Fight Against the Bald Eagle in the Fog

-RELAYING, COOPERATING AND SPECIFIC CONTRIBUTION

Antiy CERT

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

First Release Time: 23:50, March 21, 2024

Update Time: 23:50, March 21, 2024

For the Latest Report

Contents

1. Overview

On February 12, 2024, SentinelOne, an American cybersecurity company, released a report entitled "China's Cyber Revenge/Why the PRC Fails to Back Its Claims of Western Espionage" in its official website[1] (hereinafter referred to as "SentinelOne Report"). This paper interprets the relevant reports of "three prominent cybersecurity firms -- Qihoo 360, QI AN XIN, Antiy -- and the China Cybersecurity Industry Alliance" and other institutions that expose the cyber attacks of US intelligence agencies. Let's first summarize the viewpoints and key logic in the report.

The SentinelOne report sorts out our published analysis reports based on the timeline, quotes the views of some Americans, and sets the following views:

1. The Chinese reports are follow-ups to the analysis of the US by other international institutions, which are long-term lagging behind.

2. China's analysis relies heavily on the US's information leaks.

3. The Chinese reports have no "PCAP package" level technical evidence.

The logic of SentinelOne report is not to respond to the continuous analysis and exposure of US intelligence agencies' attack activities and capabilities by the global cybersecurity community and researchers in the past two decades, including the shocking truth exposed in the US's repeated information leaks, but to try to shift the international attention to whether the technical capability of Chinese cybersecurity practitioners can support their continuous independent discovery, analysis, research and attribution of US attacks, and narrow the concept of "evidence" into a specific technical format. The US and the West have been exaggerating China's cybersecurity capability from the macro level for a long time, in order to win a huge cybersecurity budget for its intelligence agencies and military-industrial complexes. At this time, however, a wave of "ridicule" that China's analysis and attribution capability is very poor has been launched at the micro level, which has been pronounced: as the bullied one, your resistance is invalid.

A large proportion of the analysis reports of China's security enterprises mentioned in SentinelOne report came from Antiy CERT. We recognize that as an enterprise-level security analysis team, it is very hard work to analyze the cyber attack activities and support system of the super cyber threat actors of the US intelligence agencies. We know that there is a huge gap in capacities, resources and some other areas. We are like an alert rabbit, trying to open our eyes wide to find and analyze the giant bald eagle that devours small animals in the foggy forest. We hope to draw its face and alert other animals in the forest to its attack.

In 2015, we put forward the term A^2PT (Advanced APT) to clarify its unprecedented capabilities and threats, and also remind ourselves how difficult it can be to counter and analyze such attack capabilities.

Analyzing and attributing APT attacks is a long-term, complex, resource-intensive, scientific and patient work, not to mention the more complicated A^2PT attacks. The process of our work is basically unknown to ordinary people, and the results of our analysis can only be fully understood by professionals. Despite the absurdity of the overall logic of the SentinelOne report, if we don't point to the SentinelOne (we like to call them US peers) a few truths that they are blind to, including sharing with them a little bit of what we (and the international cybersecurity community) really understand about APT analysis, it will be hard for people to see the deception to the world hidden under the seemingly professional and even "impartial" combing and analysis of the SentinelOne report.

We are therefore grateful to the SentinelOne report, which gives us the opportunity to link up a number of historical analysis efforts from our own retrospective perspective, including prompting us to publish some process clues from these efforts that did not appear in the historical reports. The SentinelOne report allows us to re-select some of the valuable analysis results that we once thought were covered with dust because of the length of the journey, and to re-inform and remind the world. Let all those who seek the truth put our report together with the SentinelOne report to see what sophism is and what logic and truth are.

We don't claim to be right, but we always have the right to tell our own experiences.

2. Track the Bald Eagle's Footprint by Relay

The cyber attacks by US intelligence agencies are not isolated actions, but a long-term layout based on zero-day vulnerabilities, advanced malware persistence and mixed operations of manpower, electromagnetism and cyberspace, supported by a huge engineering system. **Many iterations of large-scale malware projects may be experienced during the long-term operations,** which makes the analysis and exposure work of the international cybersecurity community look like a relay. The first relay peak was triggered by the Stuxnet event in 2010, accompanied by complex malware such as Flame, Duqu and Gauss. SentinelOne chose the wrong starting point of the timeline. The analysis work of the international cybersecurity community, including Chinese cybersecurity practitioners, started in 2010 instead of 2012, and our work was basically synchronized with that of the international peers. Some international cybersecurity enterprises first exposed relevant news on July 13, 2010 and Antiy captured samples based on the set key strings on July 15. Then, we started to build the simulation analysis environment of Stuxnet and simulate/analyze the relevant mechanisms.

Fig. 2-1 Stuxnet Simulation Analysis Sand Table Built by Antiy (July 2010)

The relay analysis of Stuxnet is composed of a lot of complicated and trivial work. For example, almost all institutions involved in the analysis found the USB device infection code, but most of them failed to trigger the reappearance of USB transmission behavior. One of Antiy's contributions is to analyze the key mechanism of its transmission in depth, and point out its USB transmission conditions, thus explaining its controlled transmission characteristics which are obviously different from other worms. In *对 Stuxnet 蠕虫的后续分析报告（The Follow-up Analysis Report on Stuxnet Worm)*[2] released on October 11, 2010, we interpreted:

Whether Stuxnet infects the USB depends on several fields in the configuration data, including:

- Offset mark bit at 0x6c, 0x70 and 0xc8
- Offset timestamp at 0x78 and 0x7c
- Offset values at 0x80 and 0x84

Only when the conditions corresponding to each domain are met will the USB be infected, wherein the bit at the offset 0xc8 is set to "not infect" by default.

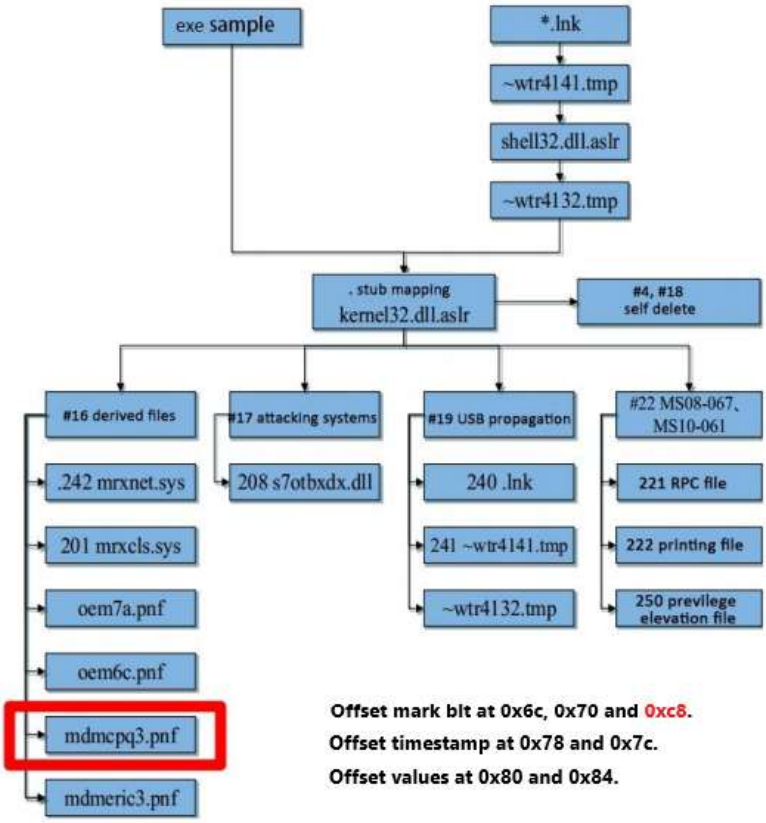


Fig. 2-1 File Release Structure and USB Transmission Logic Diagram of Stuxnet (October 2010)

However, we were not satisfied with the accuracy of the analysis. In the final report of the Stuxnet event 9 years later[3], we updated the complete mark bits:

Offset	Length	Explain
+00	Dword	Configuration file start flag
+04	Dword	Configuration file header length
+08	Dword	Configuration file checksum
+0C	Dword	Configuration file length
+6C	Dword	If the flag bit is 0, check the flag at +70 (if it is 1, directly infect USB)
+70	Dword	If the flag bit is 0, check the timestamp at +78
+78	Qword	Time to terminate USB infection
+80	Dword	Number of files required to exist on the USB
+8C	Qword	End time
+A4	Qword	Time to start infection (after 21 days, stop infecting USB)
…	…	…

Fig. 2-2 Analysis of Stuxnet Transmission Configuration (September 2019)

We acknowledged our lack of resources and experience in the face of such a complicated attack in 2010. As an emergency analysis team transformed from a virus analysis team, we were accustomed to the perspective of code function reversal, and did not verify the zero-day vulnerabilities exploited one by one, which left a serious analysis error -- regarding the exploitation of the Windows printing daemon as an attack on the printer, and left the following diagram with errors. This has also indirectly led to association errors in several domestic and international literature due to the quote of our diagram.

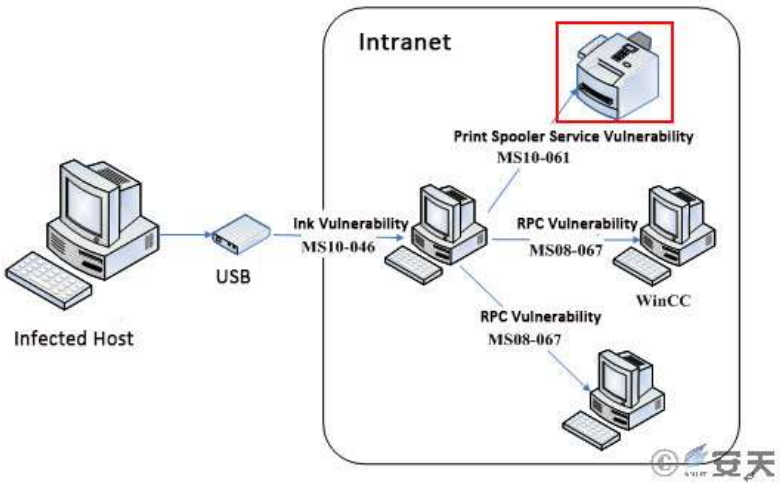


Fig. 2-3 The Wrong Illustration of the Transmission Mode of Stuxnet Worm Breaking

Through Physical Isolation Environment (September 2010)

Although an in-depth analysis and understanding of the Stuxnet event is a basic skill of all APT analysts around the world, we firmly believe that SentinelOne will not know Stuxnet better than we do, because if they have analyzed the samples, they would have known that Stuxnet would extract the host information and append it to the end of the payload. Obviously, the restoration of host information based on a large number of Stuxnet samples in our sample library will extract a lot of evidence that Chinese computers are infected. And this is exactly the evidence mentioned in the SentinelOne report.

