Mobile Cyberattacks Conducted by US Intelligence Agencies

China Cybersecurity Industry Alliance(CCIA)

March 2025

Contents

Introduction

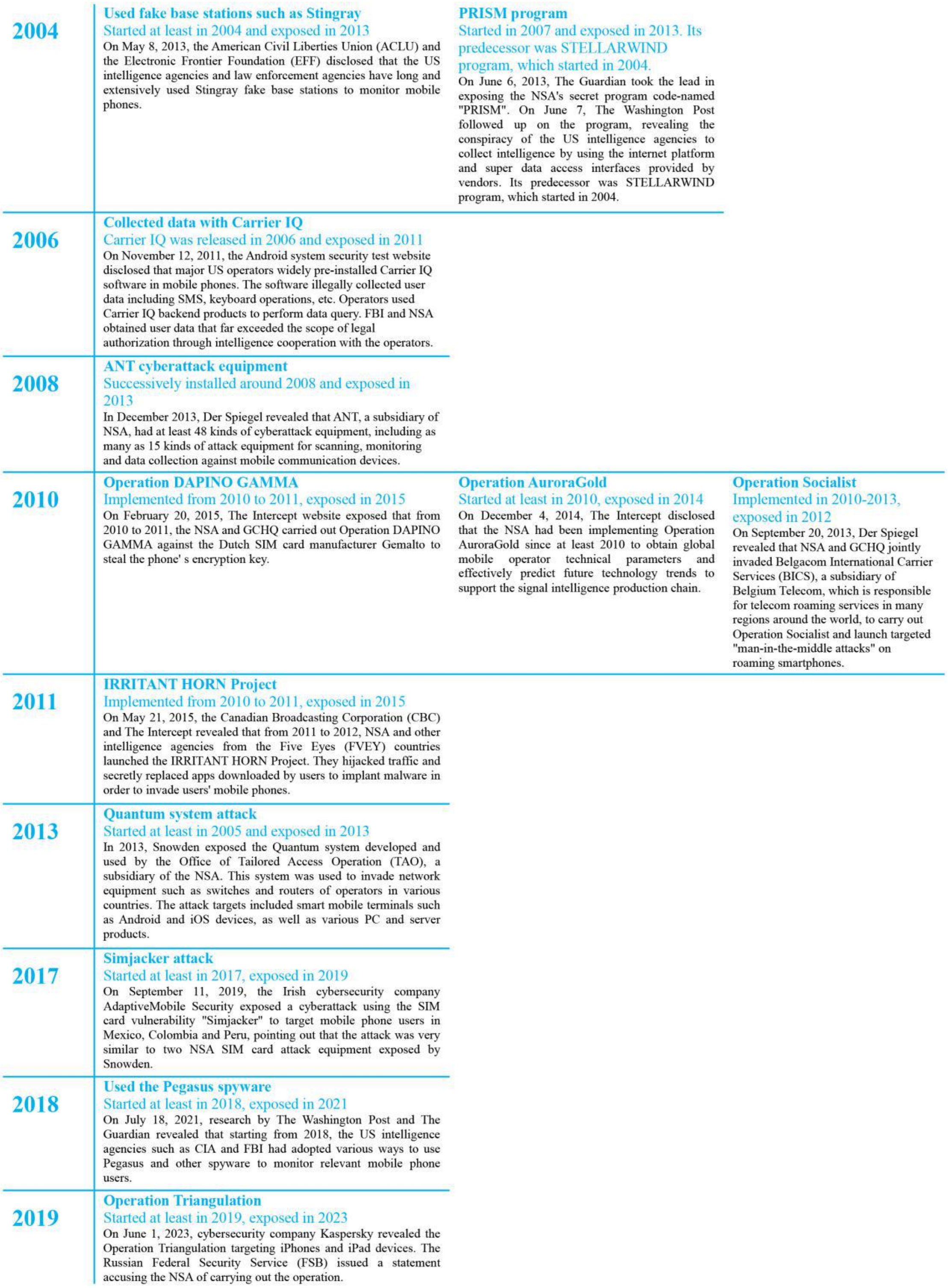
The number of global mobile smart terminal users is huge. The *2023 Facts and Figures* report released by the International Telecommunications Union (ITU) in November 2023 shows that the mobile phone ownership rate among the global population aged 10 and above is 78%, and the coverage of mobile broadband with 3G and above in the total global population is 95%. Smartphones are no longer limited to the traditional communication function of operators, but become the basic entrance for daily shopping, entertainment, social interaction, study and life services. They are also nodes for mobile offices and even identity tokens for accessing various government and enterprise intranets.

But at the same time, mobile smart terminals such as mobile phones also lurk huge cybersecurity risks. Compared with traditional PCs, they have wider sensing capabilities and are equipped with high-precision sensors, as well as signal collection devices such as cameras and microphones. Through the collection and analysis of data assets on the device, it is possible to conduct targeted, accurate portrait analysis of the targeted personnel's work and life trajectory, behavioral habits, psychological characteristics, social relationships and surrounding environment, and even control the mobile phone through vulnerability exploitation and malware delivery, so as to realize all-round wiretapping and surveillance. A compromised mobile phone is like a walking bug or monitor. No secrets can be kept wherever it goes, and everything is transparent to the attacker's "God's perspective". For smart terminal devices such as mobile phones that have been introduced into mobile office environments, once compromised, higher-value data assets related to the target may be leaked. What's worse, they may become a breakthrough and springboard for attackers to invade the intranets of government and enterprise institutions.

Mobile smart terminals such as mobile phones have been coveted by the US intelligence agencies since their appearance because of the huge value of data resources they contain. Over the past two decades, a major challenge faced by global critical information infrastructure operators, security vendors and researchers has been how to discover, analyze, and respond to cyberattacks launched by the US intelligence agencies such as the National Security Agency (NSA) and the

Central Intelligence Agency (CIA).

Compared with traditional PCs, mobile smart terminals such as mobile phones have more cybersecurity exposure and attack surfaces, including the terminal device level involving hardware, firmware, systems and applications, the information interaction level involving data interfaces, Wi-Fi, Bluetooth, cellular network, geographical positioning services such as GPS, etc.. At the same time, the security of the mobile phone system is related to the complex software and hardware supply chain system, the industrial ecology of APPs, the signal transmission of operators and the data storage and aggregation of large internet platform vendors. These are the links coveted by the US intelligence agencies and the key targets to attack. This report gathers together a large number of disclosures and analyses from the industry and academia on the network intelligence activities carried out by the US intelligence agencies against mobile smart terminals (see the figure below). It is classified and integrated from the aspects of terminal equipment, communication infrastructure, operators and internet vendors, in order to form an overall understanding of the cyberattack activities and information acquisition behaviors of the United States against mobile terminals, mobile industry chains and supply chains, operators and large internet vendors, so as to establish systematic prevention capabilities, effectively cover the mobile industry chain and application ecology, critical information infrastructure, and government and enterprise network scenarios.



2004

Used fake base stations such as Stingray

Started at least in 2004 and exposed in 2013

On May 8, 2013, the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF) disclosed that the US intelligence agencies and law enforcement agencies have long and extensively used Stingray fake base stations to monitor mobile phones.

PRISM program

Started in 2007 and exposed in 2013. Its predecessor was STELLARWIND program, which started in 2004.

On June 6, 2013, The Guardian took the lead in exposing the NSA's secret program code-named "PRISM". On June 7, The Washington Post followed up on the program, revealing the conspiracy of the US intelligence agencies to collect intelligence by using the internet platform and super data access interfaces provided by vendors. Its predecessor was STELLARWIND program, which started in 2004.

2006

Collected data with Carrier IQ

Carrier IQ was released in 2006 and exposed in 2011

On November 12, 2011, the Android system security test website disclosed that major US operators widely pre-installed Carrier IQ software in mobile phones. The software illegally collected user data including SMS, keyboard operations, etc. Operators used Carrier IQ backend products to perform data query. FBI and NSA obtained user data that far exceeded the scope of legal authorization through intelligence cooperation with the operators.

2008

ANT cyberattack equipment

Successively installed around 2008 and exposed in 2013

In December 2013, Der Spiegel revealed that ANT, a subsidiary of NSA, had at least 48 kinds of cyberattack equipment, including as many as 15 kinds of attack equipment for scanning, monitoring and data collection against mobile communication devices.

2010

Operation DAPINO GAMMA

Implemented from 2010 to 2011, exposed in 2015

On February 20, 2015, The Intercept website exposed that from 2010 to 2011, the NSA and GCHQ carried out Operation DAPINO GAMMA against the Dutch SIM card manufacturer Gemalto to steal the phone' s encryption key.

Operation AuroraGold

Started at least in 2010, exposed in 2014

On December 4, 2014, The Intercept disclosed that the NSA had been implementing Operation AuroraGold since at least 2010 to obtain global mobile operator technical parameters and effectively predict future technology trends to support the signal intelligence production chain.

Operation Socialist

Implemented in 2010-2013, exposed in 2012

On September 20, 2013, Der Spiegel revealed that NSA and GCHQ jointly invaded Belgacom International Carrier Services (BICS), a subsidiary of Belgium Telecom, which is responsible for telecom roaming services in many regions around the world, to carry out Operation Socialist and launch targeted "man-in-the-middle attacks" on roaming smartphones.

2011

IRRITANT HORN Project

Implemented from 2010 to 2011, exposed in 2015

On May 21, 2015, the Canadian Broadcasting Corporation (CBC) and The Intercept revealed that from 2011 to 2012, NSA and other intelligence agencies from the Five Eyes (FVEY) countries launched the IRRITANT HORN Project. They hijacked traffic and secretly replaced apps downloaded by users to implant malware in order to invade users' mobile phones.

2013

Quantum system attack

Started at least in 2005 and exposed in 2013

In 2013, Snowden exposed the Quantum system developed and used by the Office of Tailored Access Operation (TAO), a subsidiary of the NSA. This system was used to invade network equipment such as switches and routers of operators in various countries. The attack targets included smart mobile terminals such as Android and iOS devices, as well as various PC and server products.

2017

Simjacker attack

Started at least in 2017, exposed in 2019

On September 11, 2019, the Irish cybersecurity company AdaptiveMobile Security exposed a cyberattack using the SIM card vulnerability "Simjacker" to target mobile phone users in Mexico, Colombia and Peru, pointing out that the attack was very similar to two NSA SIM card attack equipment exposed by Snowden.

2018

Used the Pegasus spyware

Started at least in 2018, exposed in 2021

On July 18, 2021, research by The Washington Post and The Guardian revealed that starting from 2018, the US intelligence agencies such as CIA and FBI had adopted various ways to use Pegasus and other spyware to monitor relevant mobile phone users.

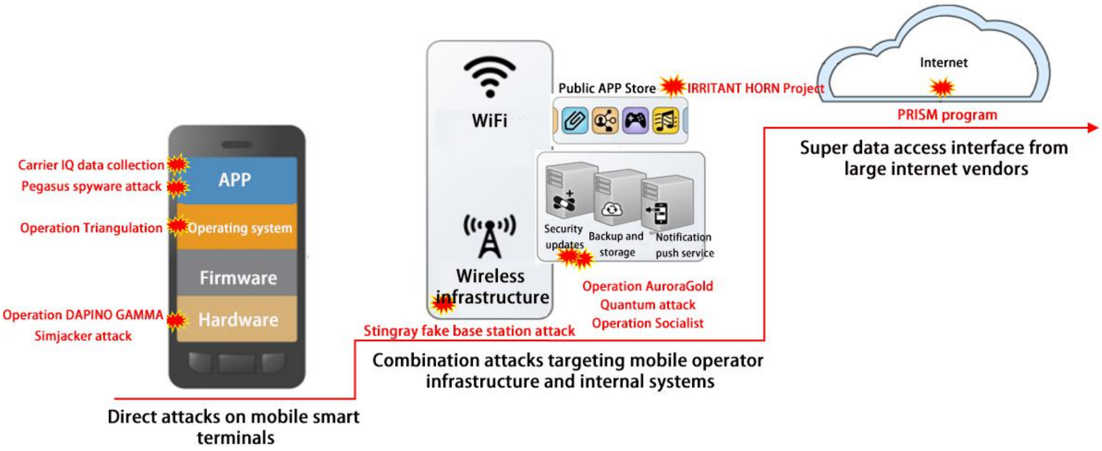
2019

Operation Triangulation

Started at least in 2019, exposed in 2023

On June 1, 2023, cybersecurity company Kaspersky revealed the Operation Triangulation targeting iPhones and iPad devices. The Russian Federal Security Service (FSB) issued a statement accusing the NSA of carrying out the operation.

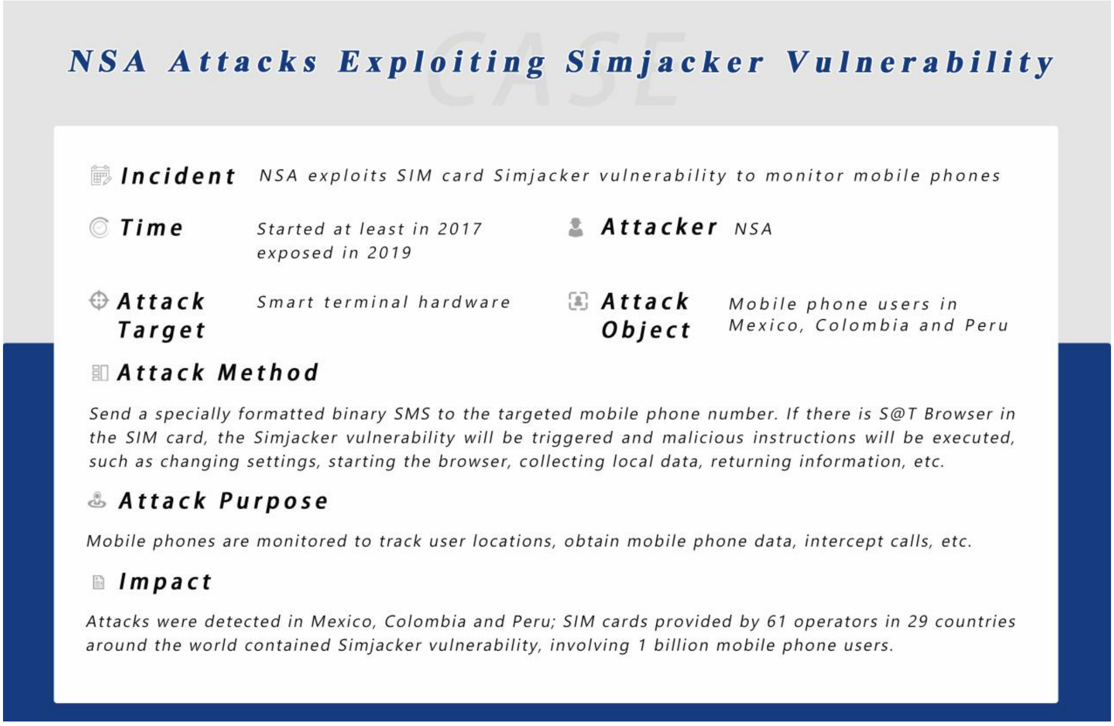
Chapter 1 to 5 focus on attacks by the US on the hardware, firmware, systems and applications of mobile smart terminals. Chapter 6 to 10 focus on attacks by the US on operator infrastructure and internal systems, with the latter two chapters focusing on combination attacks on operators and smart termi+nals. Chapter 11 re-analyzes the PRISM program, exposing the intelligence activities of the US intelligence agencies to obtain mobile smart terminal data through the super data access interface of internet vendors and perform big data analysis (see the figure below).



The analysis and research results disclosed by all walks of life around the world have jointly revealed that the US wiretapping and secret theft operations against mobile smart terminals around the world are pervasive, unscrupulous and intensified.

Chapter 1. Taking Over the Mobile Phone via SMS - Highly Sophisticated Attacks Targeting SIM Card Vulnerabilities

The SIM card is the user identification module of the mobile communication system and is used to register user identification data and information. An obvious feature of attacks exploiting SIM card vulnerabilities is that the attacks are not restricted by hardware type. Theoretically, all brands and models of mobile phones, and even IoT devices and wearable devices with SIM cards, regardless of the operating system installed, can be exploited as long as there is a vulnerability in the inserted SIM card. In September 2019, an Irish cybersecurity company exposed an attack exploiting the SIM card vulnerability Simjacker to target mobile phone users in Mexico, Colombia and Peru. It pointed out that the attack is very similar to two NSA SIM card attack equipment MONKEYCALENDAR and GOPHERSET exposed by Snowden.



NSA Attacks Exploiting Simjacker Vulnerability

Incident NSA exploits SIM card Simjacker vulnerability to monitor mobile phones

Time Started at least in 2017
exposed in 2019

Attacker NSA

Attack Target Smart terminal hardware

Attack Object Mobile phone users in Mexico, Colombia and Peru

Attack Method

Send a specially formatted binary SMS to the targeted mobile phone number. If there is S@T Browser in the SIM card, the Simjacker vulnerability will be triggered and malicious instructions will be executed, such as changing settings, starting the browser, collecting local data, returning information, etc.

Attack Purpose

Mobile phones are monitored to track user locations, obtain mobile phone data, intercept calls, etc.

Impact

Attacks were detected in Mexico, Colombia and Peru; SIM cards provided by 61 operators in 29 countries around the world contained Simjacker vulnerability, involving 1 billion mobile phone users.

Fig. 1-1 List of Cases of NSA Attacks Exploiting Simjacker Vulnerability

Incident Review

On September 11, 2019, AdaptiveMobile Security, a cybersecurity company headquartered in Dublin, Ireland, exposed an attack targeting the Simjacker vulnerability in the S@T browser of SIM cards[1]. This attack activity sends specially formatted binary SMS messages to mobile phones. If there is S@T browser in the SIM card, it will trigger Simjacker vulnerability and executes malicious instructions to achieve malicious purposes including locating and stealing secrets.

The Simjacker vulnerability attack is only related to the functional components embedded in the SIM card. In theory, all brands and models of mobile phones inserted with a SIM card containing this vulnerability may be attacked, even IoT devices and wearable devices with SIM cards. Although AdaptiveMobile Security only detected attacks in Mexico, Colombia and Peru, SIM cards provided by telecom operators in 29 countries around the world at that time contained the vulnerability, involving 1 billion users.

AdaptiveMobile Security pointed out that on the one hand, the Simjacker attack was very similar to 4 exposed attacks that exploit SIM card vulnerabilities, including two NSA SIM card attack equipment exposed by Snowden; on the other hand, the perpetrator had a very broad range of skills, experience and resources, had access to SS7 (Signaling System 7) networks, and had specific interest in mobile users in countries such as Mexico. It is believed that NSA is one of the few attack entities in the world with the above capabilities and characteristics.

Attack Method

The *Simjacker Technical Paper*[2] released in October 2019 pointed out that the Simjacker attack exploited the security configuration error of the S@T Browser in the SIM card issued by some operators of not verifying the validity of the received message to perform attacks such as remotely locating the target.

S@T Browser (SIMalliance Toolbox Browser) is SIM card built-in software. Its original purpose is to enable services such as obtaining user account balances through SIM cards, so it is not widely known. As of 2019, the S@T Browser technology has not been updated for 10 years, but at that time, the browser was a legacy technology and was defaulted as a built-in component of many brands of SIM cards.

AdaptiveMobile Security analyzed Simjacker's attack steps:

Step 1: The attacker uses an ordinary mobile phone, GSM modem or A2P SMS service to send SMS-PP (point-to-point) type text messages to the attack target. The targeted application is S@T Browser in the SIM card.

Step 2: After the attack target receives the SMS-PP type message, the logic on the mobile phone is triggered, and the S@T Browser becomes the execution environment on the SIM card. The SIM card takes over the mobile phone to receive and execute sensitive instructions.

Step 3: Once the attack code retrieves information such as location and specific device information (International Mobile Equipment Identity, IMEI) from the phone, it collates the information and triggers the logic on the phone again to send the combined information to the receiver via a "Data Message".

