Airborne Delivery and Covert Penetration: A Comparative Analysis of Two Attack Cases Targeting iOS by the A2PT Group

2025/10/20

The original report is in Chinese, and this version is an AI-translated edition.

From September 12 to 14, 2025, ChinaNet 2025, hosted by the China Computer Federation (CCF), was held in Shenyang. At the “Next-Generation Mobile Network Security Analysis Technology Forum”, Xiao Xinguang, Chief Technical Architect of Antiy, delivered a technical report titled “Airborne Delivery and Covert Penetration——Analysis of A^{2}PT Attack Cases Targeting Mobile Scenarios”.

The report presents a comparative analysis of the two attack operations of the A^{2}PT group targeting mobile users, "Quantum Penetration" and "Triangulation", disclosed by Antiy CERT and the international partner Kaspersky, respectively. The attack delivery activities carried out by relevant groups based on the "QUANTUM" system and those based on attack vectors such as iMessage and FaceTime are analyzed respectively. The report further analyzes the corresponding persistence and effectiveness mechanisms and provides extended insights.

The main content of the report is derived from Antiy's technical report titled "The Quantum System Penetrates Apple Phones——Analysis of Historical Samples of the Equation Group Attacks on iOS Systems"[1] and a series of technical reports from our international partner Kaspersky on "Triangulation"[2][3][4][5][6][7], as well as the China Cybersecurity Industry Alliance (CCIA)'s report "Mobile Cyberattacks Conducted by US Intelligence Agencies"[8]. Antiy's editor has organized this article based on the structure of PPT chapters, combined with on-site recorded content and extended references to Antiy's relevant technical reports (including some content from reports to be released).

A^{2}PT (Advanced Advanced Persistent Threat) is a term derived from "APT". In 2015, based on a summary of the operational characteristics observed in the U.S. cyber attacks, Antiy first publicly introduced the term "A^{2}PT" (Advanced Advanced Persistent Threat) in a technical report at the China Anti-Virus Conference to identify attack activities from ultra-high-capability cyber threat actors.

1 "Triangulation" and "Quantum Penetration" — The Kaspersky-Antiy Disclosure Relay

1.1 Background: The 10th Anniversary of the Snowden Leaks and a Weakly Related Disclosure Relay

On June 1, 2023, Kaspersky released its inaugural "Triangulation" report[2], exposing how the U.S. intelligence agencies targeted iPhones belonging to foreign key personnel, including Kaspersky executives. As Kaspersky had not yet fully extracted samples from the compromised hosts at that time, the report primarily focused on environmental and network-side analysis. Antiy decided to release previously unpublished findings on U.S. attack samples targeting iOS, which corroborated Kaspersky's findings. However, due to the significant time gap between the two incidents, only tactical and technical similarities between the attacks could be confirmed. It remained impossible to determine whether the historical samples analyzed by Antiy constituted an early version of the "Triangulation" attack samples.

1.2 Two Attack Operations Targeting Mobile Devices

In 2014, Antiy captured a payload targeting iOS systems. Through information comparison, it was discovered that this sample shared a common origin with samples previously analyzed by Antiy from the A^2PT group targeting Solaris and Linux systems, thereby confirming its source attribution. Based on its deployment method, the underlying attack operation was named "Quantum Penetration". In 2023, Kaspersky captured attack samples targeting iOS systems. Due to their attack phase characteristics, Kaspersky named the operation "Triangulation".

While both operations originated from the United States and targeted iOS platforms, their methodologies differed significantly, as detailed in Table 1-1. The primary distinction lies in deployment: Triangulation leveraged vulnerabilities within iMessage, whereas Quantum Penetration exploited vulnerabilities in the Safari browser on iOS systems via network-side attacks originating from the QUANTUM system.

Table 1-1 Comparison of the Two Attack Operations and Sample

	"Quantum Penetration" (Exposed by Antiy)	"Triangulation" (Kaspersky)
Revelation Timing (Estimated)	2012–	2019–

Attack Target Scope	Multiple countries worldwide, including China	Currently known to include Russia, China, etc.
Targeted Platform and Systems	iOS	iOS
Delivery Method	Quantum system traffic injection delivery	iMessages zero-click delivery
Exploited Vulnerabilities	Targeted system browser vulnerabilities	Multiple iOS system vulnerabilities
Command Module	Comm grouping	Functional modularization
Functional Purpose	Information gathering and location tracking, delivery of subsequent payloads (no follow-up payloads obtained)	Audio recording, location data acquisition, mobile device data parsing, keychain extraction

1.3 Kaspersky and Antiy Reveal A^{2}PT Attack's Relay Process Across Operating Systems

Our determination of the origin of the "Quantum Penetration" samples is based on accumulated findings from long-term tracking and analysis of the A^{2}PT attack group. Since 2005, the U.S. has progressively advanced multiple generations of large-scale advanced malware projects. Both Kaspersky and Antiy have conducted continuous follow-up analysis on these projects. Kaspersky collectively identified the first generation as the Flamer framework, from which the "Flame" 1.0, "Flame" 2.0, and "Gauss" worms originated, along with portions of the "Stuxnet" 0.5x version code. Generation II is the Tilded framework, upon which most of Stuxnet and multiple versions of Duqu are based. This aligns with Antiy's analysis at the time. In its follow-up analysis of the Flame worm, Antiy noted that although Flame was discovered later than Stuxnet, it was actually an earlier operation sample. Antiy further speculated that Flame was extensively deployed for reconnaissance operations targeting the Middle East, representing the CNE (Cyber National Enemy) phase; while Stuxnet represented the final CNA (Cyber Network Attack) execution phase. Antiy also noted that the valve pressure cascade version of Stuxnet (version 0.50), though disclosed later, was deployed prior to the centrifuge speed manipulation version (version 1.x), among other observations.

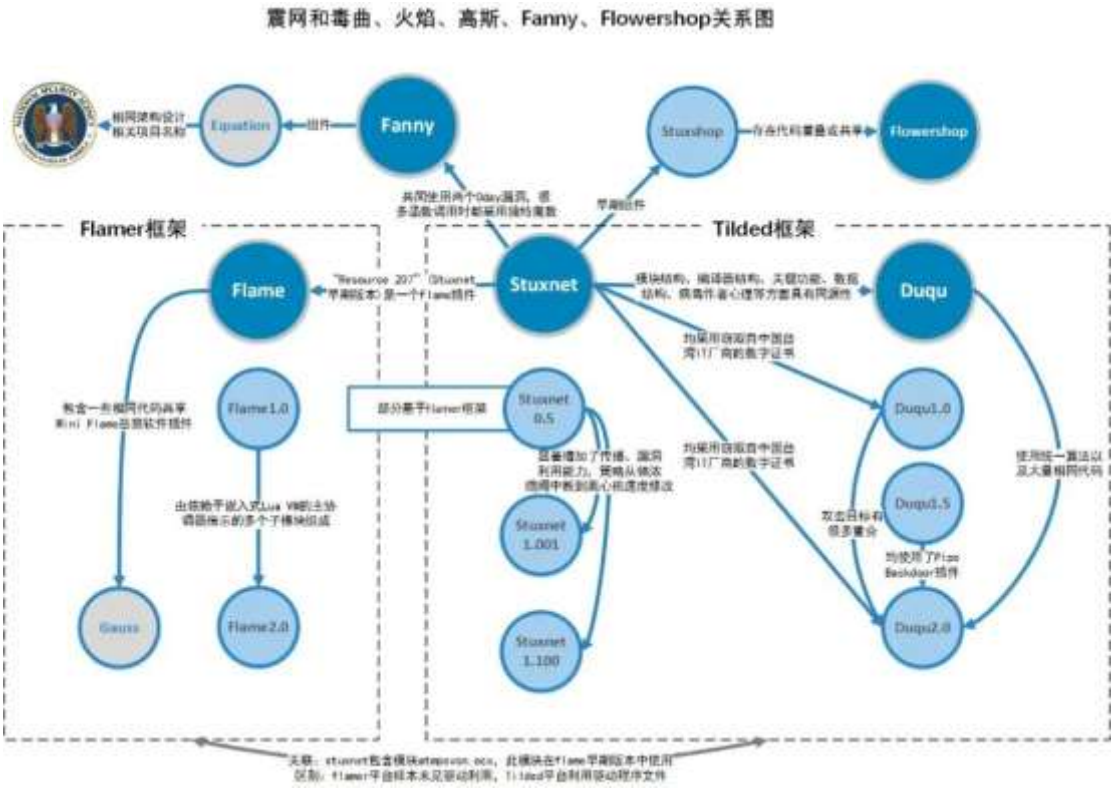

Figure 1-1: Software Engineering Relationship Diagram of Stuxnet, Duqu, Flame, Gauss, Fanny and Flowershop[9] (This diagram partially references Kaspersky's analysis findings)

Simultaneously, Kaspersky and Antiy completed the relay of multi-platform sample coverage for the Equation Group (i.e., NSA TAO). The process of first exposing samples across platforms within the Equation attack ecosystem is shown in Table 1-2: Windows and macOS samples were first disclosed by Kaspersky, while Kaspersky proposed the existence of FreeBSD samples (unpublished samples). Linux and Solaris samples were first disclosed by Antiy. iOS attack activities were first exposed by Kaspersky, but the first sample report was published by Antiy.

