、设备目标等完整的画像，从而形成比较精准的目标定位能力和情报提取能力。

移动互联网时代，大型科技公司和互联网平台上存储着海量的用户数据，包括个人信息、社交活动、在线购物记录、地理位置信息等，对于情报机构进行全民画像，追踪个体活动、行踪以及可能的关联事件非常有价值，是其十分重要的情报来源。与此同时，这些平台厂商还承载着大量政企服务，不仅包括上述数据，还包括国家经济数据、产业数据、社会数据等等，是国家重要的战略性数据资产。美情报机构的“棱镜”计划正是看上了大型科技公司和互联网平台的丰富数据资源，开展对全球用户的大规模监控与情报搜集活动。

“棱镜”计划演示文稿显示[2]，“脸书和 Skype 的任务持续呈指数级增长”。只需点击几下鼠标，并确认监控对象与恐怖主义、间谍活动或核扩散行为相关，美情报分析人员就可以完全访问脸书“针对各种在线社交网络服务的广泛搜索和监视功能”。根据一份单独的《“棱镜”计划 Skype 情报收集用户指南》显示，当 Skype 通话一端是传统电话时，可以监控该通话的音频；当 Skype 用户通过电脑网络连接时，则可以监控“音频、视频、聊天和文件传输”等所有内容。而“棱镜”计划通过谷歌平台可获取的数据内容包括 Gmail 邮件、语音和视频聊天、Google Drive 文件、照片库，以及对搜索词进行实时监控的内容。

泄露的文件显示，NSA 称赞“棱镜”计划是其最有价

值、最独特和最富有成效的情报获取途径之一[1]。NSA 夸耀“棱镜”计划使其通信数据收集量获得“强劲增长”。其中，2012 年从 Skype 获得的通信数据量增加了 248%，对脸书数据的请求增加了 131%，对谷歌数据的请求增加了 63%。

依据 2008 年美国通过的《外国情报监视法》（FISA）修正案 702 条款，“棱镜”计划允许美情报机构无需获得批准即可搜集境外非美国公民的在线通信数据。与“传统的”FISA 监控要求不同，702 条款不要求监视目标是可疑的恐怖分子、间谍或其他外国势力特工，只要监控目标是国外的非美国公民、主要目的是获取外国情报信息就行[4]。

这样的法律制度设计把美国自身霸权凌驾于全球用户隐私保护之上，为美情报机构肆意侵犯外国公民隐私、无区别的大规模搜集别国情报信息大开方便之门。

702 条款禁止以任何美国人或位于美国的任何人为目标[5]。但美外国情报监视法院 2018 年的报告显示，FBI 在没有正当理由的情况下对美国人的数据进行了数千次查询[6]。美国众议院议长和司法委员会主席 2022 年给 FBI 局长写信表达“对 FBI 使用权力的过程中忽视了美国人宪法权利的担忧”[6]。可见，美情报机构事实上已经突破了 702 条款的限制，无形中已将监控对象扩大到了美国公民。

从某种意义上来说，美政府试图证明对 FBI 的监听权力严加管束，其实是一种烟雾弹，反而成为了 CIA 和 NSA

等情报机构毫无限制的通过“棱镜”这种超级访问接口访问全球全量数据的“遮羞布”。

（三）“棱镜”计划的危害

美国作为互联网的发源地，美国的IT产业一直引领着全球IT技术和互联网技术的发展方向，在技术和应用领域的先发优势十分明显。许多全球领先的科技公司，如苹果、微软、谷歌、脸书等，总部都位于美国，这些公司在技术研发和市场拓展方面发挥着引领作用，在全球相关科技领域处于垄断地位。正是由于美国在IT和互联网领域的先发优势，叠加大型互联网平台和软硬件厂商总部都设在美国的“主场”优势，为美国的互联网平台和厂商收集用户隐私数据和政企运营数据提供了十分便利的条件。互联网平台不仅收集用户信息，还提供了数据备份功能。例如，谷歌备份功能会将用户的数据发送到谷歌的备份服务器，谷歌的密码保存功能可保存用户的各类敏感密码，这些信息一旦外泄将造成巨大危害。