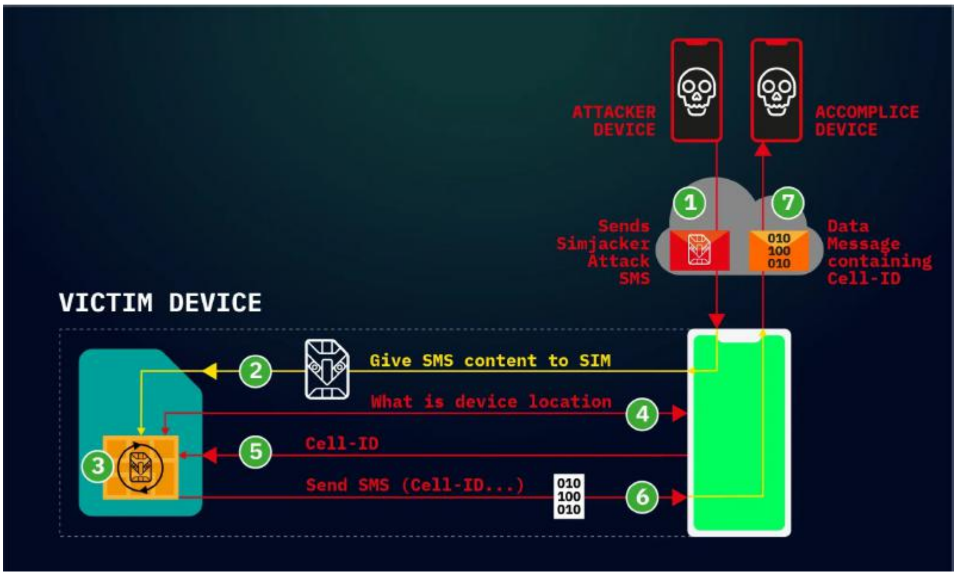


Fig. 1-2 The Technical Process of Simjacker Vulnerability Attack

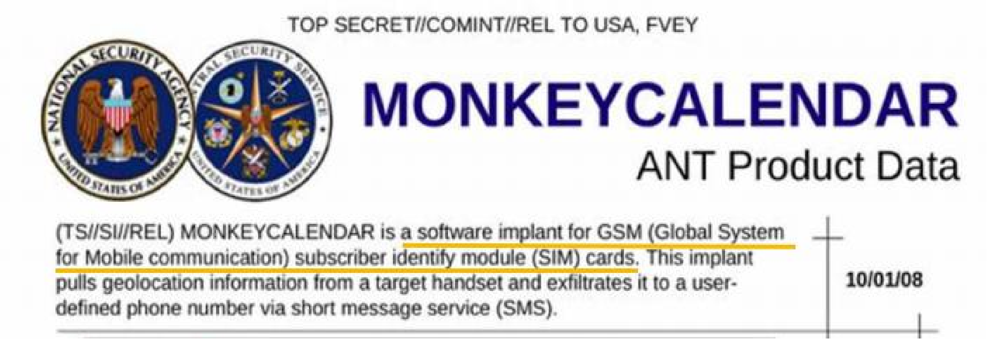
AdaptiveMobile Security believes that in theory, the commands that S@T Browser can execute include obtaining the current location of the device, IMEI information, network information, language information, sending SMS, playing audios, starting the browser, etc., so it can even use mobile phones to send false SMS, make phone calls to commit telecom fraud, open malicious websites, etc.

Cathal McDaid, the chief technology officer of AdaptiveMobile Security, said[3] that one of the special features of the Simjacker vulnerability attack was that the victim was completely unaware of the SMS received with attack messages and the data messages sent, there was no indication in any SMS inbox or outbox. The second was that the attack may be "the first real-life case of malware (specifically spyware) sent within an SMS". Previous malware sent via SMS simply sent its link, requiring the user to click on the link to download. Previous malware sent via SMS involves sending links to malware, not the malware itself within a complete message. Third, many of its attacks seem to work independent of handset types, as the vulnerability is dependent on the software on the SIM and not the device. We have observed devices from nearly every manufacturer being successfully targeted: Apple, ZTE, Motorola, Samsung, Google, Huawei, and even IoT devices with SIM cards.

Traceability Analysis

In December 2013, Der Spiegel disclosed 48 types of NSA's ANT attack equipment exposed by Snowden[4]. AdaptiveMobile Security pointed out that the Simjacker attack is quite similar to two of the attack equipment targeting SIM cards - MONKEYCALENDAR and GOPHERSET. GOPHERSET uses the SIM Toolkit (STK) application interface to send STK instructions to the designated SIM card to collect the other party's call records, SMS content and contact list, and sends the extracted data to the designated number through the SMS service. MONKEYCALENDAR is a spyware implanted into the SIM cards of GSM users. It is also based on the SIM Toolkit (STK) and is mainly used to obtain the location information of the targeted SIM card.

AdaptiveMobile Security believes that the similarities among the three are: first, the attacks all use STK instructions; second, the attacks have the same purpose and can obtain location information, contact list, SMS content, call logs, etc.; third, they all use SMS to send outbound data.



TOP SECRET//COMINT//REL TO USA, FVEY

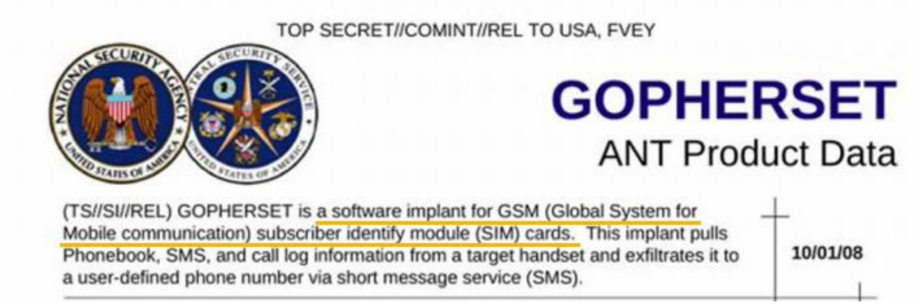
MONKEYCALENDAR

ANT Product Data

(TS//SI//REL) MONKEYCALENDAR is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls geolocation information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08

Fig. 1-3 ANT's Cyberattack Equipment MONKEYCALENDAR Against SIM Cards



TOP SECRET//COMINT//REL TO USA, FVEY

GOPHERSET

ANT Product Data

(TS//SI//REL) GOPHERSET is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls Phonebook, SMS, and call log information from a target handset and exfiltrates it to a user-defined phone number via short message service (SMS).

10/01/08

Fig. 1-4 ANT's Cyberattack Equipment GOPHERSET Against SIM Cards

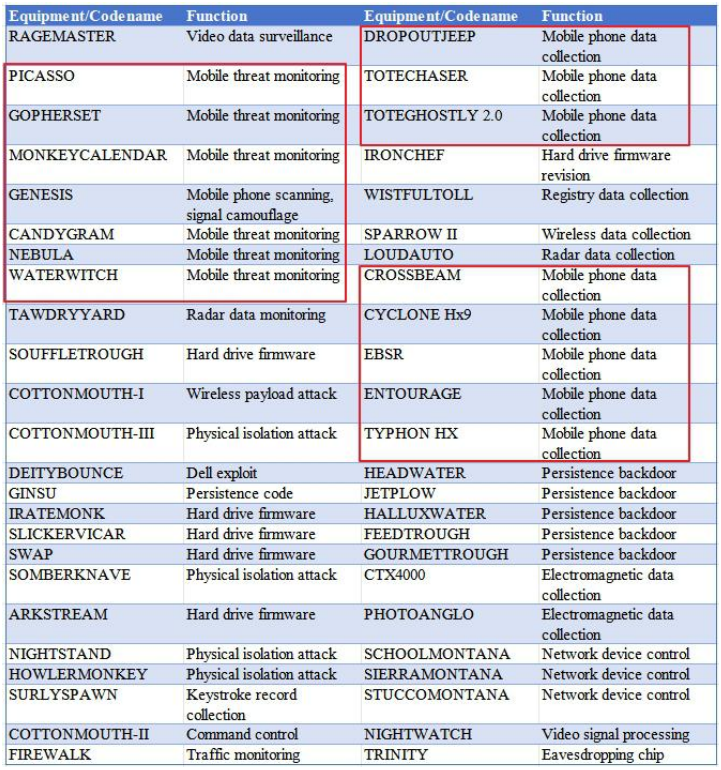
Organizations carrying out Simjacker attacks also have broad access to SS7 networks. AdaptiveMobile Security has discovered that some Simjacker victims suffered simultaneous cyberattacks via SS7 and believes the attack method is being used as a fallback in the incident that Simjacker exploits are unsuccessful. SS7 is a common channel signaling usually used among offices. It is superimposed on the operator's switching network and is an important part of the support network. The *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（Intensified Outbreak of "Nuclear Bomb" Vulnerabilities in SIM Cards and Mobile Terminals: Analysis of Top Digital Weapons in Recent Cyber Warfare）* report[5] released in 2019 pointed out that hackers who can log in to the SS7 network to launch attacks have a high probability of national backgrounds.

AdaptiveMobile Security only detected actual attacks in Mexico, Colombia and Peru. As early as July 2013, Reuters quoted O Globo, a leading Brazilian newspaper[6] that according to the information exposed by Snowden, some Latin American countries have become the main targets of NSA surveillance, especially Colombia, Venezuela, Brazil and Mexico. The report confirmed that the NSA had a specific interest in mobile users in countries such as Mexico.

AdaptiveMobile Security did not directly identify the organization that carried out the attack because of concerns that disclosing specific traceability methods would undermine its capability to detect and prevent Simjacker attacks on a global scale. However, based on its analysis of the overall situation of the Simjacker attack, technical characteristics, attack weapons, attack paths, attack targets, etc., the mastermind NSA hidden behind the Simjacker attack has surfaced.

Extended Analysis

Based on the information exposed by Snowden, Chinese cybersecurity vendor Antiy combed and found that the Advanced Network Technology (ANT), a subsidiary of NSA, had as many as 15 kinds of attack equipment for scanning, monitoring and data collection of mobile communication devices, accounting for about one-third of all the exposed 48 kinds of equipment[7].



Equipment/Codename	Function	Equipment/Codename	Function
RAGEMASTER	Video data surveillance	DROPOUTJEEP	Mobile phone data collection
PICASSO	Mobile threat monitoring	TOTECHASER	Mobile phone data collection
GOPHERSET	Mobile threat monitoring	TOTEGHOSTLY 2.0	Mobile phone data collection
MONKEYCALENDAR	Mobile threat monitoring	IRONCHEF	Hard drive firmware revision
GENESIS	Mobile phone scanning, signal camouflage	WISTFULTOLL	Registry data collection
CANDYGRAM	Mobile threat monitoring	SPARROW II	Wireless data collection
NEBULA	Mobile threat monitoring	LOUDAUTO	Radar data collection
WATERWITCH	Mobile threat monitoring	CROSSBEAM	Mobile phone data collection
TAWDRYYARD	Radar data monitoring	CYCLONE Hx9	Mobile phone data collection
SOUFFLETROUGH	Hard drive firmware	EBSR	Mobile phone data collection
COTTONMOUTH-I	Wireless payload attack	ENTOURAGE	Mobile phone data collection
COTTONMOUTH-III	Physical isolation attack	TYPHON HX	Mobile phone data collection
DEITYBOUNCE	Dell exploit	HEADWATER	Persistence backdoor
GINSU	Persistence code	JETPLOW	Persistence backdoor
IRATEMONK	Hard drive firmware	HALLUXWATER	Persistence backdoor
SLICKERVICAR	Hard drive firmware	FEEDTROUGH	Persistence backdoor
SWAP	Hard drive firmware	GOURMETTROUGH	Persistence backdoor
SOMBERKNAVE	Physical isolation attack	CTX4000	Electromagnetic data collection
ARKSTREAM	Hard drive firmware	PHOTOANGLO	Electromagnetic data collection
NIGHTSTAND	Physical isolation attack	SCHOOLMONTANA	Network device control
HOWLERMONKEY	Physical isolation attack	SIERRAMONTANA	Network device control
SURLYSPAWN	Keystroke record collection	STUCCOMONTANA	Network device control
COTTONMOUTH-II	Command control	NIGHTWATCH	Video signal processing
FIREWALK	Traffic monitoring	TRINITY	Eavesdropping chip

Fig. 1-5 ANT's Cyberattack Equipment Arsenal

The equipment involves both software and hardware. The equipment forms include malware payloads, cell towers, base stations, signal transceivers, mobile phones, etc., which can be used in combination to achieve complex attack objectives.

Tab. 1-1 ANT Cyberattack Equipment Against Mobile Communication Devices

Attack Equipment	Targeted Devices and Functions	Software Implantation Method/Hardware Deployment Location
DROPOUTJEEP	DROPOUTJEEP is a software implant for iPhones that can remotely push/pull files from the device. The data that can be collected include: SMS, contact list, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection.	The initial release will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.
GOPHERSET	GOPHERSET is a software implant for GSM (Global System for Mobile communication) subscriber identify module (SIM) cards. This implant pulls data such as contact list, SMS and call records from a targeted handset and exfiltrates it to a user-defined phone number via short message service (SMS).	It is loaded onto the SIM card using either a Universal Serial Bus (USB) smartcard reader or via over-the-air provisioning.
MONKEYCALENDAR	MONKEYCALENDAR is a software implant for GSM SIM cards. This implant pulls geolocation information from a targeted handset and exfiltrates it to a user-defined phone number via SMS.	It is loaded onto the SIM card using either a USB smartcard reader or via over-the-air provisioning.
TOTECHASER	TOTECHASER is a Windows CE implant targeting the Thuraya 2520 handset. It pulls GPS and GSM geolocation information, call records, contact list, and other user information from Thuraya 2520 handset and exfiltrates it to a user-defined phone number via SMS.	The existing version needs to be deployed directly on the Thuraya 2520 handset. A remotely deployable version is under development.
TOTEGHOSTLY 2.0	TOTEGHOSTLY 2.0 is a software implant for the Windows Mobile operating system that is based on StraitBizarre (a springboard backdoor that enables quantum injection attacks). This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection.	The initial release will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.
PICASSO	Modified GSM (targeted) handset that collects user data, location information and room audio.	Replace the targeted phone with a modified GSM phone
CROSSBEAM	CROSSBEAM is a reusable CHIMNEYPOOL-compliant GSM communications module capable of collecting and compressing voice data. It can receive GSM voice, record voice data, and transmit the received information via connected modules or 4 different GSM data modes (GPRS, Circuit Switched Data, Data Over Voice and DTMF) back to a secure facility.	GSM communication module, deployed on mobile phones.
CANDYGRAM	Mimics GSM cell tower of a targeted network. Whenever a targeted handset enters the CANDYGRAM base station's area of influence, the system sends out an SMS through the external network to registered watch phones.	GSM cell tower, deployed to the targeted network.

CYCLONE HX9	EGSM (900MGz) macro-class Network-ln-a-Box (NIB) system. Uses the existing Typhon GUI and supports the full Typhon feature base and applications.	Macro-class NIB system, deployed to base stations.
EBSR	Multi-purpose. Pico class, tri-band active GSM base station with internal 802.11/GPS/handset capability	GSM base station, deployed to the targeted network.
ENTOURAGE	Direction Finding application operating on the HOLLOWPOINT platform. The system is capable of providing line of bearing (LOB) for GSM/UMTS/ CDMA2000/FRS signals.	Direction Finding application, deployed on the HOLLOWPOINT platform.
GENESIS	Commercial GSM handset that has been modified to include a Software Defined Radio (SDR) and additional system memory. The internal SDR allows a witting user to covertly perform network surveys, record RF spectrum, or perform handset location in hostile environments.	Hand held signal transceiver, carry it with you, no need to deploy.
NEBULA	Multi-Protocol macro-class Network-ln-a-Box (NIB) system. Leverages the existing Typhon GUI and supports GSM. UMTS. CDMA2000 applications. LTE capability currently under development.	Macro-class NIB system, deployed to base stations.
TYPHON HX	Base Station Router - supporting GSM bands 850/900/1800/1900 and associated full GSM signaling and call control.	GSM Base Station Router, deployed to the base station gateway.
WATERWITCH	Hand held finishing tool used for geolocating targeted handsets in the field.	Hand held finishing tool, carry it with you, no need to deploy.

Simjacker vulnerability attack is an application case of the US ANT attack equipment. The technology, infrastructure and methods used prove that the US cyberattack capabilities have made a huge leap. The most prominent point is that the US no longer needs to install implants via close access methods or OTA remote installation (in this way the attacker needs to obtain the OTA key of the targeted SIM card). Monitoring can be started simply via SMS, which is more covert. AdaptiveMobile Security believes that the attacker has been using the Simjacker vulnerability to carry out attacks for at least two years and monitored tens of thousands of users before it was discovered and exposed.

The US intelligence agencies, represented by the NSA, have a complete set of standardized mobile attack equipment, are capable of conducting rigorously organized operations, and their operations are highly covert.

References

[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.

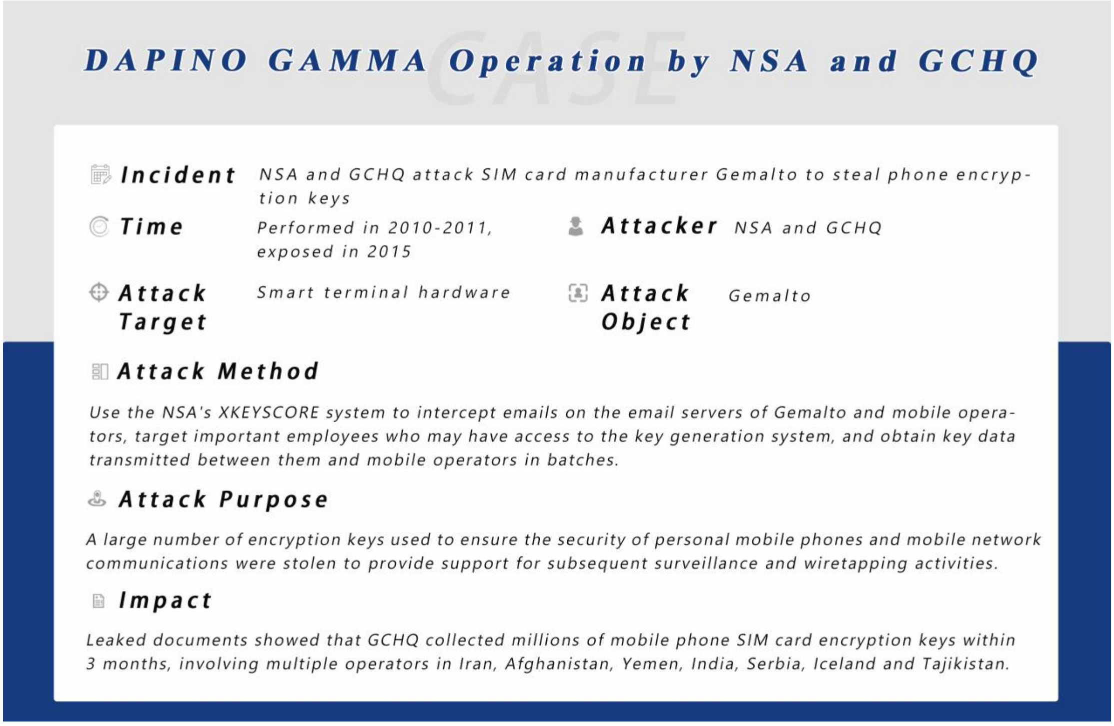
https://www.reuters.com/article/us-usa-security-latinamerica-idUSBRE96816H20130709/

[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

Chapter 2. The Stolen Key - Stealing the Encryption Key of the Mobile Phone SIM Card

SIM card encryption keys are an important part of mobile communications and one of the foundations for ensuring communication security. The authentication key in the SIM card encryption key participates in the legality authentication of mobile devices entering the network, and plays an important role in ensuring user communication security. This key is flashed into the SIM card by the SIM card manufacturer during the production process and provided to the network operator. But it is this "key" that ensures the security of mobile phone communications that has become the target of the US and British intelligence agencies. From 2010 to 2011, the US and British intelligence agencies carried out the DAPINO GAMMA operation against the Dutch SIM card manufacturer Gemalto to steal mobile phone encryption keys.



DAPINO GAMMA Operation by NSA and GCHQ

Incident NSA and GCHQ attack SIM card manufacturer Gemalto to steal phone encryption keys

Time Performed in 2010-2011, exposed in 2015

Attacker NSA and GCHQ

Attack Target Smart terminal hardware

Attack Object Gemalto

Attack Method

Use the NSA's XKEYSCORE system to intercept emails on the email servers of Gemalto and mobile operators, target important employees who may have access to the key generation system, and obtain key data transmitted between them and mobile operators in batches.

Attack Purpose

A large number of encryption keys used to ensure the security of personal mobile phones and mobile network communications were stolen to provide support for subsequent surveillance and wiretapping activities.

Impact

Leaked documents showed that GCHQ collected millions of mobile phone SIM card encryption keys within 3 months, involving multiple operators in Iran, Afghanistan, Yemen, India, Serbia, Iceland and Tajikistan.

Fig. 2-1 List of Cases of DAPINO GAMMA Operation by NSA and GCHQ

Incident Review

On February 20, 2015, The Intercept published an article titled *The Great SIM Heist - How*

Spies Stole the Keys to the Encryption Castle[1] based on the NSA documents leaked by Snowden. It was disclosed that between 2010 and 2011, the Mobile Handset Exploitation Team (MHET) composed of the NSA and the British Government Communications Headquarters (GCHQ), an important organization of the "Five Eyes" intelligence system, carried out an operation called DAPINO GAMMA against SIM card manufacturer Gemalto, aiming to steal the authentication keys used to ensure the security of communications between personal mobile phones and mobile networks. The behavior of the US and Western intelligence agencies to steal mobile phone SIM card authentication keys and then obtain mobile phone communication data has been fully exposed.