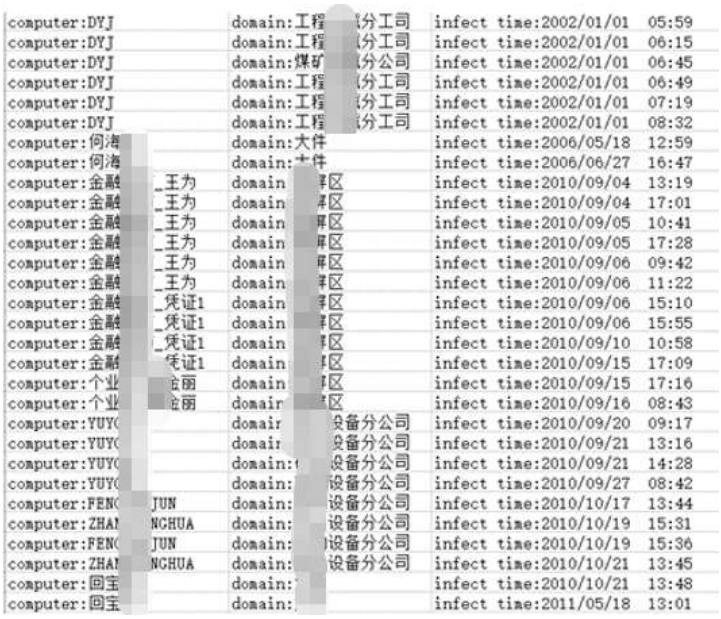


Fig. 2-4 Some Infected Computer Nodes in China Extracted and Sorted by Antiy Based on Samples

Since US leaders and government officials not only hinted at recognizing the relationship between Stuxnet and its intelligence agencies on many occasions, but even apparently used it as a declaration of strong cyber attack deterrence, the analysis of the events can no longer stay at the level of sample analysis and technical demonstration, but must judge the impact of opening the Pandora's box of information warfare in a deeper way. In the analysis of Stuxnet, Antiy quantitatively compared the Stuxnet event with Operation Scorch Sword and Operation Babylon 20

years ago, and clearly put forward the catastrophic milestone significance of Stuxnet because it proved that cyber attacks could achieve the local equivalence of traditional warfare operations.

Tab. 2-1 Comparative Analysis of Two Military Operations and Cyber Operation Against Sovereign Countries' Nuclear Programs (2015)

	Operation Scorch Sword and Operation Babylon (Traditional Warfare)	Operation Stuxnet (Cyber Warfare)
Attacker	Israel, Iran, US	US, Israel
Target	Iraqi nuclear reactor	Iran uranium centrifuge facility
Period	1977-1981	2006-2010
Personnel Input	Israeli Air Force, secret service personnel, Iranian Air Force, US Air Force and intelligence agencies	Software and cyber experts in the fields of intelligence and military intelligence, experts in industrial control and nuclear weapons in the US and Israel.
Output	Multiple rounds of preliminary reconnaissance and air strikes, nuclear reactor intelligence	Battlefield prefabrication, virus transmission, intelligence on Iran's nuclear facilities
Equipment Inputs from All Parties	Iran: 2 F-4 Phantom IIs bombed the nuclear reactor construction site with 12 MK82 bombs; 10 F-4s attacked Iraqi H-3 Air Force Base Israel: 2 F-4E(S) - reconnaissance mission; 8 F-16A (provided by the US), 4 F-15A, 2 F-15B and 16 MK84 bombs - air strike the reactor Simulate the construction of a reactor Secret service personnel assassinates key Iraqi personnel US: strategic satellites and intelligence, aerial tankers	Stuxnet virus Simulate the construction of centrifuge and control system
Cost-Effectiveness Ratio	Quick strike, long preparation period, huge cost, high consumption, complicated operation, and high risk	Long cycle, relatively low cost compared to military strikes, but more precise and covert, with less uncertain consequences
Training Costs	18 months of simulated air strike training, 2 F-4 Phantom IIs crashed, and 3 pilots died	5 years of continuous development and improvement, spanning two presidential terms
Consumption	Manpower, military strength, financial resources, equipment resources, intelligence	Manpower, financial resources, intelligence
Damage Effect	The reactor was destroyed, which frightened the French suppliers, and Iraq's nuclear weapons	1,000 to 2,000 centrifuges were paralyzed, and uranium was unable to

	program was permanently stalled	meet weapons requirements, and Iran's nuclear weapons program was almost permanently stalled

After Stuxnet, international cybersecurity community successively discovered Duqu, Flame and Gauss, and released reports to prove their relevance to Stuxnet. When faced with Flame, Kaspersky pointed out that its attack was one of the most complicated attacks discovered at that time, and it could take several years to fully analyze it. We realized that international cybersecurity vendors and practitioners need to collaborate. And we started a marathon race of analysis to try to finish more work. We analyzed the main sample of Flame[4], extracted a list of sub-modules, and analyzed the key modules. According to the current public data retrieval results, Antiy's analysis contribution at the module level accounted for the highest proportion among the community's analysis results for Flame.

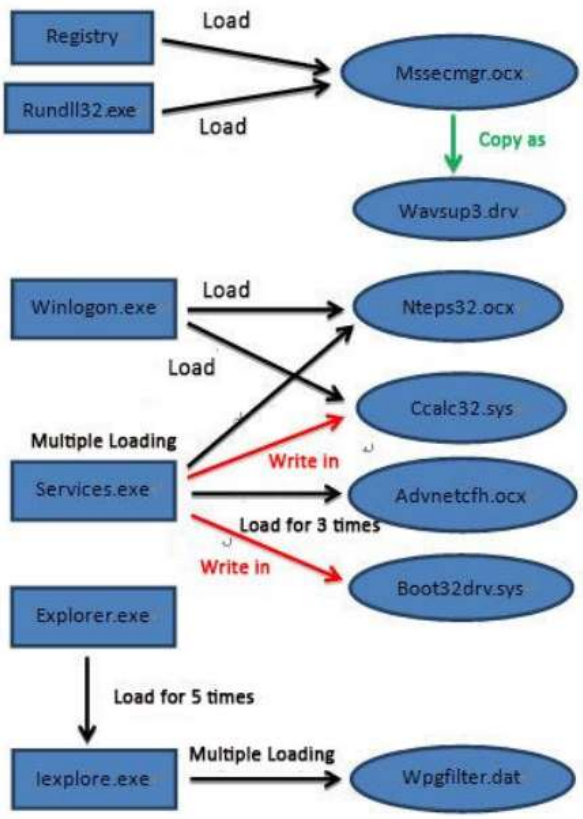


Fig. 2-5 Startup Loading Sequence of Flame's Main Modules and Sub-Modules (May 2012)

It was indeed a fact that our homology analysis report on Duqu and Stuxnet was later than that of international vendors[5]. At that time, the vendors involved in the in-depth analysis of the samples shared the common speculation and judgment that there was a homologous correlation in the Stuxnet, Flame, Duqu and Gauss series. Kaspersky showed great agility and determination in its work, while we did not translate the identified similarities into public analysis in time. But comparing two homology analyses, it was obvious that most of the homology points provided by Antiy were different from those of Kaspersky. By combining these analysis results, it could provide more complete clues and basis for the analysis of homology and code reuse proportion among APT sample systems.

Item Compared	Duqu Trojan	Stuxnet Worm
Function modularization	Yes	
Ring0 injection mode	PsSetLoadImageNotifyRoutine	
Ring3 injection mode	Hook ntdll.dll	
Inject into system process	Yes	
Resource embedded DLL module	Single	Multiple
Exploit Microsoft vulnerabilities	Yes	
Use digital signatures	Yes	
Include RPC communication module	Yes	
Configure the file decryption key	0xae240682	0x01ae0000
Registry decryption key	0xae240682	
Magic number	0x90,0x05,0x79,0xae	
There are bugs in operation mode judgment code	Yes	
There are bugs in registry operation code	Yes	
Attack industrial control systems	No	Yes
Driver compilation environment	Microsoft Visual C++ 6.0	Microsoft Visual C++ 7.0

Fig. 2-6 Comparison of Stuxnet and Duqu Homologous Key Code Genes Published by Antiy (May 2012)

APT analysis is a social collaborative process that involves many questions, and answering these questions requires long-term analysis accumulation and correlation backtracking. The Stuxnet

event was an example. For instance, no organization had officially answered for a very long time: There are only two large versions of the samples used in this highly targeted attack, and the total number of modules is only dozens. But why are there thousands of samples? Why the USB transmission switch was turned off by default in the technical verification, but it could form an infection spread chain from the Middle East to Southeast Asia and penetrating into China. We analyzed and answered the above questions in *震网事件的九年再复盘与思考 (Review and Thinking Nine Years after the Stuxnet Event)*[3]. Although the answer was late, it was original content of Chinese cybersecurity engineers. In contrast, it was difficult for organizations and researchers who were eager for quick success to achieve in-depth and systematic results.

Also, we sorted out the code reuse relationship among Stuxnet, Flame, Gauss and Duqu from the perspective of software engineering, and output a complete graph:

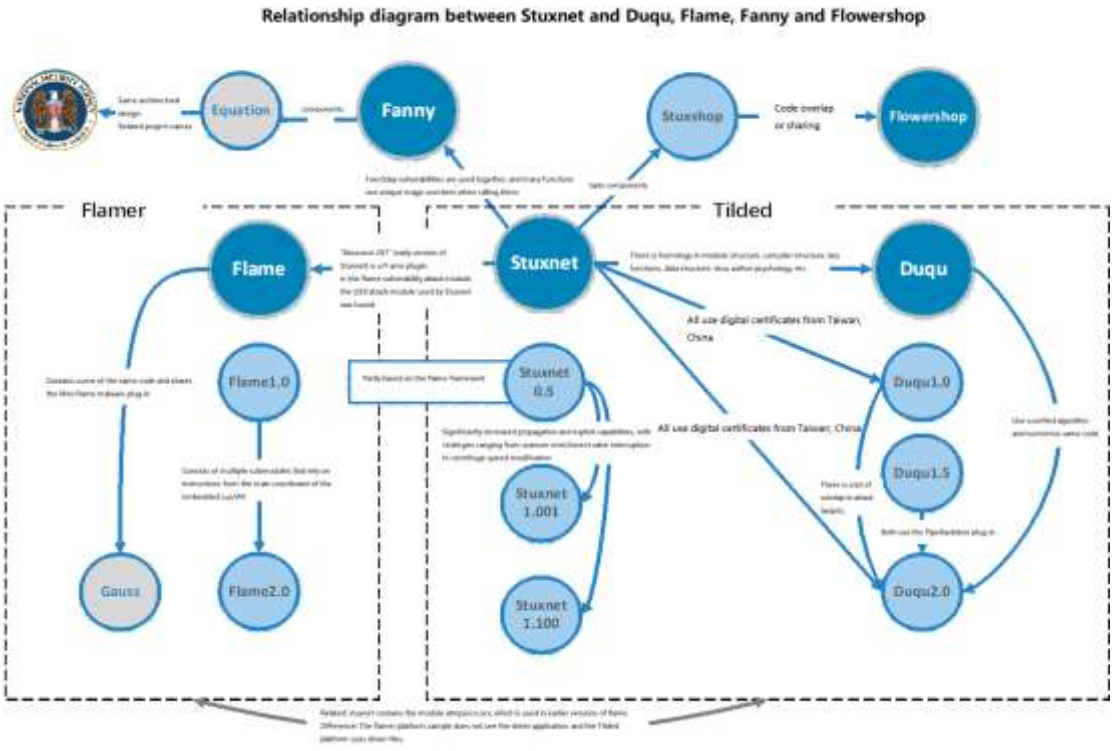


Fig. 2-7 The Relationship Diagram Between Stuxnet and Duqu, Flame, Fanny, Flowershop Released by Antiy (September 2019)

Not only race against time, but also maintain determination in front of time; Not only respect others' analytical results, but also make original contributions. This is the role that Chinese cybersecurity practitioners play in this relay.