The formal release of iOS attack samples completes a crucial piece of the puzzle in assessing the target scope and attack weapon capabilities of the Equation Group.

Table 1-2: Kaspersky and Antiy's Contributions to the Puzzle of A^{2}PT Second-Generation Attack Samples

发布时间	信息	Windows	Linux	Solaris	FreeBSD	Mac OS	iOS
2015年2月	卡巴斯基：Equation: The Death Star of Malware Galaxy	揭秘方程式攻击组织					
2015年2月	卡巴斯基：A Fanny Equation: "I am your father, Stuxnet"	Fanny组件分析					
2015年2月	卡巴斯基：Equation Group: from Houston with love	DoubleFantasy分析					
2015年2月	卡巴斯基：EQUATION GROUP: QUESTIONS AND ANSWERS	方程式组织问与答				根据网络特征提出猜测	
2015年3月	安天：修改硬盘固件的木马 探索方程式（EQUATION）组织的攻击组件	分析样本载荷和硬盘持久化能力					
2015年4月	安天：方程式（EQUATION）部分组件中的加密技巧分析	分析加密算法	三平台通用	三平台通用			
2016年10月	The Hacker News：《Shadow Brokers reveals list of Servers Hacked by the NSA》			曝光存在	曝光存在		
2016年11月	安天：EQUATION攻击组织的全平台载荷能力解析		曝光存在，分析相关载荷	分析相关载荷			
2023年6月	安天："量子"系统查获苹果手机——方程式组织攻击iOS系统的历史样本分析						样本曝光分析

2 "Quantum Penetration" — A Combined Approach Exploiting Global Communication Infrastructure and Browser Vulnerabilities

2.1 Operational Process—Deployment Mechanism of "Quantum Penetration"

The deployment principle of "Quantum Penetration" is illustrated in Figure 2-1. Its targets are individuals accessing the internet. Conventional cybersecurity understanding treats open ports and services as fixed exposure points—vulnerabilities or flaws can be exploited for attacks. However, the internet access process involves browsers or mobile apps establishing connections to fixed ports on target hosts using randomly assigned high-level ports, which are often considered secure. This is precisely where the U.S. approach targets. By compromising vast numbers of network-connected devices—such as switches and routers—operated by global operators, the attackers establish the capability to intercept internet sessions. They then analyze and extract metadata from these sessions, submitting it to corresponding systems for matching. Temporary traffic is inserted into these internet connections to achieve attack objectives. This temporary traffic can trigger browser overflows, redirect downloads to trojans, and more. Since the attack traffic is inserted temporarily into the communication process via compromised network devices, its actions are difficult to reproduce or trace back in the TCP/IP sense. Browser vulnerabilities form a key focus of U.S. cyberattack reserves. As browsers are essential tools for internet access, and with mobile terminals now dominating online activity, many so-called apps are essentially browser shells. Exploiting browser entry points offers formidable attack capabilities, including browser plugins like the highly vulnerable Flash and QuickTime plugins. Given the

U.S.'s reserve capacity, it's plausible that severe historical vulnerabilities in these browsers were exploited by the U.S. before public disclosure.

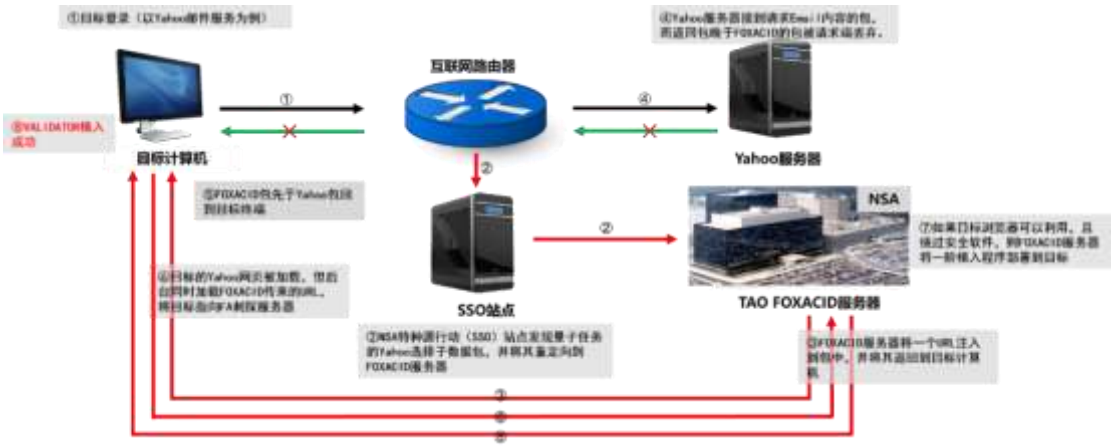

Figure 2-1 Schematic Diagram of "Quantum Penetration" Deployment Principle

2.2 Sample Overview

Table 2-1 "Quantum Penetration" Attack Sample Card

Original filename	regquerystr.exe
File Size	307KB (306,560 bytes)
File Format	BinExecute/Apple.MACHO[:x86 Little Endian]
Virus Name	Trojan/IOS.Equation[APT]