The Dutch company Gemalto is one of the world's largest SIM card manufacturers. It was acquired by the French military industry company Thales in 2019. Around 2010, its customers included nearly 450 mobile operators in 85 countries around the world, and it produced approximately 2 billion SIM cards every year[1]. Documents leaked by Snowden show that in its key harvesting "trial" operations in the first quarter of 2010, GCHQ successfully intercepted keys used by wireless network providers in Iran, Afghanistan, Yemen, India, Serbia, Iceland and Tajikistan[2]. In addition, the US and British intelligence agencies cooperated closely during the operation. GCHQ used the NSA's XKEYSCORE system to screen and lock targets, and the SIM card keys it obtained were also shared with NSA.

Attack Method

Locking targets using the NSA's XKEYSCORE system: MHET used the NSA's XKEYSCORE system to intercept a large number of emails on the email servers of Gemalto and mobile operators. Through analysis of the email content, key personnel or clues may be found who may have access to Gemalto's core network and key generation system.

XKEYSCORE is the NSA's system for retrieving and analyzing global internet data. The XKEYSCORE system intercepts data such as emails, internet calls, internet chat records, and browsing history in real time through servers distributed at 150 sites around the world[3]. Analysts can obtain the content data and metadata of the targeted network activities through various keywords such as name, phone number, IP and browser. With this system, NSA can have a panoramic view of every move of a specific target on the Internet. XKEYSCORE also has good scalability and can be integrated or interacted with NSA's TURBULENCE cyberattack operating system to automatically analyze network information collected through other channels and trigger task logic; it can also accept data from other project tasks (for example, data from foreign satellite communications collection project SKIDROWE) and provide analysis and processing functions; XKEYSCORE also provides support for the use and sharing of intelligence by the Five Eyes (FVEY) countries[4].

During the email investigation, MHET found that Gemalto used email or FTP to send SIM card encryption keys to its global operator customers in batches. When it came to transmitting key files, Gemalto only uses simple encryption methods that were easy to crack, sometimes even transmitting the key files directly without encrypting them. This extensive transmission method created conditions for the US and British intelligence agencies to intercept key files.

Intrusion into Gemalto's internal network: in order to steal SIM card encryption keys more conveniently and accurately, MHET also invaded Gemalto's internal network and implanted malware on multiple internal computers. It provides access to Gemalto's intranet and find targets for intercepting keys. Documents leaked by Snowden reveal that MHET has successfully implanted several Gemalto machines, mastered its entire network and processed the acquired data[5].

Developing programs to steal keys in batches: based on preliminary reconnaissance, MHET successfully intercepted internet communication data between multiple Gemalto personalization centers and mobile operators and obtained encryption keys. An article on the Intercept website stated, in one two-week period, they accessed the emails of 130 people associated with wireless network providers or SIM card manufacturing and personalization. This operation produced nearly 8,000 keys matched to specific phones in 10 countries. In another two-week period, by mining just six email addresses, they produced 85,000 keys[1].

In order to further steal the encryption keys transmitted between Gemalto and mobile operators on a larger scale and in larger quantities, the US and British intelligence personnel also specially developed a program to automatically intercept and collect keys. It has also been shown that although the automated method is able to return a representative set of items from bulk data, it often fails to detect all items that would be found manually[6]. Not only that, GCHQ also launched an operation called "HIGHLAND FLING" in 2011, with goals including: to look at getting into France HQ to get in to core data repositories; to get information of possible IPs that could lead to penetration into one or more personalisation centres; to start process for a new supplier Giesecke and Devriente[7].

Extended Analysis

The SIM card encryption keys is an important tool for identity authentication and channel encryption and decryption between mobile phones and mobile networks. Stealing SIM card encryption keys can provide technical support for intelligence agencies to conduct close reconnaissance of mobile phones. If the attacker has the encryption key of the targeted mobile phone, it will be easier for the attacker to achieve an authenticated connection between the fake base station and the targeted mobile phone, especially in 3G and 4G networks with higher security. Having the encryption key will make it easier to crack the communication encryption and restore the plain text communication content. As Matthew Green, a cryptography specialist at the Johns Hopkins Information Security Institute, said that with old-fashioned 2G, there are other ways to work around mobile phone security without those keys, with newer 3G, 4G and LTE protocols, however, the algorithms aren't as vulnerable, so getting those keys would be essential[1]. In addition, the US and British intelligence agencies steal inactivated SIM card encryption keys. This can also establish a SIM card encryption key database to provide support for future signal intelligence (SIGINT).

When it comes to signal intelligence acquisition, the largest one is the US-led ECHELON global signal intelligence collection and analysis system. The system was jointly established by the NSA, GCHQ, the Communications Security Authority of Canada (CSEC), the Australian Signals Directorate (ASD) and the New Zealand Government Communications Security Bureau (GCSB). The system was first established in the 1970s and was initially used during the Cold War to monitor military and diplomatic communications between the Soviet Union and its bloc. After the end of the Cold War, it began intercepting commercial and personal communications around the world. The ECHELON system identifies and extracts valuable information from massive amounts of data by indiscriminately intercepting communication data. This system has established multiple interception facilities around the world and has set up stations in the FVEY countries to perform remote intelligence collection and processing tasks.

ECHELON sites analyze and process telephone calls, faxes, emails and other traffic data around the world by intercepting communications data carried over satellite communications, switched telephone networks and microwave links. In the system, each site automatically retrieves millions of intercepted messages and performs keyword matching. The system's search list not only includes keywords set by the intelligence agency of the country where the site is located, but also includes keywords set for other agencies of the FVEY countries. Whenever it encounters data containing a keyword from a certain intelligence agency, it automatically picks out the message and sends it directly to the relevant intelligence agency[8].

Whether it is the theft of mobile phone SIM card encryption keys or the collection of global signal intelligence data through the ECHELON system, they all reflect the continuous and crazy collection of global signal intelligence data by Western intelligence agencies led by the United States. Whether they are terminal devices or backbone lines, whether they are high-value targets such as technical experts and government officials or ordinary people, they may all become targets of the US intelligence agencies' intelligence activities.

References

[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

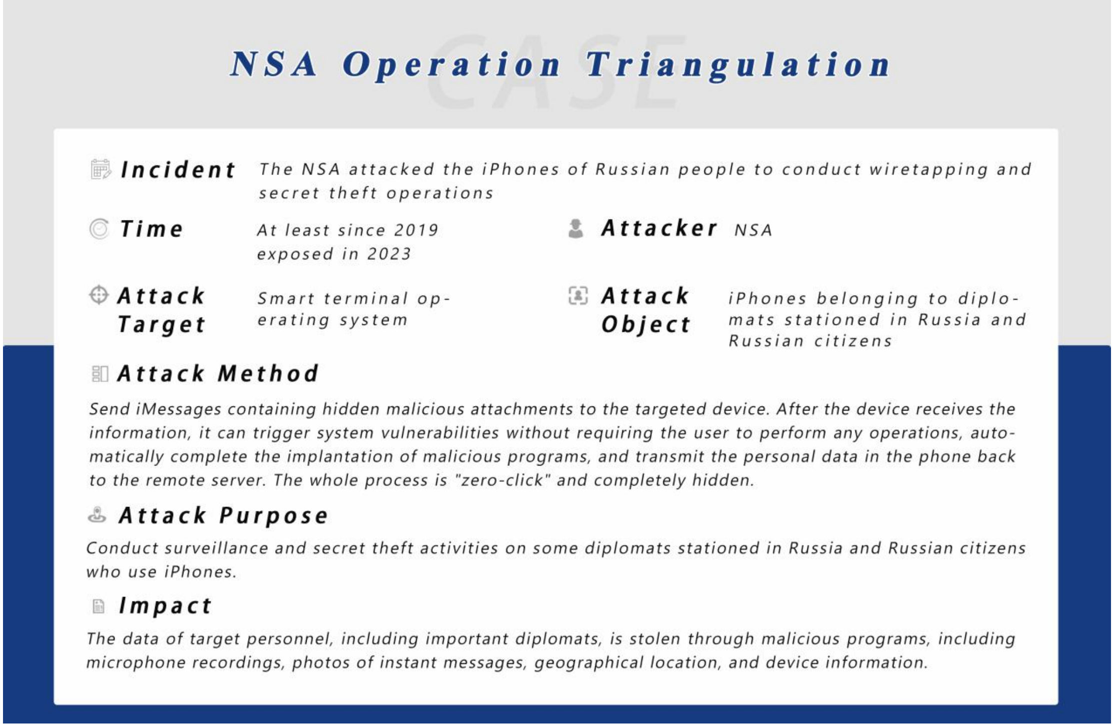
[6] Snowden Archive. PCS Harvesting at Scale. 2015.
https://grid.glendon.yorku.ca/items/show/269

[7] Snowden Archive. DAPINO GAMME 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

Chapter 3. Sneaky Intrusion - Zero-Click Attack on iPhone

The iOS system platform is a mobile operating system developed by Apple and used for mobile devices such as iPhone, iPad and iPod touch. The iOS system platform has built-in some unique functions. For example, iMessage is an instant messaging service developed by Apple. It has multiple functions such as sending and receiving text messages, images, videos, and documents, providing users with a convenient social experience. However, this type of instant messaging service has become a target by the US intelligence agencies. The US intelligence agencies use this type of service to send malware or attack payloads to iPhone users in order to steal mobile phone data. In June 2023, the Russian Federal Security Service (FSB) issued a statement accusing the NSA of carrying out Operation Triangulation against iPhones.



NSA Operation Triangulation

CASE

Incident The NSA attacked the iPhones of Russian people to conduct wiretapping and secret theft operations

Time At least since 2019 exposed in 2023

Attacker NSA

Attack Target Smart terminal operating system

Attack Object iPhones belonging to diplomats stationed in Russia and Russian citizens

Attack Method

Send iMessages containing hidden malicious attachments to the targeted device. After the device receives the information, it can trigger system vulnerabilities without requiring the user to perform any operations, automatically complete the implantation of malicious programs, and transmit the personal data in the phone back to the remote server. The whole process is "zero-click" and completely hidden.

Attack Purpose

Conduct surveillance and secret theft activities on some diplomats stationed in Russia and Russian citizens who use iPhones.

Impact

The data of target personnel, including important diplomats, is stolen through malicious programs, including microphone recordings, photos of instant messages, geographical location, and device information.

Fig. 3-1 List of Cases of NSA Operation Triangulation

Incident Review

On June 1, 2023, the cybersecurity company Kaspersky stated that the iPhones of its senior employees had been compromised. Kaspersky then released a report titled *Operation*

Triangulation: iOS devices targeted with previously unknown malware[1]. The report revealed a malicious campaign that targeted iPhones and iPad devices with "zero-click" attacks. The "zero-click" attack means that the implantation of the targeted mobile device can be completed without any interaction from the mobile phone user during the entire attack process. The oldest traces of infection happened in 2019. It performs a fingerprinting technique called Canvas Fingerprinting by drawing a yellow triangle on a pink background with WebGL and calculating its checksum. This triangle is, in fact, why Kaspersky dubbed this whole campaign Operation Triangulation[2]. Subsequently, Kaspersky successively released 6 related reports [3-6].

On the same day, the Russian Federal Security Service (FSB) issued a statement, accusing Apple of "close cooperation" with the NSA and invading thousands of iPhones through sophisticated malware, targeting mainly "foreign diplomats stationed in Russia and post-Soviet countries", including diplomats from NATO member states, Israel, Syria and China, as well as some local Russian users. The FSB stated that "Apple provides opportunities and conditions for the US intelligence agencies to carry out intelligence surveillance activities against Russia. The surveillance targets also include US partners in anti-Russian activities and US citizens"[7].

Attack Method

Operation Triangulation uses the built-in iMessage messaging service of the iOS system and four zero-day vulnerabilities in the iOS system to achieve zero-click attacks on Apple devices.

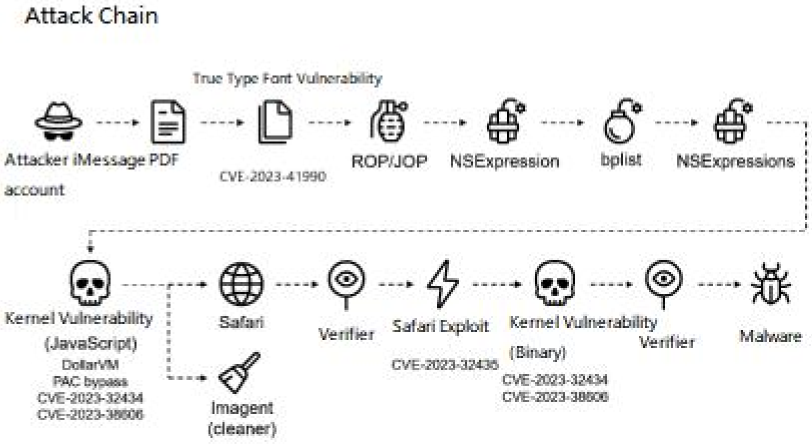


Fig. 3-2 Schematic Diagram of Operation Triangulation Attack Chain[6]

The attacker first sent iMessages containing hidden malicious attachments to the targeted iOS device through the iMessage server. After receiving the message, the device automatically triggered four zero-day vulnerabilities in the system and automatically completed the subsequent implantation of malicious programs. The attacker initially exploited WebKit memory corruption and font parsing vulnerabilities to obtain execution permissions, then used an integer overflow vulnerability to escalate to gain kernel permissions, and then used multiple memory vulnerabilities to break through Apple's hardware-level security defense functions to execute and implant malicious programs on the device. The entire process is completely hidden and does not require the user to perform any action. Malicious programs quietly and automatically transmit personal information in the phone to a set remote server. This includes microphone recordings, photos from instant messages, geolocation, and other device data.

Kaspersky analyzed the main implanted weapon and dubbed it TriangleDB. TriangleDB is deployed after the attackers obtain root privileges on the targeted iOS device by exploiting a kernel vulnerability. It is deployed in memory, meaning that all traces of the implant are lost when the device gets rebooted. Therefore, if the victim reboots their device, the attackers have to reinfect it by sending an iMessage with a malicious attachment, thus launching the whole exploitation chain again. In case no reboot occurs, the implant uninstalls itself after 30 days, unless this period is extended by the attackers[4].

The binary validator is the component responsible for cleaning up traces of the malicious iMessage. Sending this information back to the C2 server can help attackers to judge the value of the device and decide whether to execute the TriangleDB process. If executed normally, TriangleDB loads and calls multiple sub-spy modules from the C2 server, including the microphone recording module, KeyChain credential acquisition module, SQLite database secret theft module, GPS positioning module, SMS secret theft module, etc. It supports attackers to carry out platform-level secret theft operations. The sent and received messages are encrypted with symmetric (3DES) and asymmetric (RSA) cryptography. All messages are exchanged via the HTTPS protocol in POST requests. It performs a fingerprinting technique called Canvas Fingerprinting by drawing a yellow triangle on a pink background with WebGL and calculating its checksum.

On December 27, 2023, Kaspersky released the report *Operation Triangulation: The last (hardware) mystery*. The attacker wrote data to a certain physical address and also bypassed hardware-based memory protection by writing data, destination address, and data hash to unknown hardware registers of the chip unused by the firmware. Currently, it is unknown how the attacker learned to use this unknown hardware feature[6]. The report speculates that Apple may be cooperating with the US intelligence agencies.

Extended Analysis

Most mobile malware requires the user to take a click action during the process of infecting the target. Users can prevent this by improving their own security awareness. "Zero-click" attacks do not require the user to perform any action on the phone, including clicking a link or opening a file. As long as the mobile phone user receives the relevant content, the malicious program can be automatically implanted into the mobile phone. Most of the targets are unaware that their phones have been implanted with malicious programs, making it difficult to protect personal phones and privacy. "Zero-click" attacks often exploit unknown or unpatched vulnerabilities in the system. Therefore, system developers cannot discover and fix them in time. As Fortinet FortiGuard Labs cybersecurity researcher Aamir Lakhani said, "even very alert and aware users cannot avoid those double-whammy zero-day and zero-click attacks"[8].

As mobile phone systems become more and more perfect, there are fewer and fewer "zero-click" vulnerabilities that can be discovered and exploited, and the cost of "zero-click" attacks is becoming higher and higher. Zerodium, which purchases vulnerabilities on the open market, pays up to $2.5M for zero-click vulnerabilities against Android[8]. All these determine that attacks like Operation Triangulation must be carried out against high-value targets and small-scale specific groups of people. During the Operation Triangulation attack, the attacker verified a large amount of target and device information and deleted some attack traces before implanting TriangleDB. TriangleDB only exists in the phone's memory and has the ability to self-delete. These once again prove that Operation Triangulation has the characteristics of high concealment of attack methods, high complexity of attack processes, and high directionality of attack targets. Based on these characteristics, it is reasonable to infer that the action was carefully planned and implemented by organizations with a national background.

Kaspersky released a report on January 16, 2024[9] stating that investigating such cases can be complicated, costly, or time consuming due to the nature of the iOS ecosystem. As a result, related threats can often go undetected by the general public. The lightweight method for identifying a potential iPhone infection can detect the Pegasus spyware infection and other iOS malware. Among various mobile phone systems, iOS is considered to have a relatively more reasonable architecture design and a relatively complete security mechanism. However, it is precisely the activities of the US intelligence agencies that seriously affect the trust of global users in iphones.

As the Russian Ministry of Foreign Affairs said on June 1, 2023[10], **"This fact has conclusively proven what Moscow has been speaking about for a long time, namely, that the US intelligence services have been using IT giants for decades to collect internet users personal data without their knowledge." "The United States has placed itself above the law. No state has a right to abuse its technological capabilities in a sensitive sphere such as access to the personal data of smartphone users."**

References

[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

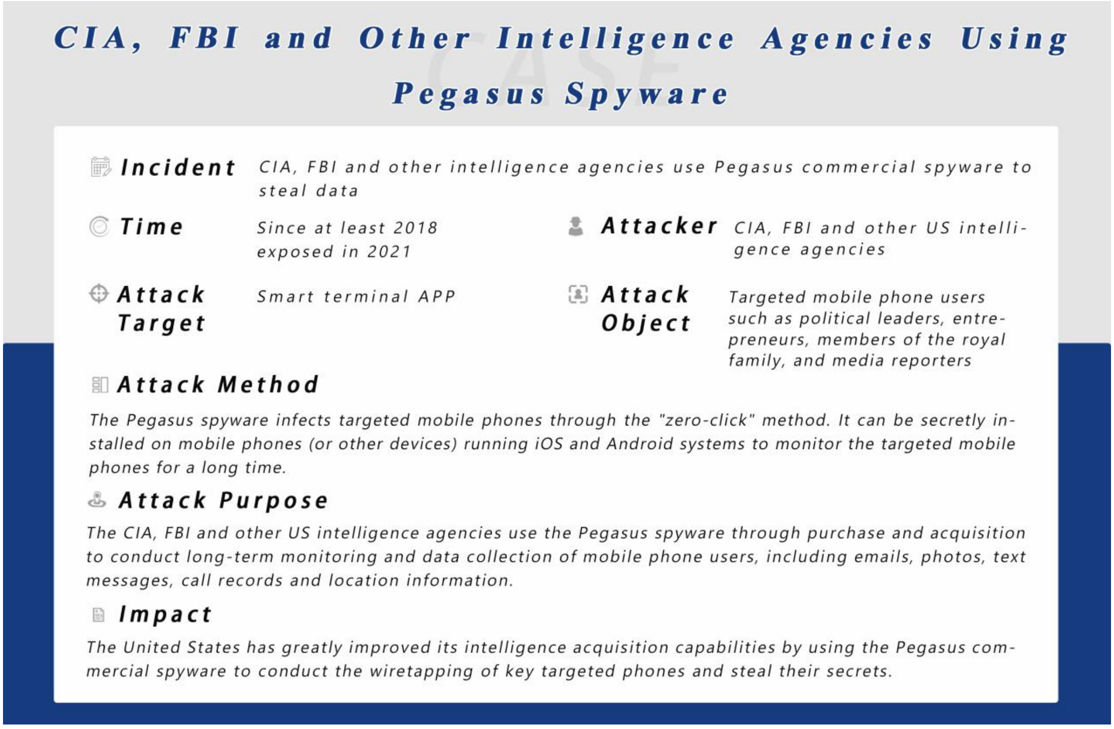
[8] Andrada Fiscutean. CSO. Zero-click attacks explained, and why they are so dangerous. 2022. https://www.csoonline.com/article/572727/zero-click-attacks-explained-and-why-they-are-so-dangerous.html

[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/

Chapter 4. Pegasus - the Use of Commercial Spyware

The Pegasus spyware is a well-known product of the Israeli cyber weapons supplier NSO Group. This software can infect the targeted mobile phone through the "zero-click" method, and is secretly installed on mobile phones (or other mobile smart terminals) running iOS and Android systems to monitor the targeted mobile phone for a long time. The Pegasus can obtain detailed data on the mobile phone, including emails, photos, text messages, call records, etc. In addition, it can also obtain the gelocation of the phone and even control the phone's camera and microphone. Since 2018, intelligence agencies such as the CIA and FBI in the United States have adopted various ways and means to use spyware such as Pegasus to monitor relevant mobile phone users.



