Examining the US Network Attack Equipment System from the perspective of the Emergence of Remote Control Trojan "NOPEN"

Antiy CERT

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

Scan QR code for the latest version of the report

Time of completion of the first draft: March 15, 2022

First published March 15, 2022

©Antiy All Rights Reserved. Reprint without loss is welcome

1 Overview

Recently, the National Computer Virus Emergency Processing Center exposed a Trojan tool named "NOPEN" (for details, see the second article "Analysis Report on Remote Control Trojan Horse" published today by Antiy Public). This tool is a powerful and comprehensive Trojan horse tool of the NSA, and one of the main cyber weapons used by the NSA for foreign attack and secret theft. Relevant leaked data show that the Trojan horse has taken control of computer systems in many countries around the world.

Since the Stuxnet event in 2010, Antiy has been continuously analyzing and tracking APT (Advanced Persistent Threat) attack activity worldwide. Among them, the US launched attack activities and attack equipment on behalf of the APT attack ceiling capability, known as A2PT (Advanced Persistent Threat). In the series of US attack equipment and activity reports released by Antiy, the persistence mechanism of "Formula Organization" writing into hard disk firmware (2015) and Trojan encryption communication protocol (2015) were demonstrated. It was the first to expose the US Solaris platform samples (2016), and completed the US Trojan module puzzle and other analysis results (2017). The "NOPEN" Trojan horse is a member of the US formulaic cyber attack equipment. in the report made public by ATEON on June 1, 2019, it traced back to the fact that the US invaded the EastNets in the Middle East and mentioned the equipment.[1]

In order to enable computer users around the world to have a more comprehensive understanding of A2PT attack equipment and attack characteristics and realize effective security protection, we will sort out the main points of the analysis reports that have been published and combine some unpublished results. Presented in this report.

2 NSA Cyber Attack Equipment and Platform

The National Security Agency (NSA) has built a systematic network attack platform and a formulaic attack equipment library, and the National Security Agency (NSA) TAO (Tailored Access Operations) is the main user of these attack equipment. The Office consists of five departments: Ant (Advanced Network Technology), DNT (Data Network Technologies) and ATO (AccessTechnologies Operations). Access Technology Business Unit), MIT (Mission Infrastructure Technologies) and TNT (Telecommunications Network Technologies). At present, the attack equipment of ANT and DNT departments has been exposed a lot, such as 48 ANT toolsets, the Fuzzbunch exploit platform of DNT department leaked by shadow broker, and the Dander Spritz remote control attack platform.

©Antiy All Rights Reserved. Reprint without loss is welcome

2.1 Ant family of attack equipment

Ant attack equipment family is an attack equipment system that the United States installed in batches around 2008, basically covering mainstream desktop hosts, servers, network equipment, network security equipment and mobile communication equipment at that time. The forms of equipment include malicious code payload, computer peripherals, signal communication equipment, etc., which can be used in combination to achieve their complex attack targets. According to the information exposed by Snowden, the United States through ANT attacks the world's mainstream network equipment, and in which the back door, a total of 48 types of attack equipment information surfaced, including software, hardware are involved. Among them, software equipment is mainly used to implant persistent backdoors into various IT equipment systems for the purpose of stealing information, and hardware equipment is mainly used to embed attack capabilities into IT hardware. Or in the form of independent hardware equipment, used for signal theft, monitoring, interception, establishment of communication channel. The following table shows 48 types of network attack equipment that have been exposed.

Table 1 ANT Network Attack Equipment Base 1

Equipment name / code number	Functions	Equipment name / code number	Functions
Ragemaster	Video data monitoring	Dropoutjeep	Cell phone data collection
Picasso	Cell phone threat monitoring	Totechaser	Cell phone data collection
Gopherset	Cell phone threat monitoring	Toteghostly 2.0	Cell phone data collection
Monkeycalenda	Cell phone threat monitoring	Ironchef	Hard disk firmware modification
Genesis	Cell phone scanning, signal masking	Wistfultoll	Registry data collection
Candygram	Cell phone threat monitoring	Sparrow II	Wireless data collection
Nebula	Cell phone threat monitoring	Loudauto	Radar data collection
Waterwitch	Cell phone threat monitoring	Crossbeam	Cell phone data collection
Tawdryyard	Radar data monitoring and control	Cyclone Hx9	Cell phone data collection
Souffletrorough	Hard disk firmware	Ebsr	Cell phone data collection
Cotton MOUTH-I	Wireless payload attack	Entourage	Cell phone data collection
Cotton MOUTH-III	Physical isolation attacks	Typhon HX	Cell phone data collection