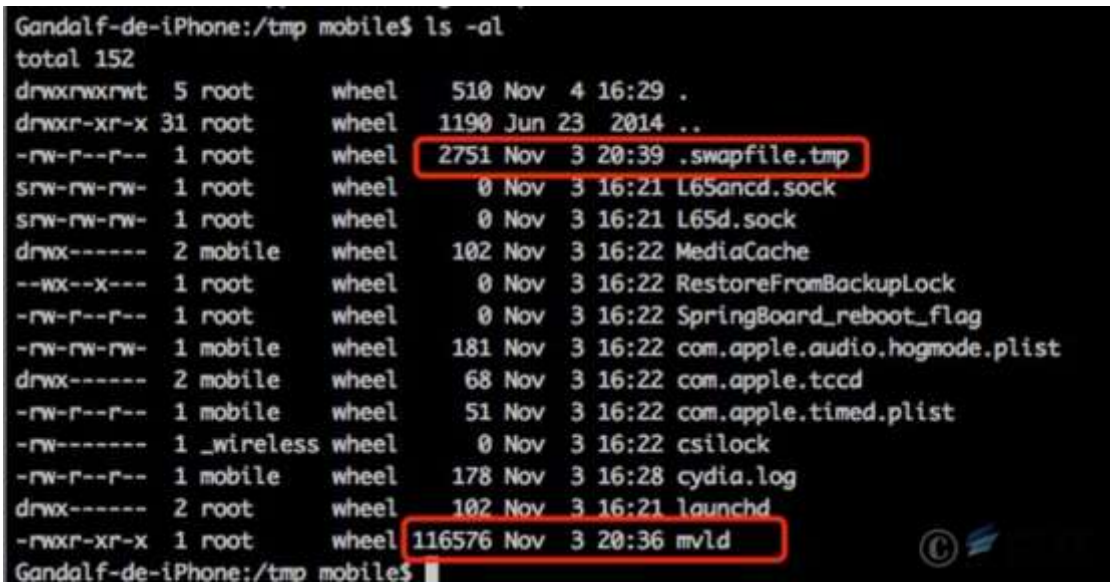

Figure 2-2 File Directory Information of the iOS Sample File

2.3 Analysis of Trojan Commands and Stolen Information Lists

As shown in Figure 2-3, Table 2-2, and Table 2-3, the command formats and stolen information structures across multiple platform samples are largely consistent, aligning with the functional positioning of an identity and location probe.

```
  v87 = decode_str47(v21, "030:0\n", 7);
  sub_C848(&v111, v87);
  v88 = decode_str47(&v89[v22], &unk_19878, 9);
  sub_C848(&v111, v88);
}
v31 = decode_str47(&v89[33 * (v20 & 3)], "032:iOS\n", 9);
sub_C848(&v111, v31);
v108 = 0;
v109 = 0;
v110 = 0;
systemVersion(&v108);
v32 = decode_str47(&v89[33 * ((v20 + 1) & 3)], "049:%s\n", 8);
sub_C848(&v111, v32, &v108);
v33 = decode_str47(&v89[33 * ((v20 + 2) & 3)], "033:%s\n", 8);
sub_C848(&v111, v33, &v100);
v34 = decode_str47(&v89[33 * ((v20 + 3) & 3)], "034:%s\n", 8);
sub_C848(&v111, v34, &v98);
v35 = decode_str47(&v89[33 * ((v20 + 4) & 3)], &unk_19884, 8);
sub_C848(&v111, v35, &v99);
v36 = decode_str47(&v89[33 * ((v20 + 5) & 3)], "MACHTYPE", 9);
v37 = v20 + 6;
v38 = getenv(v36);
if ( !v38 )
  v38 = &"";
v39 = decode_str47(&v89[33 * (v37 & 3)], "036:%s\n", 8);
v40 = v37 + 1;
sub_C848(&v111, v39, v38);
v41 = decode_str47(&v89[33 * (v40 & 3)], "037:\n", 6);
v42 = v40 + 1;
sub_C848(&v111, v41);
tzset();
v43 = decode_str47(&v89[33 * (v42 & 3)], "038:%s\n", 8);
v44 = v42 + 1;
sub_C848(&v111, v43, tzname[0]);
v45 = decode_str47(&v89[33 * (v44 & 3)], "TZ", 3);
```

```
switch ( v7 )
{
  case 0x42:
    v10 = sub_4304(&v13, v8);
    break;
  default:
    v10 = 153;
    v11 = 1;
    goto LABEL_11;
  case 0x4A:
  case 0x92:
    v10 = rw_chmod_unlink(&v15, &v13, v8);
    break;
  case 0x4B:
    v10 = sub_3D98(&v15, &v13, v8);
    break;
  case 0x60:
    v10 = upload_info(&v15);
    break;
  case 0x70:
    v10 = sub_3830(&v15, &v13, v8);
    break;
  case 0x75:
    v10 = sub_37C8(&v15, &v13, v8);
    break;
  case 0x76:
    v10 = sub_39FC(&v15, &v13, v8);
    break;
  case 0x78:
    v10 = sub_4910(&v15, &v13, v8);
    break;
  case 0x79:
    v10 = sub_6148();
    break;
  case 0x80:
    v10 = sub_3AD8(&v15, &v13, v8);
```

Figure 2-3 “Quantum Penetration” Trojan Information Acquisition and Command Control Code

Table 2-2 Trojan Remote Control Commands

Hexadecimal Instruction Code	Instruction Function
0x42	Traffic packet verification
0x4B	Read file upload
0x60	Collect and transmit large amounts of information (see Table 2-3 for details)
0x70	Update C2 address
0x75	Modify heartbeat packet interval
0x76	Update configuration file
0x78	Update configuration file
0x79	Update configuration file
0x80	Delete file
0x92	Receive file execution
0x94	Update configuration file
0x95	Execute program
0xA2	Update configuration file

Table 2-3 Format Specifications for Trojan Acquisition Environment and Configuration Information

Label	Description	Label	Description	Label	Description
000	MAC Address	033	Unknown	042	Unknown
001	Unknown	034	Unknown	043	Language
002	IP Address	035	Operating System Type	044	Unknown
003	Unknown	036	Unknown	045	System Runtime
004	Proxy Settings Information	037	Unknown	046	Unknown
005	Unknown	038	Time Zone	047	Unknown
030	Username	039	Unknown	048	Sample Execution Path
031	Password	040	Local Time	049	System Version Number
032	Operating System Type (iOS)	041	System Time		

2.4 Antiy's Attribution Analysis of the "Quantum Penetration" Source

(1) Technical Evidence: The internal FAID of the "Quantum Penetration" Trojan matches the FAID of the leaked NSA payload

Based on prior analysis of encryption algorithms in related samples, Antiy decrypted and reconstructed the internal configuration information of this iOS Trojan, as shown in Table 24. The FAID identifier (FOXACID) contains "ace02468bdf13579", which matches the unique identifier code of an exposed NSA operation. This identifier appears in the SecondDate weapon within the Equation Group arsenal leaked by the Shadow Brokers. Collectively, these findings indicate that this Trojan originates from the Equation Group, an organization under the U.S. intelligence agency NSA.

Table 2-4 Configuration Information and Content of the "Quantum Penetration" Trojan

Configuration Name	Content	Description
CI	3600	Heartbeat
CIAE	120	
cop1	80	C2 Port 1
cop2	443	C2 Port 2
CSF	/private/var/tmp/.swapfile.tmp	
FAID	***_ace02468bdf13579_***	
ID	*****00171	
lp1	**********[.]com	C2 Address 1
lp2	80[.]*[.]*[.]*	C2 Address 2
os1	www.google.com	Test network connectivity
os2	www.yahoo.com	Test network connectivity
os3	www.wikipedia.org	Test network connectivity
os4	www.apple.com	Test network connectivity
PV	12	
SDE	/usr/gated/gated.deb	

(II) Supporting Evidence: Cross-Verification with Snowden Leaks

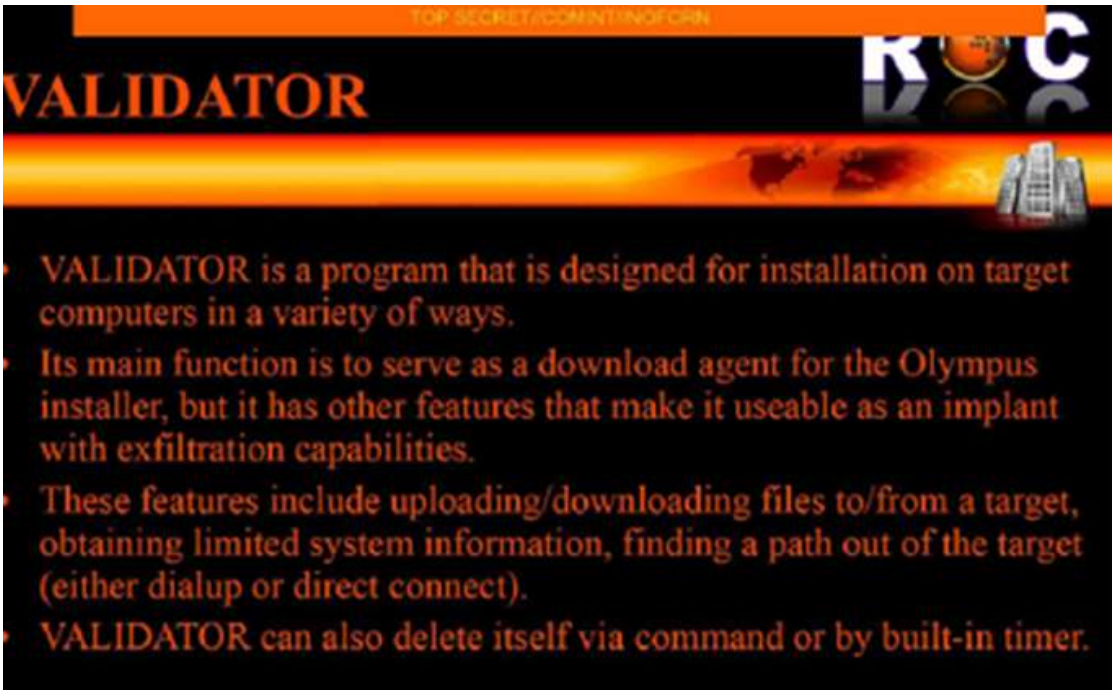

Figure 2-4 Relevant Validator Content in Snowden's Leaked Materials

Among the Snowden leaks, one document page describes the Validator. Related documentation indicates this Trojan acts as a probe to verify the identity and location of other Trojans. Once confirmed, it delivers either OLYMPUS or UNITEDRAKE (i.e., the Equation Trojan EquationDrug).

