

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	1
第一篇 一条短信“接管”手机——针对 SIM 卡漏洞的高度复杂攻击.....	5
(一) 事件回顾.....	6
(二) 攻击方式.....	7
(三) 溯源分析.....	9
(四) 延伸分析.....	11
参考资料.....	14
第二篇 被偷走的“钥匙”——窃取手机 SIM 卡加密密钥.....	15
(一) 事件回顾.....	16
(二) 攻击方式.....	17
(三) 延伸分析.....	19
参考资料.....	20
第三篇 悄无声息的入侵——针对苹果手机的“零点击”攻击.....	22
(一) 事件回顾.....	23
(二) 攻击方式.....	23
(三) 延伸分析.....	26
参考资料.....	27
第四篇 “飞马”风波——对商用间谍软件的利用.....	29
(一) “飞马”间谍软件事件回顾.....	30
(二) 美情报机构对“飞马”等间谍软件的利用.....	30
(三) 延伸分析.....	33
参考资料.....	34
第五篇 无法卸载的 APP——通过运营商广泛预置软件收集数据.....	36
(一) 事件回顾.....	37
(二) 事件分析.....	38
(三) 延伸分析.....	39
参考资料.....	40
第六篇 窥探底数——获取全球移动运营商技术参数.....	42

(一)	事件回顾.....	43
(二)	攻击方式.....	43
(三)	延伸分析.....	47
	参考资料.....	48
第七篇	伪装的基站——广泛使用伪基站监控手机.....	50
(一)	美情报机构和执法部门广泛使用伪基站.....	51
(二)	伪基站成为监视和网络攻击的途径.....	53
	参考资料.....	54
第八篇	入侵运营商内网——利用 Regin 软件攻击移动网络.....	57
(一)	事件回顾.....	58
(二)	溯源分析.....	59
(三)	延伸分析.....	61
	参考资料.....	62
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.....	64
(一)	事件回顾.....	65
(二)	溯源分析.....	65
(三)	“量子”系统揭秘.....	66
(四)	延伸分析.....	68
	参考资料.....	69
第十篇	APP“调包计”——“怒角”计划的植入式攻击.....	71
(一)	事件回顾.....	72
(二)	“怒角”计划揭秘.....	73
(三)	延伸分析.....	74
	参考资料.....	75
第十一篇	“棱镜”背后的阴谋——构建超级数据访问接口.....	76
(一)	“棱镜”事件回顾.....	77
(二)	“棱镜”计划的运作.....	79
(三)	“棱镜”计划的危害.....	82
	参考资料.....	83
结 语		85
附录一：缩略语表		90

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。

2004	利用Stingray等伪基站 至少始于2004年 曝光于2013年	“棱镜”计划 始于2007年，曝光于2013年，前身为始于2004年的“星风”计划
2005	“量子”系统攻击 至少始于2005年 曝光于2013年	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。6月7日《华盛顿邮报》对该计划进行了跟进报道，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。该计划前身为始于2004年的“星风”计划。
2006	利用Carrier IQ收集数据 软件发布于2006年 曝光于2011年	
2008	ANT网络攻击装备 2008年前后陆续列装 曝光于2013年	
2010	“DAPINO GAMMA”行动 实施于2010—2011年 曝光于2015年	“金色极光”行动 至少始于2010年 曝光于2014年
2011	“怒角”计划 实施于2011—2012年 曝光于2015年	“社会主义行动” 实施于2010—2013年 曝光于2013年
2017	“Simjacker”攻击 至少始于2017年 曝光于2019年	
2018	利用“飞马”间谍软件 至少始于2018年 曝光于2021年	
2019	“三角测量行动” 至少始于2019年 曝光于2023年	

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。

NSA 利用 Simjacker 漏洞实施攻击

事件名称	NSA 利用 SIM 卡 Simjacker 漏洞监控手机		
时间	至少始于 2017 年 曝光于 2019 年	攻击方	NSA
攻击目标	智能终端硬件	攻击对象	墨西哥、哥伦比亚和秘鲁手机用户