CIA, FBI and Other Intelligence Agencies Using Pegasus Spyware

Incident CIA, FBI and other intelligence agencies use Pegasus commercial spyware to steal data

Time Since at least 2018 exposed in 2021

Attacker CIA, FBI and other US intelligence agencies

Attack Target Smart terminal APP

Attack Object Targeted mobile phone users such as political leaders, entrepreneurs, members of the royal family, and media reporters

Attack Method

The Pegasus spyware infects targeted mobile phones through the "zero-click" method. It can be secretly installed on mobile phones (or other devices) running iOS and Android systems to monitor the targeted mobile phones for a long time.

Attack Purpose

The CIA, FBI and other US intelligence agencies use the Pegasus spyware through purchase and acquisition to conduct long-term monitoring and data collection of mobile phone users, including emails, photos, text messages, call records and location information.

Impact

The United States has greatly improved its intelligence acquisition capabilities by using the Pegasus commercial spyware to conduct the wiretapping of key targeted phones and steal their secrets.

Fig. 4-1 List of Cases of CIA, FBI and Other Intelligence Agencies Using Pegasus Spyware

Incident Review of the Pegasus Spyware

On July 18, 2021, 17 internationally renowned media organizations[1] from more than ten countries around the world, including The Washington Post and The Guardian, jointly published a report after several months of investigation into the Israeli spyware Pegasus. The report revealed that multiple heads of state and political figures were monitored by this spyware, including French President Macron, Iraqi President Saleh, South African President Ramaphosa, Pakistani Prime Minister Imran Khan, Egyptian Prime Minister Ma Debry, etc., in addition to many royal family members, government officials, business executives, media reporters and other public figures from various countries. After the Pegasus attack was exposed by the media, it caused an uproar in the international community. This incident has given people a deeper understanding of the ultra-high attack capabilities of commercial spyware.

The US Intelligence Agencies Use Spyware (Pegasus)

The powerful attack, penetration and monitoring capabilities of the Pegasus have attracted global attention and become a hot target for governments and intelligence agencies of relevant countries. The United States is very fond of the Pegasus. The DEA, the Secret Service and the US Military Africa Command had all held discussions with NSO[2]. Intelligence agencies such as the CIA and FBI have also carried out in-depth co-operations with the NSO.

1. Technical Origins of CIA and Pegasus

According to a report by the New York Times in January 2022[3], as early as 2018, the US CIA bought Pegasus to assist its government in counterterrorism operations. The CIA arranged and paid for the government of Djibouti. An investigative report published by the Forbes website in March 2017[4] showed that "the CIA's techniques for getting persistence on a hacked iPhone were similar to those from an Israeli cyber weapons dealer called NSO Group", "they both use the same vulnerability, but implementation differs a bit". It can be seen that the technical relationship between CIA and NSO is very deep. There may be a deeper partnership between them.

2. In-depth cooperation between the FBI and NSO Group

In addition to the CIA, the FBI is also a client of the NSO Group. The Times revealed in January 2022 that the FBI had purchased Pegasus in 2018. Over the next two years, the FBI had tested the spyware at a secret facility in New Jersey[3]. In June 2019, three Israeli computer engineers arrived at a New Jersey building used by the FBI. They demonstrated and tested the functions and performance of Pegasus.

NSO engineers' demonstration of the functionality of the Pegasus spyware aroused the FBI's keen interest. However, due to Israeli government restrictions, the regular version of the Pegasus software cannot monitor American mobile phone numbers. During a presentation to officials in Washington, the company demonstrated a new system, called Phantom, that could hack any phone number in the United States that the FBI decided to target. Israel had granted a special license to NSO, one that permitted its Phantom system to attack US numbers. The license allowed for only one type of client: the US government agencies. NSO's US subsidiary declared, Phantom allows American law enforcement agencies and intelligence agencies to get intelligence by extracting and monitoring crucial data from mobile devices. It is an independent solution that requires no cooperation from AT&T, Verizon, Apple or Google. The system will "turn the target's smartphone into an intelligence gold mine"[2].

3. Purchase NSO Products through Shadow Companies

According to a report by the New York Times in April 2023[5], a secret contract was finalized between a company that had acted as a front for the US government and the American affiliate of a notorious Israeli hacking firm on November 8, 2021. Under the arrangement, the Israeli firm, NSO Group, gave the US government access to one of its most powerful weapons Landmark, a geolocation tool that could covertly track mobile phones around the world without the phone user's knowledge or consent. If the veiled nature of the deal was unusual, it was signed for the front company by a businessman using a fake name. Only a few days earlier, the White House placed NSO on a Commerce Department blacklist. This also fully demonstrates the duality and hypocrisy of the US government in terms of cyber weapons proliferation and citizen privacy monitoring.

4. The US Intelligence Agencies Authorize Defense Contractor to Acquire the NSO Group

In 2022, a potential deal with L3Harris, the American defense giant, to buy NSO hacking tools and take on the bulk of its workforce was far more advanced than previously known[5]. Despite NSO being on the Commerce Department blacklist, L3Harris executives had discussions with Commerce Department officials about the potential deal, according to internal department records, and there was a draft agreement in place to finalize it before the White House publicly objected and L3Harris dropped its plans. This incident fully demonstrates the US intelligence agencies' intention to control commercial spyware to carry out intelligence activities.

5. Continued Exploitation of Other Israeli Spyware

The US government agencies continue to use spyware with similar functionality to Pegasus. The media revealed that the US Drug Enforcement Administration (DEA) is one of the largest customers of the Israeli company Paragon's Graphite software. Paragon has learned from NSO's experience and established close communication channels with the US government. Paragon also reportedly asked for US guidance on its target customer list; deliberately sought funding from two US-based venture capital firms, Battery Ventures and Red Dot, in order to have American backing. Paragon hired a US political consultancy to advise it on what it should and shouldn't do to win government orders. Through these measures, Paragon actually obtained the acquiescence of the US government, and the US government indirectly gained strong control over Paragon[6].

It is worth noting that although the DEA is a law enforcement agency that combats illegal drug trade, it has inextricable ties with the US intelligence agencies. The DEA often uses its convenient status in combating drug trade to provide help and cover for intelligence agencies to carry out activities abroad[7]. Although the US government banned the Pegasus software, similar spyware is still used to carry out intelligence activities.

Extended Analysis

On the surface, the United States restricts other countries from using its software by sanctioning the NSO Group, but secretly it purchases spyware through shadow companies and instructs defense contractors to acquire the NSO Group. The FBI cooperated with NSO under the guise of testing to develop Phantom system that can attack mobile phones in the United States; the FBI also used the Landmark spyware through the contractor Riva Networks to conduct long-term mobile phone monitoring activities in Mexico[8].

Intelligence coordination between the United States and Israel includes: Israeli companies have provided commercial espionage tools for the United States to use; the United States has developed attack weapons for both parties. Famous incidents include Stuxnet and Duqu 2.0 (for Kaspersky). **The US intelligence agencies have further strengthened their surveillance and intelligence acquisition capabilities in the mobile network field by utilizing and controlling commercial spyware.**

On April 5, 2022, The Washington Post reported[9] that the FBI signed a record-breaking software service contract of up to $27 million with Babel Street to strengthen its search and tracking capabilities for social media content. The FBI bidding conditions clearly require: ability to search and translate in "at least seven foreign languages"; ability to search for a certain geographical area; ability to perform correlation analysis and sentiment analysis on the poster, and also has additional functions such as expression analysis, predictive analysis, and machine detection. **The US intelligence agencies use commercial software to maximize their already "armed to the teeth" network intelligence collection capabilities.**

References

[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/

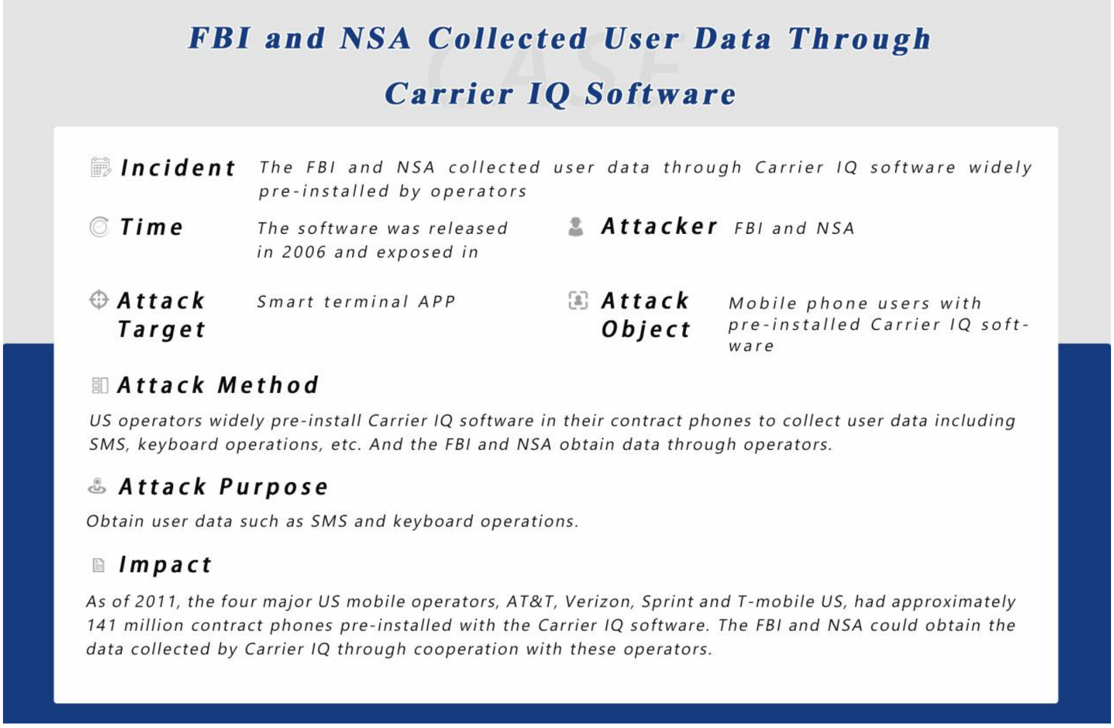
[7] Ben Buchanan. The Hacker and The State. 2020.
https://gerdab.ir/files/fa/news/1400/6/23/49615_176.pdf

[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] Washington Post. 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/

Chapter 5. Apps That Cannot Be Uninstalled - Collecting Data Through Software Widely Preinstalled by Operators

Android is one of the most important mobile operating systems in the world. In pursuit of better performance, user interface and functions, mobile phone vendors often choose to deeply customize the native Android system. Some vendors will pre-install certain applications in the Read-Only Memory (ROM), which may become tools for the US intelligence agencies to obtain user data. In 2011, it was disclosed that US operators AT&T, Verizon, Sprint and T-mobile US had widely pre-installed the Carrier IQ software in mobile phones. The software illegally collected user data, including SMS, keyboard operations, etc. The operators used the Carrier IQ backend product to conduct data query, and the FBI and NSA obtained user data that far exceeds the scope of legal authorization through intelligence cooperation with operators.



FBI and NSA Collected User Data Through Carrier IQ Software

Incident The FBI and NSA collected user data through Carrier IQ software widely pre-installed by operators

Time The software was released in 2006 and exposed in

Attacker FBI and NSA

Attack Target Smart terminal APP

Attack Object Mobile phone users with pre-installed Carrier IQ software

Attack Method

US operators widely pre-install Carrier IQ software in their contract phones to collect user data including SMS, keyboard operations, etc. And the FBI and NSA obtain data through operators.

Attack Purpose

Obtain user data such as SMS and keyboard operations.

Impact

As of 2011, the four major US mobile operators, AT&T, Verizon, Sprint and T-mobile US, had approximately 141 million contract phones pre-installed with the Carrier IQ software. The FBI and NSA could obtain the data collected by Carrier IQ through cooperation with these operators.

Fig. 5-1 List of Cases in Which the FBI and NSA Collected User Data Through Carrier IQ Software

Incident Review

Carrier IQ, founded in 2005, is an American privately owned mobile software company. Its products consist of embedded software (IQ Agent) on mobile devices and server-side analytics applications to enable mobile operators to understand in detail a wide range of performance and usage characteristics of mobile services and devices. IQ Agent was first shipped in 2006 on embedded feature phones and had since been implemented on other devices such as USB modems and tablets[1].

On November 12, 2011, American white-hat hacker Trevor Eckhart posted an article on the Android system security testing website (androidsecuritytest.com)[2], disclosing that the Carrier IQ software collected both network-facing information such as core voice and data offerings, as well as non-network-facing information, including device type, available memory and battery life, the type of applications resident on the device, the geographical location of the device, the end user's pressing of keys on the device and usage history of the device, and sent back to Carrier IQ's server for statistical analysis. The backend products provided by Carrier IQ allowed operators and other users to conduct detailed history queries on any device based on IMEI or IMSI (International Mobile Subscriber Identity), so users' privacy was completely exposed to Carrier IQ and mobile operators using its services. Typically, Carrier IQ software was deeply pre-installed into ROM. Therefore, in order to completely excise the software, users must first root the phone and then re-flash the phone's ROM thoroughly, which is difficult for the ordinary users to operate.

On November 28, 2011, Eckhart posted a video on YouTube showing the Carrier IQ software recording various keystrokes in plain text[3], including plain text capture of security website passwords, and activities performed when cellular networks were disabled.

In November 2011, Antiy released *对 Carrier IQ 木马的综合分析报告 (A Comprehensive Analysis on Carrier IQ)*[4], which confirmed that Carrier IQ not only actively captured and read SMS content on users' mobile phones, monitored users' keyboard operations and keystrokes, but even recorded and transmitted the data it obtained.

Incident Analysis

The four major telecom operators in the United States - AT&T, Verizon, Sprint and T-Mobile US - were all customers of Carrier IQ and had pre-installed the software in several types of phones, involving Android, Symbian, BlackBerry, iOS and other platforms. It was reported that 141 million devices were affected[5]. And Carrier IQ software was pre-installed in several brands of mobile phones including BlackBerry, HTC and Samsung, while mobile phone vendors claimed that it was US operators that forced them to install the software on their devices.

In December 2011, the FBI refused to disclose Carrier IQ-related documents in accordance with the Freedom of Information (FOI) ACT request, and was forced to admit that the data collected by Carrier IQ was used in "investigative documents compiled for law enforcement purposes"[6].

In June 2013, Bloomberg published an article titled *The NSA Could Collect Far More Than Your Phone Records*[7], which pointed out that after the data collection of Carrier IQ was exposed, many US carriers and device makers excised Carrier IQ from their handsets, but the fact remained that carriers had installed hidden monitoring software on their customers' handsets. It wouldn't be difficult for the NSA to collect and aggregate that data from carriers networks, just as it's reportedly doing with Web giants Google.

Extended Analysis

After the data collection by Carrier IQ was exposed, AT&T admitted that it had installed the software on its devices since March 2011[8]. In December 2015, AT&T acquired Carrier IQ in a low-profile manner and did not disclose details about the acquisition. Major US operators have a long history of cooperation with intelligence agencies. According to the information exposed by Snowden, AT&T had a decades-long partnership with the NSA[9] and the PRISM program showed that the US intelligence agencies deeply mined and obtained data from operators and large internet vendors. On June 5, 2013, The Guardian, a British newspaper, reported that the NSA had requested Verizon to provide millions of private phone records[10].

Major US operators had obtained a large amount of private user data far exceeds their traffic optimization needs through the Carrier IQ software. Based on the deep cooperative relationship between the US telecom operators such as AT&T and Verizon and the US intelligence agencies, **global mobile users had reason to suspect that the US intelligence agencies, through telecom operators in the country, had widely pre-installed network diagnostic software such as Carrier IQ in users' mobile phones to collect data on mobile users in the United States at an extremely low cost. In fact, they had turned mobile operators into their intelligence resources.**

Although the Freedom of Information ACT, passed by the US Congress in June 2015, requires the US intelligence agencies to cease large-scale collection of phone data within six months, and to apply to the Foreign Intelligence Surveillance Court (FISC) for approval before accessing phone data on specific targets from telecom companies. However, the US intelligence agencies have not complied with this regulation at all. On November 20, 2023, the American magazine Wired published an article titled *Secretive White House Surveillance Program Gives Cops Access to Trillions of US Phone Records*[11], pointed out that a surveillance program now known as Data Analytical Services (DAS) had for more than a decade allowed federal, state, and local law enforcement agencies to mine the details of Americans' calls, analyzing the phone records of countless people who are not suspected of any crime, including victims. The DAS program, formerly known as Hemisphere, was run in coordination with the telecom giant AT&T, which captured and conducted analysis of US call records for law enforcement agencies, from local police and sheriffs' departments to the US customs offices and postal inspectors across the country. The exposure of the DAS program fully proves that **the extensive wiretapping activities of the US intelligence agencies are pervasive, and even the rights and interests of Americans cannot be guaranteed.**

References

[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

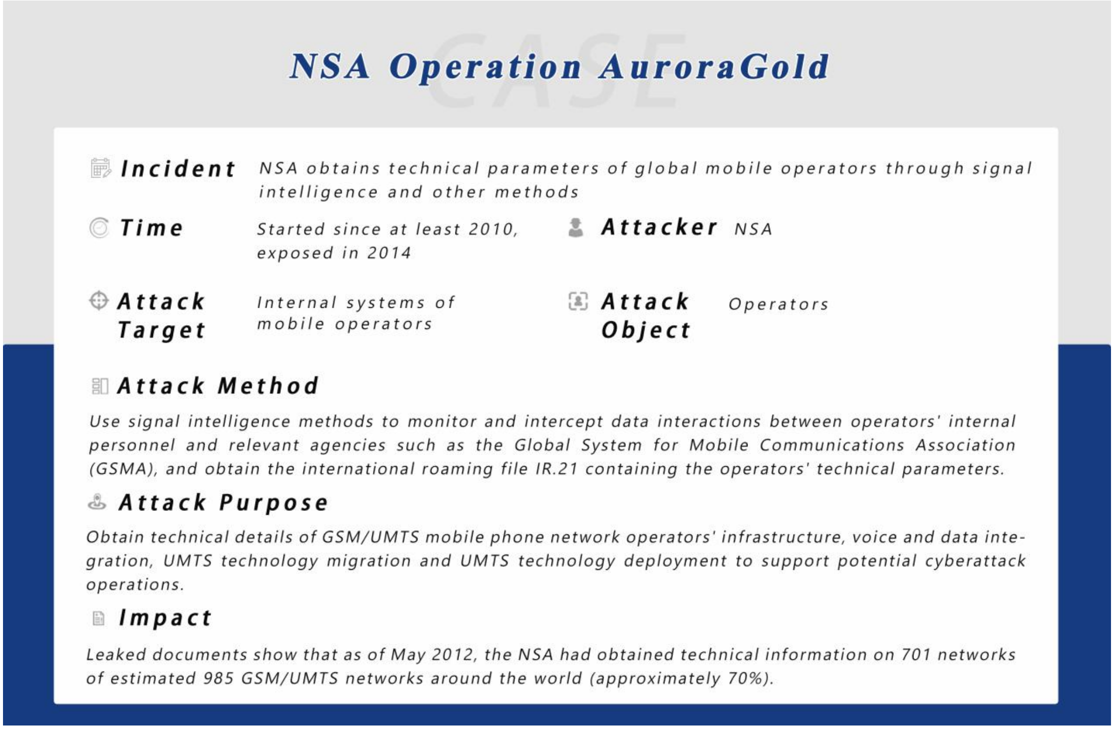
[9] NSA Spying Relies on AT&T’s ‘Extreme Willingness to Help’. 2015.
https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help

[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/

Chapter 6. Getting to the Bottom - Obtaining Technical Parameters of Global Mobile Operators

Since the concept of "cellular network" was proposed by Bell Laboratories in the 1970s, mobile communication technology has been rapidly iterated and updated. Global mobile operators have different business environments and operating models, so the network standards, infrastructure types, encryption methods, protocols and other technical parameters they adopt are also different. In order to obtain technical parameters of global mobile operators and exploit vulnerabilities for targeted attacks, the NSA has been implementing operation AuroraGold since at least 2010. The operation used signal intelligence methods to obtain non-public data - the international roaming file IR.21 of various mobile operators, integrated it with public data, and formed a global mobile operator technical parameter database, which supported the NSA SIGINT production chain to carry out secret theft, wiretapping and eavesdropping on mobile phone users.



