Unknown Title

空中投放与隐蔽突防——A2PT组织对iOS手机的两起攻击案例的对比解析

APT2天前更新 admin 104 0 0
点击上方”蓝字”
关注我们吧！

2025年9月12日-14日，由中国计算机学会（CCF）主办的第三届中国网络大会在沈阳召开，在“新一代移动网络安全分析技术论坛”上，安天首席技术架构师肖新光作了题为《空中投放与隐蔽突防——针对手机场景的A^{2}PT攻击案例解析》的技术报告。

报告对安天CERT团队和国际友商卡巴斯基分别披露的A^{2}PT组织对针对手机用户的两起攻击行动“量子击穿”与“三角测量”进行了对比分析，分别分析相关组织基于“量子”(QUANTUM)系统进行的攻击投放活动和基于iMessage、FaceTime等攻击入口的投放活动过程，解析对应的持久化和致效过程，并做了扩展分析。

报告主要内容来自安天技术报告《“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]和国际友商卡巴斯基“三角测量”系列技术报告[2][3][4][5][6][7]，中国网络安全产业联盟报告《美情报机构针对全球移动智能终端实施的监听窃密活动》[8]。安天小编按照PPT章节的结构，结合现场记录内容、扩展引用安天相关技术报告（含少量待发布报告内容），整理成为本文。

A^{2}PT（高级的高级持续性威胁）是基于“APT”派生出的术语。2015年，基于美方网络攻击的活动作业特点的总结，安天在中国反病毒大会技术报告中首次公开使用A^{2}PT（即高级的高级持续性威胁）这一术语，以此来标定来自超高能力网空威胁行为体的攻击活动。

01
“三角测量”与“量子击穿”——卡巴斯基和安天的曝光接力

1.1背景：斯诺登事件十周年，一场与斯诺登弱相关的发布接力

2023年6月1日，卡巴斯基发布了首篇“三角测量”报告[2]，曝光美方情报机构攻击了他国关键人员包括卡巴斯基高层管理者的苹果手机。基于当时卡巴尚未将样本从主机中完成提取，报告内容主要为环境和网络侧分析，安天决定发布一份历史未公开的美方攻击iOS的样本分析成果，与卡巴斯基成果相互印证。但由于两事件有较长

的时间间隔，只能确定两起攻击有战术和技术相似性，无法判定安天分析的历史样本，是否是“三角测量”攻击样本的早期版本。

1.2两起针对移动智能终端的攻击行动

2014年，安天捕获一个针对iOS系统的载荷，经过信息比对发现，该样本与之前安天所分析的A^{2}PT组织的Solaris、Linux样本存在同源关系，因此确定了来源归属。基于其投放方式，我们将其背后的攻击行动命名为“量子击穿”行动。2023年，卡巴斯基捕获针对iOS系统的攻击样本，由于其攻击阶段特性，卡巴斯基将其行动命名为“三角测量”行动。

除攻击发起方都来自于美国、攻击的目标平台都是iOS以外，这两起行动和对应手法存在差异，详见表1-1。两起攻击的主要差异是：“三角测量”攻击样本是依托iMessage的漏洞投放。“量子击穿”的相关攻击样本来自“量子”（QUANTUM）系统在网络侧针对iOS系统Safari浏览器漏洞利用投放。

表1–1两起攻击行动和样本对比

	“量子击穿”（安天曝光）	**“三角测量”（卡巴斯基）**
启示作业时间（猜测）	2012年~	2019年~
攻击目标范围	包括中国在内的全球多个国家	目前已知包含俄罗斯、中国等
攻击目标平台系统	iOS	iOS
投放方式	量子系统流量注入投递	iMessages消息零点击投递
使用漏洞	目标系统浏览器漏洞	多个iOS系统漏洞
指令模块	指令分组	功能模块化
功能目的	信息刺探与定位、投递下一阶段载荷（未获取到后续载荷）	录音、位置信息获取、手机内数据解析、秘钥链获取

1.3卡巴斯基和安天曝光A^{2}PT攻击操作系统覆盖的接力过程

我们能判定“量子击穿”样本的来源归属，是基于对A^{2}PT攻击组织的长期跟进分析的成果积累。美方在2005年开始，陆续推动了多代大规模高级恶意代码工程。卡巴斯基、安天都对此做出了持续跟进分析。卡巴斯基整体提出了第I代为Flamer框架，“火焰”（Flame）1.0、“火焰”2.0和“高斯”（Gauss）蠕虫均来自这个框架，也包括“震网”（Stuxnet）0.5x版本的部分代码。第II代为Tilded框架，“震网”的大部分和“毒曲”（Duqu）多个版本基于Tilded框架。这与安天在当时的分析判断是一致的，包括跟进“火焰”蠕虫的分析中，安天提出尽管“火焰”比“震网”发现更晚，但其实是更早运营的样本，并进一步猜测，“火焰”的运用广泛面对中东实施的侦查环节，属于CNE（网络情报利用）阶段；而“震网”是最终实施CNA（网络作战打击）的攻击环节。并认为“震网”的阀门级联压力版本（即0.50版本）虽然曝光在后，但其是先于离心机转数篡改版本（即1.x版本）使用的等等。

图1–1 震网和毒曲、火焰、高斯、Fanny、Flowershop软件工程关系图[9]（该图部分参考了卡巴斯基的分析成果）

同时，卡巴斯基和安天也完成对方程式组织（即NSA TAO）多平台样本覆盖的接力，关于方程式攻击体系中各平台样本的首发曝光过程，如表1-2所示，Windows、macOS样本由卡巴斯基率先曝光，FreeBSD平台存在样本由卡巴斯基提出了猜测（未公开样本），Linux、Solaris样本由安天率先曝光。针对iOS攻击活动最早由卡巴斯基曝光，但首篇样本报告是由安天发布的。

iOS攻击样本的正式发布，补齐了对方程式组织作业目标和攻击武器覆盖能力评估的重要拼图。

表1–2卡巴斯基和安天对A^{2}PT第二代攻击样本的拼图

02
“量子击穿”——基于入侵全球通讯体系和浏览器漏洞结合的打击方式

2.1作业过程——“量子击穿”的投放原理

“量子击穿”的投放原理如图2-1。“量子击穿”的攻击对象是访问互联网的目标人群。在一般的网络安全认知中，通常开放的端口和服务是一种固定的暴露面，如果有相关漏洞、缺陷即可发起攻击。而上网过程是浏览器或手

机APP对目标主机的固定端口建立的连接，并使用随机高位端口，往往被认为是安全的，但这恰恰是美方的一种打击方式。通过入侵全球大量运营商的交换机、路由器等网联设备，构建获取上网过程的能力，由此判断提取上网行为元数据提交对应系统匹配，在上网链接中插入临时流量实现攻击目标。该临时流量可以实现浏览器溢出、引流下载木马等等。由于攻击流量是基于通讯过程中被攻陷网络设备临时插入的，因此其行动难以实现TCP/IP意义上的复现和溯源。浏览器漏洞是美方网络攻击漏洞储备重点，浏览器确实是上网必备工具，在目前移动终端成为上网主流的背景下，很多所谓的APP是一个浏览器的壳。利用浏览器入口具有非常强的打击能力，也包括浏览器插件，比如漏洞极多的Flash、QuickTime插件等等，反向猜测由于美方的储备能力，在这些浏览器上历史存在过的一些严重漏洞有可能在曝光之前被美方使用过。