Based on functional analysis, Antiy determined that the iOS sample captured by Antiy is the Validator targeting mobile terminals developed by the Equation Group.

3 "Triangulation" — Kaspersky's Masterpiece Analysis of A^{2}PT Attacks

3.1 iMessage—A2PT's Persistent Attack Entry Points

Kaspersky's analysis of the exposed "Triangulation" attack utilizes iMessage as its entry point. iMessage is an "enhanced" messaging service developed by Apple, enabling internet-based communication between Apple devices and supporting large custom-format attachments. The combination of precise Apple account-based addressing and support for oversized attachments makes iMessage an ideal entry point for targeted format-based attacks against Apple devices.

While its end-to-end encryption appears as a "security" feature compared to traditional SMS, **when exploited by attackers, it also constitutes a bypass of operator-side security monitoring capabilities**. Another similar entry point is the FaceTime service.

Table 3-1 Differences Between iMessage Service and Operator SMS Service (AI Compilation)

Comparison Dimensions	iMessage	Standard SMS/MMS
Service Launch Year	2011 with iOS 5 release	Since 2002, promoted by operator services
Transmission Method	Transmitted via the internet (Wi-Fi or cellular data), relying on Apple servers	Transmitted via operator cellular networks, relying on cell towers and infrastructure
Sending/Receiving Addresses	Apple ID	Mobile phone number
Billing	Based on data usage (or Wi-Fi) Traffic charges	Billed based on operator SMS service
Compatibility	Apple devices only (iPhone, iPad, Mac, etc.), requires service activation on both devices	Compatible with all mobile devices (including Android and feature phones), no device restrictions
Encryption and Security	End-to-end encryption	Initially unencrypted; later partially encrypted using A5/1, A5/3, A5/4, etc.
Features	Text, high-resolution images, videos, files (up to 25MB), location, etc.	Text, images/videos (typically limited to 300KB–1MB)
Message Indicators	Blue bubble	Green bubble
Network Dependency	Requires internet connection (Wi-Fi or cellular data)	Requires operator cellular network signal, no internet connection needed
Other	May automatically downgrade to SMS delivery if sending fails	

3.2 "Triangulation" — Kaspersky Reveals Attack Chain Targeting iOS Systems

Kaspersky mapped the attack chain as shown in Figure 3-1. Attackers leverage Apple's iMessage service to send a specially crafted iMessage to the target device. As Apple's proprietary enhanced messaging protocol, iMessage supports sending highly rich composite-format content.

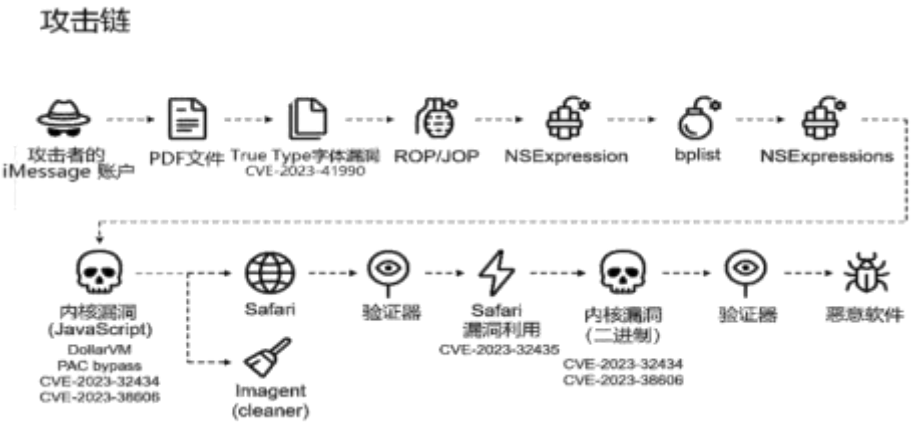

Figure 3-1 Schematic Diagram of the "Triangulation" Operation Attack Chain (Adapted from Kaspersky's Analysis Report)

The initial delivery mechanism for "Triangulation" Operation was a specially crafted PDF file containing a maliciously constructed TrueType font file. This exploited the CVE-2023-41990 vulnerability, This vulnerability enables remote code execution (RCE) during font parsing. When iOS "adjusts" (ADJUST) the TrueType font, it executes the maliciously crafted code. This serves as the attackers' entry point, though they do not yet gain full system privileges. Due to iOS's Harvard architecture design, where each application operates in an isolated memory space, attackers cannot directly access system resources or other process memory at this stage and have not achieved persistence. Subsequently, ROP/JOP (Return-Oriented Programming/Jump-Oriented Programming) techniques are employed. By leveraging the existing PAC pointer authentication mechanism (gradually introduced during iOS updates), attackers bypass controls and achieve control flow hijacking. NSExpression is used as the execution vehicle to call patch JavaScript kernel, deploying the "bplist" (binary task list). Ultimately, approximately 11,000 lines of highly obfuscated JavaScript code are deployed, achieving kernel-level patching and restructuring of JavaScriptCore to elevate privileges. The attacker utilizes the patched JavaScript engine to invoke the kernel debugging interface "$VM", enabling read/write access to engine memory and API calls. They then exploited the CVE-2023-32434 vulnerability's memory-mapped integer overflow, enabling user-mode programs to read and write the entire system's physical memory. Subsequently, they leveraged the CVE-2023-38606 vulnerability to manipulate hardware memory-mapped I/O (MMIO) registers, bypassing the page protection layer. After exploiting this vulnerability, they gained kernel-mode operation capabilities. The Imagent process is launched to clean up traces from earlier exploitation, initiate browser processes, and deploy a validator. This validator assesses whether the environment meets conditions for payload delivery. Upon validation, it repeatedly exploits CVE-2023-32434 and CVE-2023-38606 until successful payload delivery is achieved.

3.3 Analysis of "Triangulation" Sample Delivery and Control Command Information

The "Triangulation" sample tags are listed in Table 3-2.

Table 3-2 "Triangulation" Sample Tags

Virus Name	Trojan/MacOS.TriangleDb
MD5	063db86f015fe99fdd821b251f14446d
Processor Architecture	ARM64
File Size	677,168 bytes
File Format	BinExecute/Apple.MACHO[:x64 Little Endian]

VT First Upload Date	2023-06-21 11:15:33
VT Detection Results	33/60

Four zero-day vulnerabilities were exploited in the attack operation, including CVE-2023-41990, CVE-2023-32434, CVE-2023-38606, and CVE-2023-32435. Detailed information is provided in Table 3-3.

Table 3-3: 0day Vulnerability IDs and Information Used in "Triangulation"

Vulnerability ID	Vulnerability Details
CVE-2023-41990	Remote Code Execution Vulnerability in ADJUST TrueType Font Instructions
CVE-2023-32434	Integer Overflow Vulnerability in XNU Memory-Mapped System Calls
CVE-2023-38606	Bypassing Page Protection Layers Using Hardware Memory-Mapped I/O (MMIO) Registers
CVE-2023-32435	Memory Corruption in Web Content Handling May Lead to Arbitrary Code Execution

"Triangulation" control instruction information is shown in Table 3-4.