由于“棱镜”事件曝光于2013年，此时移动APP还没有充分取代PC浏览器成为个人使用互联网的主入口，导致公众对“棱镜”计划的理解还停留在基于PC浏览器和PC客户端的服务访问。而今天全球用户基本依赖手机APP提供的各类互联网相关服务，常用的APP包括Chrome、Gmail、Google Maps、Youtube、Facebook、Safari、

iMessage、FaceTime、iCloud Drive、Skype、eBay、PayPal等，涉及邮件通信、即时通信、社交平台、金融支付、购物消费、导航出行等服务，生成的服务数据都存储在互联网平台和厂商的数据库中。“棱镜”计划正是构建了美情报机构面向互联网企业数据库的“超级访问接口”，支撑了美情报机构对所有这些数据的超级访问能力。

美情报机构与大型互联网平台和厂商达成秘密的数据挖掘协议，不仅违背了用户授权互联网平台和厂商收集用户数据的初衷，更是把广大用户作为“待宰羔羊”，成为其进行无差别大规模监控与窃密活动的对象。

尽管美情报界已经建设了IC Cloud（情报云）这样的大规模数据基础设施，但仍不足以满足其获取全球网络用户数据的欲望。**“棱镜”这样数据超级接口的存在，使美方在不承担大规模数据中心成本基础上把各大互联网厂商的数据中心变成自己的“硬盘”，可随时按需提取用户数据。美方的基础IT产品服务已沦为美情报机构对用户进行大规模监控窃密的“帮凶”。**

参考资料

[1] Glenn Greenwald, Ewen MacAskill. NSA Prism program taps in to user data of Apple, Google and others. 2013. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[2] Barton Gellman, Laura Poitras. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. 2013. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

[3] Barton Gellman, Ashkan Soltani. NSA tracking cellphone locations worldwide, Snowden documents show. 2013. https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

[4] Section 702: What It Is & How It Works. 2017. https://cdt.org/wp-content/uploads/2017/02/Section-702.pdf

[5] Targeting Under FISA Section 702. https://www.intelligence.gov/foreign-intelligence-surveillance-act/1242-targeting-under-fisa-section-702

[6] Sutton Tyson, Catitlin Yilek. Feds push for FISA Section 702 wiretapping reauthorization amid heightened potential for violence. 2023. https://www.cbsnews.com/news/feds-push-for-fisa-702-reauthorization/

结 语

美国是计算机、现代互联网和智能手机的诞生地。这些在人类历史上非常重要的创新成果，是美国工业界和科学工作者的创新之光，是美国人民智慧和创造力的结晶，也是美国作为全球技术领先国家的标志和支撑。但与此同时，对于美国寡头资本和政客来说，网络空间也成为可借着先发技术优势实现地缘政治目的的新高地。正是在这种领先性和霸权的双重作用下，全球各国人民才无奈地接受了美国在信息技术和产业体系上的上游垄断，依赖于美国的产品和服务。但实际上，美国没有履行一个负责任国家应有的网络安全责任，没有针对世界各国政府和人民所关注的“推进网络空间军事化、滥用供应链和信息链的优势”等问题做出任何承诺。

美国情报机构不遗余力地针对人类的网络家园，开发覆盖全场景、全环节、全流程的网络攻击装备，持续发动一系列网络攻击，滥用供应链上游优势，预置脆弱性，削弱加密强度，降低攻击难度，构建“棱镜”计划等互联网平台超级访问接口，获取、窥探用户数据。

美国情报机构针对移动智能终端和通讯体系，构建了全层次的攻击渗透能力，从 SIM 卡、固件、操作系统到软件应用的每一个设备层次，从数据线、Wi-Fi、蓝牙、蜂窝

网络、GPS 等数据接口，到运营商体系，乃至整个移动产业生态体系以及大型互联网和 IT 厂商的数据中心，无孔不入。对智能终端设备的生产制造过程、应用场景和网络通联各个击破，对全球人员、账号、设备、链路、码号、位置进行全面获取，绘制完整网空作战地图，进行全方位、大纵深网络情报活动，严重危害他国国家安全，应得到全球各方高度关注与密切防范。

曾在 1999 年至 2009 年接连担任 NSA 和 CIA 负责人的退役美空军四星上将迈克尔·海登将其十年情报工作感受总结为“情报的力量与局限”，坦言美国情报机构必须通过窃取那些未经授权的信息达成情报效益。其所标榜的所谓司法审批体制，实际只覆盖 FBI 等执法部门，而对 NSA、CIA 等情报部门，无论是对于美国公民还是他国人员机构的行为活动，已经没有任何约束力。