NSA Operation AuroraGold

Incident NSA obtains technical parameters of global mobile operators through signal intelligence and other methods

Time Started since at least 2010, exposed in 2014

Attacker NSA

Attack Target Internal systems of mobile operators

Attack Object Operators

Attack Method

Use signal intelligence methods to monitor and intercept data interactions between operators' internal personnel and relevant agencies such as the Global System for Mobile Communications Association (GSMA), and obtain the international roaming file IR.21 containing the operators' technical parameters.

Attack Purpose

Obtain technical details of GSM/UMTS mobile phone network operators' infrastructure, voice and data integration, UMTS technology migration and UMTS technology deployment to support potential cyberattack operations.

Impact

Leaked documents show that as of May 2012, the NSA had obtained technical information on 701 networks of estimated 985 GSM/UMTS networks around the world (approximately 70%).

Fig. 6-1 List of Cases of NSA Operation AuroraGold

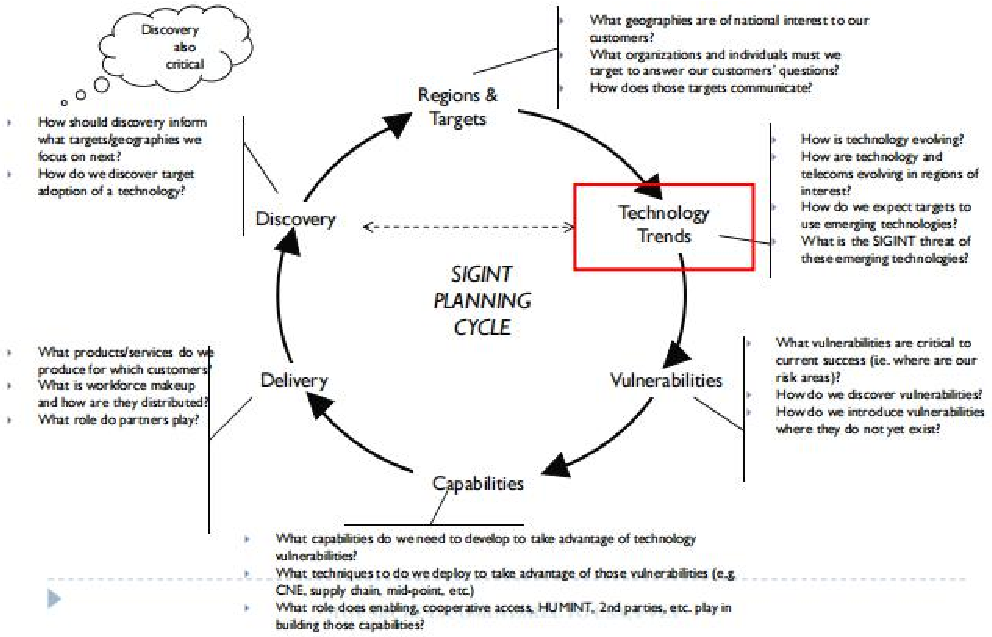
Incident Review

On December 4, 2014, The Intercept published relevant documents leaked by Snowden, which disclosed that the NSA had been implementing operation AuroraGold[1] since at least 2010, aiming to obtain global mobile operator technical parameters and effectively predict future technology trends, so as to support the SIGINT production chain. In addition, information gathered by operation AuroraGold was widely shared within the intelligence agencies of the FVEY countries.

As of May 2012, the NSA had obtained the technical information of 701 networks of estimated 985 GSM/UMTS networks around the world (approximately 70%) through operation AuroraGold, covering almost all countries, including allies close to the US, such as the UK, Australia, New Zealand, Germany and France.

Attack Method

Since at least 2010, the NSA has proposed the SIGINT planning cycle project to systematize the SIGINT production chain, which consists of six links: discovery, regions & targets, technology trends, vulnerabilities, capabilities, and delivery. Operation AuroraGold is part of the "technology trends" link.



- What geographies are of national interest to our customers?
- What organizations and individuals must we target to answer our customers' questions?
- How does those targets communicate?

- How should discovery inform what targets/geographies we focus on next?
- How do we discover target adoption of a technology?

- How is technology evolving?
- How are technology and telecoms evolving in regions of interest?
- How do we expect targets to use emerging technologies?
- What is the SIGINT threat of these emerging technologies?

- What products/services do we produce for which customers?
- What is workforce makeup and how are they distributed?
- What role do partners play?

- What vulnerabilities are critical to current success (ie. where are our risk areas)?
- How do we discover vulnerabilities?
- How do we introduce vulnerabilities where they do not yet exist?

- What capabilities do we need to develop to take advantage of technology vulnerabilities?
- What techniques to do we deploy to take advantage of those vulnerabilities (e.g. CNE, supply chain, mid-point, etc.)
- What role does enabling, cooperative access, HUMINT, 2nd parties, etc. play in building those capabilities?

Fig. 6-2 Schematic Diagram of the NSA SIGINT Planning Cycle

In the subsequent "vulnerabilities" link, the NSA explicitly proposed to use the technical trend data provided by operation AuroraGold to identify vulnerabilities that could be exploited and introduce vulnerabilities that did not yet exist in order to exploit in the "capabilities" link.

Many cybersecurity experts including Karsten Nohl, German security expert and cryptographer, and Mikko Hypponen, senior researcher at Finland-based F-Secure, have expressed shock at the NSA's deliberate operation AuroraGold to introduce new vulnerabilities in the global communication system for espionage purposes. Security experts pointed out[1] that criminal hackers and foreign government adversaries could be among the inadvertent beneficiaries of any security vulnerabilities inserted by the NSA. This controversial tactic could expose ordinary people to hackers and other criminals.

NSA documents show that in March 2011, two weeks before the western countries intervened in the Libyan civil war, AFRICOM used the data intelligence database of operation AuroraGold to acquire information concerning the SMS Gateway domains for the only two mobile providers in Libya, and used the information to invade mobile networks in Libya for SMS monitoring.

Operation AuroraGold integrated public data and non-public data. After data analysis and extraction, it built a data intelligence database containing global mobile operators' technical parameters and mobile technology development trends, and output the data in a visualized way. The public data included a complete replica of World Cellular Information Service (WCIS) queryable database, the International Telecommunication Union (ITU) operational announcements and other data, while the non-public data were mainly IR.21.

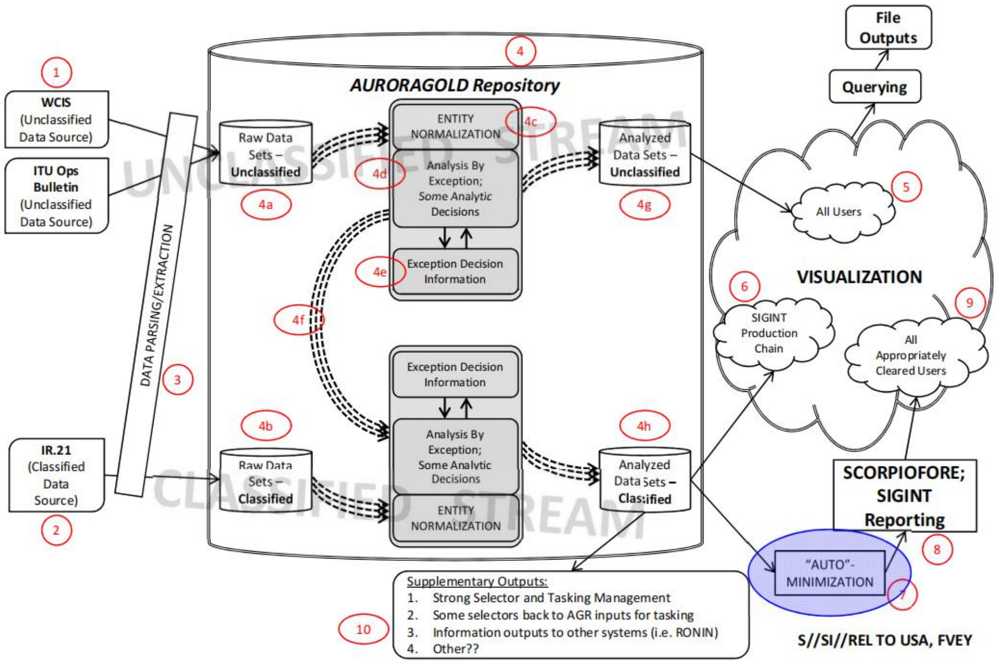

1
WCIS
(Unclassified Data Source)
ITU Ops Bulletin
(Unclassified Data Source)
DATA PARSING/EXTRACTION
3
IR.21
(Classified Data Source)
2
4
AURORAGOLD Repository
UNCLASSIFIED STREAM
Raw Data Sets – Unclassified
4a
ENTITY NORMALIZATION
4c
Analysis By Exception; Some Analytic Decisions
4d
Exception Decision Information
4e
Analyzed Data Sets – Unclassified
4g
4f
CLASSIFIED STREAM
Raw Data Sets – Classified
4b
Exception Decision Information
Analysis By Exception; Some Analytic Decisions
ENTITY NORMALIZATION
Analyzed Data Sets – Classified
4h
File Outputs
Querying
All Users
5
VISUALIZATION
6
SIGINT Production Chain
9
All Appropriately Cleared Users
SCORPIOFORE; SIGINT Reporting
8
"AUTO"-MINIMIZATION
7
10
Supplementary Outputs:
1. Strong Selector and Tasking Management
2. Some selectors back to AGR inputs for tasking
3. Information outputs to other systems (i.e. RONIN)
4. Other??
S//SI//REL TO USA, FVEY

Fig. 6-3 AuroraGold Data Flow & Process Overview

IR.21 is the international roaming document and an important specification document for GSM international roaming operators to produce counterparty data, in order to enable their customers to use international roaming services overseas. The IR.21 document standard format is developed by the Global System for Mobile Communications Association (GSMA). Founded in 1995, the GSMA is an organization in the global mobile communications industry. Its members include nearly 800 mobile operators from 220 countries and regions, as well as more than 230 companies in a broader mobile ecosystem.

The NSA assessment suggested that IR.21 contained "the specific information necessary for targeting and exploitation", and could obtain GSM/UMTS mobile phone operator infrastructure, voice and data integration, UMTS technology migration and UMTS technology deployment and other technical details through IR.21 to support subsequent intelligence work.

Tab. 6-1 NSA Assessment of SIGINT Value of IR.21

IR.21 Field	What is it?	How is it used?
Mobile Country Code (MCC)/ Mobile Network Code (MNC)	A decimal digit code which uniquely identifies a mobile network. The MCC which identifies the country is used as the first three digits of any user's IMSI, followed by the two digit MNC which identifies the network within that country.	Provide unique identification of networks to identify network boundaries, interfaces, protocols, software, hardware, etc.

Mobile Subscriber Integrated Services Digital Network Number (MSISDN)	A number uniquely identifying a subscription in a GSM or a UMTS mobile network (the telephone number to the SIM card in a mobile/cellular phone).	Allow identification of real phone number dialed.
TADIG Codes	A number allocated by the GSMA for use as primary identifiers, both within file contents and file names. Also used as a more generic entity identifier in the mobile industry.	Identify the network for billing purposes and help identify targets.
Signaling Connection Control Part (SCCP)	A network layer protocol that provides extended routing, flow control, segmentation, connection-orientation, and error correction facilities in Signaling System 7 telecommunications networks.	Provides routing information within the Public Land Mobile Network and provides access to applications such as 800-call processing and calling card processing to identify targets and other information.
Subscriber Identity Authentication	This field indicates whether or not authentication is performed for roaming subscribers at the start of GSM service and the type of A5 cipher algorithm version in use.	It would also show the emergence of new cipher algorithms and support target analysis, trending and the development of exploits.
Mobile Application Part (MAP)	A SS7 protocol which provides an application layer for the various nodes in GSM and UMTS mobile core networks and GPRS core networks to communicate with each other in order to provide services to mobile phone users. The Mobile Application Part is the application-layer protocol used to access the Home Location Register, Visitor Location Register, Mobile Switching Center, Equipment Identity Register, Authentication Center, Short message service center and Serving GPRS Support Node (SGSN).	Provides a clearer understanding of network features when roaming agreement information is published. Current information about subscribers, mobility management and applications can be used for targeting and target development.
Network Element Information	Specific network components, their manufacturer, software & hardware versions, etc.	This specific information is necessary for targeting and exploitation. Includes core and radio interface information.
Packet Data Services Information	Packet Data Services identifies the affected GPRS networks. An Access Point Name is also included in this information. APNs can identify the type of service provided by GPRS networks provided to mobile users. APNs also help identify the network and operator's packet network involved in the IR.21 and could be used for targeting.	This data element also provides information on the WAP gateway being access and multimedia messaging services gateway IP addresses which is useful for target development. Insight into the GPRS Tunneling Protocol versions being used within the networks is provided as well. GPRS, EDGE and HSPA technologies are covered.

In order to obtain the IR.21 of each operator, operation AuroraGold used signal intelligence methods to monitor and intercept the data interaction between the MNO roaming coordinators and GSMA working groups and other relevant agencies, as well as more than 1200 email messages.

In addition to obtaining IR.21, operation AuroraGold continues to monitor industry organizations, such as GSMA and ITU, to obtain information on new technical standards, new global mobile communications technologies and their development trends as early as possible to support other links of the NSA SIGINT planning cycle.

Extended analysis

In the operation AuroraGold, the NSA targeted global mobile operators, and pertinently built its cyberattack capabilities by acquiring technology trends and other data intelligence. The NSA CamberDADA program exposed by Snowden in June 2015 showed the same US intelligence activity strategy. In the CamberDADA program[2], the NSA mainly utilized the traffic acquisition capabilities used by the US to invade global operators, monitored communications between anti-virus vendors and their users such as Kaspersky, and obtained new virus samples to assist in planning cyberattacks that could bypass detection and develop exploitable attack weapons. The follow-up targets of the program also include 23 major global cybersecurity vendors from 16 countries, including Chinese cybersecurity vendor Antiy.

In the operation AuroraGold, the NSA collected operators' IR.21 containing information on communications encryption, which could be used to crack encryption and eavesdrop on conversations. The Register, a British technology media, published an article analyzing the AuroraGold incident and pointed out that the NSA's Target Technology Trends Center (TTTC) worked within standard bodies like the GSM Association to get advanced copies of new security protocols so that it could work out how to break them ahead of deployment[3]. In fact, the NSA has always coveted the crypto system. In early September 2013, many US and UK media reported that the NSA had hidden backdoors in the SP 800-90A standard released by the National Institute of Standards and Technology (NIST)[4][5], confirming rumors that the industry had long worried and suspected. **The NSA has been systematically manipulating the crypto system for a long time and exploited vulnerabilities in encryption standards to carry out global surveillance, which has undermined global trust in cyber technology and caused great damage to the global cybersecurity ecosystem.**

References

[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

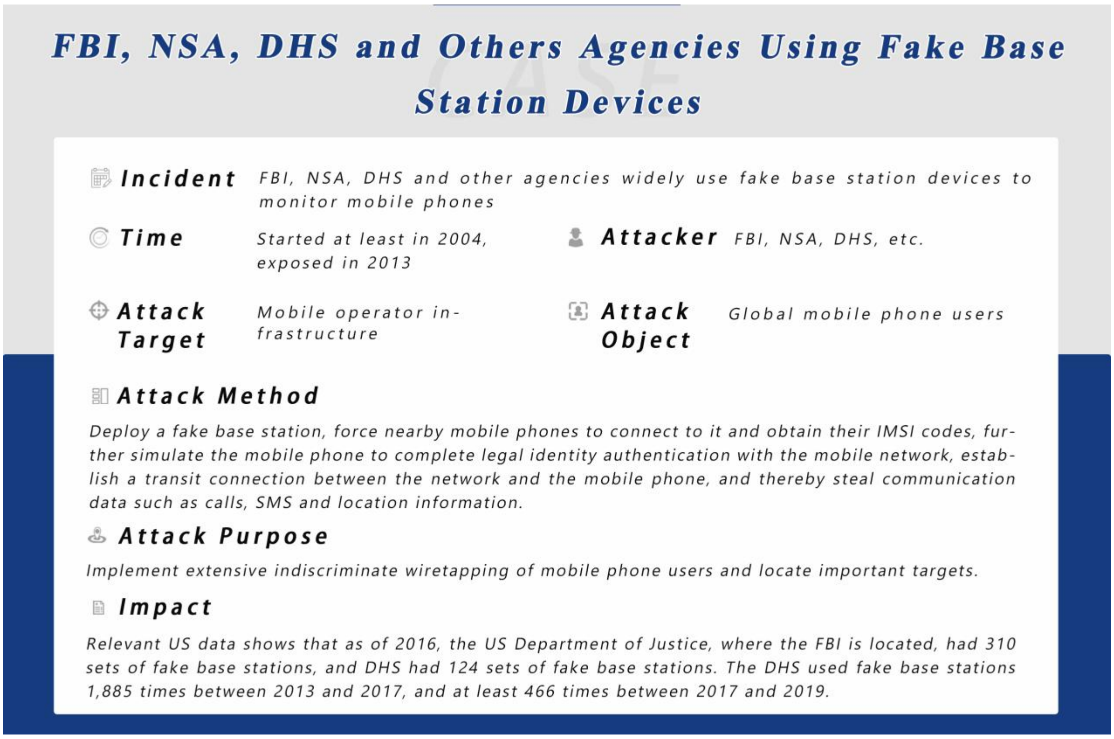
[3] Iain Thomson. The Register. Snowden files show NSA's AURORAGOLD pwned 70% of world's mobe networks. 2014. https://www.theregister.com/2014/12/04/snowden_files_show_nsas_auroragold_pwned_70_of_worlds_mobile_networks/

[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

Chapter 7. Camouflaged Base Stations – Fake Base Stations Are Widely Used to Monitor Mobile Phones

The International Mobile Subscriber Identity (IMSI) is used to identify mobile phone users worldwide. IMSI is located on the SIM card of a mobile phone and consists of 15 digits, including country code, mobile network code, subscriber identification code and other information. When the mobile phone establishes a connection with the mobile network, it uses IMSI to complete the authentication and legally accesses the network. Attackers use fake base stations to force mobile phones to connect to it, obtain the mobile phone's IMSI, simulate identity authentication, establish a transit connection between the network and the mobile phone, and thereby steal communication data. The US intelligence agencies and law enforcement agencies have long and extensively used Stingray and other fake base stations to monitor mobile phones.



FBI, NSA, DHS and Others Agencies Using Fake Base Station Devices

Incident FBI, NSA, DHS and other agencies widely use fake base station devices to monitor mobile phones

Time Started at least in 2004, exposed in 2013

Attacker FBI, NSA, DHS, etc.

Attack Target Mobile operator infrastructure

Attack Object Global mobile phone users

Attack Method

Deploy a fake base station, force nearby mobile phones to connect to it and obtain their IMSI codes, further simulate the mobile phone to complete legal identity authentication with the mobile network, establish a transit connection between the network and the mobile phone, and thereby steal communication data such as calls, SMS and location information.

Attack Purpose

Implement extensive indiscriminate wiretapping of mobile phone users and locate important targets.

Impact

Relevant US data shows that as of 2016, the US Department of Justice, where the FBI is located, had 310 sets of fake base stations, and DHS had 124 sets of fake base stations. The DHS used fake base stations 1,885 times between 2013 and 2017, and at least 466 times between 2017 and 2019.

Fig. 7-1 List of Cases of FBI, NSA, DHS and Others Agencies Using Fake Base Station Devices

Fake Base Stations Are Widely Used by the US Intelligence Agencies and Law Enforcement Agencies

On May 8, 2013, the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF) published a brief[1] disclosing that the FBI used invasive eavesdropping technology and device to collect mobile phone information. The device involved was Stingray, a fake base station manufactured by the US defense contractor Harris Corporation.

Stingray is an IMSI catcher[2] that works through a "man-in-the-middle" attack. The base station believes Stingray is a mobile phone, while mobile phone believes Stingray is a base station.