3. Solve the Mystery of Sphinx

An important feature of the A^2PT group's attack equipment is that malware, vulnerability exploitation tools and attack weapons covering almost all platforms and scenarios. Mapping out this complete picture has become a Sphinx mystery that can only be solved by the joint efforts of excellent cybersecurity research institutions around the world. After 2013, the analysis and collaboration of the Equation Group (NSA-TAO) was a collective puzzle-solving experience. The key difference between Equation Group's new attack activity and the previous Stuxnet and Flame series of attacks was that Stuxnet's attack operation aimed at isolated networks, so the payload must contain all functional module components, which facilitated complete correlation analysis. The new attack activities mainly relied on the high modularity of the internet side and were launched on demand according to the scenario. Since the IT infrastructure environment of each country and the customer scenarios provided by each security vendors were very different, it was impossible for any cybersecurity vendor to completely capture the samples of each platform and various functional modules in a short period of time. If our research on Stuxnet, Flame, Duqu and Gauss relied on the analysis relay formed by the correlation of homologous clues, then our analysis of Equation Group actually relied on our own perception and capture ability. We unraveled the group's Anti-AntiVirus abilities on each platform, and eventually unraveled its full-platform coverage abilities.

It took a long time to capture, analyze, stitch and expose. And it had been 8 years since we exposed the iOS sample and when we officially completed the analysis. Relying on our own capture abilities, we had successively captured attack samples on Windows, Solaris, Linux, and iOS platforms, and cracked the encryption mechanism of the samples. Collaborated with the

international cybersecurity community, we completed the analysis of its full operating system platform coverage ability, and ultimately made it fully exposed.

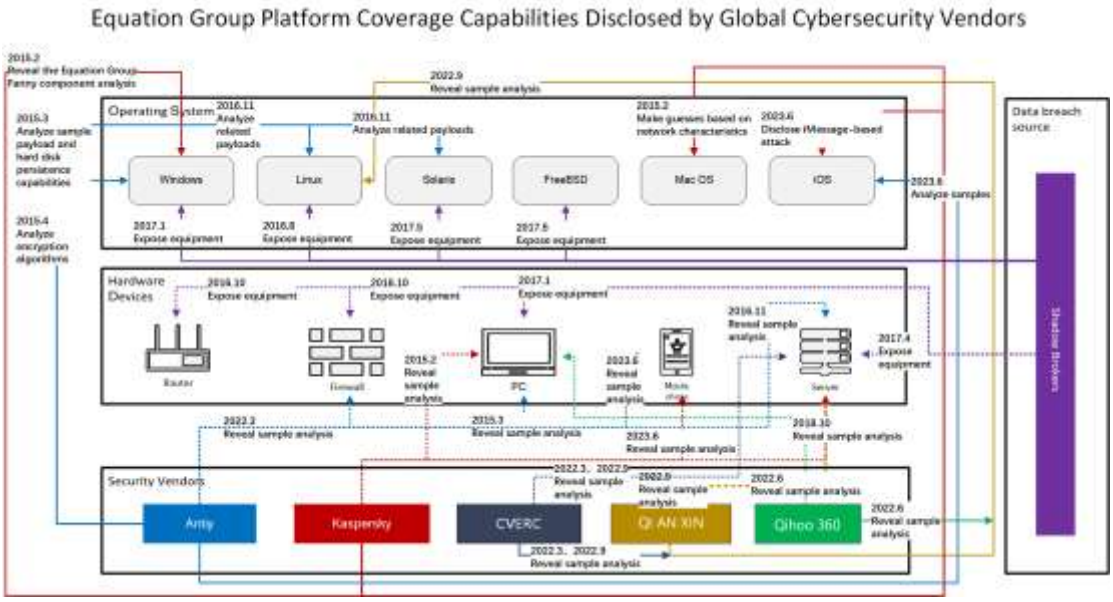


Fig. 3-1 Equation Group Platform Coverage Capabilities Disclosed by Global Cybersecurity Vendors

In early 2015, Kaspersky took the lead in announcing the attack ability of Equation Group on hard disk firmware, and Antiy followed up and released an analysis report[6], which provided valuable results on the attack component structure, communication instruction code and control structure.

C&C are as follows:

advancing-technology[.]com
avidnewssource[.]com
businessdealsblog[.]com
businessedgeadvance[.]com
charging-technology[.]com
computertechanalysis[.]com
config.getmyip[.]com - SINKHOLED BY KASPERSKY LAB
globalnetworkanalys[.]com
melding-technology[.]com
myhousetechnews[.]com - SINKHOLED BY KASPERSKY LAB
newsterminalvelocity[.]com - SINKHOLED BY KASPERSKY LAB
selective-business[.]com
slayinglance[.]com
successful-marketing-now[.]com - SINKHOLED BY KASPERSKY LAB
taking-technology[.]com
techasiamusicsvr[.]com - SINKHOLED BY KASPERSKY LAB
technicaldigitalreporting[.]com
timelywebsitehostesses[.]com
www.dt1blog[.]com
www.forboringbusinesses[.]com
Ign***list.com
Dat***cemgmt.net
Imp***today.com
Bud***nessnews.com

New keys:

37 08 EF 89 29 A7 4B 6B AB 3E 5D 03 F6 B0 B5 B3
66 39 71 3C 0F 85 99 81 20 19 35 43 FE 9A 84 11
8B 4C 25 04 56 85 C9 75 06 33 C0 5E C2 08 31 F6
32 EC 89 D8 0A 78 47 22 BD 58 2B A9 7F 12 AB 0C

Fig. 3-2 Captured C2 and Communication Keys Published by Antiy (March 2015)

In this report, Antiy conducted analysis and process research on the hard disk firmware writing module, and conducted firmware extraction and comparison analysis on the host hard disk that may be persisted at that time.

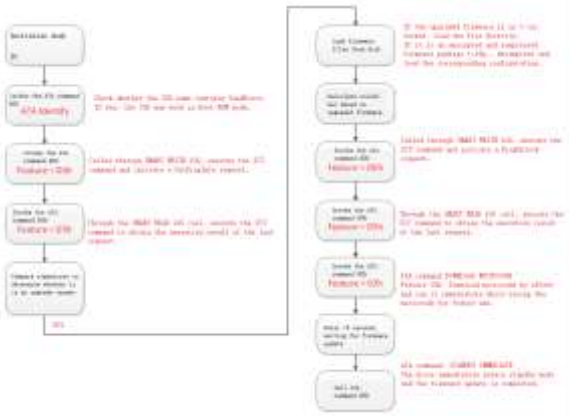


Fig. 3-3 Antiy's Analysis of Hard Disk Firmware Upgrade Process (March 2015)

In our capture analysis of the Equation Group in 2013, we monitored and discovered a large number of machines that were connected back to the attacker C2, and identified that there were targets domestically.

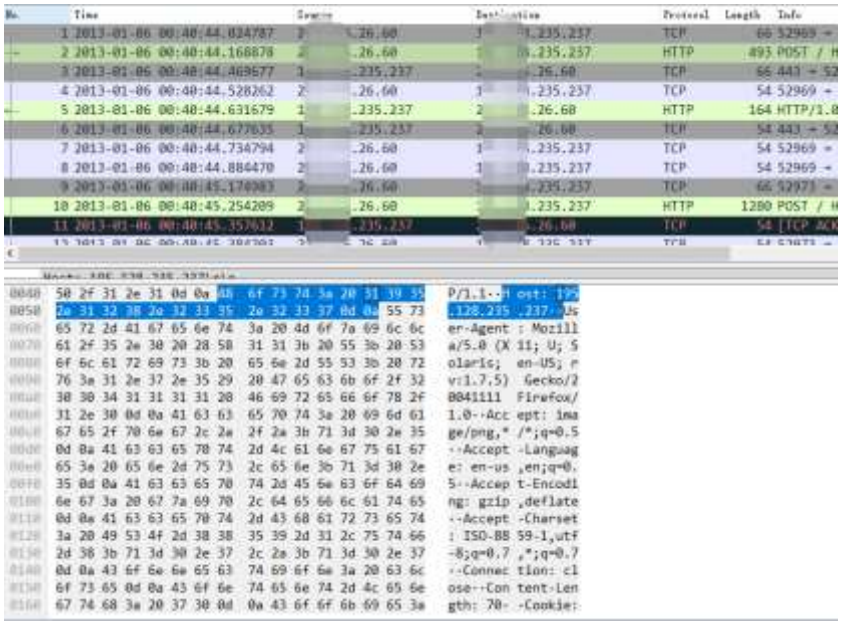
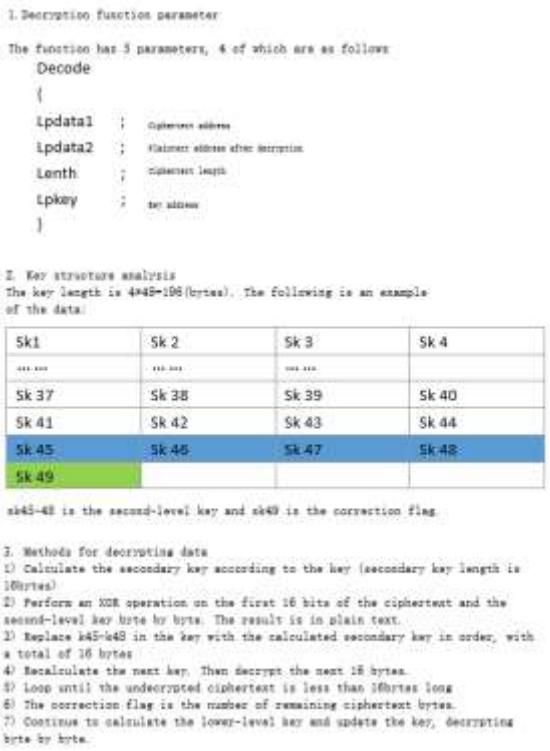


Fig. 3-4 Domestic Back-Connection Equation Group C2 Monitoring Traffic

In May 2015, Antiy released a report, disclosing the built-in data encryption and network communication encryption algorithms of the Equation Group, as well as the decryption keys and decryption algorithms[7].



1. Decryption function parameter

The function has 5 parameters, 4 of which are as follows

```
Decode
(
Lpdata1   ;
Lpdata2   ;
Lenth     ;
Lpkey     ;
)
```

2. Key structure analysis
The key length is 4*49=196(bytes). The following is an example of the data:

Sk1	Sk 2	Sk 3	Sk 4
……	……	……	
Sk 37	Sk 38	Sk 39	Sk 40
Sk 41	Sk 42	Sk 43	Sk 44
Sk 45	Sk 46	Sk 47	Sk 48
Sk 49			

sk45-48 is the second-level key and sk49 is the correction flag

3. Methods for decrypting data
1) Calculate the secondary key according to the key (secondary key length is 16bytes)
2) Perform an XOR operation on the first 16 bits of the ciphertext and the second-level key byte by byte. The result is in plain text.
3) Replace k45-k48 in the key with the calculated secondary key in order, with a total of 16 bytes
4) Recalculate the next key. Then decrypt the next 16 bytes.
5) Loop until the undecrypted ciphertext is less than 16bytes long
6) The correction flag is the number of remaining ciphertext bytes.
7) Continue to calculate the lower-level key and update the key, decrypting byte by byte.