©Antiy All Rights Reserved. Reprint without loss is welcome

Deitybounce	Dell exploit	Headwater	Permanent back doors
Ginsu	Persistence code	Jetplow	Permanent back doors
Iratemonk	Hard disk firmware	Halluxwater	Permanent back doors
Slickervicar	Hard disk firmware	Feedtrough	Permanent back doors
Swap	Hard disk firmware	Gourmettrough	Permanent back doors
Somberknave	Physical isolation attacks	Ctx4000	Electromagnetic data collection
Arkstream	Hard disk firmware	Photoanglo	Electromagnetic data collection
Nightstand	Physical isolation attacks	Schoolmontana	Control of network equipment
Howlermonkey (HM)	Physical isolation attacks	Sierramontana	Control of network equipment
Surlyspawn	Key record collection	Stucconmontana	Control of network equipment
Cotton MOUTH-II	Command control	Nightwatch	Mutual benefit of video signal erasure
Firewalk	Flow monitoring	Trinity	Eavesdropping on the chip

2.2 Dnt attack equipment

On April 14, 2017, the Shadow Brokers Group exposed the NSA's Fuzzbunch Vulnerability Attack Platform and the DanderSpritz Remote Control Platform, saying the attack gear was linked to the Formula Organization. In accordance with relevant analysis and data, these attack equipment are at that level developed by the United state several years ago, involving a large number of system-level 0day exploit tools and advanced backdoor procedures. It exposed the US's vulnerability reserve capability and attack technology.

©Antiy All Rights Reserved. Reprint without loss is welcome

Figure 1 Structure analysis of NSA / DS-FB platform 1

2.2.1 Fuzzbunch Vulnerability Attack Platform

Fuzzbunker is a penetration, attack platform, responsible for using the vulnerability to implant the target host payload (generated by DanderSpritz), in the process of implantation can be directly memory executed, no entity files will be generated.