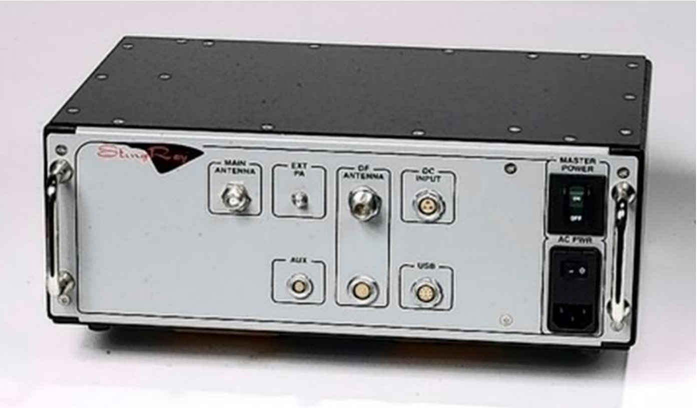


Fig. 7-2 Stingray Fake Base Station

Once the connection is established, Stingray is able to intercept communication content. It can not only collect IMSI and location information of mobile phones, but also steal call, SMS and web browsing information. When the user is using a mobile network of 3G or above, Stingray can force phones to downgrade to 2G, a less secure protocol, and tell the phone to use either no encryption or use a weak encryption that can be cracked, as a way to achieve surveillance purpose[3]. The Stingray family of devices can be mounted in vehicles, on airplanes, helicopters and unmanned aerial vehicles. Hand-carried versions are referred to under the trade name KingFish and can be used anywhere.

On July 31, 2020, The Intercept published an article[2], disclosing that the US law enforcement agencies use Stingray to locate targeted phones, obtain information such as SMS, emails and voice calls, and master the identity and address of the targeted phone holder, and obtain communication relationships with the assistance of operators through intelligence cooperation. The Stingray device can accurately locate the target within a meter range and lock the target by measuring the signal strength between the mobile phone and the Stingray device.

On November 13, 2014, The Wall Street Journal disclosed[4] that the US Marshals Service had installed a fake base station called "Dirtbox" on small general-purpose aircraft since 2007. The device is manufactured by Digital Receiver Technology (DRT), a subsidiary of the US military contractor Boeing, and is used to collect personal and location information from mobile phone users on a large scale[5]. The Dirtbox can scoop data from tens of thousands of mobile phones in a single flight, collecting their identifying information and general location. And it can accurately locate the targeted phone within three meters on the plane. Compared with Stingray on the ground, the Dirtbox in the air can collect more data and move over a wide area more conveniently and quickly.

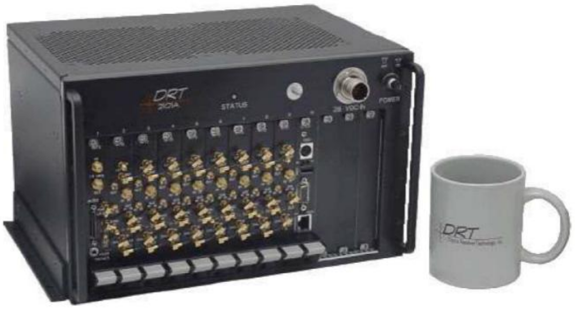


Fig. 7-3 Dirtbox (DRT 2101A) Fake Base Station

With the development of mobile network technology, the US intelligence agencies and law enforcement agencies are constantly updating and purchasing these devices. Harris Corporation has developed a variety of fake base stations for 3G and 4G networks. And the US intelligence agencies and law enforcement agencies also purchase fake base stations manufactured by Octasic, a Canadian company, whose devices are capable of targeting eight frequency bands including GSM (2G), CDMA2000 (3G), and LTE (4G)[6].

Fake base stations are widely used by the US government departments and the military. The American Civil Liberties Union[7] disclosed that Stingray and other IMSI catchers were used by many government agencies and military agencies such as the US Army, US Navy, US Marine

Corps, FBI, US Department of Homeland Security, and the US Marshals Service. In a media interview[8], an FBI agent described using Stingray more than 300 times over a decade and indicated that it was used on a daily basis by the US Marshals, the Secret Service and other federal agencies. Data disclosed by the American Civil Liberties Union and the US media showed that the DHS used Stingray 1,885 times between 2013 and 2017[9], and at least 466 times between 2017 and 2019[10]. The report of the US House Oversight Committee showed that the US Department of Justice had 310 sets of fake base stations, and DHS had 124 sets of fake base stations. From FY2010 to FY2014, the US Department of Justice spent more than $71 million on fake base station technology, and the US DHS spent more than $24 million on fake base station technology[11].

Fake Base Stations Become Avenues for Surveillance and Cyberattacks

Fake base stations turn mobile phones into surveillance tools. On July 22, 2013, The Washington Post published an article, which mentioned that as early as 2004, "a new NSA technique enabled the agency to find mobile phones even when they were turned off. JSOC troops called this 'The Find', and it gave them thousands of new targets in Iraq[12]." On June 6, 2014, the CNN website published an article titled *How the NSA can 'turn on' your phone remotely*[13], stating that the NSA sends a command to the baseband chip of the phone through a fake base station, telling the phone to fake any shutdown and stay on. While the phone on standby can either turn on the microphone for environmental wiretapping, or can send location information for locating.

Fake base stations become avenues for cyberattacks. According to an article on the website The Intercept[2], the fake base stations used by the US intelligence agencies could send phishing messages, and could also enable mobile phones to send and receive text messages through a server the military controls instead of the mobile carrier's server for surveillance purposes. The US intelligence agencies could potentially inject malware into targeted phones through fake base stations. If there were vulnerabilities in targeted phones' browser, they could also inject spying software onto specific phones or direct the browser of a phone to a website where malware can be loaded onto it.

Michael Hayden, the former director of the CIA, admitted that the NSA surveillance program did not play a role in counter-terrorism, but it allowed intelligence analysts to track people's online behavior[14]. **The US intelligence agencies and law enforcement agencies abuse fake base stations to conduct large-scale and indiscriminate surveillance of personal mobile phones by any means necessary, which greatly infringes on the communication rights and interests of citizens around the world, and poses a serious threat to the national security of other countries.**

References

[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.

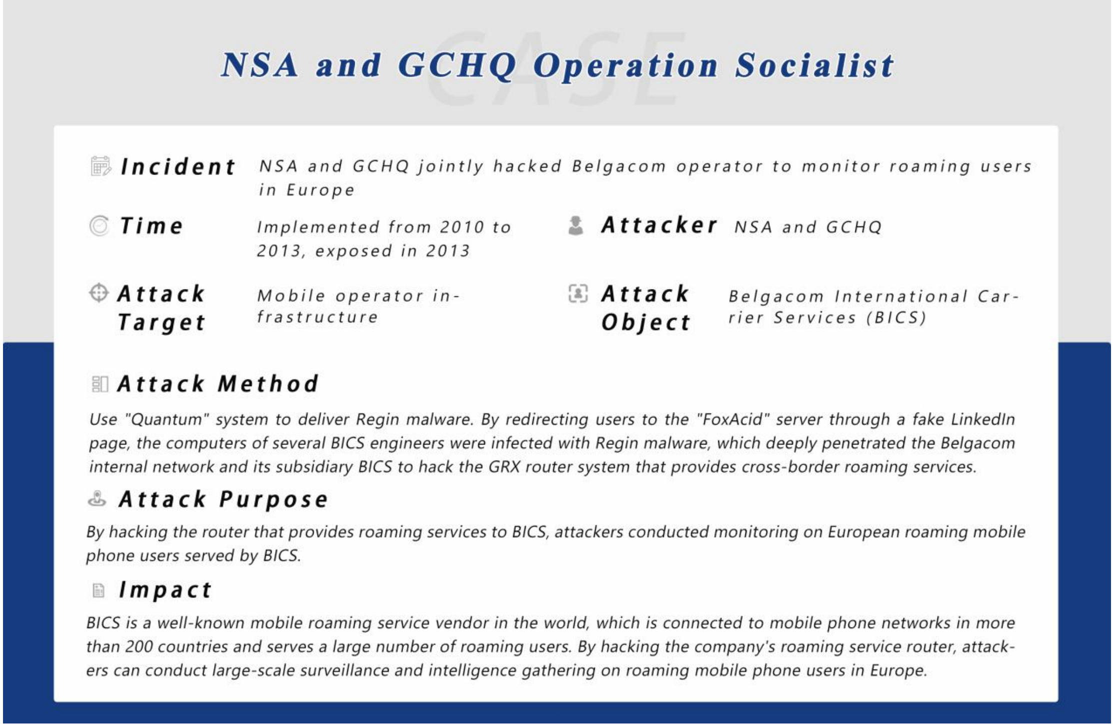
https://money.cnn.com/2014/06/06/technology/security/nsa-turn-on-phone

[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

Chapter 8. Hacking the Operator Intranet - Using Regin to Attack Mobile Network

Regin is a particularly powerful malware developed by the NSA and shared with partners of the FVEY countries, which has advanced technology, complex structure and strong "stealth" capabilities. It can customize functions and targeted deployment according to different targets to conduct remote monitoring and intelligence gathering. From 2010 to 2013, the NSA and GCHQ used Regin to jointly hack the internal networks of Belgacom and its subsidiary International Carrier Services, invaded the GRX router system that provides cross-border roaming services, and carried out targeted "man-in-the-middle attack" on roaming smartphones.



NSA and GCHQ Operation Socialist

Incident NSA and GCHQ jointly hacked Belgacom operator to monitor roaming users in Europe

Time Implemented from 2010 to 2013, exposed in 2013

Attacker NSA and GCHQ

Attack Target Mobile operator infrastructure

Attack Object Belgacom International Carrier Services (BICS)

Attack Method

Use "Quantum" system to deliver Regin malware. By redirecting users to the "FoxAcid" server through a fake LinkedIn page, the computers of several BICS engineers were infected with Regin malware, which deeply penetrated the Belgacom internal network and its subsidiary BICS to hack the GRX router system that provides cross-border roaming services.

Attack Purpose

By hacking the router that provides roaming services to BICS, attackers conducted monitoring on European roaming mobile phone users served by BICS.

Impact

BICS is a well-known mobile roaming service vendor in the world, which is connected to mobile phone networks in more than 200 countries and serves a large number of roaming users. By hacking the company's roaming service router, attackers can conduct large-scale surveillance and intelligence gathering on roaming mobile phone users in Europe.

Fig. 8-1 List of Cases of NSA and GCHQ Operation Socialist

Incident Review

On September 20 and November 11, 2013, Der Spiegel successively revealed that the NSA and GCHQ had jointly carried out Operation Socialist[1] from 2010, hacking into the GRX router system of Belgium Telecom International Carrier Service (BICS), which conducted targeted "man-in-the-middle attacks" on roaming smartphones. The incident drew widespread global attention, because it was the first revealed cyberattack that occurred among EU countries.

On December 13, 2014, The Intercept further reported Operation Socialist, saying that Belgium Telecom began to detect network anomalies in the summer of 2012, and it was only confirmed in June 2013 that its computer system had been infected with highly sophisticated malware. The malware "disguises itself as legitimate Microsoft software" to quietly steal data. The Regin cyberattack platform was a malware used by Operation Socialist. The documents leaked by Snowden indicated that GCHQ and NSA are the developers and operators of the Regin platform. From 2010 to 2013, GCHQ used the Regin platform to hack into Belgacom. As one of the largest roaming service operators in Europe, when foreign tourists enter Europe, many of them will connect to the international roaming network provided by Belgacom. Regin has entered the public's field of vision and has become a malware of continuous concern in the field of cybersecurity.

In June 2019, Reuters exclusively revealed that "the Western intelligence agencies hacked Russia's Google Yandex in late 2018"[3] saying that hackers implanted a rare malware Regin in the Russian search engine Yandex to spy on Yandex users' accounts. Vikram Thakur, technical director at the US Symantec Security Response said, "Regin is the crown jewel of attack frameworks used for espionage. Its architecture, complexity and capability sits in a ballpark of its own"[3]. The incident proved that Regin has been active in the next several years.

Traceability Analysis

On November 23, 2014, Symantec released an analysis report titled *Regin: Top-tier espionage tool enables stealthy surveillance*[4] saying, Regin is an extremely complex piece of software that can be customized with a wide range of different capabilities, which can be deployed depending on the different target. It is built on a covert framework that is designed to sustain long-term intelligence-gathering operations. It goes to extraordinary lengths to disguise itself and its activities on compromised computers. Its stealth activities combine many of the most advanced techniques.

Symantec reported that the main purpose of Regin is intelligence gathering and it has been implicated in data collection operations against government institutions, infrastructure operators, businesses, academics, and private individuals. Regin is a multi-stage, modular threat with the flexibility to load capabilities tailored to individual targets when required. This modular method has been seen in other sophisticated malware families such as Flamer and Weevil, while the multi-stage loading architecture of Regin is similar to that seen in the Duqu/Stuxnet family of threats. Regin is capable of installing a large number of additional payloads, some highly customized for the targeted computer. More advanced payload modules designed with specific goals in mind were also found in Symantec's investigations.

On November 24, 2014, the day after Symantec released its report, Kaspersky released a more detailed technical analysis of Regin titled, *The Regin Platform Nation-State Ownage of GSM Network*[5]. In the report, Kaspersky pointed out that "Regin is a cyberattack platform, which the attackers deploy in victim networks for conducting total remote control at all levels." Kaspersky found that "the most interesting aspect we have found so far regarding Regin relates to an infection of a large GSM operator."

Kaspersky reported that Regin is the first known attack platform capable of penetrating and monitoring GSM networks in addition to conducting other standard espionage tasks. The attackers behind the platform have compromised computer networks in at least 14 countries around the world. The main targets of the group include telecom operators, governments institutions, financial institutions, research institutions, multinational political bodies and individuals involved in advanced mathematical/cryptographic research.

On January 17, 2015, Der Spiegel published a copy of the FVRY countries malware program code-named QWERTY based on information exposed by Snowden. QWERTY is designed to invisibly record all key strokes from the infected Windows computer. Through careful comparison, Kaspersky analysts concluded that the "QWERTY" is identical in functionality to the Regin 50251 plugin[6]. Kaspersky has technically proved Regin's homology to QWERTY, another NSA spying module. Kaspersky concluded that the QWERTY developers and the Regin developers are the same or working together.

Extended Analysis

According to Der Spiegel[8], the US and Western intelligence agencies used "Quantum" system to deliver Regin malware in the attack on Belgacom. By redirecting users to "FoxAcid" server through fake LinkedIn pages, the computers of several BICS engineers were infected with Regin malware, which enabled the GCHQ spies to deeply penetrate the Belgacom internal network and its subsidiary BICS to hack the GRX router system that provides cross-border roaming services, and carried out targeted "man-in-the-middle attack" on roaming smartphones. The report pointed out that **the attack operations could capture the entire internet communication traffic of the targeted mobile phone, track the location or implant spying software to conduct large-scale surveillance on roaming mobile users.**

According to Kaspersky, Regin's ability to penetrate and monitor GSM network is perhaps the most unusual and interesting aspect of these operations. In today's world, people have become too reliant on mobile phone networks that use older communication protocols, while there is almost no security assurance for end users. Although all GSM networks have embedded mechanisms that allow law enforcement agencies to track suspects, there are other entities that can also acquire this capability and then abuse it to launch other types of attacks against mobile users.

In fact, the NSA's attacks on telecom operators are long-standing. Antiy released a report titled *方程式组织 CDR 解析器样本分析报告（Equation Group CDR Parser Sample Analysis Report*)[9], based on the information disclosed by the Shadow Broker in 2016, analyzed the analytic extraction tool of Equation Group for telecom Call data (Call Detai Record,CDR) in detail. CDR data generated by telecom devices such as telephone switches, including various call attributes such as call time, duration, completion status, source number, and destination number. The CDR parser of Equation Group can match the specified matching conditions (such as time range, etc.) to collect CDR files, and then parse the collected CDR file data based on the contents of the encrypted parameter file (such as location area code, phone number, etc.). The Antiy report pointed out that this tool is only responsible for data screening, acquisition, and encrypted storage, and is not responsible for return transmission. This operation method is in line with the US's modular operation and strict encryption habits and characteristics.This operational method is consistent with the modular operation and strict encryption habits and characteristics of the US. After the intrusion, the attacker can construct various conditional rules by parameters for targeted data acquisition, and use data decryption and data return tools to conduct a complete intrusion and secret theft attack.

As a critical node for data communication and aggregation, operators have great strategic value in the eyes of the US intelligence agencies and have been their target for a long time. According to the information exposed by Snowden, MAINWAY and NUCLEON in STELLARWIND program are specialized in collecting global telecommunications call data and wiretapping. MAINWAY obtains relevant data by establishing cooperation with operators, while NUCLEON intercepts the conversation content and keywords in telephone calls to obtain specified data. **The US intelligence agencies implement their all-round and in-depth network intelligence activities in the communication field by attacking operators.**

References

[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/

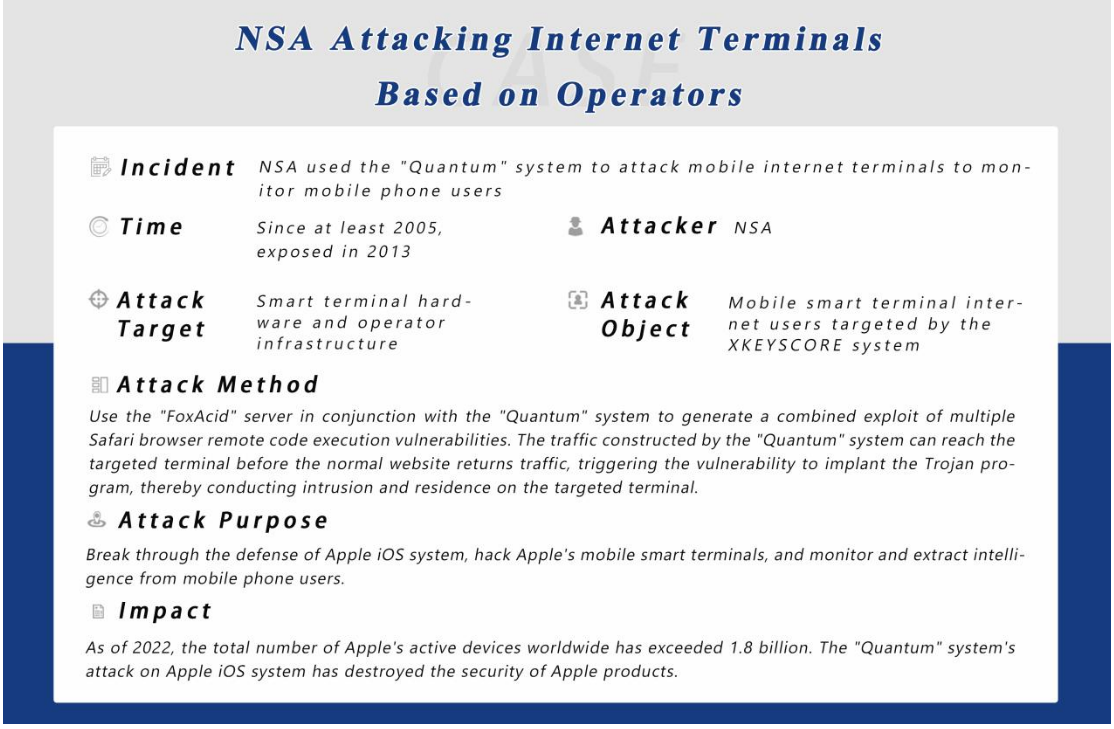
[7] Pierluigi Paganini. REGIN AND QWERTY KEYLOGGER ARE LINKED WITH FIVE EYES INTELLIGENCE. 2015.
https://securityaffairs.com/32818/intelligence/regin-qwerty-keylogger-fiveeyes.html

[8] GCHQ Used Fake LinkedIn Pages to Target Engineers. 2013.

[9] Equation Group CDR Parser Sample Analysis Report. 2024.
https://www.antiy.cn/research/notice&report/research_report/Equation_CDR.html

Chapter 9. Attacking Internet Terminals Based on Operators - The Attack Ability of "Quantum" System on Mobile Phones and Internet PCs

All mobile terminals such as mobile phones and various internet terminals rely on the operator system to access the network and various applications. The US intelligence agencies uses the "Quantum" system to invade the switching and routing network equipment of operators in various countries, transforming the global operation system into a delivery system that can be used to attack Internet users. The attack scope includes smart mobile terminals such as Android and iOS, and various internet PCS and server products. The "Quantum" system, first exposed by Snowden in 2013, was developed and used by the Office of Tailored Access Operation (TAO), a subsidiary of the NSA, which is a set of engineering systems and intrusion tools for conducting cyberattacks on high-value targets.



NSA Attacking Internet Terminals Based on Operators

Incident NSA used the "Quantum" system to attack mobile internet terminals to monitor mobile phone users

Time Since at least 2005, exposed in 2013

Attacker NSA

Attack Target Smart terminal hardware and operator infrastructure

Attack Object Mobile smart terminal internet users targeted by the XKEYSCORE system

Attack Method

Use the "FoxAcid" server in conjunction with the "Quantum" system to generate a combined exploit of multiple Safari browser remote code execution vulnerabilities. The traffic constructed by the "Quantum" system can reach the targeted terminal before the normal website returns traffic, triggering the vulnerability to implant the Trojan program, thereby conducting intrusion and residence on the targeted terminal.