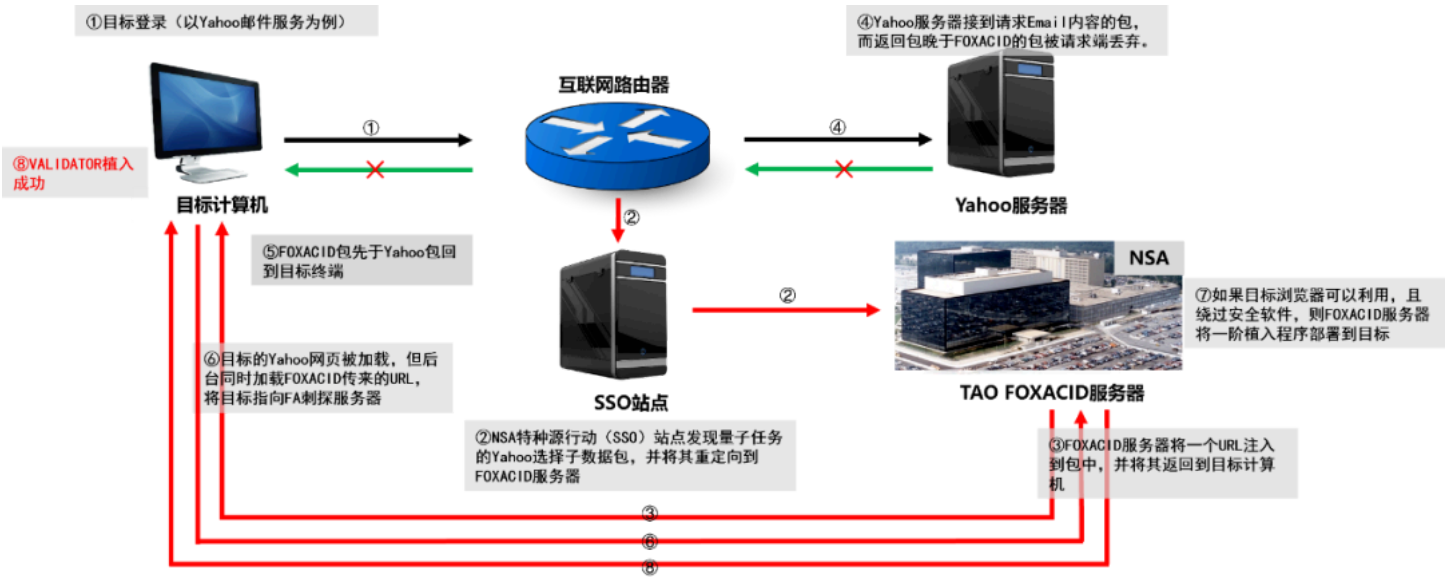

图2–1“量子击穿”投放原理示意图

2.2样本基本情况

表2–1“量子击穿”攻击样本卡片

原始文件名	regquerystr.exe
文件大小	307KB (306,560 bytes)
文件格式	BinExecute/Apple.MACHO[:x86 Little Endian]
病毒名	Trojan/IOS.Equation[APT]

图2–2iOS样本的文件目录信息

2.3木马指令及窃取信息列表分析

如图2-3、表2-2和表2-3所示，多个平台样本的指令与窃取信息格式基本一致，符合身份和位置刺探器的功能定位。

图2–3“量子击穿”木马获取信息与指令控制代码

表2–2木马远程控制指令

16进制指令代码	指令功能
0x42	流量包校验
0x4B	读取文件上传
0x60	收集大量信息回传（详见表2-3）
0x70	更新C2地址

0x75	修改心跳包间隔
0x76	更新配置文件
0x78	更新配置文件
0x79	更新配置文件
0x80	删除文件
0x92	接收文件执行
0x94	更新配置文件
0x95	执行程序
0xA2	更新配置文件

表2–3木马获取环境和配置信息格式说明

标号	说明	标号	说明	标号	说明
000	MAC地址	033	未知	042	未知
001	未知	034	未知	043	语言
002	IP地址	035	操作系统类型	044	未知
003	未知	036	未知	045	系统运行时间
004	代理设置信息	037	未知	046	未知
005	未知	038	时区	047	未知
030	用户名	039	未知	048	样本执行路径
031	密码	040	本地时间	049	系统版本号
032	操作系统类型（iOS）	041	系统时间		

2.4安天对“量子击穿”的来源归因判断

(一)技术证据：“量子击穿”木马内部FAID与泄露的NSA载荷的FAID一致

安天基于此前分析相关样本的加密算法，还原解密出该iOS木马内部配置信息如表24。其中标识FAID（FOXACID，酸狐狸平台）所含有的“ace02468bdf13579”与已曝光的NSA作业唯一标识代码一致。该标识存在于“影子经纪人”泄露的方程式武器库中SecondDate武器中，种种信息表明：该木马来自美方情报机构NSA下属的方程式组织。

表2–4“量子击穿”木马配置信息及内容

配置名称	内容	说明
CI	3600	心跳
CIAE	120	
cop1	80	C2端口1
cop2	443	C2端口2
CSF	/private/var/tmp/.swapfile.tmp	

FAID	***_ace02468bdf13579_***	
ID	*****00171	
lp1	**********[.]com	C2地址1
lp2	80[.]*[.]*[.]*	C2地址2
os1	www.google.com	测试网络联通
os2	www.yahoo.com	测试网络联通
os3	www.wikipedia.org	测试网络联通
os4	www.apple.com	测试网络联通
PV	12	
SDE	/usr/gated/gated.deb	

(二)**资料佐证：与斯诺登泄露资料相互验证**

图2–4斯诺登泄露资料中相关Validator（验证器）内容

斯诺登**泄露**资料中，有一个内容页面介绍了Validator（验证器）。相关文档描述，该木马作为验证木马身份和位置的刺探器，一旦确认便会投递OLYMPUS或UNITEDRAKE（即方程式木马EquationDrug）。

安天基于功能分析，判定安天捕获的iOS样本就是方程式组织针对移动终端的Validator（验证器）。

03

“三角测量”——卡巴斯基针对A2
PT攻击的分析杰作

3.1iMessage——A^2PT的长期攻击入口

卡巴斯基分析曝光的“三角测量”攻击以iMessage服务为攻击入口，iMessage服务是苹果系统开发的一种信息发送的“增强”服务，通过互联网在苹果设备间进行信息发送，包括支持较大的自定义格式附件。基于苹果账户的精确寻址+超大附件，这两个特性使iMessage为面向苹果设备实施精确投放的格式构造攻击提供了入口。

而其端到端的加密的特点，虽然和传统短信相比似乎是一种“安全”特性，但**当其被攻击利用的时候，也构成了对运营商侧安全监测能力的感知穿透**。与其类似的另一入口为FaceTime服务。