从网络攻击活动层面来看，对于美方入侵、持久化、窃取等攻击活动，通过提升场景安全防护能力、强化手机产品和安全防护能力，可逐步实现发现、削弱乃至阻断拒止。但这需要长期、持续的努力，需要极高水平的检测分析防御能力支撑，也需要巨大的投入，整体增加了全球各国政府、产业体系和组织机构的安全投入成本压力。

但是，类似“棱镜”计划等构建的超级访问接口，与整个手机以及移动互联网生态深深地耦合在一起，成为一

种近乎无解之痛。只能通过针对特定场景、特定人员对产品、服务和应用进行限制，并通过持续的外交努力要求美方立即停止相关行径。各国提高治理能力，强化数据本地化和合规要求，捍卫自身网络主权，最终结果也必然是更多国家希望打破对美国的智能终端和互联网产品体系的绝对依赖。

从具体应对来看，对于美情报机构针对智能终端体系的这种强大的、体系化、针对性攻击，各国政府都需要面向产业链场景、运营商场景、手机使用场景、关键人员场景，针对性建设威胁与风险分析研判机制、高级持续性威胁发现与猎杀机制、关键场景和关键人员防御保障能力等。对于缺乏自身独立产业体系的国家，还需要重点警惕那些与美方情报机构进行过协同合作、提供了“棱镜”访问接口的“前科”厂商的设备、产品与服务。在重要场景重要人员设备使用方面，引入自主或负责任的国家生产的安全性和隐私保护功能更强、安全承诺更可靠的设备。对于各国自身的移动终端产业体系，如 SIM 卡、手机生产制造、关键 APP 研发、互联网服务等，还要针对性地提升相关产品与软件代码安全工程能力，涵盖研发生产环节的全生命周期的防护能力。

与此同时，各国政府还需加强对手机厂商、运营商以及互联网厂商的安全联动赋能能力，强化管理要求。对智

能终端、网络运营商、APP 开发服务商提出有针对性的网络安全标准，敦促其履行相应安全义务并做出明确安全服务承诺，推动硬件、软件供应链透明化机制。推动恶意代码等威胁检测、内核防护等安全机制成为手机和其他智能终端设备的强制性要求，将对威胁分析、留存可溯源性的支撑要求变成强制要求。既强化安全主体责任，也给予安全能力赋能。

上述这些工作的展开和资源投入，是支撑发现和防御美方攻击的基础工作和必要条件，其一定程度上能提升美方的攻击成本、缩短发现其攻击的时间。但面对其超高能力、无孔不入的攻击，还需要进行更有针对性的建设投入和政策更新，包括：建立针对性场景威胁分析猎杀的专门环境与队伍、构建专项装备、鼓励和奖励发现高级持续性攻击行为的线索。

美国情报机构大面积的网络攻击和信息窃取窥探是霸权主义和单边主义对网络空间的撕裂。虽然针对移动智能终端的攻击活动已曝光的内容就已经令人不寒而栗，但更为可怕的是，我们不知道还有多少攻击武器、设施、行动，仍不为人所知。一如海登在回忆录《发挥到极致——恐怖时代下的美国情报》中所说，“间谍活动的定律就是你只知道那些失败的，不会知道成功的”，目前浮出水面的只是美方大规模情报活动的冰山一角。当世界各地的人们在享受