Fig. 3-5 Analysis of Equation Group Communication Encryption and Decryption Algorithm (April 2015)

In 2016, Antiy's report exposed the Equation Group's attack samples against Linux systems and SPARC-based Solaris systems for the first time[8]. The report analyzed the main functions, communication modes and instruction characteristics of the samples. Superimposed with Kaspersky and other vendors' reports, it formed a full-platform malware ability diagram of the A^2PT attack group.

Information	Windows	Linux	Solaris	FreeBSD	Mac OS
Antiy: The Trojan Modify Firmware Exploration in Attack Components of Equation Group, March 2015	Analysis of sample payload and harddisk persistence capability				
Antiy: Analysis of Encryption Skills Usedin Equation Group Attack Components, April 2015	Eneryption algorithm analysis				
Antiy: Revealing the Multi-platform Loading Capability of Equation Group, November 2016		Existed,analysis of related payloads	Analysis of related payloads		
The Hacker News: Shadow Brokers reveals List of Servers Hacked by the NSA, October 2016			Existed	Existed	
Kaspersky Equation: The Death Star of Malware Galay, February 2015	Revealing Equation Group				
Kaspersky A Fanny Equation:"I am your father,Stuxnet" . February 2015.	Fanny component analysis				
Kaspersky Equation Group: from Houston with love, February 2015	Doublefantasy analysis				
Kaspersky EQUATION GROUP: QUESTIONS AND ANSERS,. February 2015	Equation Group Questions and Answers				Speculation based on network features

Fig. 3-6 Equation Group's Multi-platform Operating System Coverage Abilities (November 2016)

In 2023, Antiy exposed the samples of the Equation Group targeting iOS[9]. This report interacted with Kaspersky's report *Operation Triangulation*, respectively exposed how the US used the Quantum system and the iMessage vulnerabilities in mobile phone to hijack and launch attacks on iOS phones. In the report, Antiy also released the attack ability diagram of the Quantum system and the relationship diagram of US's support for the operation of attack systems.

Fig. 3-7 Graphical Analysis of Attackable Scenarios of Quantum Systems (June 2023)

Obviously, the writer of the SentinelOne report may not have carefully read any APT analysis reports released by Chinese vendors. The writer's research habit is to make correlations and inferences based on the release time of reports from various security institutions, and does not realize (or are unwilling to admit) that in every relay, Chinese cybersecurity vendors are releasing different results from international peers. And apparently, the writer lacks the experience of in-depth analysis of APT incidents and the ability to form heavyweight analysis reports. Therefore, the writer was unable to realize that the reason why Chinese vendors were able to quickly follow up and release relevant results after other international peers released analysis results was because the main part of these reports had already been formed. In fact, Chinese vendors are just waiting for the opportunity to publish. And we are certain that the writer does not understand the *Operation Triangulation* report released by Kaspersky on June 1, 2023, and the *量子系统击穿苹果手机 (Quantum System Breaks down iPhone)* report released by Antiy on June 9. Because it is obvious that the reports of Kaspersky

and Antiy, in addition to both targeting iOS, describe two totally different attack activities. The attack exposed by Kaspersky is based on iMessage, while the attack exposed by Antiy is based on the Quantum system and is delivered through traffic hijacking. When the report was released on June 1, 2023, Kaspersky had not yet conducted sample analysis, but released attack traffic and behavior analysis (Kaspersky sample analysis results were released in December 2023). What Antiy exposed was a reserved report of an early captured iOS sample. These are two sets of independent analysis results. We are just providing an assist for international peers.

4. Intercept the Out-of-Control Clone

It is not just the A^2PT attack itself that has brought great pressure and interference to global cybersecurity practitioners. Judging from statistical indicators such as the number of incidents and the scope of attacks, the US's connivance with the proliferation of cyber armaments and cyber crimes caused by out-of-control cyber arsenal management have brought greater trouble to the world.

In 2015, we discovered an APT attack targeting an organization in China[10]. From the first captured encrypted data packet to the later discovery of its persistence using registry data blocks, we all thought this was an attack launched by the A^2PT group. But it was not until we imported it into Antiy Cyberbrain platform for homology comparison that we discovered it was an attack payload generated by Cobalt Strike, an automated attack testing platform released by an American enterprise and was used to attack us.

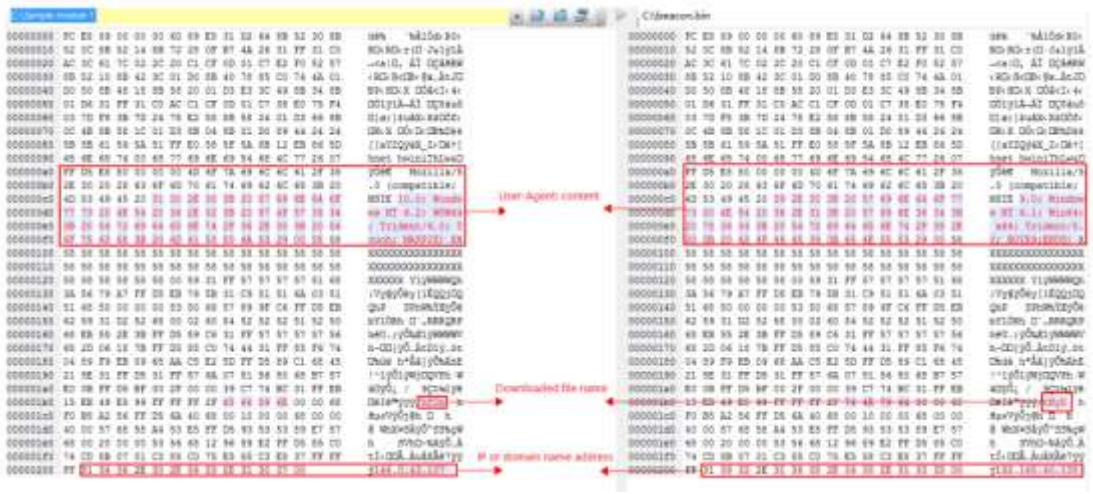


Fig. 4-1 Comparative Analysis Diagram of Sample Module and Beacon Generation Module (May 2015)

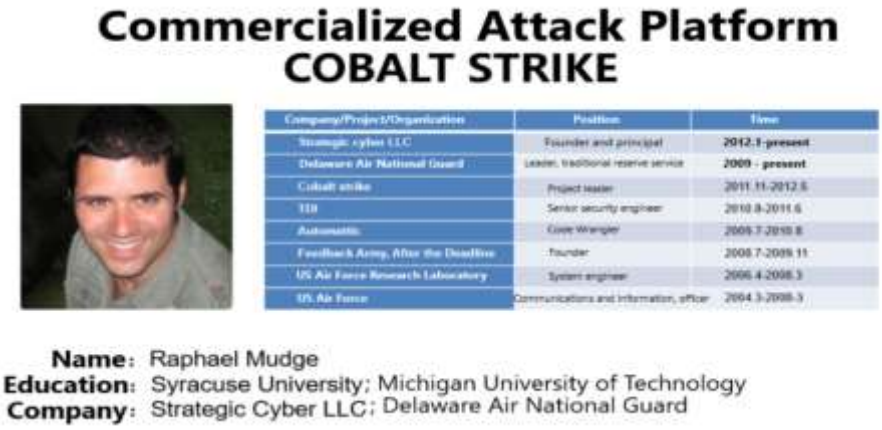


Fig. 4-2 Analysis of Military Background of the Founder of Cobalt Strike (May 2015)

Antiy pointed out that "there are already serious risks of cyber armaments proliferation in cyberspace. Can superpowers reasonably control the speed and scale of their own cyber armaments development? Regarding possible armaments proliferation due to their failure to effectively perform their responsibilities, can effective intervention and control be carried out? This is a key factor in whether we can achieve a safer online world."

The results proved prophetic. Two years later, the US has brought greater trouble to the world. The US Shadow Brokers leakage incident led to the WannaCry worm incident using the EternalBlue

vulnerability, which was exploited in the US NSA's cyber arsenal to create a huge global network disaster.

Although we predicted the possible convergence of ransomware viruses and worms in the 2016 Cybersecurity Threat Annual Report[11], we did not expect that it would manifest itself in such a rapid manner a few months later. Despite this, we still adhere to the objectivity and rigor of Chinese cybersecurity practitioners in determining the origin of WannaCry. Although these advanced vulnerability exploitation tools came from US weapons leakage, we still relied on multiple sets of clues such as the origin of WannaCry's historical samples to provide the China Cyber Security Emergency Response Organization with our judgment on the origin of WannaCry (including the conclusion that it was not developed by the US). But this conclusion does not mean that WannaCry victims, including Chinese users, do not need to hold the US responsible for out-of-control cyber armaments. This incident forced Antiy, as an important enterprise in China's emergency response system, to launch a 72-hour continuous emergency response and support a comprehensive response that lasted for dozens of days.

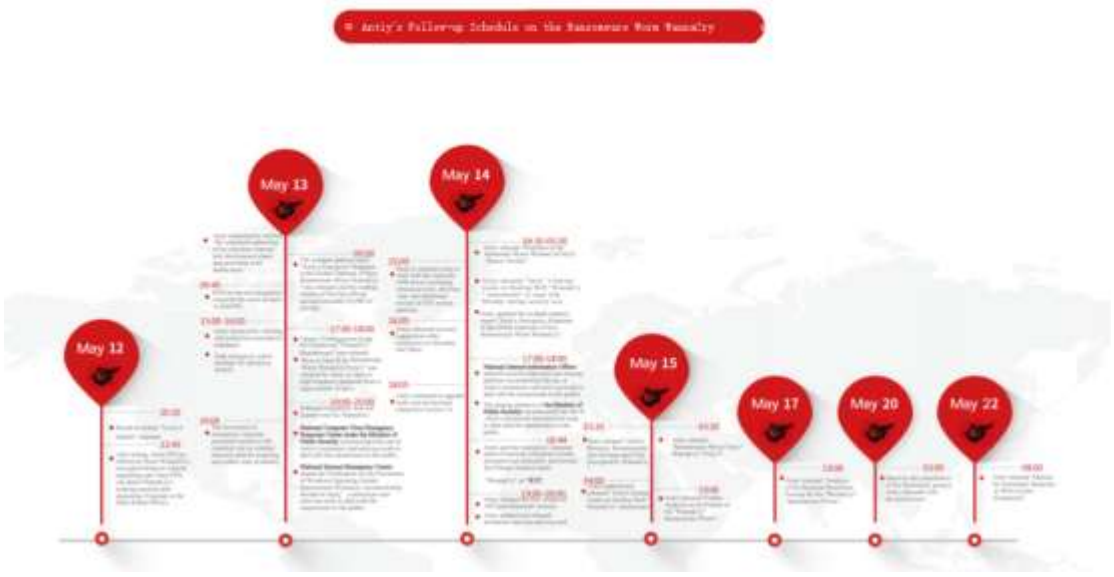


Fig. 4-1 Antiy's Follow-up Schedule on the Ransomware Worm WannaCry (May 2017)

The relevant risks brought by Shadow Brokers leakage are not only EternalBlue, each of its vulnerability exploitation tools brought a huge risk to the information system. To this end, we have released an operation manual on systematic response to NSA cyber armament[12], and drawn a risk diagram of these vulnerabilities, as shown in the figure below.