表3–1iMessage服务与运营商短信服务的差异（AI整理）

对比维度	iMessage	普通短信（SMS/MMS）
服务起始年份	2011年随iOS 5发布	2002年器由运营商业务推广
传输方式	通过互联网（Wi-Fi 或蜂窝数据）传输，依赖苹果服务器	通过运营商蜂窝网络传输，依赖信号塔和运营商基础设施
收发地址	苹果账户	手机码号
计费	基于数据流量（或Wi-Fi）流量费用	基于运营商短信服务计费
兼容性	仅限苹果设备（iPhone、iPad、Mac等），需双方启用服务	兼容所有手机设备（包括Android 和功能机），无设备限制
加密与安全	端到端加密	早期不加密，后期部分使用A5/1、A5/3、A5/4等算法加密
功能特性	文本、高清图片、视频、文件（最大支持25MB）、位置等	文本、图片/视频（通常限制 300KB–1MB）
消息标识	蓝色气泡	绿色气泡
网络依赖	需互联网连接（Wi-Fi或蜂窝数据）	需运营商蜂窝网络信号，无需互联网
其他	发送失败时可能自动降级为短信发送	

3.2“三角测量”——卡巴斯基曝光的针对iOS系统的攻击链

卡巴斯基绘制了攻击链如图3-1。攻击者基于苹果iMessage服务向目标设备发送一条特制的iMessage消息。iMessage作为苹果自有增强型消息协议，支持发送非常丰富的复合格式内容。

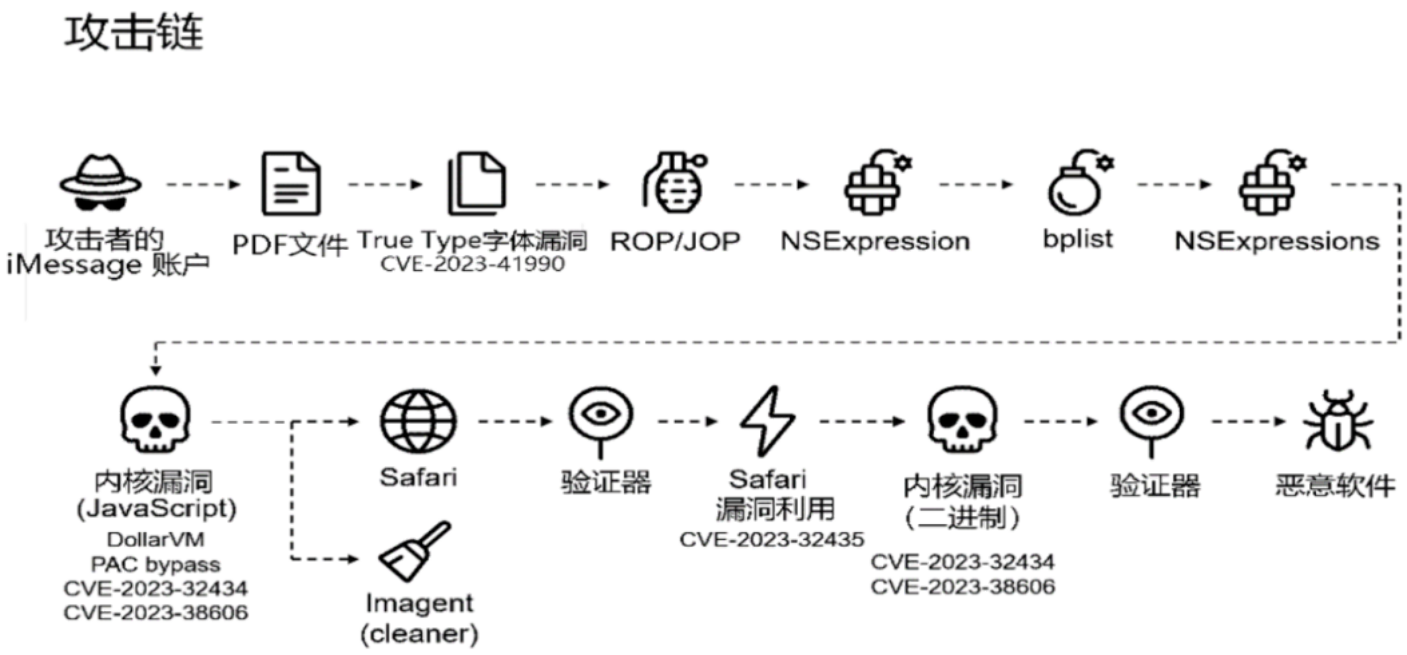

图3–1“三角测量”行动攻击链示意图（汉化自卡巴斯基分析报告）

“三角测量”行动的初始的投放物是针对iOS系统的攻击链中在所发布的恶意附件是特殊构造的PDF文件，其带有特定构造字体文件（TrueType字体格式），利用CVE-2023-41990漏洞，该漏洞为远程代码执行（RCE）漏洞，在字体解析上下文过程中触发，当iOS“调整”（ADJUST）TrueType字体时，会执行恶意构造的代码。这是攻击者的入口，此时并未获得完整的系统权限。由于iOS系统采用哈佛架构设计，每个应用拥有独立的内存空间，此时攻击者无法直接访问系统资源或其他进程内存，也没有完成持久化。接下来，使用“ROP/JOP”技术（面向返回跳转编程技术），利用已有的PAC指针认证机制（在iOS升级过程中逐渐具备的）绕过并实现控制流劫持。利用NSExpression作为执行载体调用patchJavaScript内核完成“bplist”（二进制任务清单）部署。最终部署约11,000行高度混淆的JavaScript代码，完成对JavaScriptCore的内核级Patch与重构，实现提权。攻击者通过Patch后的JavaScript引擎，调用内核调试接口“$VM”实现对引擎内存的读写和API调用。再利用CVE-2023-32434漏洞内存映射整数溢出使得用户态程序可以实现整机物理内存读写。又利用CVE-2023-38606漏洞利用硬件内存映射I/O(MMIO)寄存器来绕过页面保护层，在该漏洞执行后已具备内核态操作能力。启动Imagent进程清理前期利用痕迹、拉起浏览器进程并部署验证器。验证器用于判断环境是否满足投递Payload的条件，通过验证后，反复利用CVE-2023-32434漏洞和CVE-2023-38606漏洞直至实现Payload成功投递。

3.3“三角测量”样本投放和控制指令信息的分析

“三角测量”样本标签如表3-2。

表3–2“三角测量”样本标签

病毒名称	Trojan/MacOS.TriangleDb
MD5	063db86f015fe99fdd821b251f14446d
处理器架构	ARM64
文件大小	677,168字节

文件格式	BinExecute/Apple.MACHO[:x64 Little Endian]
VT首次上传时间	2023-06-21 11:15:33
VT检测结果	33/60

攻击活动中共使用4个0day漏洞，包括CVE-2023-41990、CVE-2023-32434、CVE-2023-38606、CVE-2023-32435。具体内容详见表3-3。

表3–3“三角测量”使用0day漏洞编号及信息

漏洞编号	漏洞信息
CVE-2023-41990	ADJUST TrueType字体指令中的远程代码执行漏洞
CVE-2023-32434	XNU内存映射系统调用中的整数溢出漏洞
CVE-2023-38606	利用硬件内存映射I/O(MMIO)寄存器来绕过页面保护层
CVE-2023-32435	处理Web内容可能会导致任意代码执行的内存损坏问题