移动智能终端带来的便利、快捷、愉悦的同时，也不要忘记超级大国所打造的巨大深渊正在贪婪地吸吮我们的数据源流。你在凝视手机屏幕的时候，手机背后的深渊也在凝视你。

附录一：缩略语表

缩略语	英文	中文
A2P	Application to Person	应用到个人
A^2PT	Advanced Advanced Persistent Threat	高级的高级持续性威胁
ACLU	American Civil Liberties Union	美国公民自由联盟
ANT	Advanced Network Technology	先进网络技术部
AOL	America Online	美国在线
APN	Access Point Name	接入点名称
APP	Application	应用程序
ARM	Advanced RISC Machines	先进的精简指令集机器
ASD	Australian Signals Directorate	澳大利亚信号局
AT&T	American Telephone and Telegraph Company	美国电话电报公司
BICS	Belgacom International Carrier Services	比利时电信国际载波服务公司
CALEA	Communication Assistance for Law Enforcement Act	《通信协助执法法案》
CBC	Canadian Broadcasting Corporation	加拿大广播公司
CDMA	Code Division Multiple Access	码分多址
CDR	Call Detail Record	呼叫详细记录
CIA	Central Intelligence Agency	美国中央情报局
CNN	Cable News Network	美国有线电视新闻网
CSEC	Communications Security Establishment Canada	加拿大通信安全局
DAS	Data Analytical Services	数据分析服务
DEA	Drug Enforcement Administration	美国缉毒署
DRT	Digital Receiver Technology, Inc.	数字接收器技术公司
DTMF	Dual Tone Multi Frequency	双音多频
ECPA	Electronic Communications Privacy Act	《电子通信隐私法》
EDGE	Enhanced Data Rate for GSM Evolution	增强型数据速率 GSM 演进技术
EFF	Electronic Frontier Foundation	电子前沿基金会
eUICC	Embedded Universal Integrated Circuit Card	嵌入式通用集成电路卡
FBI	Federal Bureau of Investigation	美国联邦调查局
FISA	Foreign Intelligence Surveillance Act	《外国情报监视法》
FISC	Foreign Intelligence Surveillance Court	外国情报监视法院
FOI	Freedom of Information	信息自由法
FRS	Family Radio Service	家庭无线电服务
FSB	Federal Security Service	俄罗斯联邦安全局
GCHQ	Government Communications Headquarters	英国政府通信总部
GCSB	Government Communications Security Bureau	新西兰政府通信安全局
GPRS	General Packet Radio Service	通用分组无线业务
GPS	Global Positioning System	全球定位系统
GRX	GPRS roaming exchange	GPRS 漫游交换
GSM	Global System for Mobile Communications	全球移动通信系统

GSMA	Global System for Mobile communications Association	全球移动通信系统协会
HSPA	High-Speed Packet Access	高速分组接入
IMEI	International Mobile Equipment Identity	国际移动设备识别码
IMSI	International Mobile Subscriber Identity	国际移动用户识别码
IP	Internet Protocol	互联网协议
ISP	Internet Service Provider	网络业务提供商
IT	Information Technology	信息技术
ITU	International Telecommunication Union	国际电信联盟
KUMA	Unified Monitoring and Analysis Platform	统一监控和分析平台
LOB	Line of Bearing	方位线
LTE	Long Term Evolution	长期演进技术
MAP	Mobile Application Part	移动应用部分
MCC	Mobile Country Code	移动国家号
MHET	The Mobile Handset Exploitation Team	移动手机开发小组
MNC	Mobile Network Code	移动网号
MSISDN	Mobile Subscriber International ISDN/PSTN Number	移动用户国际号码
MVT	Mobile Verification Toolkit	移动验证工具包
NIB	Network-in-a-box	盒中网络
NSA	National Security Agency	美国国家安全局
NTAT	Network Tradecraft Advancement Team	网络情报技术推进小组
OTA	Over-the-Air Technology	空中下载技术
PC	Personal Computer	个人电脑
PLMN	Public Land Mobile Network	公共陆地移动网
RAT	Remote Access Trojan	远程访问木马
RF	Radio Frequency	射频
ROM	Read-Only Memory	只读存储器
SCCP	Signaling Connection Control Part	信令连接控制部分
SDR	Software Defined Radio	软件无线电
SGSN	Serving GPRS Support Node	服务 GPRS 支持节点
SIGINT	Signal Intelligence	信号情报
SIM	Subscriber Identity Module	用户身份模块
SMS	Short Messaging Service	短信业务
SMS-PP	Point to Point	点对点
SS7	Signaling System 7	7 号信令
STK	SIM Tool Kit	用户识别应用发展工具
TAO	Tailored Access Operations	特定入侵行动办公室
TTTC	Target Technology Trends Center	美国目标技术趋势中心
UDC	Utah Data Center	犹他州数据中心
UICC	Universal Integrated Circuit Card	通用集成电路卡
UMTS	Universal Mobile Telecommunications System	通用移动通信系统
USB	Universal Serial Bus	通用串行总线
UTT	Unified Targeting Tool	统一瞄准工具
VoIP	Voice over Internet Protocol	互联网电话