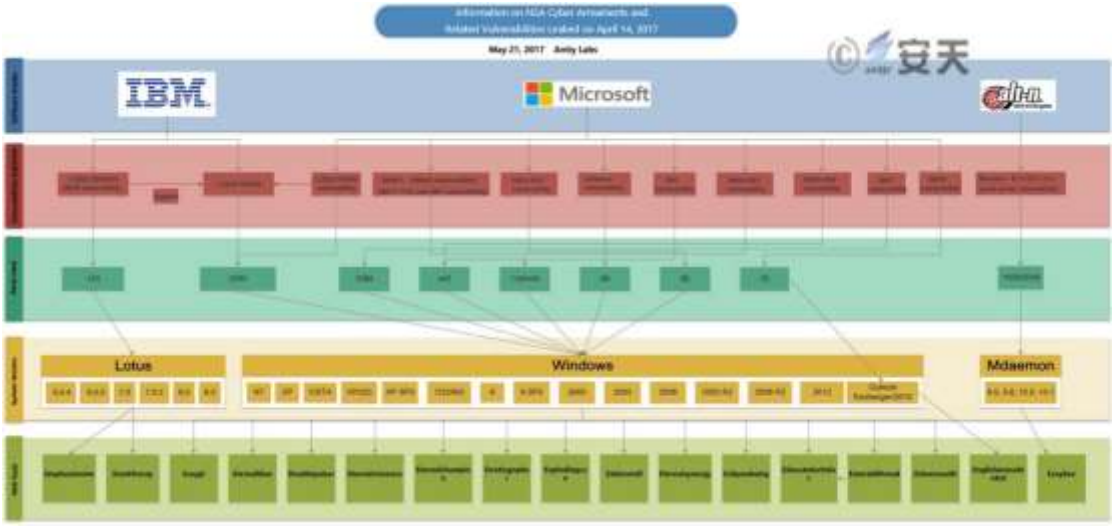


Fig. 4-2 Relationship Between Leaked NSA Cyber Armaments, Related Vulnerabilities, and System Versions (May 2017)

Reviewing these works will help clarify the stereotypes about analyzing APT attack targets from Chinese cybersecurity practitioners. Helping customers deal with security threats and prevent security risks is the first dimension of our work. Identifying attackers and troublemakers is only part of the value of our analysis.

5. Paint the Ferocious Panorama

The biggest difference between A^2PT attacks and other cyber attacks is that their attack activities are not a simple combination of vulnerabilities and malicious code, but complex operations based on a huge intelligence engineering system. If you want to fully understand the A^2PT attack, you must analyze this huge engineering system. Theoretically, this analysis can not be accomplished with live environments, samples, vulnerabilities, and tactical exploits.

The most hilarious ridicule of the SentinelOne report on Chinese cybersecurity practitioners is that all our work came from following up and imitating the analysis results of other international security agencies, or relying on a series of broken windows effects brought by the US intelligence agencies, including information leakage, such as Snowden, Shadow Brokers, WikiLeaks, etc. From the experience we introduced earlier, we can see that Chinese cybersecurity practitioners have their own original results in their analysis work. But in the face of these huge engineering systems, without Snowden and WikiLeaks, it would be impossible for the people of the world to know the truth.

In 2017, Antiy published a series of articles providing in-depth analysis of the STELLARWIND project in the documents leaked by Snowden. Antiy's report sorted out a large number of US signal intelligence acquisition projects and plans. The United States obtains various types of signal intelligence through large-scale submarine optical cable monitoring, key special areas monitoring, computer network exploitation (CNE, or network intrusion), satellite monitoring, and third-party intelligence sharing to achieve a complete picture of global targets. This has resulted in a relatively accurate target positioning capability, forming a super engineering support for the US to build cyberspace hegemony at the strategic level and implement cyber attacks at the micro level.

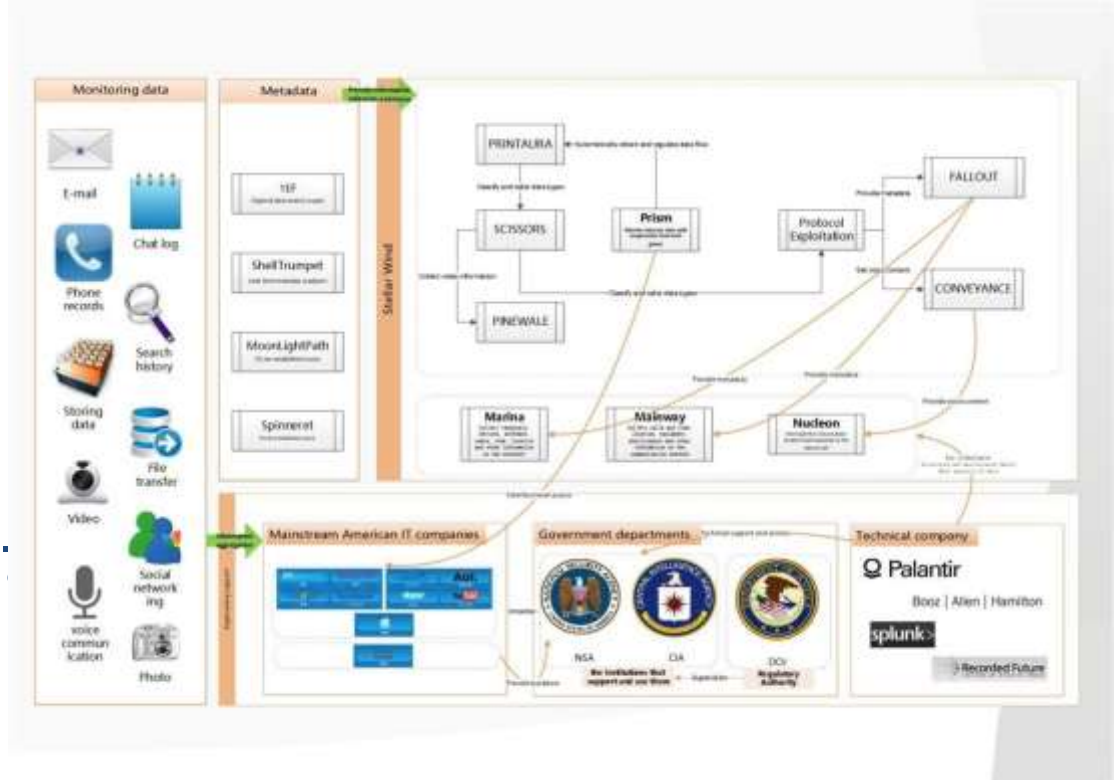


Fig. 5-1 Antiy's Analysis of the STELLARWIND Project Structure (March 2018)

	Chinese name	English name	Function / Object
Intelligence System	湍流架构	TURBULENCE	Automated attacks and intelligence harvesting against global targets
	风停	WINDSTOP	Monitor and obtain data
	肌肉	MUSCULAR	Overseas eavesdropping and data acquisition
	香炉	INCENSER	Monitor and obtain data
	混乱系统	TURMOIL	Passive Intelligence Gathering System
	涡轮系统	TURBINE	Initiative Intelligence Gathering System
	X 关键得分项目	X-KEYSCORE	Data Collection and Analysis System
	梯队系统	ECHELON	Intelligence collection and analysis
	公正观察	FAIRVIEW/US-990	Get phone metadata
	风暴酝酿	STORMBREW/US-983	Get international cable, router and switch data across U.S. borders
	花言巧语	BLARNEY/US-984	Access global cyber intelligence data
	栎树明星	OAKSTAR	Interception of phone and internet communication data
	灯芯绒系统	PINWALE	Collect and retrieve digital intelligence
	主核	MAINCORE	Mass surveillance of foreign mobile phone users
	舞动绿洲	DANCINGOASIS	Monitor optical cable data in Europe and the far east of Asia
	海螺	SHELL TRUMPET	Collect metadata
	数字采集系统网	DCSNet	Data Access Analysis System; Monitor, store, and analyze mobile phones and landline phones in the United States
	精灵项目	GENIE	Network data and signals intelligence acquisition; Direct attack
	神秘计划	MYSTIC	Data system that intercepts, stores and analyzes phone records
	奔牛/边山	BULLRUN	Monitor encrypted data and decrypt it

	碟火	DISHFIRE	Global mobile data monitoring and collection system
	细线	THINTHREAD	Intercept and analyze internet traffic
	开拓者	TRAIBLAZER	Obtain data and organize it (stopped in 2006)
	神奇灯笼	MAGIC LANTERN	Keylogging software: obtain passwords and keys for encryption software
	食肉动物系统	CAMIVORE/DCS1000	Get ISP server data
	光塔	MINRET	Spying on anti-government and anti-terrorists
	棱镜项目	PRISM/US-984XN	Monitor and obtain data
	主干道项目	MAINWAY	Communication metadata collection
	码头项目	MARINA	Internet metadata collection and analysis
	核子项目	NUCLEON	Global phone content monitoring, analysis and storage
	特等舱	STATEROOM	Interception of sensitive information regarding espionage, nuclear weapons, terrorism and drug transportation
	老鹰哨兵	SENTRY EAGLE	Signal intelligence collection; Discover and report abnormal network activities by deploying defense systems
	瑞晶	REGIN	Highly complex spyware for large-scale data collection and intelligence gathering
	拱形计划	CamberDADA	It mainly monitors targets such as the Russian Kaspersky Company to obtain new virus samples and other information.
	陷入泥潭	DROPMIRE	Spying on encrypted fax machines inside the EU embassy in Washington
	三叶草	SHAMROCK	Gathering intelligence for the President of the US
	滑翔桨手	SKIDROWE	Signal intelligence operation project for foreign satellite communications
Attacking system	湍流架构	TURBULENCE	Automated attacks and intelligence acquisition harvesting against global targets
	量子项目	QUANTUM	Attack mechanism & intrusion toolset
	狐酸系统	FOXACID	System capable of attacking target computers in a variety of different ways; the NSA's internal code name is "Vulnerability Coordinator."
	精灵项目	GENIE	Network data and signals intelligence acquisition, direct attack
	怪物大脑	MonsterMind	Anti-intrusion software system to carry out automated defense and attack

Support System	优先	PREFER	Supporting analysis tools for DISHFIRE
	ICREACH 架构	ICREACH	The largest intelligence system in the United States, a search engine similar to Google
	无尽线人	Boundless Information	Big data analysis, statistics and display platform
	藏宝图	TREASUREMAP	Provide common cyber warfare maps, situational awareness, etc.
Plan/Project	星风计划	STELLARWIND	Primarily collects metadata, targeting U.S. natives and citizens
	上游项目	UPSTREAM	Intercept phone and network traffic from the Internet backbone (including high-capacity cables, switches, routers, etc. that communicate within and outside the United States)
	石头鬼冢	Stone Ghost	Sharing and exchanging data among Five Eyes Alliance

Tab. 5-1 US Cyberspace Engineering, Projects, and Plans (June 2017)

Our follow-up work is to analyze these engineering systems and the attack platforms, advanced malware, and tactical use of vulnerability exploitation tools in A^2PT attacks. Among front-end attacks, the most noteworthy are signaling devices.These signaling equipment are not traditional network operating equipment, but are inherited from traditional electromagnetic operating equipment. In other words, from the perspective of US intelligence agencies, there is no real concept of cyber attacks. The US only has two concepts: intelligence operations and military strikes. "CNE/CE" is just one path choice among numerous systems and equipment.