“三角测量”控制指令信息如表3-4。

表3–4“三角测量”控制指令信息

命令ID	功能	备注
0xF901	根据CRXUpdateRecord的iM参数，将数据写入文件或向植入物添加新模块。	包含参数fN文件名（iM=0时，附加写入到fN对应文件中，iM=1添加到植入物中）
0xF902	向植入物添加新模块并启动它。	
0xF601	通过FTS API获取指定目录的列表	
0xF801	检索给定文件的元数据（属性、权限、大小、创建、修改和访问时间戳）。	
0xF401	根据命令的参数，删除植入模块或删除具有指定名称的文件。	
0xF402	检索正在运行的进程的列表。	
0xF501	检索指定文件的内容。	
0xFB03	检索受感染设备的秘钥链条目。它开始监视屏幕锁定状态，并在设备解锁时，从/private/var/Keychains/keychains/2.db数据库中转储 genp（通用密码）、inet（Internet 密码）、密钥和证书表（证书、密钥和数字身份）中的秘钥链项。请注意，植入物的代码可以与不同的秘钥链版本一起使用，从iOS 4中使用的版本开始。	
0xFB44	终止具有指定PID的进程，使用SIGKILL或SIGSTOP，具体取决于命令的参数。	
0xFA01	根据命令的参数，删除植入模块或删除具有指定名称的文件。	

0xFA02	通过反射式加载其Mach-O可执行文件来启动具有指定名称的模块。
0xFC11	停止执行CRXPollRecords 命令。
0xFD01	检索有关已安装的iOS应用程序的信息
0xFC10	开始监视名称与指定正则表达式匹配的文件的目录。
0xFC01	检索与指定正则表达式匹配的文件。

3.4安天对“三角测量”的复现、验证和归因关联

安天CERT基于卡巴斯基发布的攻击样本，参考卡巴斯基的分析报告[2][3][4][5][6][7]内容，通过搭建环境模拟C2通信与指令下发等操作触发还原通信过程，包括构建动态调试环境复现音频窃取、压缩实现极小数据量录音等操作。并进行了归因关联分析。

(一)通讯复现

复现“三角测量”载荷与C2通信流量数据，复现数据（包括心跳包、信息获取等功能）内容如下所示：

心跳包数据中包含系统架构、系统特殊文件夹等数据，如图3-2、图3-3。

```
POST / HTTP/1.1
Host: 192.168.132.1:8081
Accept: */*
Content-Type: application/x-www-form-urlencoded
Connection: keep-alive
Cookie: g=(null)
User-Agent: Mozilla/5.0 (iPad; CPU iPhone OS 14_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.1 Mobile/15E1
48 Safari/604.1
Content-Length: 1784
Accept-Language: en-us
Accept-Encoding: gzip, deflate, br

DVKXVHBsmK3sjdS8yB6oUqBO1YdgIUTWrgJKNuf8VuR3SmOV88znphLr38JdbJg8MAXqvmgXnAuIgvFvUVpoOb+5oNOyM3vw5MiEvbao7Y3UY8hfvNlrr1AK7/uSEQLTMO10
Qsd3RmQ0lCx8X1L0oWqsebqY6cGEBC6rNt/J4qpVCr+zmcgtwJmXiRhpfCpR2ZM7hTT20gLtOnhOLCIFWIHfDSZ46zzCskesEmri1xp6yoHhSry+3yNJBCZwXov/98Qc2HJq
VlzyQkRR20ZgPnSkOx72XiUOxwiKdmd4KP6trM6A4bPkZuHh5zJgS8jMxYXqpo2+E0i0oSli2XTSHMgA+zRkONU3WyujgzdYTV6AR7VAYc/Q2D+1kQZ1tDHJSPd/Mc0aTAG18
p7sD4ELMPNGxt5u/HdcxgXy9hj4PzaNSy1kmISYnWJ/2udVjQSlj9ktcNnx1SD4hNS2l8pgIY4bpmeRbNCEbwoEh5b88cCt6eXsndRt+6+eAI5NM8K9awKn1/LA8d7UIjA2A
BkCKlX0I1DfqHSmRB826m6EH1NV4H/JgaU3VLuuvz3I/dUxRhphOuTlDtn2QNoN4fe1wAaopSjUbKCXGqXV5Ro1DMtjwE0NuFui2UJphc4Rs8TMaWCVY9jmGtGjWoX2OpprB
pevHIuv2HUXaiGxLM9kSdZxZwmnKKNk99Za8+p1UfYA/X59uLkMNnZe+CdxPTR1gWk8thgHuvLprZ9Ztdxeiiw05wPNO44yokJ176dVUYCNDdUftS1u1OFrjE1ilLZwf4r8F
oqP86DEglFUQ/6Tb8+GLoZsJfxpbBK2g25yVdR3uqqyFVojZ4xM8iWhaMn6qYkMQMBwvnTwdZVMz9/NA0BH3zRw6y46QVTC4e0hwITKTPOfOqtRNzYnIVHLQbu64mFVZ0ZF1
B8iJXtZJ+bOFXn1U8bYOYhI+GJpQ8jAR+bciLb2GudpavKSjvV2tVaTCPaOdCIjUCxCWP1cdkR/VKRE5iqfGRU/Sue2rOkIZDKvbrwpJfDvvI2Gieb7hQQZdJ0ruSTd7v2Otg
A4POnSxowZm9gURDuTPj/Dj9sCBQFXacJiy5O+JtYJzxZ6Fpw1L/DtqtJ3cPuXAVDWYk0teo9TCy3P0Subjj1gb5PvFL95hmNQ5Twl0iauK/kuHkT07jSelp3W4qLSHivS6o
walmZQ7SvrS59v5PviCzM8bCB8KR5LKUOJZiXqo4x9JqE021XtDEiTzHIhsaVxc2ZlpGiEqDldjlZYq1S9N/PJX+/QxoTK7QgvvFCoqitfMVLsUWgHpXe0q4e+lDpDwW1TKM
uvetBhK4AK8lLsumT7sRZuZVGvkDZf+NRapTW3tFnd56Unn3/5PwAu4d3Wq33naByAgRYMrTeK4jYq3+/N+iTN1SOieYljd3sxy/ZY8vg6vQrqqHmjrmAGyK0nIb+F2o7h5L
+iGNfyXxkH9O1mGhJTLnGYEROYK+VaGu79JHfNauGBY+nUoTvd45d+0qwCG1O8L6BT1L9A1vxgUuzUvMPVJw3QclSZH5obpjVa8mPVLIQyF0nBJ7Bp85aDiJpK5/Ar+3RW07
GaPAe8Kci7u3Sqtu8JOA73yVJeu/7w7RGfDgmTep6dIedx7Ti+WVTFXv92eWHSArPUifnHF02Bh8jAGVULuCeVtzEEDd8RgLvBW4UeZVoqj0NNEk4DwuJKpFo75h10uvhFsw
n1R0ZyizY2XcYcNIqNczUko64RQ+cO6T2LgLgHIvE8+B4frpzQC49eKZqQcKmlQexg==
HTTP/1.0 200 OK
Server: BaseHTTP/0.6 Python/3.9.2
Date: Thu, 16 May 2024 06:54:25 GMT

U
□□□□-□ □□%□□□@Qj%a□□□□(c.□□□□sKKH,¿Gk□□□o□□□`□□L'□3W□f□d□□□)□□□□@□□□□□1□□□□□□□t
```