Attack Purpose

Break through the defense of Apple iOS system, hack Apple's mobile smart terminals, and monitor and extract intelligence from mobile phone users.

Impact

As of 2022, the total number of Apple's active devices worldwide has exceeded 1.8 billion. The "Quantum" system's attack on Apple iOS system has destroyed the security of Apple products.

Fig. 9-1 List of Cases of NSA Attacking Internet Terminals Based on Operators

Incident Review

On June 9，2023，Antiy released a report titled *"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* (*"Quantum" System Breaks Down iPhone - Analysis of Historical Samples of Equation Group's Attack on iOS System)*[1], revealing that the Equation Group, a subsidiary of NSA launched attacks on internet terminals of iOS system on the network side based on the "Quantum" platform in the early years, and exploited browser vulnerabilities to deliver backdoor for penetration activities. Previously, Kaspersky released an analysis report tiled *Operation Triangulation: iOS Devices Targeted with Previously Unknown Malware*[2]*,* pointing out that the malware attacked iOS devices through a "zero-click" approach.

The "Quantum" system attacks on the iOS systems disclosed by Antiy's report and the Operation Triangulation attacks exposed by Kaspersky come from the Equation Group, but the attack paths and samples revealed by the two reports are completely different. They are two different attack methods. The attack exposed by Kaspersky relied on iMessage vulnerabilities to deliver samples;the attacks of the Equation Group on the iOS platform discovered by Antiy may have appeared in 2013 or earlier. The attack samples were delivered through the "Quantum" system.

Traceability Analysis

The iOS attack samples analyzed by Antiy report are not regular iOS APP installation package, but the Trojan targeting the underlying iOS. The main body of the Trojan is disguised as a PE format file named regquerystr.exe for delivery. Its true format is the Mach-O executable program of the ARM architecture, using vulnerabilities or sandbox escape to complete the release and execution of the backdoor program. The Trojan first detects the kernel version and user permissions, and then releases the backdoor mvld, which is mainly used to collect device information and communicate with remote servers. After the program runs, it will generate log files and delete its own files.

The attack sample contains 13 command codes, which are very similar to the DoubleFantasy series instructions of the Equation Group Windows and Solaris Trojan exposed by Antiy[3]. In addition, the mvld Trojan internally decrypted the information FAID, in which ace02468bdf13579 is consistent with the mandatory unique identification code required for NSA operations previously exposed. This identification also exists in the SecondDate weapon in the Equation arsenal leaked by the Shadow Brokers. The information all points to: the Trojan comes from the Equation Group , a subsidiary of the US intelligence agency NSA.

Antiy reported that by comparing and analyzing the iOS Trojan with the DoubleFantasy Trojan equipment sequence of Equation Group, we can draw the following results: they are almost identical in functions, behaviors, algorithms, information collection and command control sets. The Trojan uses the most commonly used value 0x47 in the Equation Group encryption algorithm. The collection terminal information format is consistent with DoubleFantasy, and the control instruction code structure is basically consistent with DoubleFantasy, which fully proves the connections between the iOS Trojan and the Equation Group.

Revealing the Secrets of "Quantum" System

The "Quantum" system project, first exposed by Snowden in 2013, was initiated by the NSA and jointly implemented with GCHQ and the National Defence Radio Establishment (Swedish: Försvarets radioanstalt, FRA). It is used to develop and operate engineering systems and intrusion tool sets that carry out cyberattacks to conduct intervention and control of network status in cyberspace, which was developed and used by TAO under the NSA.

As Wired reported in April 2015[4], the hacking technology known as "Quantum Injection" has been used by NSA and its partner GCHQ to break into high-value, hard-to-reach systems and implant malware since 2005. "Quantum Injection" works by hijacking the targeted browser when it attempts to access a web page and forcing it to access malicious web pages. The "highly successful" technology allowed the NSA to implant 300 kinds of malware on computers around the world in 2010 by hijacking them to the malicious web pages.

The "Quantum Injection" technology requires the fast-acting servers relatively near a target's machine that are capable of intercepting browser traffic swiftly in order to deliver malicious web page to the targeted machine before the legitimate web page reach. To achieve this, NSA used the code-named "FoxAcid" server and the special high-speed server known as "Shooter" placed at key points around the internet. The closer the traffic-sniffing and shooter machines are to the target, the more likely the rogue servers will win the race to the victim's machine.

The operational fulcrum of the "Quantum" system is the intrusion and hijack of critical routers and gateways of network communication infrastructure, thereby having the capabilities of analyzing and hijacking the online process of the attack target. First, by relying on the XKEYSCORE system, it identifies the relevant IP, code number, link, identity account or other identification of the Internet device to determine whether it meets the requirements for the attack target and verifies whether the attack has been successfully carried out on the device. If it is the target to be attacked, it will further determine whether there are available vulnerabilities, and then selects the corresponding tools to perform secret intrusion. Antiy drew a spectrum conjecture diagram of the attack capability of the "Quantum" system in the report, believing that the "Quantum" attack capabilities completely cover all major internet terminals in the world, including various types of PCs, servers, mobile smartphone terminal devices and related browsers[1].

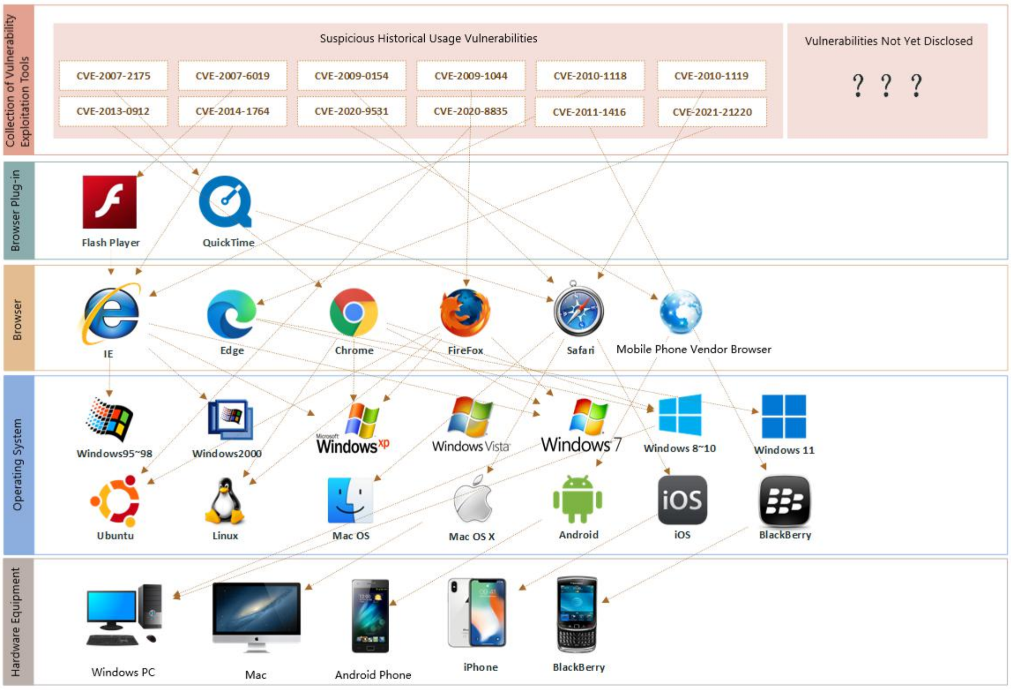


Fig. 9-2 Graphical Analysis of Attackable Scenarios of the Quantum System Drawn by Antiy

Extended Analysis

On the one hand, the operation capabilities of the "Quantum" system come from the large number of undisclosed vulnerability resources and the reserve of vulnerability exploitation tools under its control. On the other hand, they come from the degree of attack control of the Equation Group on the global critical network communication devices. For example, to trick targets into accessing the "FoxAcid" server, NSA relied on its secret cooperative relationship with US telecommunications companies to deploy "Shooter" server at critical locations in the Internet backbone network[5]. It can be seen that **the close cooperation between the US intelligence agencies and the owners of telecommunication infrastructure is the key to the success of its cyberattack operations. It is also an important part of the US pre-preparation of the global cyberspace battlefield. It achieves proactive pre-preparation by invading and hijacking global operators to shape the cyberspace environment for subsequent cyberattacks operations.**

The "Quantum" attack mechanism not only causes harm to mobile phones and other internet terminals, but has actually become an important means of the systematic deployment of US cyber military operations. Through the "Quantum" system, the US malicious code can be deployed on switches and routers in the key targeted networks after cross-network intrusion, including network equipment such as firewalls, thereby building an intrusion bridgehead on the intranet. It will improve the mobility of cyber forces, enable them to enter and control key terrain when necessary, and **ensure that the US military conduct expeditionary cyberspace operations when necessary, without establishing a physical presence in foreign territories for power projection.**

In summary, the "Quantum" delivery system, the vulnerability library for browsers and network clients, and the capability system of the A2PT organization not only provide support and guarantee for the US military operations in cyberspace, but **make all PCs and mobile devices at risk of being attacked and penetrated by the US intelligence agencies, thus putting mobile phone users and internet users around the world under the "Quantum" hanging sword of Damocles.**

References

[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/

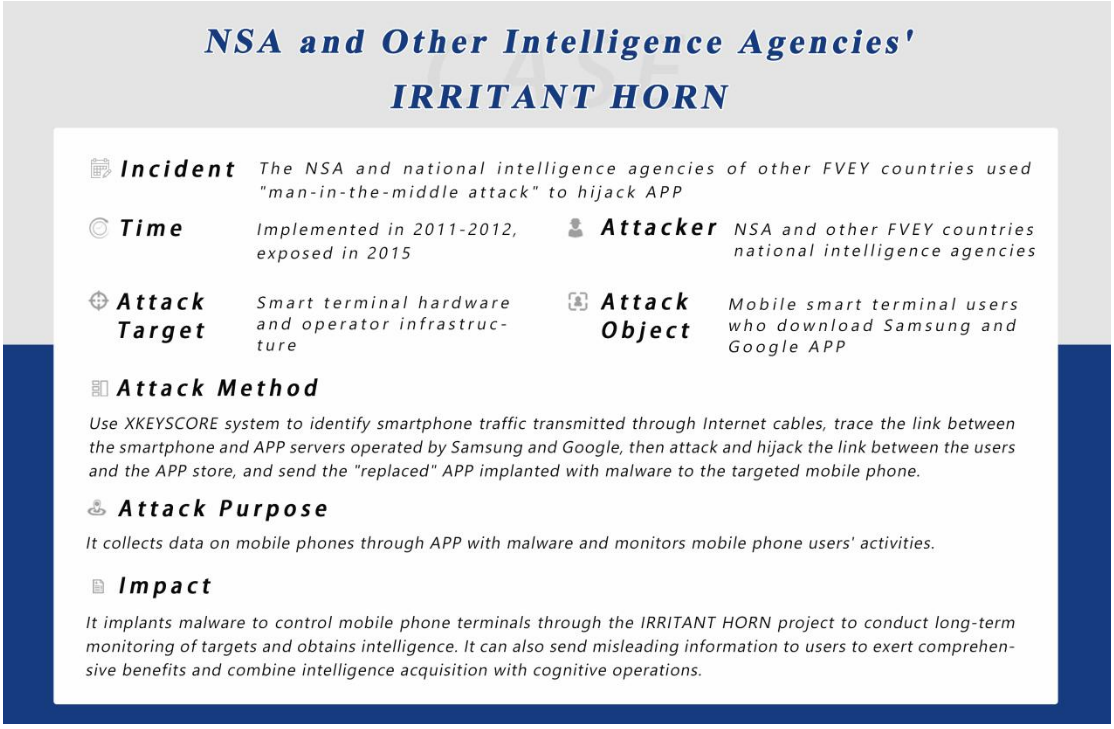
[3] 从“方程式”到“方程组” EQUATION攻击组织高级恶意代码的全平台能力解析. 2016. https://www.antiy.com/response/EQUATIONS/EQUATIONS.html

[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

Chapter 10. APP Replacing - Implanted Attacks of IRRITANT HORN

In the era of mobile internet, the rich functions of mobile smart terminals such as mobile phones come from the support of various applications (APP). The official APP store of mobile phone vendors and operating system suppliers provide users with safe and convenient download channels. However, the huge trusted resource that can reach users' mobile phones has also become a coveted target for network attackers. The leaked information showed that from 2011 to 2012, the NSA and national intelligence agencies of other FVEY countries launched the IRRITANT HORN project to tamper users' downloaded APP with malware through traffic hijacking to hack users' mobile phones.



NSA and Other Intelligence Agencies' IRRITANT HORN

Incident: The NSA and national intelligence agencies of other FVEY countries used "man-in-the-middle attack" to hijack APP

Time: Implemented in 2011-2012, exposed in 2015

Attacker: NSA and other FVEY countries national intelligence agencies

Attack Target: Smart terminal hardware and operator infrastructure

Attack Object: Mobile smart terminal users who download Samsung and Google APP

Attack Method

Use XKEYSCORE system to identify smartphone traffic transmitted through Internet cables, trace the link between the smartphone and APP servers operated by Samsung and Google, then attack and hijack the link between the users and the APP store, and send the "replaced" APP implanted with malware to the targeted mobile phone.

Attack Purpose

It collects data on mobile phones through APP with malware and monitors mobile phone users' activities.

Impact

It implants malware to control mobile phone terminals through the IRRITANT HORN project to conduct long-term monitoring of targets and obtains intelligence. It can also send misleading information to users to exert comprehensive benefits and combine intelligence acquisition with cognitive operations.

Fig. 10-1 List of Cases of the NSA and Other Intelligence Agencies' IRRITANT HORN

Incident Review

On May 21, 2015, the Canadian Broadcasting Corporation (CBC), The Intercept and other

Western media and related institutions published an article[1] that exposed the implementation of the IRRITANT HORN project by the NSA and national intelligence agencies of other FVEY countries, pointing out that "NSA plans to hijack Google App Store to attack smartphones." The leak of the IRRITANT HORN project revealed the shady story of the long-term attack and monitoring on mobile phone users by the national intelligence agencies of FVEY countries led by the US.

Top-secret documents leaked by Snowden revealed that[2] the IRRITANT HORN project was jointly launched by the NSA and national intelligence agencies of other FVEY countries. By hijacking download links from Google and Samsung APP stores, intelligence agencies modified the content of data packets passed between the targeted smartphone and the APP server when users downloaded or updated APPs, and then sent them to the phone to trick users into installing "transformed" APP implanted with malware. Attackers exploited vulnerabilities in mobile phones' APP to closely monitor targeted mobile phones, collected massive amounts of users information, and carried out intelligence extraction operations.

Previously, documents leaked by Snowden have shown that the national intelligence agencies of the FVEY countries have designed spyware for iPhone and Android smartphones. After infecting the targeted phones, it can acquire emails, text messages, history, call records, videos, photos and other stored files. But how the intelligence agencies of the FVEY countries infected the targeted phones with its spyware is not known. Apparently, the exposure of the IRRITANT HORN project allowed the outside world to understand the "man-in-the-middle attack" activities of the national intelligence agencies of the FVEY countries[1].

Reveal the Secrets of the IRRITANT HORN Project

To implement the IRRITANT HORN project, the intelligence agencies of the FVEY countries led by the US established the "Network Tradecraft Advancement Team (NTAT)", which includes intelligence officers from the US, Canada, the UK, New Zealand, and Australia. From November 2011 to February 2012, NTAT held a series of secret technology seminars in Australia and Canada to find the new ways to use smartphone technology to monitor mobile users, plan to hijack the data links in Google and Samsung APP stores, and infect smartphones with spyware.

NTAT used XKEYSCORE system to identify smartphone traffic transmitted through Internet cables, traced the link between the smartphone and APP servers operated by Samsung and Google, then attacked and hijacked the link between the users and the APP store, and sent APP implanted with malware to the targeted mobile phone to trick users to install it. These implanted spyware can collect data from the phone without the users' noticing.

In order to respect agreements not to spy on each others' citizens, the intelligence agencies of the FVEY countries focused their attention on APP servers in non-FVEY countries, including France, Switzerland, the Netherlands, Cuba, Morocco, the Bahamas and Russia. The intelligence agencies also sought to match their targets' smartphone devices to their online activities, using databases of emails, chats and browsing histories kept in the FVEY countries powerful XKEYSCORE tool to help build profiles on the people they were tracking[3].

NTAT also discovered security vulnerabilities in UC Browser, which is widely used in China, while looking for a way to break into mobile APP store servers. The UC Browser APP leaked users' phone numbers, SIM card numbers, and device details to servers in China, which facilitated the theft of Chinese users information by the IRRITANT HORN project[1]. Citizen Lab has discovered "major security and privacy issues" after analyzing the corresponding version of UC Browser for Android, pointing out that it can leak a variety of data, including some users' search queries, SIM card numbers and unique device identification numbers that can be used to track people. Analysis report by Citizen Lab confirmed the authenticity of the privacy vulnerabilities in UC Browser discovered by the FVEY countries[4].

But the intelligence agencies of the FVEY countries wanted to do more than just use APP stores as a launching pad to infect phones with spyware. They were also keen to find ways to hijack phones as a way of sending "selective misinformation to the targets' handsets" that are used to spread propaganda or confuse adversaries to conduct cognitive warfare[1].

Extended Analysis

The IRRITANT HORN project relies on the NSA's top-secret surveillance project

XKEYSCORE to conduct traffic analysis, screen targets, select attack paths, and establish tracking personnel files, so that intelligence agencies can have a more comprehensive and specific understanding of surveillance objects and conduct more targeted intelligence collection operations. The XKEYSCORE project provides strong data support for the targeted screening and continuous monitoring of the IRRITANT HORN project, which fully reflects the powerful systematic monitoring and attack capabilities of the US intelligence agencies. In addition, the traffic hijacking and "man-in-the-middle attack" way based on the IRRITANT HORN project are similar to the "Quantum" system. There is a reason to suspect that the hijacking and delivery system of the IRRITANT HORN project on the traffic side may be the "Quantum" system. The function of IRRITANT HORN project may be carried by the "Quantum" system.

The US and Western intelligence agencies used the IRRITANT HORN project to implant malware to control targeted mobile phone terminals and implement long-term surveillance and secret theft. At the same time, it is also possible to send targeted misleading information to users through implanted malware combining intelligence acquisition with cognitive operations to obtain greater comprehensive intelligence benefits. The IRRITANT HORN project is part of the US huge network intelligence operating system project, supporting its spying and wiretapping activities against mobile smart terminals around the world.

References

[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/

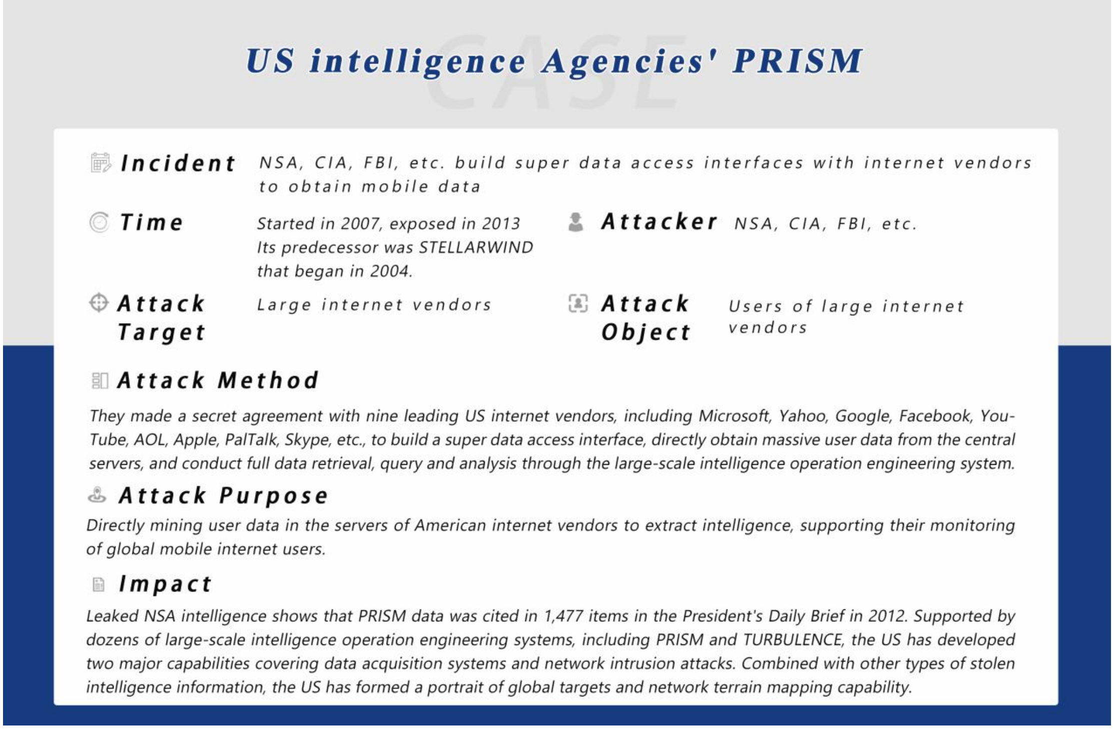
[2] Five Eyes presentation: Synergising Network Analysis Tradecraft.
https://www.documentcloud.org/documents/2083944-uc-web-report-final-for-dc.html

[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/

Chapter 11. The Conspiracy Behind PRISM - Building Super Data Access Interface

No matter large internet vendors such as Google, Facebook, or smartphone vendors such as Apple, or basic IT vendors such as Microsoft, all use mobile APP as the main form to provide services for users. The APP has the ability to collect basic user information, operational behavior, and other data. These collected data are aggregated into the data center of vendors that provide services. Relying on various APP applications and user interaction, large internet platform vendors store APP data on their platforms, and PRISM builds a super interface for accessing these data. The PRISM program disclosed by Snowden revealed the conspiracy of the US intelligence agencies to collect intelligence by using internet platforms and super data access interfaces provided by vendors.