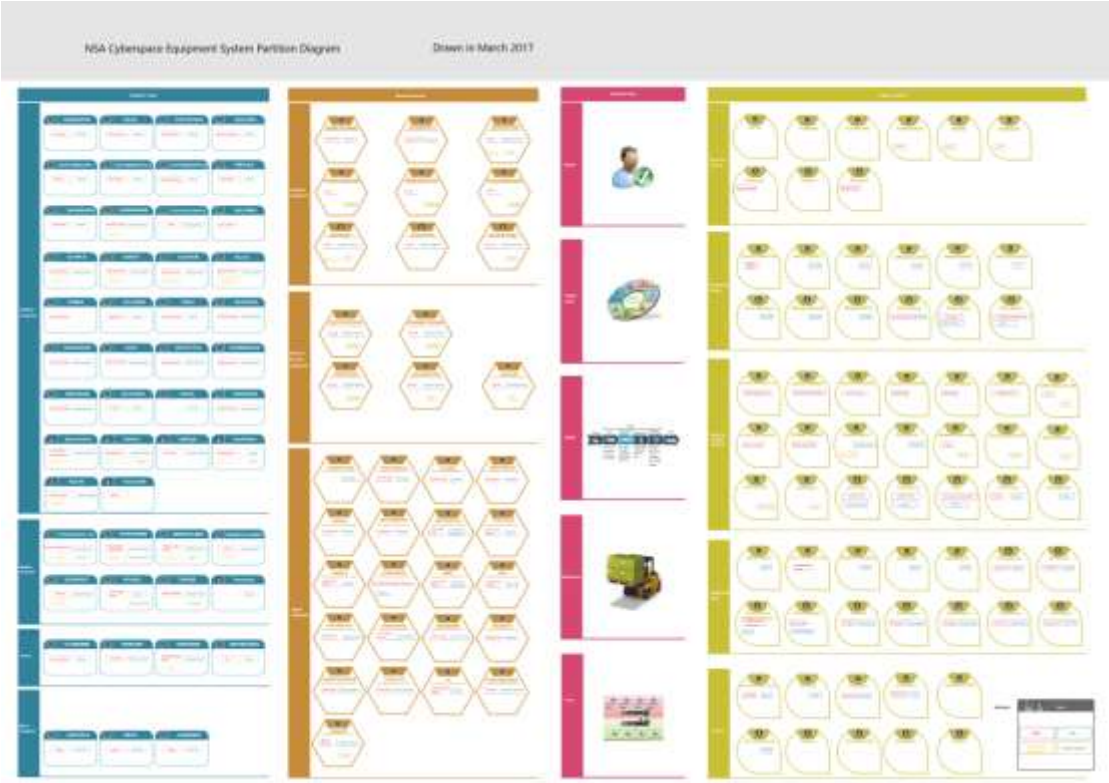


Fig. 5-2Cyber Attacks Equipment System, Support System and Operation Way Diagram (January 2018)

In addition, we also need to pay attention to the operation mechanism of the system, including why the operation mechanism can acquire a variety of vulnerabilities and technologies. There have been many reasonable speculations for a long time, but they have not been sorted out in-depth analysis, including how hacker competitions like Pwn2Own are related to US intelligence agencies.

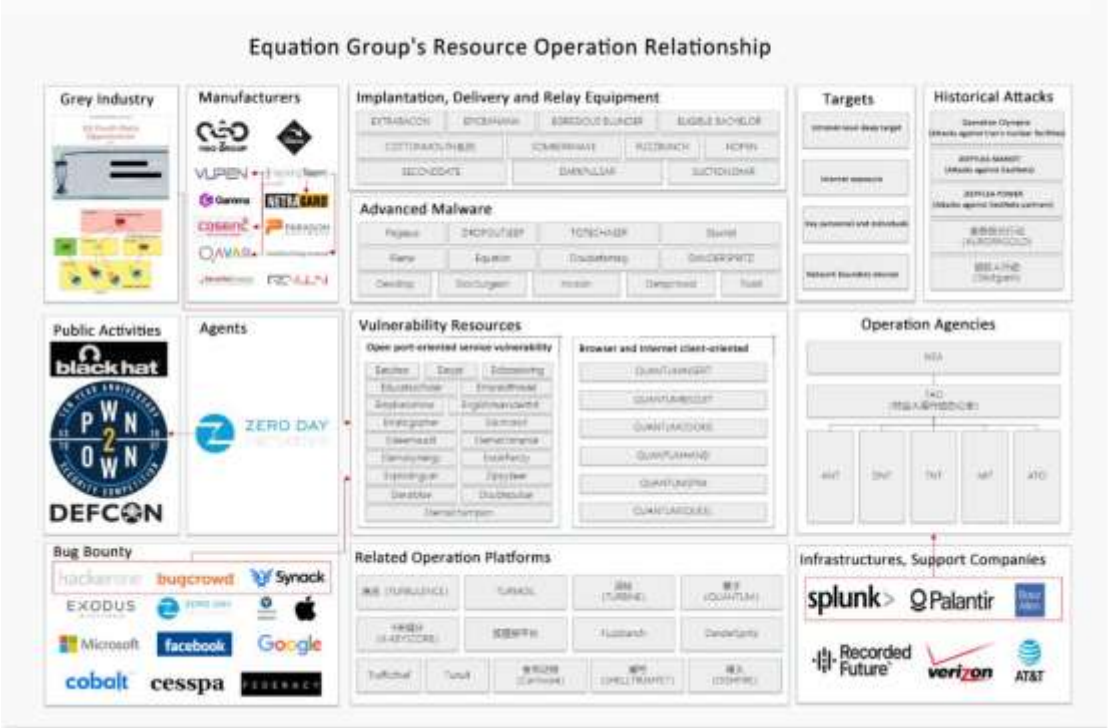


Fig. 5-3 Equation Group's Resource Operation Relationship Diagram (June 2023)

From the perspective of internationalist responsibility, Chinese security practitioners sort out and analyze the US intelligence engineering system based on the massive amount of leaked information. In general, most security enterprises analyze and expose attack activities, more in order to promote their own products and services by showing their threat discovery capabilities. Obviously, such a huge system attack requires the construction of a high-level dynamic and comprehensive defense system and a large amount of resource investment, rather than simply deploying products and purchasing services. We hope to bring these warnings and reminders by making the analysis results public.

6. Restore the Complete Scene

In early 2024, further details of previous attacks by A^{2}PT group were revealed[13]. For example, US intelligence agencies bribed Dutch engineer to drop Stuxnet during the installation and maintenance of industrial systems in Iran. "When the US conducts cyber attacks against other

countries' physical isolation systems or high-value targets, they often use manpower, electromagnetic and other means to assist, showing obvious characteristics of hybrid operations." Obviously, there is no complete chain of attack activities at the TCP/IP level, and in the face of such hybrid attacks, even if the lateral movement of packets is captured in the intranet, it can not provide a clear direction at the technical level.

The difference between A^2PT and APT is not only in the complexity of front-end exploits and samples, but relying on the huge operation system, which constructs the operation form of the US in cyber attacks, provides anti-traceability support, and creates a large number of weapons to hijack third parties, making the US to mix attack traffic into normal traffic. At the same time, the stolen data can also be recovered by means such as hijacking submarine optical cables. Apparently, A^2PT's hybrid operation and non-internet closed-loop paradigm make SentinelOne have the confidence to demand the PCAP package, like a bully asking a "gunshot" victim to produce evidence of a "knife" attack.

However, this hybrid operation is not all of the A^2PT attacks, there is also a closed loop of attack operations completed on the network. In view of the information records of the US and the information leaked in the Shadow Brokers incident, Antiy successfully integrated the leaked incident information with historical sample analysis to completely review the Equation Group attack on EastNets[14], the largest SWIFT financial service provider in the Middle East. The analysis report, released in June 2019, is the first analysis report to fully restore the attack mid-point, operation path, equipment usage, tactical process, scenario environment and consequences of the US in the global cybersecurity community's analysis and exposure of the US attack activities.

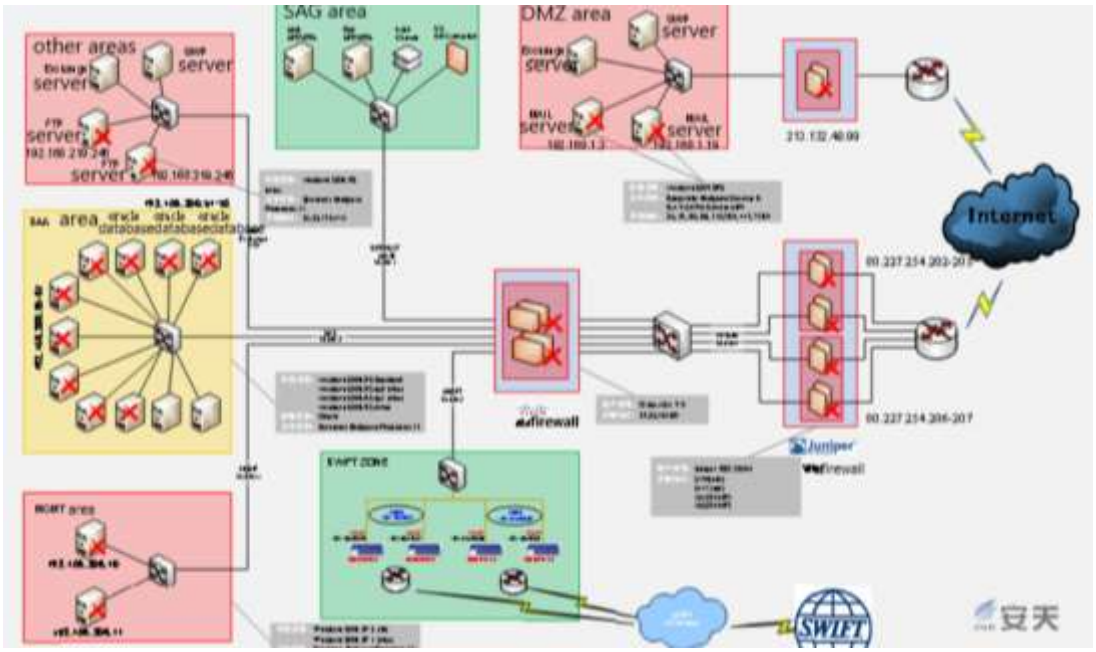


Fig. 6-1 Review of the Overall Attack Process of Equation Group on the EastNets Network (June 2019)

In the report, Antiy summarized the information of the attack equipment used by the US in this operation. According to the functional purposes, it has been divided into three types: vulnerability exploits, persistent implanted weapons and control backdoor. The report described weapon functions, application scenarios and associated vulnerabilities. The report pointed out that the US has full-platform and full-system attack capabilities and a large reserve of zero-day vulnerabilities.