图3–2“三角测量”载荷与C2通信心跳包（TLS解密后）

图3–3心跳包明文包含系统内容

appinfo（命令ID：0xFD01）是一个典型的信息获取命令，其返回数据包含应用名称、执行文件路径、版本等数据，如图3-4、图3-5。

图3–4命令appinfo流量（TLS解密后）

图3–5appinfo明文内容

(二)攻击样本动态运行调试复现录音窃密功能

1.搭建动态运行调试环境

图3–6搭建动态运行调试环境记录

2.**修复样本并执行，搭建服务器模拟C2进行远程交互**

图3–7动态运行过程

3.复现窃取音频功能，分析确认音频压缩、加速后实现极小数据量录音

图3-8是正常录音音频所包含的波形频谱，图3-9为使用三角测量复现的录音频谱，虽然进行对比的正常音频采样频率和位深度都比三角测量录音的样本要高，但是在相同的时间内（1秒），三角测量录音中包含更多数据量，其波形变化比正常录音音频更加密集。

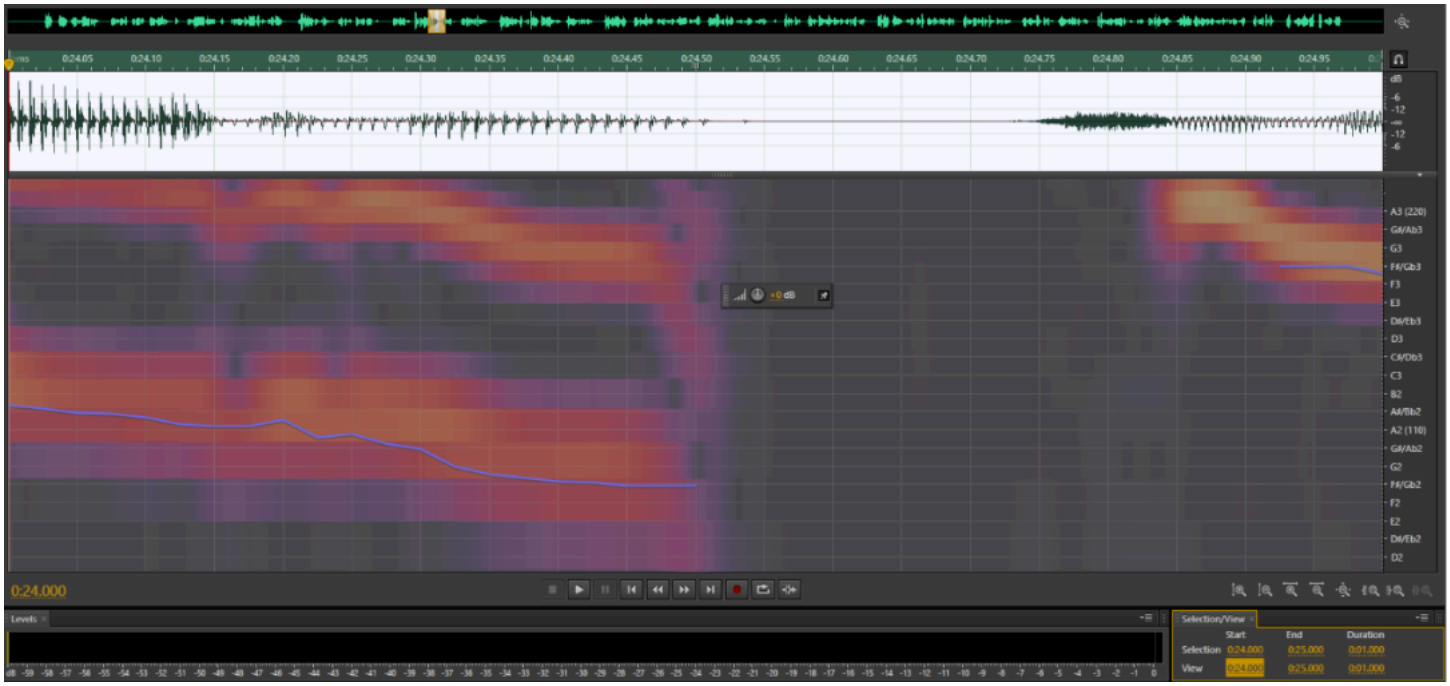

图3–8正常音频一秒，48000Hz，24bit波形

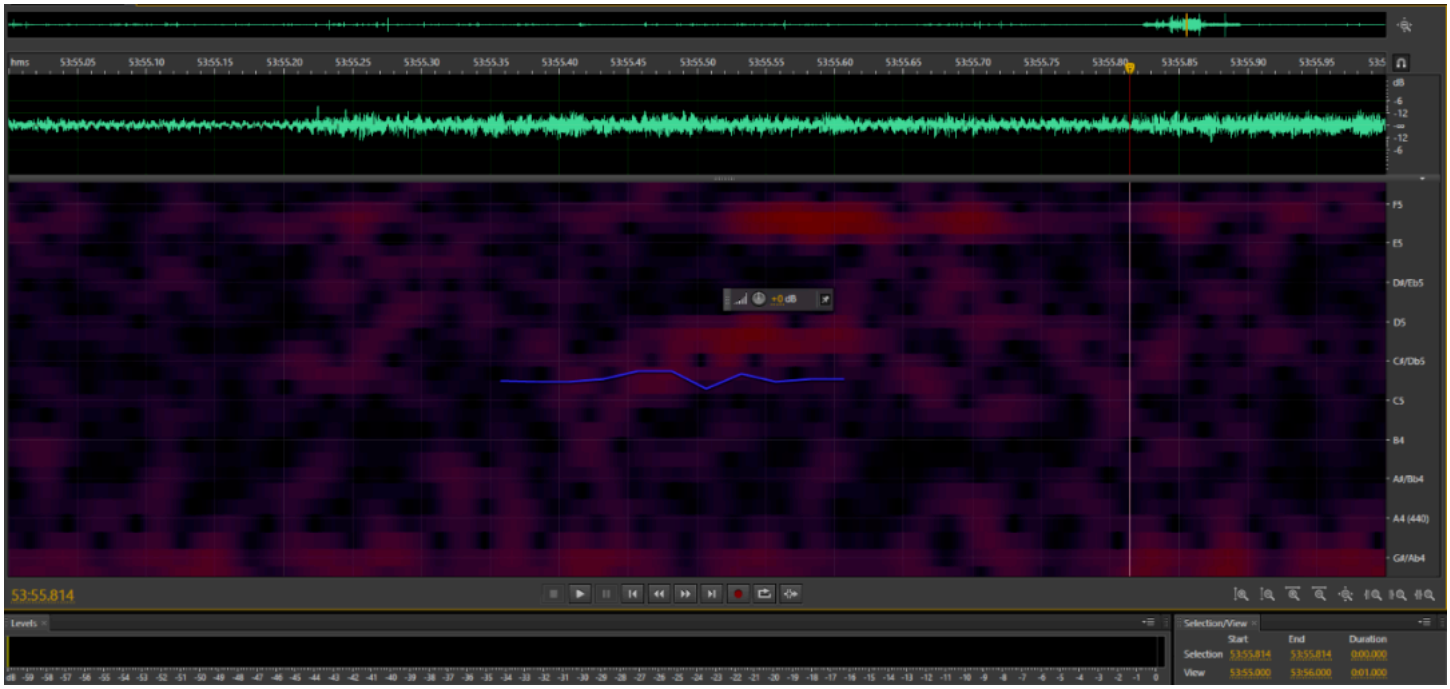

图3–9“三角测量”处理后的录音一秒，44100Hz，16bit波形

(三)基于样本、流量、C2的维度分析“三角测量”的组织归因关联

在进行了完整复现后，进行了基于样本、流量、C2的维度分析“三角测量”的组织归因关联。

1.静态分析与功能推测

在感染目标的初始阶段，受害者收到一个无需点击的带有漏洞的iMessage附件，该漏洞不会直接植入最终的TriangleDB，而是先进行两个验证器进行验证：JavaScript验证器、二进制验证器。

2.**动态分析与行为验证**

➢动态调试TriangleDB获取木马指令

➢中间人劫持解密JavaScript验证器

3.**组织关联与归因**

➢投放模式：零点击攻击，不依赖邮件或者其他需交互的攻击方式，被攻击目标全程无感

➢C2相似性：与方程式域名采用域名的随机单词组合，流量采用严格强加密模式

➢作业模式相似性：功能模块化作业

04
延展分析

4.1基于验证器的范式作业

“三角测量”活动与方程式作业手法类似，都是首先植入一个“验证器”，根据验证器刺探情况决定是否下发进一步的载荷。