US intelligence Agencies' PRISM

Incident NSA, CIA, FBI, etc. build super data access interfaces with internet vendors to obtain mobile data

Time Started in 2007, exposed in 2013 Its predecessor was STELLARWIND that began in 2004.

Attacker NSA, CIA, FBI, etc.

Attack Target Large internet vendors

Attack Object Users of large internet vendors

Attack Method

They made a secret agreement with nine leading US internet vendors, including Microsoft, Yahoo, Google, Facebook, YouTube, AOL, Apple, PalTalk, Skype, etc., to build a super data access interface, directly obtain massive user data from the central servers, and conduct full data retrieval, query and analysis through the large-scale intelligence operation engineering system.

Attack Purpose

Directly mining user data in the servers of American internet vendors to extract intelligence, supporting their monitoring of global mobile internet users.

Impact

Leaked NSA intelligence shows that PRISM data was cited in 1,477 items in the President's Daily Brief in 2012. Supported by dozens of large-scale intelligence operation engineering systems, including PRISM and TURBULENCE, the US has developed two major capabilities covering data acquisition systems and network intrusion attacks. Combined with other types of stolen intelligence information, the US has formed a portrait of global targets and network terrain mapping capability.

Fig. 11-1 List of Cases of the US intelligence Agencies' PRISM

Incident Review of PRISM

In June 2013, Snowden handed over two top-secret documents to The Guardian and The Washington Post, and agreed on a publication time with the media. On June 6, 2013, The Guardian first exposed the secret program PRISM code-named by the NSA[1], revealing the inside story of the US intelligence agencies secretly monitoring users around the world through American technology companies, which caused strong repercussions in the international community. The Washington Post carried out a follow-up report on June 7[2], stating that the NSA and the FBI started a secret surveillance plan PRISM in 2007, which directly accessing the central servers of large US technology companies to mine data and collect intelligence. Nine international internet giants participated in this program, including Microsoft, Yahoo, Google, Facebook, YouTube, AOL, Apple, PalTalk and Skype. The NSA and the FBI tapped directly into the central servers of nine leading US internet companies to extract audio and video chats, photographs, emails, documents and connection logs that enable analysts to track global targets, according to a top secret document obtained by The Washington Post.

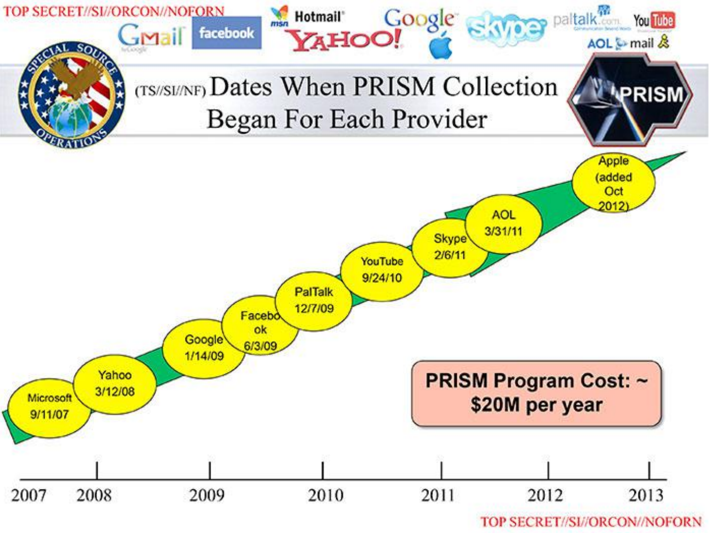


Fig. 11-2 Large American Technology Companies Involved in PRISM

According to The Washington Post[2], the NSA regarded the identities of its private partners as PRISM's most sensitive secret, fearing that the companies would withdraw from the program if exposed. "98 percent of PRISM production is based on Yahoo, Google and Microsoft; we need to make sure we don't harm these sources." An internal presentation of the NSA described the new tool as the most prolific contributor to the President's Daily Brief, which cited PRISM data in 1,477 items in 2012. According to the documents obtained by The Washington Post, "NSA reporting increasingly relies on PRISM" as its leading source of raw material, accounting for nearly 1 in 7 intelligence reports. The Washington Post reported on December 4, 2013[3] that the NSA is gathering nearly 5 billion records a day on the whereabouts of mobile phones around the world, enabling the agency to track the movements of individuals and map their relationships. Obviously, the NSA's powerful data collection and intelligence mining capabilities are inseparable from the PRISM program.

Tab. 11-1 Details of American Technology Companies' Participation in PRISM

Vendors	**Time**	**Data resources that may be accessed**
Microsoft	September 11, 2007	Emails, user data, files
Yahoo	March 12, 2008	Search terms, emails, user data, files
Google	January 14, 2009	Search terms, emails, text messages, call records, contact information, user passwords, files, user data, etc
Facebook	June 3, 2009	User data, contacts, photos, location information
PalTalk	December 7, 2009	Chat - video, voice
YouTube	September 24, 2010	Video
Skype	February 6, 2011	Chat - video, voice
AOL	March 31, 2011	Emails, user data, files
Apple	October 2012	Emails, text messages, call records, contact information, user data, files, user passwords, location information, chat records, etc

Operation of PRISM

According to documents leaked by Snowden, the US government launched the STELLARWIND program to conduct large-scale wiretapping and intelligence gathering operations in 2004. Later, STELLARWIND was split into PRISM, MAINWAY, MARINA and NUCLEON, which were implemented by the NSA. PRISM is a top-secret intelligence collection action that has been implemented since 2007, mainly using data interfaces provided by major internet companies in the United States. MAINWAY and MARINA respectively store and analyze hundreds of millions of "metadata" on communications and the Internet. NUCLEON is responsible for intercepting the conversation content and keywords of telephone callers. Compared with MAINWAY and MARINA, NUCLEON focuses more on obtaining information, and realizes daily monitoring by intercepting calls and the locations mentioned by callers. PRISM and these intelligence collection programs together constitute a systematic intelligence operation capability, allowing the US intelligence agencies to achieve a complete landscape of global targets like internet personnel, channels and devices, so as to form more accurate locating and intelligence extraction capabilities.

In the era of mobile internet, large technology companies and internet platforms store massive user data, including personal information, social activities, online shopping records, geographical location information, etc. It is very valuable for intelligence agencies to carry out national portraits, track individuals' activities, whereabouts and possible related events, and is a very important source of intelligence. At the same time, these platform vendors also host a large number of government and enterprise services, including not only the above-mentioned data, but also national economic data, industrial data, social data, etc., which are important strategic data assets of the country. PRISM has taken advantage of the rich data resources of large technology companies and internet platforms to carry out large-scale monitoring and intelligence gathering operations on global users.

There has been "continued exponential growth in tasking to Facebook and Skype" according to the PRISM slides[2]. With a few clicks and an affirmation that the subject is believed to be engaged in terrorism, espionage or nuclear proliferation, an analyst obtains full access to Facebook's "extensive search and surveillance capabilities against the variety of online social networking services." According to a separate "User's Guide for PRISM Skype Collection", that service can be monitored for audio when one end of the call is a conventional telephone and for any combination of "audio, video, chat, and file transfers" when Skype users connect by computer alone. Google's offerings include Gmail, voice and video chat, Google Drive files, photo libraries, and live surveillance of search terms.

In the document, the NSA hails PRISM as "one of the most valuable, unique and productive accesses for NSA"[1]. It boasts of what it calls "strong growth" in its use of PRISM to obtain communications. The document highlights the number of obtained communications increased in 2012 by 248% for Skype. There was also a 131% increase in requests for Facebook data, and 63%

for Google.

According to Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendment Act enacted by Congress in 2008, the PRISM program allows the US intelligence agencies to collect online communication data of non-US citizens abroad without obtaining approval. Unlike "traditional" FISA surveillance, Section 702 does not require that the surveillance target be a suspected terrorist, spy, or other agent of a foreign power. Section 702 only requires that the targets be non-US persons located abroad, and that a "significant purpose" of the surveillance be to obtain "foreign intelligence information"[4].

The design of such a legal system puts the hegemony of the United States above the privacy protection for global users, and opens the door for the US intelligence agencies to wantonly violate the privacy of foreign citizens and indiscriminately collect intelligence information from other countries.

Section 702 prohibits the targeting of any United States persons or anyone assessed to be located in the United States[5]. In 2018, the Foreign Intelligence Surveillance Court (FISC) reported that the FBI had conducted thousands of queries for Americans' data without proper justification[6]. In 2022, the Speaker of the House and the House Judiciary Chairman wrote to FBI Director to call for reforms to address concerns they had about FBI oversight of the program and their fear that the FBI has disregarded Americans' constitutional rights in the course of using the authority[6]. It can be seen that the US intelligence agencies have actually broken through the restrictions of Section 702 and invisibly expanded the surveillance targets to US citizens.

In a sense, the US government's attempt to prove strict control over the FBI's wiretapping powers is actually a smokescreen. Such behavior instead allows intelligence agencies such as the CIA and NSA to have unrestricted access to all global data through PRISM.

Deleterious Effect of PRISM

As the birthplace of the Internet, the US IT industry has always led the development direction of global IT technology and internet technology, and has obvious first-mover advantages in technology and application fields. Many of the world's leading technology companies, such as

Apple, Microsoft, Google, Facebook, etc., are headquartered in the United States. These companies play a leading role in technology research and development and market share, and have a monopoly position in related global technology fields. It is precisely because of the first-mover advantage of the United States in the IT and the Internet fields, combined with the "home court" advantage that large internet platforms and software and hardware vendors are headquartered in the United States, that internet platforms and vendors in the United States have very convenient conditions to collect user privacy data and operational data of governments and enterprises. Internet platforms not only collect user information, but also provide data backup functions. For example, Google's backup function will send user data to Google's backup servers, and Google's password saving function can save various sensitive passwords of users. Once the information is leaked, it will cause huge harm.

Since the PRISM incident was exposed in 2013, at this time, mobile apps had not fully replaced PC browsers as the main entrance for individuals to use the Internet, resulting in the public's understanding of PRISM still staying in the service access based on PC browsers and clients. Today, global users basically rely on various internet services provided by mobile apps, such as mail communication, instant communication, social platforms, financial payment, shopping, navigation and travel services. Common apps include Chrome, Gmail, Google Maps, Youtube, Facebook, Safari, iMessage, FaceTime, iCloud Drive, Skype, eBay, PayPal, etc. The generated service data are stored in internet platforms and vendor's databases. PRISM has built a "super access interface" for the US intelligence agencies to the databases of internet enterprises, supporting the US intelligence agencies' ability to access all these data.

The US intelligence agencies made a secret data mining agreement with large internet platforms and vendors, which not only violated the original intention of users to authorize internet platforms and vendors to collect data, but also regarded users as "lambs to the slaughter", making them the targets of indiscriminate large-scale monitoring and secret theft operations.

Although the US intelligence community has built large-scale data infrastructure such as IC Cloud (Intelligence Community Cloud), it still does not satisfy its desire to obtain global network user data. **With the help of a super data interface like PRISM, the United States can turn the data centers of major internet vendors into its own "hard disk" without bearing the cost, and can extract user data on demand at any time. The basic IT products and services of the United States have become "accomplices" in the large-scale monitoring and secret theft operations initiated by the US intelligence agencies.**

References

[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/

Summary

The US is the birthplace of the computer, the modern internet and the smartphone. These important innovative achievements in human history are the shining light of innovation of the American industry and scientists, the outcome of the wisdom and creativity of the American people, and the symbol and support of the US as a global technological leader. But at the same time, for American oligarchic capitals and politicians, cyberspace has become "a new highland" where they can leverage their first-mover technological advantages to achieve geopolitical purposes. It is precisely under the dual effects of leadership and hegemony that people around the world have helplessly accepted the upstream monopoly of the US in information technology and industrial systems and relying on its products and services. But in fact, the US has not fulfilled its cybersecurity responsibilities as a responsible major country, and has not made any commitments to the issues that governments and people around the world are concerned about, such as "promoting the militarization of cyberspace and abusing the advantages of supply chains and information chains."

The US intelligence agencies spare no effort to develop cyberattack equipment covering the whole scenarios, the whole link and the whole process for the cyber home of mankind, continue to launch a series of cyberattacks, abuse the upstream advantages of the supply chain, preset vulnerabilities, weaken the encryption strength, reduce the difficulty of attacks, build super access interfaces for internet platforms such as PRISM to obtain and spy on user data.

The US intelligence agencies have built a comprehensive attack penetration capability for mobile smart terminals and communication systems. From SIM cards, firmware, operating systems to software applications, from data lines, Wi-Fi, Bluetooth, cellular network, GPS and other data interfaces to operator systems, and even the entire mobile industry ecosystem, as well as the data centers of large internet and IT vendors, the attack penetration capability of the US intelligence agencies is pervasive. The US intelligence agencies have broken down the production and manufacturing processes, application scenarios and network communication of smart terminal devices one by one, comprehensively gained access to global personnel, accounts, equipment, links, code numbers and locations, drawn complete cyberspace operation maps, and conducted all-round and in-depth network intelligence activities, which seriously endangers the national security of other countries, and should be highly concerned and closely guarded by all parties around the world.

Michael Hayden, a retired four-star general in the US Air Force who served as the director of the NSA and the CIA from 1999 to 2009, summed up his ten-year experience in intelligence work as "the power and limitations of intelligence", and admitted that the US intelligence agencies must achieve intelligence benefits by stealing unauthorized information. The so-called judicial approval system that it advertises actually only covers law enforcement agencies such as the FBI, but has no binding force on intelligence agencies such as the NSA and CIA for their behaviors and activities against US citizens or foreign personnel and agencies.

From the level of cyberattack activities, for the invasion, persistence, theft and other attack activities carried out by the US, we can gradually realize the discovery, weakening, blocking and denial by improving and strengthening the security protection capabilities of scenarios and mobile phone products. However, it requires long-term and sustained efforts, the support of extremely high-level detection, analysis and protection capabilities, as well as huge investment, which increases the security investment cost pressure on governments, industrial systems and organizations around the world.

However, super access interfaces such as PRISM are deeply coupled with the entire mobile phone and mobile internet ecosystem, which became an almost insoluble pain. Only by restricting products, services and applications for specific scenarios and personnel, and urges the US to immediately end such moves by continuous diplomatic efforts. All countries should improve their governance capabilities, strengthen data localization and compliance requirements, and safeguard their cyber sovereignty. The ultimate result will inevitably be that more countries hope to break their absolute dependence on the US smart terminals and internet product systems.

For such powerful, systematic and targeted attacks by the US intelligence agencies on smart terminal systems, governments need to build targeted threat and risk analysis and judgment mechanisms and advanced persistent threat discovery and hunting mechanisms (for the industrial chain scenarios, operator scenarios, mobile phone usage scenarios, key personnel scenarios). In addition, governments should improve their defense and support capabilities for key scenarios and personnel. Countries that lack their own independent industrial system also need to be wary of devices, products and services from vendors with "criminal records" that have collaborated with US intelligence agencies and provided PRISM access interfaces. In terms of the use of devices in important scenarios and personnel, introduce devices produced independently or from responsible countries, with stronger security and privacy protection functions and more reliable security commitments. Each country's own mobile terminal industry system (such as SIM cards, mobile phone manufacturing, key APP research and development, internet services, etc.) must improve relevant product and software code security engineering capabilities in a targeted manner, and have full life cycle protection capabilities in R&D and production.

At the same time, governments also need to strengthen their security linkage and empowerment capabilities for mobile phone vendors, operators and internet vendors, and strengthen management requirements. Governments should propose targeted cybersecurity standards for smart terminals, network operators, and APP development service providers, urge them to fulfill corresponding security obligations and make clear security service commitments to promote a transparent mechanism for hardware and software supply chain. Security mechanisms such as threat detection and kernel protection have become mandatory requirements for mobile phones and other smart terminal devices. Governments will make it mandatory to support threat analysis, retention and traceability, which not only strengthens the responsibility of security subjects, but empowers security capabilities.

The work and resource investment mentioned above are the basis and necessary conditions to support the detection and defense of the US attacks, which can increase the cost of attacks by the US to a certain extent and shorten the time to detect attacks. However, in the face of ultra-high capabilities and pervasive attacks, more targeted construction investment and policy updates are needed, including establishing a specialized environment and team for targeted scenario threat analysis and hunting, building specialized equipment, encouraging and rewarding the discovery of clues of advanced persistent attacks.

The large-scale cyberattacks and information theft by the US intelligence agencies are the tearing apart of cyberspace by hegemonism and unilateralism. While the exposed content of attacks against mobile smart terminals are chilling, what is even more frightening is that we still don't know how many attack weapons, facilities, and operations are still unknown. As Hayden said in his memoir *Playing to the Edge: American Intelligence in the Age of Terror*, "the law of espionage is that you only know those who fail, not those who succeed", what has surfaced so far is just the tip of the iceberg of large-scale intelligence operations launched by the United States. When people around the world enjoy the convenience, speed, and pleasure brought by mobile smart terminals, do not forget that the huge abyss created by the superpower is greedily sucking our data sources. When you are staring at the phone, the abyss behind the phone is also staring at you.

Appendix 1 – Acronyms

Acronym	Definition
A2P	Application to Person
A^2PT	Advanced Advanced Persistent Threat
ACLU	American Civil Liberties Union
ANT	Advanced Network Technology
AOL	America Online
APN	Access Point Name
APP	Application
ARM	Advanced RISC Machines
ASD	Australian Signals Directorate
AT&T	American Telephone and Telegraph Company
BICS	Belgacom International Carrier Services
CALEA	Communication Assistance for Law Enforcement Act
CBC	Canadian Broadcasting Corporation
CDMA	Code Division Multiple Access
CDR	Call Detail Record
CIA	Central Intelligence Agency
CNN	Cable News Network
CSEC	Communications Security Establishment Canada
DAS	Data Analytical Services
DEA	Drug Enforcement Administration
DRT	Digital Receiver Technology, Inc.
DTMF	Dual Tone Multi Frequency
ECPA	Electronic Communications Privacy Act
EDGE	Enhanced Data Rate for GSM Evolution
EFF	Electronic Frontier Foundation
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FOI	Freedom of Information
FRA	National Defense Radio Establishment
FRS	Family Radio Service
FSB	Federal Security Service
GCHQ	Government Communications Headquarters
GCSB	Government Communications Security Bureau
GPRS	General Packet Radio Service
GPS	Global Positioning System
GRX	GPRS roaming exchange
GSM	Global System for Mobile Communications
GSMA	Global System for Mobile communications Association
HSPA	High-Speed Packet Access
IMEI	International Mobile Equipment Identity

IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
KUMA	Unified Monitoring and Analysis Platform
LOB	Line of Bearing
LTE	Long Term Evolution
MAP	Mobile Application Part
MCC	Mobile Country Code
MHET	The Mobile Handset Exploitation Team
MNC	Mobile Network Code
MSISDN	Mobile Subscriber International ISDN/PSTN Number
MVT	Mobile Verification Toolkit
NIB	Network-in-a-box
NSA	National Security Agency
NTAT	Network Tradecraft Advancement Team
OTA	Over-the-Air Technology
PC	Personal Computer
PLMN	Public Land Mobile Network
RAT	Remote Access Trojan
RF	Radio Frequency
ROM	Read-Only Memory
SCCP	Signaling Connection Control Part
SDR	Software Defined Radio
SGSN	Serving GPRS Support Node
SIGINT	Signal Intelligence
SIM	Subscriber Identity Module
SMS	Short Messaging Service
SMS-PP	Point to Point
SS7	Signaling System 7
STK	SIM Tool Kit
TAO	Tailored Access Operations
TTTC	Target Technology Trends Center
UDC	Utah Data Center
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
UTT	Unified Targeting Tool
VoIP	Voice over Internet Protocol