攻击方式

将特殊格式的二进制数据短信发送给目标手机号码，如其 SIM 卡内存在 S@T 浏览器，则触发 Simjacker 漏洞，执行恶意指令，如更改设置、启动浏览器、收集本地数据、回传信息等。

攻击目的

对手机进行监控，以跟踪用户位置、获取手机数据并拦截电话等。

影响

墨西哥、哥伦比亚和秘鲁检测到实际攻击行为，全球 29 个国家的 61 家运营商提供的 SIM 卡都含有 Simjacker 漏洞，涉及 10 亿手机用户。

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。

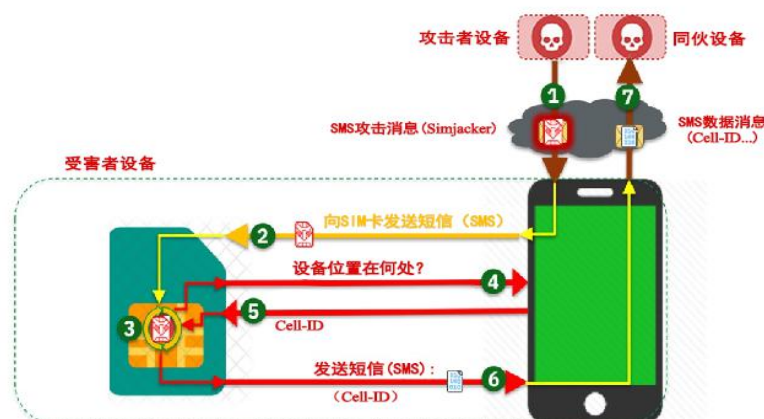


图 1-2 Simjacker 漏洞攻击技术流程

“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 McDauid）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。

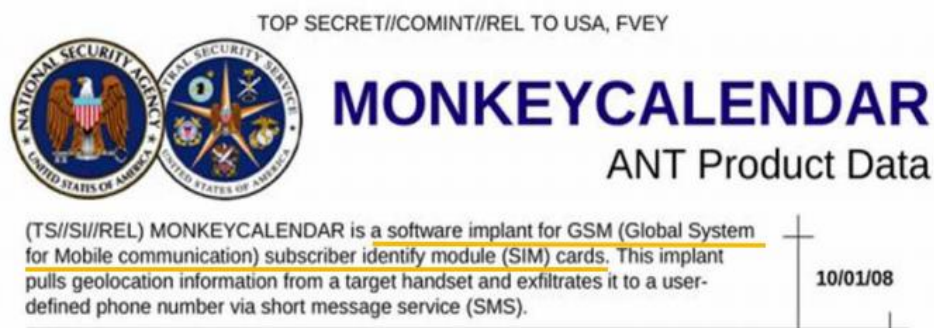


图 1-3 ANT 针对 SIM 卡的网络攻击装备 MONKEYCALENDAR

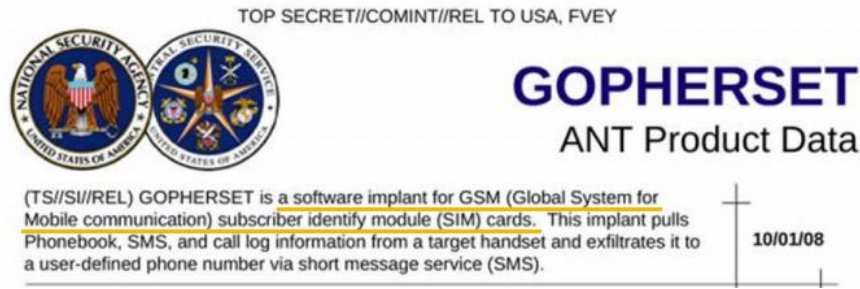


图 1-4 ANT 针对 SIM 卡的网络攻击装备 GOPHERSET

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 attack 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	DROPOUT/JEEP	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
TAWDRYARD	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	无线数据攻击	ENTOURAGE	手机数据收集
COTTONMOUTH-III	物理隔离攻击	TYPHON HX	手机数据收集
DEITYBOUNCE	DeHLL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。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/886121041010011102>