“三角测量”的关键功能模块化，如本次发现的位置信息窃取、麦克风监听、SQL数据库窃取、苹果秘钥链窃取，均为独立设计的模块，通过远程投递使用，如图4-1。这与方程式组织的UNITEDRAKE（联合耙）、DanderSpritz（怒火喷射）攻击平台设计思路一致。

图4–1“三角测量”行动的验证模式与独立的窃密模块分析

4.2“量子击穿”与“三角测量”作业模式的结合

两作业模式虽入口不同，但仍具有可结合点，如图4-2。一种是基于量子投放，在“三角测量”行动攻击链中预埋漏洞，可导致浏览器容易被入侵。另一种将“三角测量”行动攻击链视作引子，攻击浏览器时未必需要本机发起对木马的直接下载，而是可以触发过程中的空中劫持性投放。

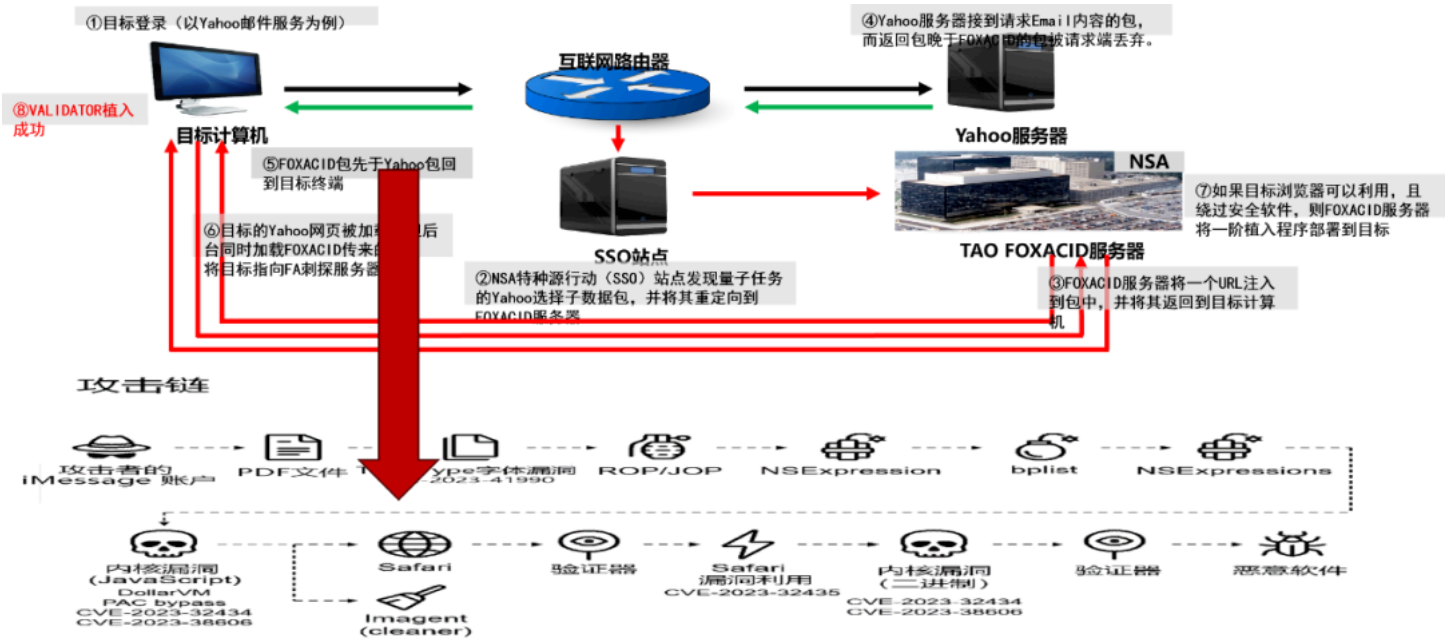

图4–2两种作业模式的结合点分析

4.3A^{2}PT组织的恶意代码的武器生产模式

A^{2}PT组织所展现出的复杂、持久且高效的网络攻击能力，其核心支撑是一个高度工程化、分工明确的恶意代码武器生产体系。该体系已从早期的技术团队创新，演进为由国家情报机构主导、依托国防工业基础进行大规模集成与生产的成熟模式。

(一)研发：体系化与工程化的自研体系

量子击穿和三角测量行动中被捕获分析的样本，都符合A^{2}PT组织自研样本的风格特点。从A^{2}PT组织早期行动，结合因其情报破窗效应的技术资料源码**泄露**事件。较长时间中，恶意代码武器库的研制工作主要由NSA等机构自研，或少数关系紧密、具备最高安全保密资质的核心承包商长期承担。这种深度绑定模式保障了攻击工具的在最核心、最敏感的网络行动中，以及技术发展的可控性。

其行动样本可以对应到、超大规模的软件工程体系。这些平台（如Flamer、Tilded等）呈现出高度的模块化、以及“滚动迭代”的更新能力。

(二)外部采购：商用武器的整合与应用

基于FBI曾被曝光采购以色列NSO集团的“飞马”（Pegasus）间谍软件及意大利Hacking Team公司的“伽利略”（Galileo）远程控制系统。因此可见通过商业采购并整合至自有攻击平台成为另一重要来源。由于自研能力不足，商用武器可能是美执法机构实施攻击性取证和隐秘监控的主要能力来源。同时其情报机构也可能采用商用载荷。