Table 3-4 "Triangulation" Control Instruction Information

Command ID	Function	Remarks
0xF901	Writes data to a file or adds a new module to the implant based on the iM parameter in CRXUpdateRecord.	Includes parameter fN File name (When iM=0, appends to the file corresponding to fN; when iM=1, adds to the implant)
0xF902	Adds a new module to the implant and activates it.	
0xF601	Retrieve the list of files in the specified directory via the FTS API.	
0xF801	Retrieve metadata for a given file (attributes, permissions, size, creation, modification, and access timestamps).	
0xF401	Delete an implant module or a file with the specified name based on command parameters.	
0xF402	Retrieves a list of running processes.	
0xF501	Retrieve the contents of the specified file.	
0xFB03	Retrieves keychain entries from the infected device. It begins monitoring the screen lock status and, upon device unlock, dumps keychain items from the /private/var/Keychains/keychains/2.db database within the genp (General Passwords), inet (Internet Passwords), and the keys and certificates tables (certificates, keys, and digital identities). Note that the implant's code can operate with different Keychain versions, starting from the version used in iOS 4.	
0xFB44	Terminates the process with the specified PID using SIGKILL or SIGSTOP, depending on the command's parameters.	

0xFA01	Delete an implant module or remove a file with the specified name, based on the command's parameters.	
0xFA02	Launches a module with the specified name by reflexively loading its Mach-O executable.	
0xFC11	Stop executing the CRXPollRecords command.	
0xFD01	Retrieve information about installed iOS applications.	
0xFC10	Begin monitoring directories for files whose names match the specified regular expression.	
0xFC01	Retrieve files matching the specified regular expression.	

3.4 Antiy's Reproduction, Verification, and Attribution of "Triangulation"

Based on attack samples released by Kaspersky and referencing Kaspersky's analysis reports[2][3][4][5][6][7], Antiy CERT simulated C2 communication and command issuance operations by setting up an environment to trigger and reconstruct communication processes. This included building a dynamic debugging environment to reproduce audio theft and compression techniques achieving minimal recording data sizes. Attribution analysis was also conducted.

(1) Communication Reproduction

The reproduced "Triangulation" payload and C2 communication traffic data, including functionality such as heartbeat packets and information gathering, are detailed below:

Heartbeat packet data contains system architecture and system-specific folder information, as shown in Figures 3-2 and 3-3.

Figure 3-2: Triangulation Payload and C2 Communication Heartbeat Packet (After TLS Decryption)

Figure 3-3: Heartbeat Packet Plaintext Containing System Information

appinfo (Command ID: 0xFD01) is a typical information retrieval command. Its return data includes application name, executable file path, version, etc., as shown in Figures 3-4 and 3-5.

Figure 3-4: Command appinfo Traffic (After TLS Decryption)

Figure 3-5: Plaintext Content of appinfo

(II) Reproduction of Audio Eavesdropping Functionality through Dynamic Analysis and Debugging of the Attack Sample

1. Setting Up the Dynamic Debugging Environment

恶意代码基本信息：

架构：x86_64 arm64 arm64e

工具：

硬件：越狱 ipad 或 iphone（开启 ssh 通道）、mac 虚拟机

软件：ldid、ios_deploy、IDA、mac_server*、debugserver

流程：

1、用 ldid 修改恶意代码和 debugserver 权限

权限内容：

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
Property<plist version="1.0">
<dict>
 <key>task_for_pid-allow</key> <true/>
 <key>get-task-allow</key> <true/>
 <key>platform-application</key> <true/>
 <key>com.apple.springboard.debugapplications</key> <true/>
 <key>run-unsigned-code</key> <true/>
 <key>com.apple.system-task-ports</key> <true/>
</dict>
</plist>
```

将以上内容保存为 123.plist

执行：

Ldid -S123.plist debugserver/恶意代码

2、把恶意代码和 debugserver 传入越狱设备以进行调试：

首先使用 ios_deploy 利用 usb 连接转接出 ssh 端口：

```
Ios_deploy usbproxy -r 22 -l 2222
```

之后用 scp 将软件传入：

```
Scp -P 2222 debugserver root@localhost:
Scp -P 2222 恶意代码名称 root@localhost:
注意：不要忘记最后的:，另外默认密码 alpine
```

Ssh 连接设备启动 debugserver:

```
Ssh -p 2222 root@localhost
Iphone:/debugserver 127.0.0.1:1234
注意：debugserver 无法开启 0.0.0.0，只能使用 127.1 这个地址
```

Figure 3-6: Dynamic Debugging Environment Setup Log

2. Fixing and Executing the Sample, Setting Up a Server to Simulate C2 for Remote Interaction

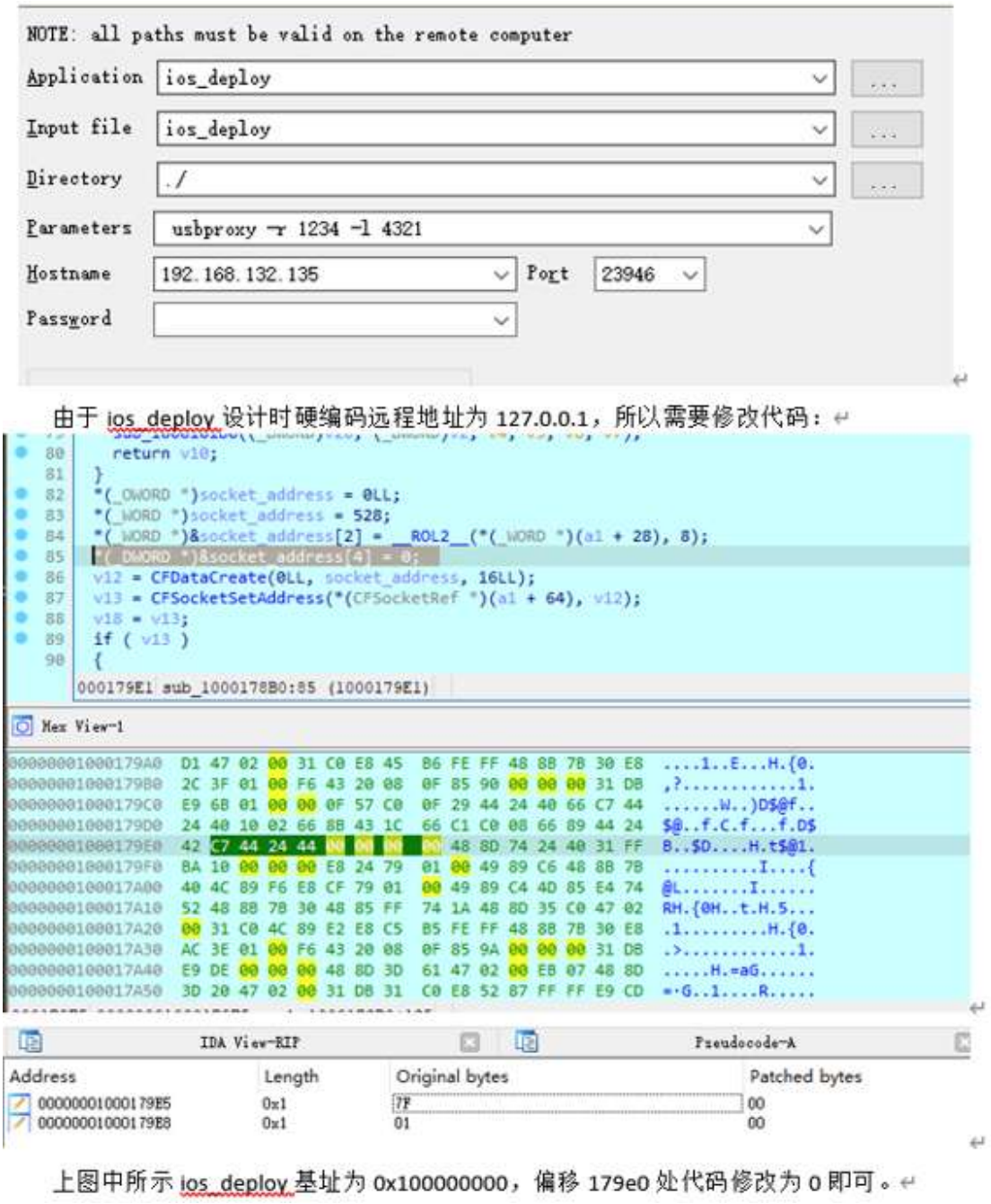

Figure 3-7 Dynamic Execution Process

3. Reproduce Audio Theft Functionality, Analyze and Confirm Audio Compression and Acceleration Enable Minimal-Data Recording

Figure 3-8 shows the waveform spectrum of a normal audio recording. Figure 3-9 displays the spectrum of the recording reproduced via triangulation. Although the normal audio sample has a higher sampling rate and bit depth than the triangulation recording, within the same timeframe (1 second), the triangulation recording contains more data volume, with waveform changes appearing denser than those in the normal audio recording.

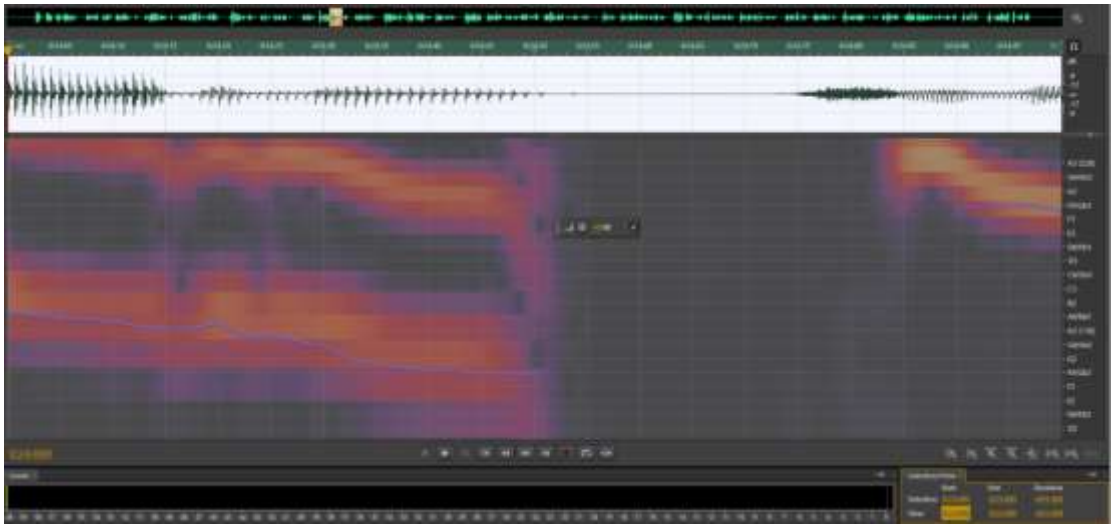

Figure 3-8: One Second of Normal Audio, 48000Hz, 24-Bit Waveform

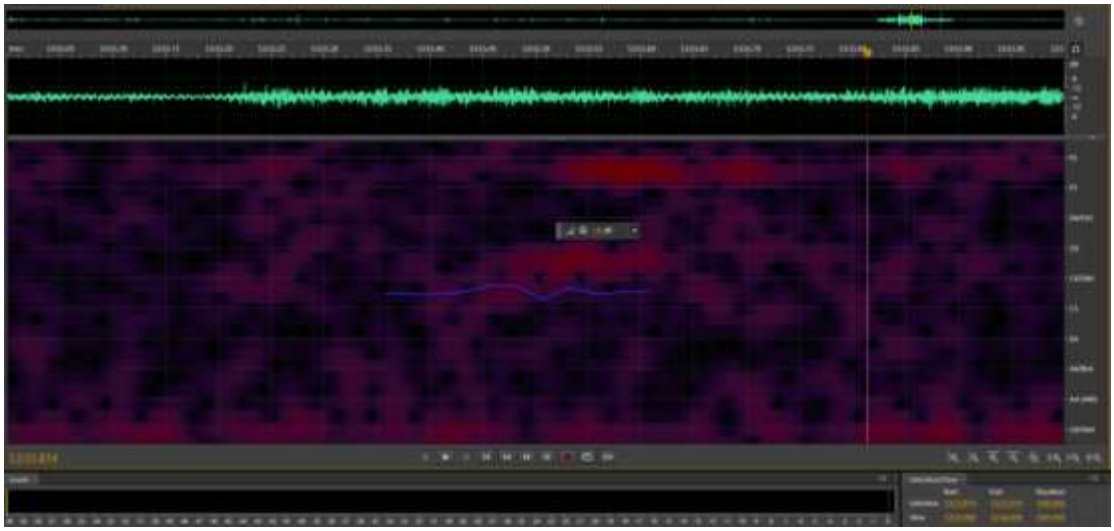

Figure 3-9: One Second of Triangulation-Processed Recording, 44100Hz, 16-Bit Waveform

(3) Group Attribution Analysis of "Triangulation" Based on Sample, Traffic, and C2 Dimensions

Following complete reproduction, organizational attribution analysis of the "Triangulation" technique was conducted across sample, traffic, and C2 dimensions.

1. Static Analysis and Functional Inference

During the initial infection stage, victims received a click-free, vulnerable iMessage attachment. This vulnerability did not directly implant the final TriangleDB but instead underwent verification by two validators: a JavaScript validator and a binary validator.

2. Dynamic Analysis and Behavioral Validation

➢ Dynamically debug TriangleDB to obtain trojan commands

➢ Man-in-the-middle hijacking to decrypt JavaScript validators

3. Organizational Association and Attribution

➢ Delivery model: Zero-click attacks that do not rely on emails or other interactive methods, leaving targets completely unaware throughout the attack.

➢ C2 similarity: Uses random word combinations in domain names like "Equation", with traffic employing strict strong encryption mode.

➢ Operation pattern similarity: Modularized functional operations

4 Extended Analysis

4.1 Validator-Based Paradigm Operations

The "Triangulation" operation employs tactics similar to the Equation Group operations, beginning with the implantation of a "validator". Based on the validator's reconnaissance findings, it determines whether to deploy further payloads.

The key functional modules of "Triangulation"—such as the location information theft, microphone eavesdropping, SQL database theft, and Apple Keychain theft discovered in this case—are all independently designed modules deployed via remote delivery, as shown in Figure 4-1. This aligns with the design philosophy of the Equation Group's UNITEDRAKE and DanderSpritz attack platforms.

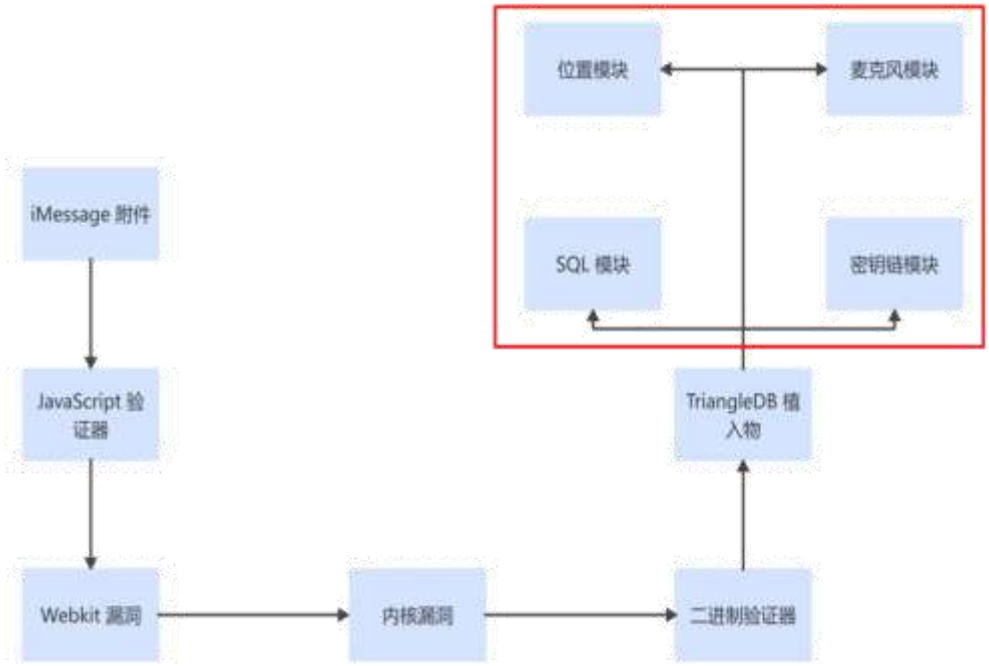

Figure 4-1: Triangulation Operation Authentication Model and Analysis of Independent Stealth Modules

4.2 Integration of "Quantum Penetration" and "Triangulation" Operation Models

Though these two operation modes have distinct entry points, they share potential integration points, as illustrated in Figure 4-2. One approach leverages quantum delivery to pre-embed vulnerabilities within the Triangulation attack chain, making browsers susceptible to compromise. Another treats the Triangulation attack chain as a precursor, where browser attacks may not require direct local downloads of the trojan but can instead trigger in-flight hijacking delivery during the process.

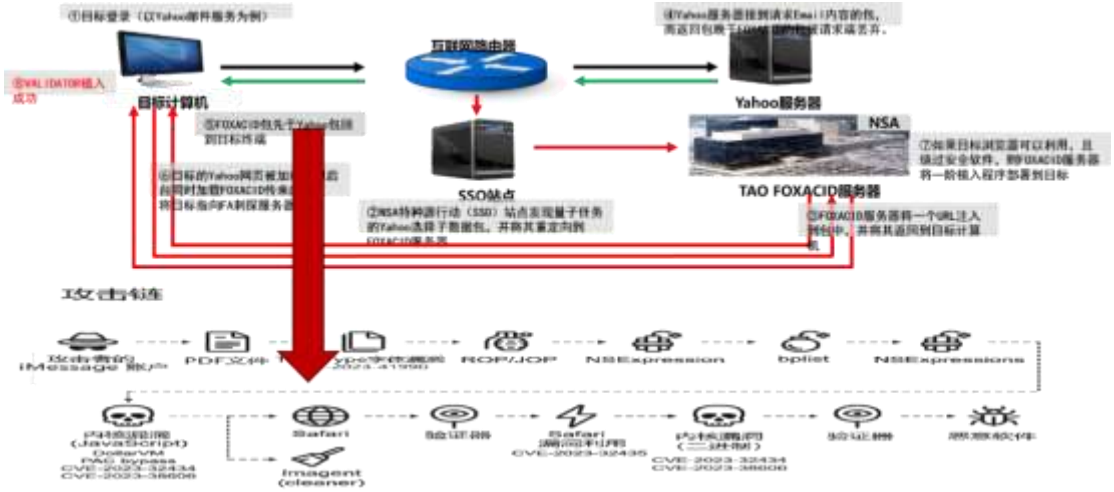

Figure 4-2 Analysis of Integration Points Between Two Operation Models

4.3 A2PT Group's Malicious Code Weapon Production Model

The complex, persistent, and highly effective cyberattack capabilities demonstrated by the A2PT group are underpinned by a highly engineered, specialized malicious code weapon production system. This system has evolved from early technical team innovations into a mature model dominated by national intelligence agencies, leveraging the defense industrial base for large-scale integration and production.

(1) R&D: A Systematic and Engineering-Oriented Self-Developed System

Samples captured and analyzed during Quantum Penetration and Triangulation operations align with the stylistic characteristics of A2PT's self-developed samples. Early A2PT operations, combined with technical source code leaks resulting from intelligence window effects, reveal that for an extended period, malicious code weapon development was primarily undertaken through R&D by organizations like the NSA or entrusted to a small number of closely affiliated, top-security-cleared core contractors. This deeply integrated model ensured attack tools remained under strict control at their most critical stages. For an extended period, the development of malicious code arsenals was primarily undertaken in-house by agencies like the NSA or entrusted to a small number of closely affiliated, top-security-cleared core contractors. This deeply integrated model ensured the controllability of attack tools in the most critical and sensitive cyber operations, as well as the manageability of technological advancements.

Their operation samples correspond to massive-scale software engineering systems. These platforms (e.g., Flamer, Tilded) exhibit high modularity and "rolling iteration" update capabilities.