Table 6-1 List of Exploit Tools Used by Equation Group to Attack EastNets (June 2019)

Attack Equipment Name	Vulnerability Number	Targeted Devices and Functions
Unknown Equipment A	CVE-2015-7755	Unknown equipment A is a vulnerability attack equipment targeting Juniper ScreenOS (the operating system used by Juniper SSG and NetScreen firewall products). There is an authentication bypass vulnerability when logging into the Juniper firewall through SSH and Telnet.
EPICBANANA	CVE-2016-6367	EPICBANANA is a vulnerability attack equipment targeting the command-line interface (CLI) parser in Cisco ASA and PIX devices.
EXTRABACON	CVE-2016-6366	EXTRABACON targets the SNMP service (ports 161, 162) vulnerability attack equipment of Cisco ASA equipment.

ENTERNALCHAMPION	CVE-2017-0146	ENTERNALCHAMPION is an "Eternal" series of vulnerability attack equipment targeting Windows Server 2008 SP1 x86, etc., which exploits the SMBv1 remote code execution vulnerability of Windows.
ETERNALSYNERGY	CVE-2017-0146	ETERNALSYNERGY is an "Eternal" series of vulnerability attack equipment targeting Windows 8 and other equipment , which exploits the SMBv1 remote code execution vulnerability of Windows.
ETERNALBLUE	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148	ETERNALBLUE is an "Eternal" series vulnerability attack equipment targeting Windows 7/8/XP, etc., which exploits the SMBv1 remote code execution vulnerability of Windows.
ETERNALROMANCE	CVE-2017-0143	ETERNALROMANCE is an "Eternal" series of vulnerability attack equipment targeting Windows XP, Vista 7, Windows Server 2003/2008/2008 R2, etc., which exploits the SMBv1 remote code execution vulnerability of all Windows platforms.
EXPLODINGCAN	CVE-2017-7269	EXPLODINGCAN is an attack equipment that exploits the IIS6.0 webDAV vulnerability.

Anyone around the world who wants to fully understand the threat of A^2PT attacks can read this review analysis report.

7. Back to the Timeline - Moving Forward Together

The SentinelOne report used a timeline to show the trajectory of results released by global cybersecurity agencies to the US to prove that Chinese vendors are not primacy, but just imitators of international vendors. In order to avoid turning a blind eye, Antiy combed and completed its "negligence and omission" of the key analysis report. Above the timeline is the original timeline in the SentinelOne report, and below the timeline are some of our key analysis reports that were "inadvertently omitted". We have also marked the value of key outcomes at each time point, and the new timeline presents interesting changes.

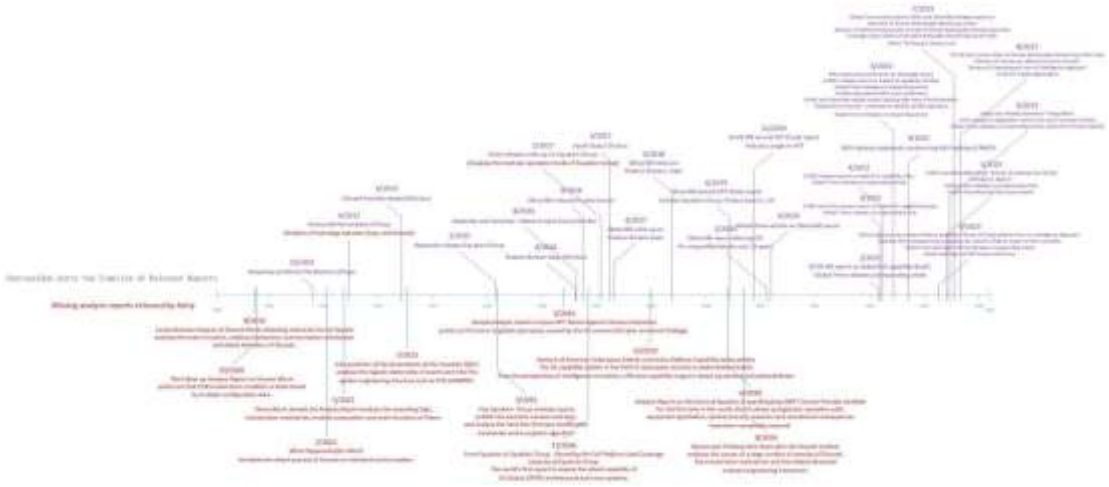


Fig. 7-1 Comparison of the Timeline of Global Analysis of US Reports Sorted by SentinelOne and the "Negligence and Omission" of Antiy Report

China, like many other countries in the world, is a victim of A^{2}PT attacks. Chinese cybersecurity practitioners like those in the global community who exposed A^{2}PT attacks, are warriors against threats. We are both warriors and students. We have always highly recognized the performance of international advanced vendors in the early analysis work and their guidance to us, and have been comparing and reviewing our own gap.

Table 7-1 Antiy Reflects on the Gap with International Well-Known Vendors in Technical Report (February 2012)

Time Stage	Time	Analysis Progress
①	June 17, 2010	Virusblokada reported the sample
	July 13, 2010	The sample detected by Symantec was W32.Temphid
	July 15, 2010	Kaspersky's three blog posts discussed LNK vulnerabilities and signature drivers
	July 15, 2010	Antiy captured the first sample
	July 16, 2010	Microsoft released LNK vulnerability alarm
	July 16, 2010	Symantec blog post introduced the basic situation of Stuxnet
	July 19, 2010	Kaspersky blog post introduced the principle of LNK vulnerability
	July 20, 2010	Symantec detected C&C traffic
	July 20, 2010	Kaspersky blog post introduced Stuxnet certificates
	July 20, 2010	Symantec blog post introduced Stuxnet propagation method
②	July 19, 2010	Siemens reported Stuxnet attack on its SCADA system
	July 23, 2010	Kaspersky published the fourth and fifth articles in the series of blog posts Myrtus and Guava and began to study industrial control

		systems.
	August 6, 2010	Symantec published a blog post claiming it is the first rootkit targeting industrial control systems
	August 18, 2010	Antiy released a sample analysis report
	September 21, 2010	Symantec published a blog post describing the process of Stuxnet infecting PLCs
	September 26, 2010	Kaspersky published a series of blog posts, Myrtus and Guava, introducing relations with Iran
	September 26, 2010	Symantec published a blog post introducing how Stuxnet infects the Step7 project
	September 27, 2010	Antiy released first version of complete report
	September 30, 2010	Symantec demonstrated PLC system at VB conference
	October 11, 2010	Antiy added a follow-up report
③	November 16, 2010	Symantec released a blog post stating that Stuxnet's attack target was a uranium enrichment facility at an Iranian nuclear power plant.
④	February 2, 2011	Kaspersky released a correlation analysis of Stuxnet's timestamps
	December 28, 2011	Kaspersky released correlation analysis between Stuxnet and Duqu
	January 23, 2012	Antiy completed the analysis of the specific impact of WINCC on uranium centrifugation
	January 23, 2012	Antiy completed homology analysis of Stuxnet and Duqu and released report

It is in this constant reflection growth, we gradually achieved more analysis results. With the efforts of all parties around the world for more than a decade, the giant cyberspace bald eagle of the US has gradually emerged from the fog. Through the organizations revealed by all parties, capability resources, cyberspace engineering systems, weapon equipment, operation methods and operating ways, we can see the huge system scale and in-depth technical capability reserves of the US cyberspace attacks. In the current relay competition, some have already withdrawn. European and American vendors revealed US cyberspace samples at an early stage, but had to keep silent during subsequent research. While some consistently maintain a high level of output, Kaspersky maintains a consistent level of continuous disclosure. Chinese security vendors are also growing through continuous follow-up analysis and exposure. The analysis results contributed by Chinese security

enterprises have accounted for an increasingly higher proportion. With the joint efforts of security vendors and organizations, the full picture of this behemoth has been gradually spliced out.

Fig. 7-2 The Composition of the US Cyberspace Weapons and the Proportion Disclosed by Various Security Vendors

(Based on various reports accumulated by Antiy Cyberbrain platform, if you think there are any statistical issues, please contact us.)

Since the Stuxnet event was discovered in 2010, the analysis of the US has been exposed continuously by all parties, due to the huge scale of the US attack system, it is difficult to independently form a complete analysis. It has become normal for the international cybersecurity community and researchers to collaborate on analysis and exposure, and the analysis results complement or verify each other. This collective collaborative analysis is the common recognition of the US cyberattacks by the global cybersecurity academia and community. We have sorted out the analysis data of current global cybersecurity agencies on the US's cyberspace capabilities and weapons, and mapped them in the form of Sankey diagrams. From the figure below, it can be seen that global cybersecurity agencies work together to analyze the actions of the US intelligence agencies and jointly attempt to decrypt the US cyberspace devil.

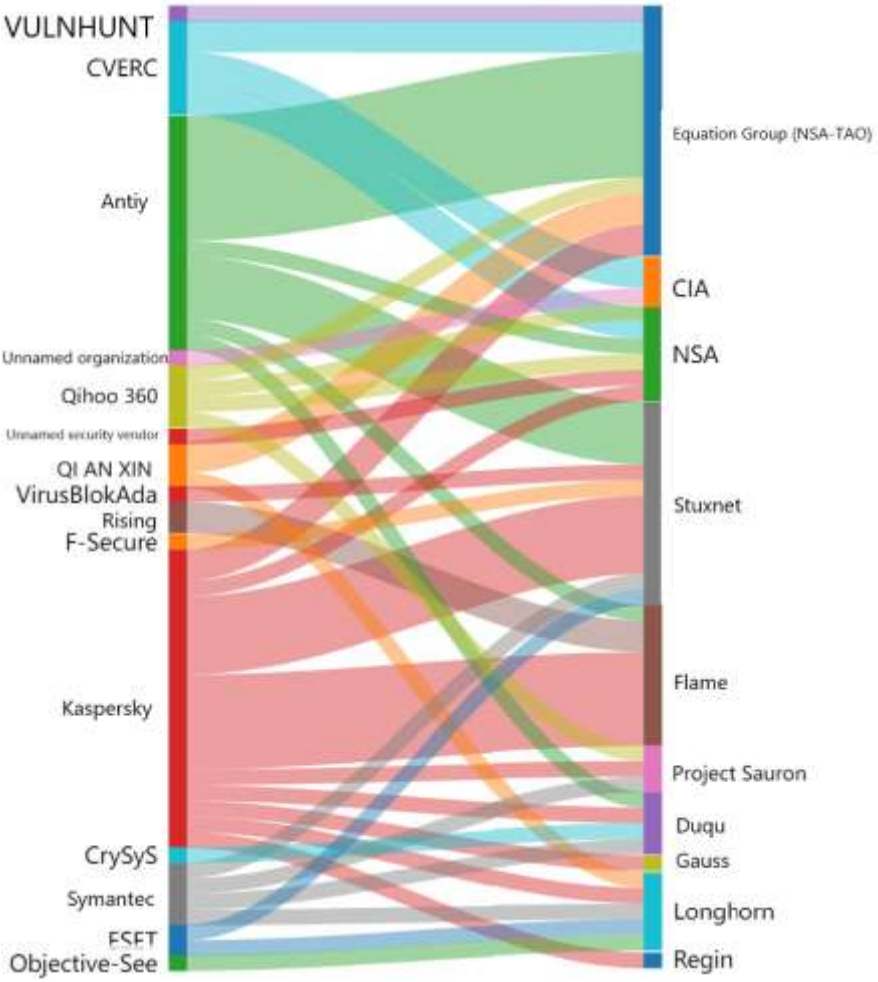


Fig. 7-3 Analysis of Global Security Vendors on the United States' Cyber Attacks and Activities

(Based on various reports accumulated by Antiy Cyberbrain platform, if you think there are any statistical issues, please contact us.)