具体方式包括：

➢直接采购成熟武器：存在直接从商业监控公司购买成熟间谍软件并投入使用的记录。例如，FBI曾被曝光采购以色列NSO集团的“飞马”（Pegasus）间谍软件及意大利Hacking Team公司的“伽利略”（Galileo）远程控制系

统。

➢武器的整合与部署：所采购的商用工具并非孤立使用，而是通常作为有效载荷（Payload），由自有攻击平台（如“量子”系统）进行投送。在通过初始攻击突破目标后，这些工具被植入以实现持久化驻留和深度情报搜集，从而构建完整的“突破–投送–控制”杀伤链。

(三)走向工业化：军工信息复合体可能成为新的开发/集成方

随着网络攻击作为一种独立的预算从情报体系建设中独立，依托美方的旋转门运行机制，可以判断必然出现的情况是：网络攻击武器的生产与军工复合体转化为军工信息复合体的节奏一致。以波音（Boeing）、洛克希德·马丁（Lockheed Martin, LMT）、雷神（Raytheon）为代表的国防军工巨头，会取代原有的中小情报承包商和商业木马企业，成为核心一级供应商。而这就使其能更好的进行整合。

例如，美国军工承包商曾在情报部门默许下试图收购NSO集团，显示出防务巨头意图将顶级商业攻击能力直接纳入其供应链的战略动向。

(四)资源复用：对第三方恶意代码的再利用

基于CamberDaDa计划的信息披露，NSA从较早开始了获取第三方样本感染机会劫持利用，和第三方样本重用的情况。这是一种成本更低，同时直接带有假旗效应的运用方式。

4.4A^{2}PT的漏洞资源分析

(一)漏洞分布重点的分析

安天CERT多次判断，美方的重点漏洞储备分布在两个方向，一种是基于类似浏览器客户端软件的漏洞，针对目标为移动终端、互联网终端和内网主机，由于这类目标或者没有固定的公网IP+开放端口服务，或者不暴露在互联网上，A^{2}PT攻击中需要通过类似的软件通信作为攻击入口；二是面向操作系统、应用平台开放的服务（静态端口）的漏洞，针对目标为具有公网IP服务器、终端，通过其暴露的公网IP端口作为攻击入口。

表4–1A^{2}PT组织针对浏览器和针对开放端口服务的两个漏洞集合对比表

	浏览器	开放服务（端口）
打击目标	移动终端、互联网终端、内网主机、	公网IP服务器、终端
打击方式	流量劫持注入（量子系统）、短信链接、iMessage等方式发送	跳板机、代理转发工具建立连接发送攻击流量
主要漏洞机理	缓冲区溢出、逻辑漏洞、组件插件漏洞、沙箱逃逸	缓冲区溢出、提权、防护机制（DEP、ASLR等）绕过
主要针对的软件和服务	IE、Chrome、Firefox、Safari等	HTTP（80）、NetBIOS（139）、IMAP（143）、SMB（445）、RDP（3389）等

(二)针对浏览器和互联网客户端的漏洞库猜测

针对浏览器和互联网客户端的漏洞库，我们称之为漏洞集合（C），即Client，客户端。这部分漏洞是配置到“量子”或类似系统使用，较少的人可以直接接触使用。量子系统可攻击场景图谱化分析如图4-3。

图4–3量子系统可攻击场景图谱化分析

(三)针对开放端口和服务的漏洞库分析（影子经纪人曝光泄露）

针对开放端口和服务的漏洞库（影子经纪人曝光泄露），我们称之为漏洞集合（S），即Service，服务端；这部分漏洞集成到可本地部署FuzzBunch漏洞攻击平台使用，内部使用传播范围更广。NSA已经**泄露**的攻击开放端口和服务的漏洞图谱[10]如图4-4。

图4–4NSA攻击开放端口和服务的漏洞图谱

4.5A^{2}PT组织的武器、漏洞资源和体系

美方情报机构通过公开安全活动、代理人模式、漏洞悬赏合作以及与网络军火商采购的模式在全球搜集、采购0day漏洞，并通过与网空防务承包商、电信基础设施公司和互联网公司构建网空项目、武器、基础设施和大数据支撑，依托在全球部署的项目和作业平台，利用植入、运载和中继装备，通过漏洞投放各类高级恶意代码，针对全球IT目标发起大量攻击行动，其组织运营和作业关系图谱如图4-5。

图4–5方程式组织资源运营和作业关系图谱

05
延伸阅读

本报告的第四章内容为介绍中国网络安全产业联盟在2025年03月25日发布的报告《美情报机构针对全球移动智能终端实施的监听窃密活动》[8]。

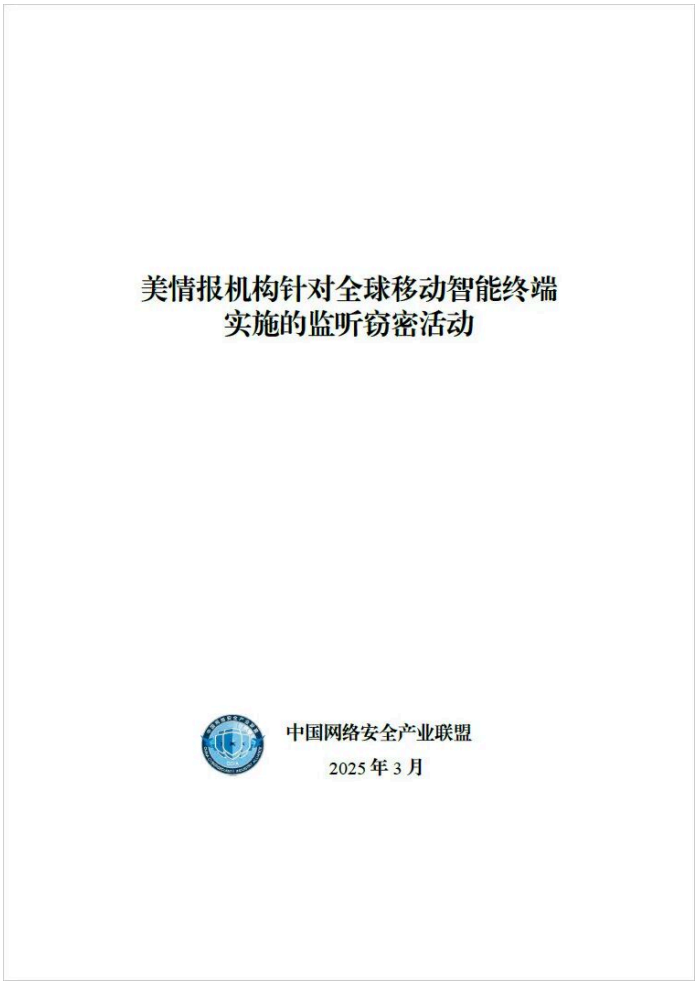

图5–1《美情报机构针对全球移动智能终端实施的监听窃密活动》封面

06
结束语：我们的斗争

2022年美国国会听证会报告点名安天等两家中国网络安全企业分析了NSA和CIA的“网络空间行动”（即网络入侵攻击），首次将中国网络安全主体点名扩展到了防御和分析侧。但在对应报告内容中，不愿承认我们直接捕获了美方攻击，而认为我们的分析成果依赖于“影子经纪人”的**泄露**。深入分析开源情报和技术资源本身是安全企业的常态，“影子经纪人”**泄露**的美方样本，我们当然高度关注、并全面跟进分析。但同时从时间上可以看到安天对方程式组织的发布的第一篇报告《修改硬盘固件的木马——探索方程式（EQUATION）组织的攻击组件》[11]、第二篇报告《方程式（EQUATION）部分组件中的加密技巧分析》[12]都是早于“影子经纪人”**泄露**事件。而在这次听证会上，美国并明确提出了超越“点名羞辱”，将既有“威胁”实力的中国企业纳入打击名单，公开将具备防御和分析能力的中国安全企业视为打击对象。