(2) External Procurement: Integration and Application of Commercial Tools

Based on the FBI's previously exposed procurement of the Israeli NSO Group's "Pegasus" spyware and the Italian Hacking Team's "Galileo" remote control system, it is evident that commercial procurement and integration into proprietary attack platforms constitute another significant source. Due to insufficient in-house development capabilities, commercial weapons may be the primary source of capability for U.S. law enforcement agencies to conduct offensive forensics and covert surveillance. Simultaneously, intelligence agencies may also utilize commercial payloads.

Specific methods include:

➢ Direct procurement of mature tools: There is documented history of directly purchasing mature spyware from commercial surveillance companies for operational use. For instance, the FBI was exposed for acquiring Israel's NSO Group's "Pegasus" spyware and Italy's Hacking Team's "Galileo" remote control system.

➢ Integration and deployment of tools: Purchased commercial tools are not used in isolation but typically serve as payloads delivered via proprietary attack platforms (e.g., the "Quantum" system). After penetrating targets through initial attacks, these tools are implanted to achieve persistent residency and deep intelligence gathering, thereby establishing a complete "penetrate-delivery-control" kill chain.

(3) Moving Toward Industrialization: The Military-Industrial-Information Complex May Emerge as a New Developer/Integrator

As cyberattack capabilities gain independent budgetary status separate from intelligence infrastructure development, the U.S. revolving door mechanism suggests an inevitable outcome: the production of cyberattack weapons will synchronize with the military-industrial complex's transformation into a military-cyber-industrial complex. Defense giants like Boeing, Lockheed Martin (LMT), and Raytheon will replace existing small-to-medium intelligence contractors and commercial malware firms as core Tier-1 suppliers. This shift enables superior integration capabilities.

For instance, U.S. defense contractors attempted to acquire NSO Group with tacit approval from intelligence agencies, revealing a strategic move by defense giants to directly incorporate top-tier commercial attack capabilities into their supply chains.

(IV) Resource Reuse: Repurposing Third-Party Malicious Code

Based on disclosures from the CamberDaDa project, the NSA began early on to acquire third-party samples for infection opportunity hijacking and reuse. This approach offers lower costs while inherently carrying false flag effects.

4.4 Vulnerability Resource Analysis of A²PT

(1) Analysis of Vulnerability Distribution Priorities

Antiy CERT has repeatedly assessed that the U.S. prioritizes vulnerability stockpiling in two directions: first, vulnerabilities in browser-like client software targeting mobile terminals, internet-connected devices, and internal network hosts. Since such targets either lack fixed public IP addresses with open port services or remain unexposed

to the internet, A²PT attacks require leveraging such software communications as entry points. The second category targets vulnerabilities in services (static ports) exposed by operating systems and application platforms, targeting servers and terminals with public IP addresses and exploiting their exposed public IP ports as entry points.

Table 4-1 Comparison of Vulnerability Sets: A²PT Groups Targeting Browsers vs. Open Port Services

	Browser	Open Services (Ports)
Targets	Mobile terminals, internet terminals, internal network hosts,	Public IP servers, terminals
Attack Methods	Traffic hijacking injection (Quantum System), SMS links, iMessage, and other methods to send	Establishing connections via jump servers and proxy forwarding tools to transmit attack traffic
Primary Vulnerability Mechanisms	Buffer overflow, logical flaws, component/plugin vulnerabilities, sandbox escape	Buffer overflows, privilege escalation, bypassing protection mechanisms (DEP, ASLR, etc.)
Primary Targeted Software and Services	Internet Explorer, Chrome, Firefox, Safari, etc.	HTTP (80), NetBIOS (139), IMAP (143), SMB (445), RDP (3389), etc.

(2) Speculation on Vulnerability Databases Targeting Browsers and Internet Clients

For the vulnerability repository targeting browsers and internet clients, we refer to it as the vulnerability collection (C), standing for Client. These vulnerabilities are configured for use in "Quantum" or similar systems, with limited direct access for users. The attack scenario mapping analysis for the Quantum system is shown in Figure 4-3.

Figure 4-3: Graphical Analysis of Quantum System Attack Scenarios

(III) Analysis of Vulnerability Repositories Targeting Open Ports and Services (Shadow Brokers Exposure Leak)

The vulnerability repository targeting open ports and services (exposed by the Shadow Brokers leak) is referred to as the vulnerability collection (S), standing for Service. These vulnerabilities are integrated into the locally deployable FuzzBunch vulnerability exploitation platform for use, with broader internal propagation. The NSA's leaked vulnerability map targeting open ports and services[10] is shown in Figure 4-4.

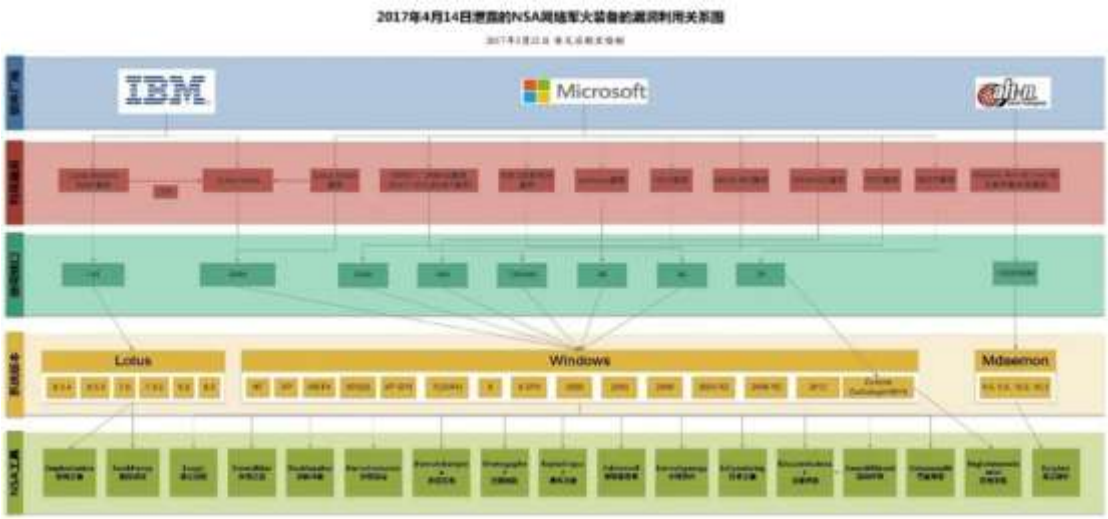

Figure 4-4 NSA Exploit Map Targeting Vulnerabilities in Open Ports and Services

4.5 A²PT Group's Weapons, Vulnerability Resources, and System