Fig. 7-4 Analysis of Global Security Vendors on the United States' Series of Cyber Attacks and Activities (Gantt Chart)

(Based on various reports accumulated by Antiy Cyberbrain platform, if you think there are any statistical issues, please contact us.)

Struggling against such cyberspace devil requires immense courage and may also face various comprehensive risks. Our statistical data comes from the automatic statistics of various analysis

reports on Antiy Cyberbrain platform, which may not be complete and fully reflect the analysis results of our peers. We will make corrections based on feedback. Listing data is not to prove how strong our abilities are, but to show that analyzing the giant bald eagle requires collaboration and joint efforts from multiple parties.

8. Significance and Regularity of A^{2}PT Analysis

APT stands for "Advanced Persistent Threat". "Advanced" refers to both the capabilities, resources, tactics and other elements of the attacker, as well as the asymmetry and gap between the attacker and the defender. "Persistent" reflects the attacker's strategic intent and even strategic determination. It involves not only long-term waiting for the emergence of penetration windows at the tactical level, but also maintaining long-term control connection and information theft after achieving persistence. What's more, under the long-term strategy, it is reflected in the repeated redeployment, adjustment and upgrade of attack weapons in the face of defense and hunting, and the continuous iteration of the engineering system to support the attack. The life cycle of an APT can be decades long.

Because APT is such a long-term and continuous operation process, defense activities such as identification, shaping, protection, detection, and response must be a continuous iterative process. Based on clues and assumptions, through comprehensive analysis of motivation, tactics, weapons, risks, etc., we can gain a deeper understanding of threat activities, improve defense deployment, production rules and strategies, and threat intelligence, and enhance security products and services. That is the main value of our APT analysis work. Publishing analysis results and exposing APT activities is just one part of our overall efforts. This is to enable customers and the public to understand the threat landscape, achieve wider sharing of strategic and technical intelligence, respond on a larger scale, and increase costs for attackers. Nor can disclosure and analysis be one-off tasks. At the same time, in order to further explore the regularity and characteristics of complex attack activities and find the context and correlation, APT analysis must also be regarded as a

continuous research activity to associate with new conditions and samples in the massive samples and clue data with old history, so as to find correlations, discover doubts and answer questions. Therefore, the value of APT analysis results does not entirely depend on who publishes and exposes the initial clues first, but also depends more on who can promote the iteration of defense capabilities more continuously and who can maintain long-term research focus.

Obviously, analyzing A^2PT attacks is more difficult than analyzing typical APT attacks, requiring more patience and determination, greater resource investment, and stronger analytical capabilities. We refer to attacks from the US intelligence agencies as A^2PT, which is based on the characteristics of operational capabilities. This is not our exclusive opinion. Let's take a look at the statements from international researchers. Mike Cloppert's viewpoint in *Why Stuxnet Is Not APT*[15] is that "The level of sophistication of Stuxnet is by every account very high. The code is relatively difficult to reverse engineer, contains a PLC rootkit, multiple zero-day exploits, and code that can run on processors with different chipsets. More often than not, the binaries in APT intrusions are relatively straightforward, and exploit a single vulnerability most often in client applications."

Defending against A^2PT attacks is a huge challenge, but so is exposing A^2PT attacks. China is not just a victim of cyber attacks. In the international public opinion field dominated by the West, China is a vulnerable party. When Chinese cybersecurity enterprises release an analysis report alone, it often does not attract any attention. Our analysis results prior to 2014 were no exception. Therefore, Chinese cybersecurity enterprises often do not choose to immediately disclose their analysis results, but wait for international researchers to release relevant results before following up. Relying on reserve of analysis results formed by precipitation and accumulation, our analytical reports can quickly keep pace with international peers after 2015. Moreover, Chinese culture is introverted and introspective. Chinese agencies do not lobby for budget spending by advocating victimization like American agencies, and do not believe that being attacked is something worth publicizing. Therefore, we do not directly release specific data on victims in analysis results.

But in the process of unveiling this giant bald eagle's veil in the global security industry, we have contributed unique value and played a key role, just like a crucial baton in a relay race. The primary goal of our work is not to create accusations. For security enterprises, the primary goal is to improve the detection and defense capabilities of products, in order to provide better protection. For countries and regions at risk of A^2PT, they need to deeply understand what risks these attacks will bring and how to deal with them.

There is no point in trying to zero out wrongdoing that has already been uncovered by allegedly not seeing the PCAP package. The US has established the world's largest attack infrastructure, developed cyber attack weapons covering all scenarios and platforms, and built the largest attack team. The US has not only continued to launch a series of cyber attacks, but also carried out a number of malicious activities that abuse the upstream advantages of the supply chain, preset vulnerabilities, and weaken standards. What the US should do is to actively promise to restrain its cyber attacks and surveillance actions, not abuse its upstream advantages in the supply chain and data collection capabilities, and provide security guarantees to other countries, rather than relying on its clever means to avoid the detection of the victim, and maintain its lasting cyber hegemony.

9. Summary: The Morning Light Will Eventually Shine Through the Fog

SentinelOne report is full of arrogance, and we are well aware of the power behind this obvious "revolving door" organization. From the "Square Agreement" to the long-arm jurisdiction, from Alstom in France to Huawei in China, when any nation achieves a harvest through diligent work, this power will strike as expected, and the A^2PT attacks are only a small part of it. But no organization or enterprise in the world can independently resist such attacks, even Kaspersky, which is regarded as the strongest force in the European cybersecurity field. Kaspersky has suffered many waves of attacks, such as being targeted by NSA's CamperDaDa program, being hacked by Duqu 2, source code being stolen, and key personnel's iOS mobile phones being implanted with Trojans. It

can even be said that, the entire security industry in most countries in the world is not strong enough to fight against this behemoth, let alone a security enterprise. So there's always someone trying to remind us: The disparity in power is like how humans from primitive tribes facing the gods on Mount Olympus, asking us not to resist, but we still hope to unravel the truth behind the A^2PT attacks. In the eastern legend, Yu Gong could eventually move away the mountains; In Western mythology, Prometheus would bring the spark to the human world. The US intelligence agencies, including their "revolving door" organizations, are like the bald eagle pecking at Prometheus' liver, not only continuing to inflict damage, but also restraining the hands of the injured from resisting. When the inflictor ridicules the victim's incapacity as an original sin, what we see is the arrogance that colonizers and aggressors have been accustomed to for 200 years, treating colonization, invasion, and the victim's lack of sufficient resistance as an original sin.

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

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

Launching attacks is a fact, and causing harm is also a fact, which is the truth that our work restores.

The morning light will eventually shine through the fog!

Appendix 1: References

[1] China's Cyber Revenge | Why the PRC Fails to Back Its Claims of Western Espionage
https://www.SentinelOne.com/labs/chinas-cyber-revenge-why-the-prc-fails-to-back-its-claims-of-western-espionage/

[2] Subsequent Analysis Report on Stuxnet Worm
https://www.antiy.cn/research/notice&report/research_report/20101011.html

[3] Re-examination and Reflection on the Stuxnet Incident Nine Years Ago
https://www.antiy.com/response/20190930.html

[4] Flame Worm Sample Set Analysis Report
https://www.antiy.com/response/flame/Analysis_on_the_Flame.html

[5] Exploring the Mystery of the Origin of the Duqu Trojan
https://www.antiy.cn/research/notice&report/research_report/261.html

[6] A Trojan That Modifies the Hard Disk Firmware: Exploring the Attack Components of the

EQUATION Organization

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

[7] Analysis of Encryption Techniques in Some Components of EQUATION

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

[8] From "Equation" to "Equation Group": Analysis of the Full-Platform Capabilities of the Advanced Malicious Code of the EQUATION Attack Organization

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

[9] "Quantum" System Breaks Through Apple Mobile Phone - Analysis of Historical Samples of Equation Group Attacking IOS System

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

[10] Analysis of Samples Used in a Quasi-APT Attack Against Chinese Institutions

https://www.antiy.com/response/APT-TOCS.html

[11] Review and Outlook of Cyber Security Threats in 2016

https://www.antiy.com/response/2016_Antiy_Annual_Security_Report.html

[12] Antiy's Operation Manual on Systematic Response to NSA's Cyber Arms and Equipment

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

[13] Sabotage in Iran: een missie in duisternis

https://www.volkskrant.nl/kijkverder/v/2024/sabotage-in-iran-een-missie-in-duisternis~v989743/

[14] Equation Group Attack on SWIFT Service Provider EastNets

https://www.antiy.com/response/20190601.html

[15] Why Stuxnet Isn't APT

https://www.sans.org/blog/why-stuxnet-isnt-apt/

Appendix 2: About Antiy

Antiy is committed to comprehensively improving customers' network security defense capabilities and effectively responding to security threats. After 20 years of independent research and development, Antiy has formed the technological leading edge in threat detection engine, advanced threat confrontation and automated large-scale threat analysis. Antiy has developed a series of products (including ASS, IEP, PTF, PTD, ACS, PTA, TDS and ZTC), building the security cornerstone of asset operation and maintenance, endpoint protection, boundary protection, flow monitoring, diversion capture, in-depth analysis, and emergency handling for customers. By building a situational awareness platform system for customers, Antiy forms the nerve center of network security operation, enhances customers' unified security operation and maintenance capabilities, and continuously empowers customers through fast and accurate threat intelligence. Antiy's products and solutions ensure the overall security of customers from office intranet, private cloud and hybrid cloud to industrial production network, and ensure the security of customers' key data assets and business continuity, so that customers can effectively deal with different levels of threats from virus infection, online extortion and even intelligence-level attacks, and escort customers' digital transformation.

Antiy provides overall security solutions for high-security demand customers, such as network and information authorities, the military, confidentiality, ministries and commissions, key information infrastructure departments and etc.. The products and services of Antiy have ensured manned space flight, lunar exploration projects, space station docking, the first flight of large aircraft, capital ship escort and other major national projects. Antiy has participated in the security work of several major political and social activities after 2005, and won many titles such as outstanding contribution award and advanced security team.

Antiy is also a core enabler on the world's fundamental infrastructure security supply chain. Nearly 100 well-known security enterprises and IT enterprises around the world have chosen Antiy as their partner of detection capability. The detection engine of Antiy has provided security protection for over 1.3 million network devices and network security devices, and over 3 billion intelligent terminal devices. Among them, Antiy's mobile detection engine won the 2013 authoritative evaluation award from internationally renowned testing institutions.

Antiy is the significant enterprise node of China emergency response system, which has provided early warning and comprehensive emergency support in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". As for the dozens of advanced cybersecurity actors (such as APT groups) and their attack actions such as "Equation", "White Elephant", "Lotus" and "Greenspot", Antiy carries out continuous monitoring and in-depth analysis, and assists customers to form effective protection under "considerate enemy situation". Through in-depth analysis of the operational capability of advanced cyber threat actors, Antiy has established a combat-scenario-oriented capability system.