2024年2月，SentineLabs报告点名歪曲安天等三家中国企业和中国网络安全产业联盟对美方攻击活动和样本的分析工作，认为中国安全企业没有独立发现能力，依赖跟随国际厂商研究成果和美方情报机构泄露信息。此后，安天发布了报告《如何让鹰鹫在迷雾中显形——接力协同与我们的贡献》[13]回应，并梳理了对A^2PT攻击样本全球安全机构分析成果发布情况，中国安全企业在揭露A^2PT攻击中扮演了非常关键的作用。

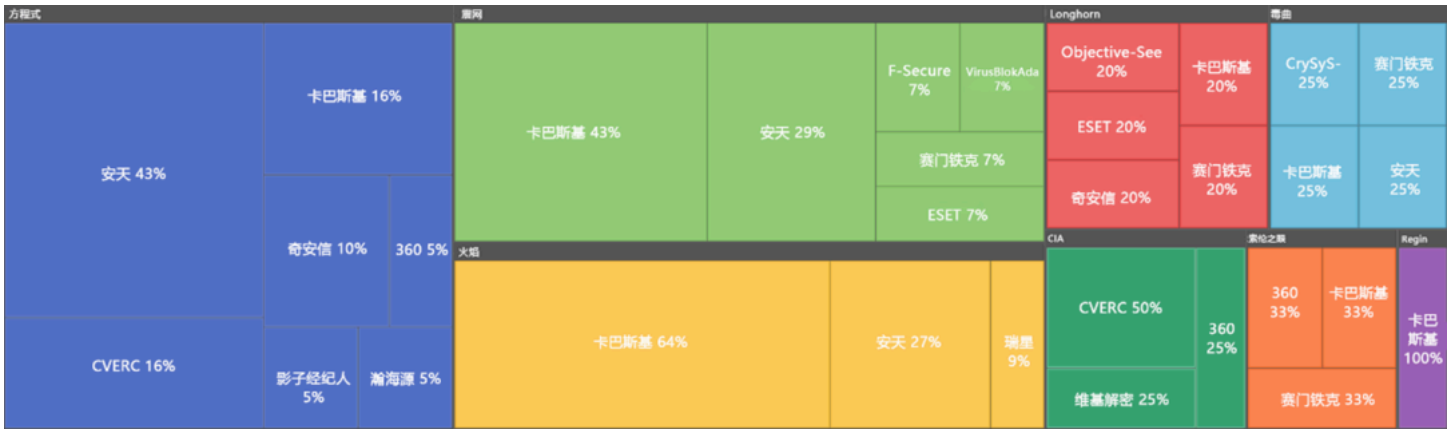

图6–1已披露美方网空武器组成及各安全厂商披露占比

当施加伤害的一方将被害方能力的不足作为一种原罪来奚落的时候，我们看到的是两百年来的殖民者与侵略者习惯的傲慢，将被殖民、被侵略和被伤害者没有足够的反抗实力视为一种原罪。

当基于上帝模式作业，依托其庞大的情报工程体系、大规模建制化的攻击队伍、覆盖全平台全场景的攻击武器，基于人力、电磁和网空混合作业的A^2PT攻击者，自以为可以“杀人于无形”，“事了拂衣去”，又反过来嘲笑被攻击方时，我们是不是读到了两百年来同样的剧本。

施害者不因施害的高明而高贵，反抗者不因反抗的艰难而卑微。

图6–2内容摘选《如何让鹰鹫在迷雾中显形——接力协同与我们的贡献》[13]结束语

我们不因阶段性的弱小而感到自卑和不安，也不因阶段性的困难而产生动摇和恐慌，因为我们站在历史的进步性和正义性的一边！

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[R/OL].(2022-10-24)

https://www.antiy.com/response/EQUATION_iOS_Malware_Analysis.html

[2].Operation Triangulation: iOS devices targeted with previously unknown malware [R/OL].(2023-06-01)

https://securelist.com/operation-triangulation/109842/

[3].In search of the Triangulation: triangle_check utility [R/OL].(2023-06-02)

https://securelist.com/find-the-triangulation-utility/109867/

[4].Dissecting TriangleDB, a Triangulation spyware implant [R/OL].(2023-06-21)

https://securelist.com/triangledb-triangulation-implant/110050/

[5].The outstanding stealth of Operation Triangulation [R/OL].(2023-10-23)

https://securelist.com/triangulation-validators-modules/110847/

[6].How to catch a wild triangle [R/OL].(2023-10-26)

https://securelist.com/operation-triangulation-catching-wild-triangle/110916/

[7].Operation Triangulation: The last (hardware) mystery [R/OL].(2023-12-27)

https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/

[8].美情报机构针对全球移动智能终端实施的监听窃密活动[R/OL] .(2025-03-25)

https://www.china-cia.org.cn/AQLMWebManage/Resources/kindeditor/attached/file/20250324/20250324141948_8988.pdf

[9].震网事件的九年再复盘与思考[R/OL] .(2019-09-30)

https://www.antiy.cn/research/notice&report/research_report/20190930.html

[10].安天关于系统化应对NSA网络军火装备的操作手册[R/OL] .(2017-05-22)

https://www.antiy.com/response/Antiy_Wannacry_NSA.html

[11].修改硬盘固件的木马——探索方程式（EQUATION）组织的攻击组件[R/OL] .(2015-03-05)

https://www.antiy.com/response/EQUATION_ANTIY_REPORT.html

[12].方程式（EQUATION）部分组件中的加密技巧分析[R/OL] .(2015-04-19)

https://www.antiy.com/response/Equation_part_of_the_component_analysis_of_cryptographic_techniques.html

[13].如何让鹰鹭在迷雾中显形——接力协同与我们的贡献[R/OL] .(2024-03-21)

https://www.antiy.cn/research/notice&report/research_report/How_to_make_the_Eagle_appear_in_the_fog.html

往期推荐:

“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

修改硬盘固件的木马——方程式探秘

方程式（EQUATION）部分组件中的加密技巧分析

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

安天发布方程式组织Drug攻击平台初步解析

如何让“鹰鹭”在迷雾中显形——接力协同与我们的贡献

重磅发布 | 中国网络安全产业联盟发布《美情报机构针对全球移动智能终端实施的监听窃密活动》（中英文版）

本篇文章来源于微信公众号: 安天集团

上一篇

蔓灵花（APT-Q-37）以多样化手段投递新型后门组件

下一篇

没有更多了...

相关文章