The U.S. intelligence agencies globally collect and procure zero-day vulnerabilities through public security activities, agent models, vulnerability bounty collaborations, and procurement from cyber arms dealers. By establishing cyber programs, weapons, infrastructure, and big data support with cyber defense contractors, telecommunications infrastructure companies, and internet firms, they leverage globally deployed project and operation platforms. Utilizing implant, carrier, and relay equipment, they deploy various advanced malicious codes through vulnerabilities. launching extensive attack operations against global IT targets. The organizational operations and operation relationship diagram is shown in Figure 4-5.

Figure 4-5: The Equation Group Resource Operations and Operation Relationship Diagram

5 Further Reading

Chapter 4 of this report introduces the report released by the China Cybersecurity Industry Alliance released on March 25, 2025:《Mobile Cyberattacks Conducted by US Intelligence Agencies》[8].

Figure 5-1 Cover of "Mobile Cyberattacks Conducted by US Intelligence Agencies"

6 Conclusion: Our Struggle

The 2022 U.S. Congressional hearing report specifically named two Chinese cybersecurity enterprises, including Antiy, for analyzing NSA and CIA "cyberspace operations" (i.e., cyber intrusions and attacks). This marked the first time Chinese cybersecurity entities were explicitly identified in the context of defense and analysis. However, the corresponding report refuses to acknowledge our direct capture of the U.S. attack methods, instead attributing our analytical findings to leaks from the "Shadow Brokers". In-depth analysis of open-source intelligence and technical resources is standard practice for security enterprises. Naturally, we closely monitored and comprehensively analyzed the U.S. samples leaked by the Shadow Brokers. However, chronologically, both Antiy's first report on the Equation Group, "Hard Drive Firmware-Modifying Malware: Investigation of the Equation Group's Attack Components" [11], and its second report, "Analysis of Encryption Techniques in Selected Components of the Equation Group" [12], predate the Shadow Brokers leak incident. At this hearing, the U.S. explicitly proposed going beyond "naming and

shaming" to include Chinese enterprises with established "threat" capabilities on its sanctions list, openly targeting Chinese security enterprises possessing defensive and analytical capabilities.

In February 2024, a Sentinel Labs report singled out three Chinese enterprises including Antiy and the China Cybersecurity Industry Alliance, distorting their analysis of U.S. attack activities and samples. It claimed Chinese security enterprises lack independent discovery capabilities, relying instead on following international vendors' research findings and intelligence leaks from U.S. agencies. Subsequently, Antiy released a report titled "Fight Against the Bald Eagle in the Fog"[13], responding to these claims and compiling the global security community's analysis findings on the A^{2}PT attack samples. Chinese security enterprises played a crucial role in exposing the A^{2}PT attack.

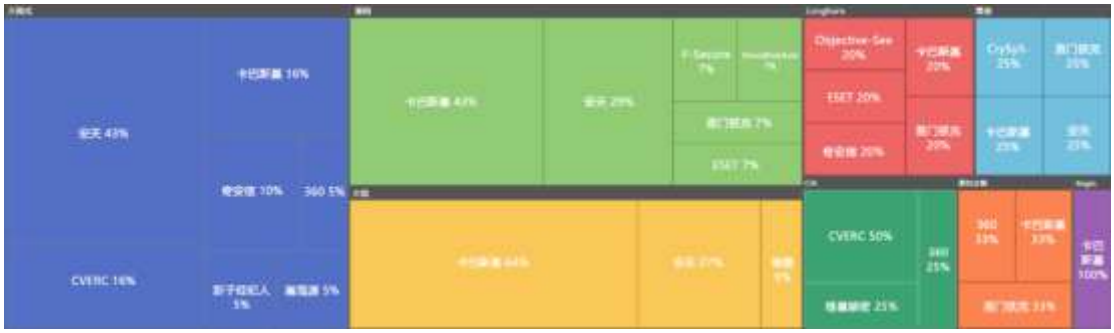

Figure 6-1: Composition of Disclosed U.S. Cyber Weapons and Disclosure Shares by Security Vendors

When the inflictor ridicules the victim's incapacity as an original sin, what we see is the arrogance that colonizers and aggressors have been accustomed to for 200 years, treating colonization, invasion, and the victim's lack of sufficient resistance as an original sin.

Based on God mode, relying on their huge intelligence engineering system, large-scale organized attack teams, and attack weapons covering all platforms and scenarios, the A^{2}PT attackers who operate on a mix of manpower, electromagnetic and cyberspace think they can be invisible and stride away after causing harm, and then ridicule the attacked party, just like what they did in the past 200 years.

The perpetrator is not noble due to the cleverness of the perpetration, and the resister is not humble due to the difficulty of resistance.

Excerpt from "Fight Against the Bald Eagle in the Fog"[13] Conclusion

We feel no inferiority or unease over our temporary weakness, nor do we waver or panic in the face of temporary difficulties—for we stand on the side of history's progress and justice!

7 References

[1]. The Quantum System Penetrates Apple Phones——Analysis of Historical Samples of the Equation Group Attacks on iOS Systems [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]. Mobile Cyberattacks Conducted by US Intelligence Agencies [R/OL]. (2025-03-25)

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

[9].A Nine-Year Retrospective and Reflections on the Stuxnet Incident [R/OL]. (2019-09-30)

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

[10]. Antiy's Operation Manual for Systematically Countering NSA Cyber Weapons [R/OL]. (2017-05-22)

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

[11].Hard Drive Firmware-Modifying Malware: Investigation of the Equation Group's Attack Components [R/OL]. (2015-03-05)

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

[12].Analysis of Encryption Techniques in Selected Components of the Equation Group [R/OL]. (2015-04-19)

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

[13].Fight Against the Bald Eagle in the Fog[R/OL] .(2024-03-21)

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