©Antiy All Rights Reserved. Reprint without loss is welcome

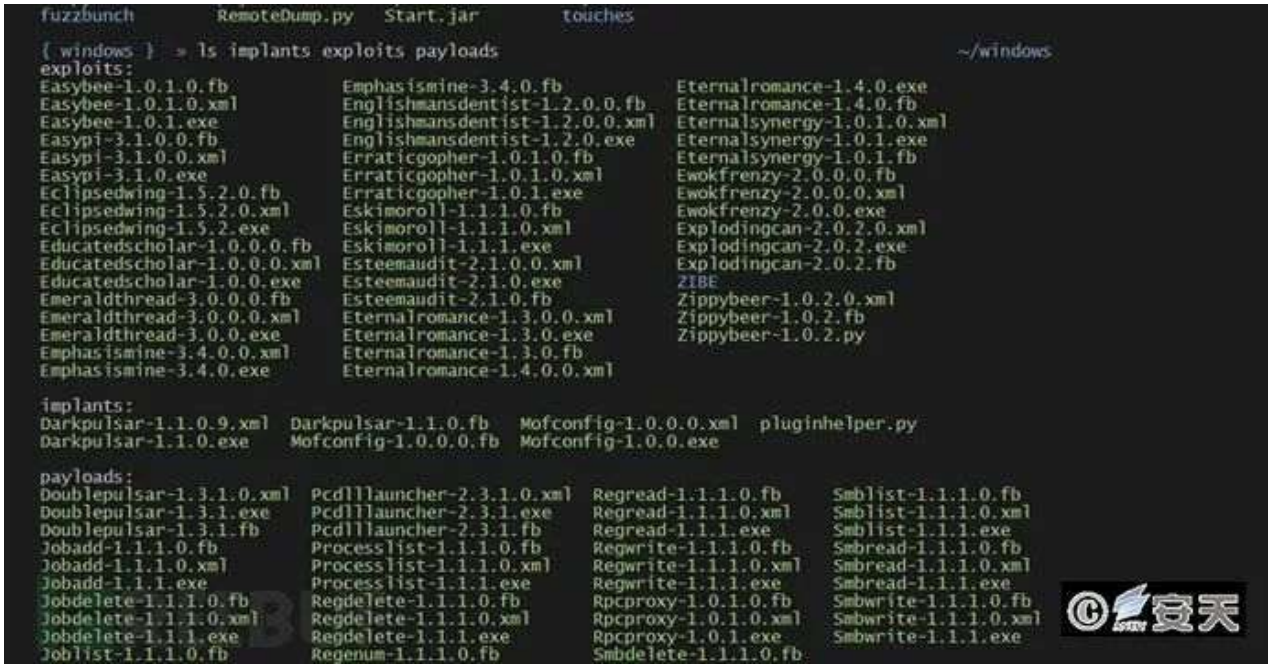

Figure 2 Platform for vulnerability attack of Fuzzbunch 2

After the attack platform was leaked, the "Eternal Blue" vulnerability was used by the WannaCry worm to spread, causing serious losses to the global network, and the "Eternal Blue" vulnerability is only one of the many vulnerabilities in the vulnerability library. Other vulnerabilities have superior lateral mobility. In May 2017, Antiy combed through the vulnerabilities as shown in Figure 3.Figure 3 The relationship between the utilization of the Fuzzbunch vulnerability 3

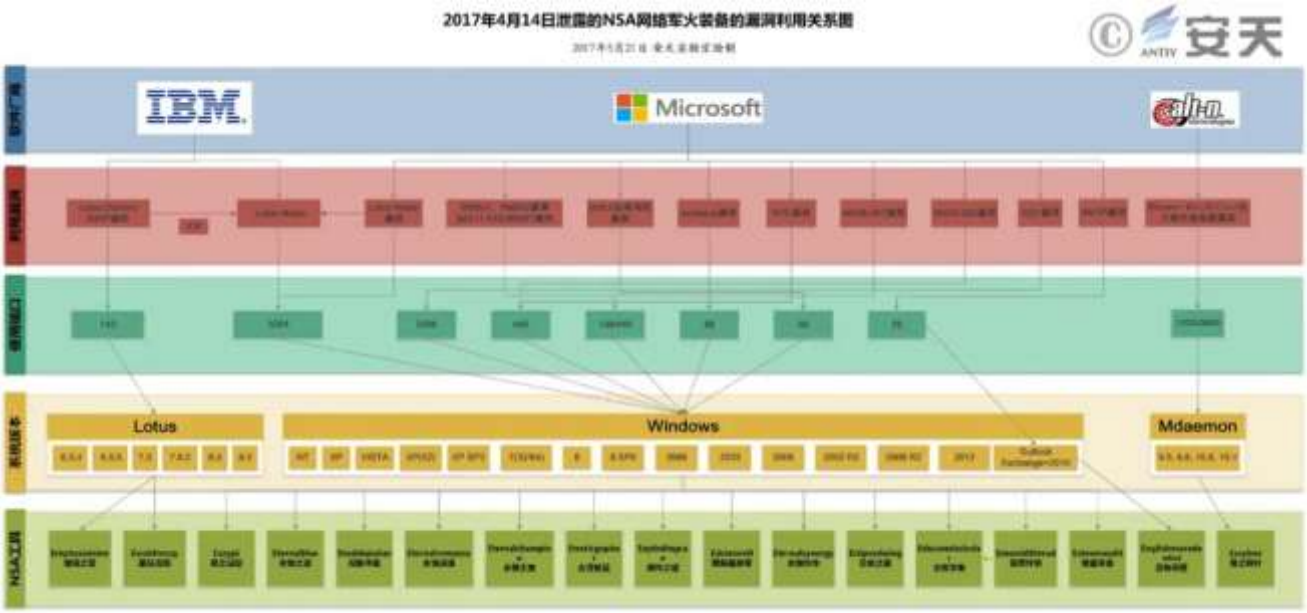

Figure 3 The relationship between the utilization of the Fuzzbunch vulnerability 3

©Antiy All Rights Reserved. Reprint without loss is welcome

2.2.2 Danderspritz remote control platform

Danderspritz is a remote control platform, and once the load generated by it is implanted into the remote host, complete control of the target host can be achieved. It uses a covert way to activate communication, uses strict encryption in the communication process, and can complete any task (such as stealing data, throwing more advanced attack payload, etc.) through a series of extension plug-ins.

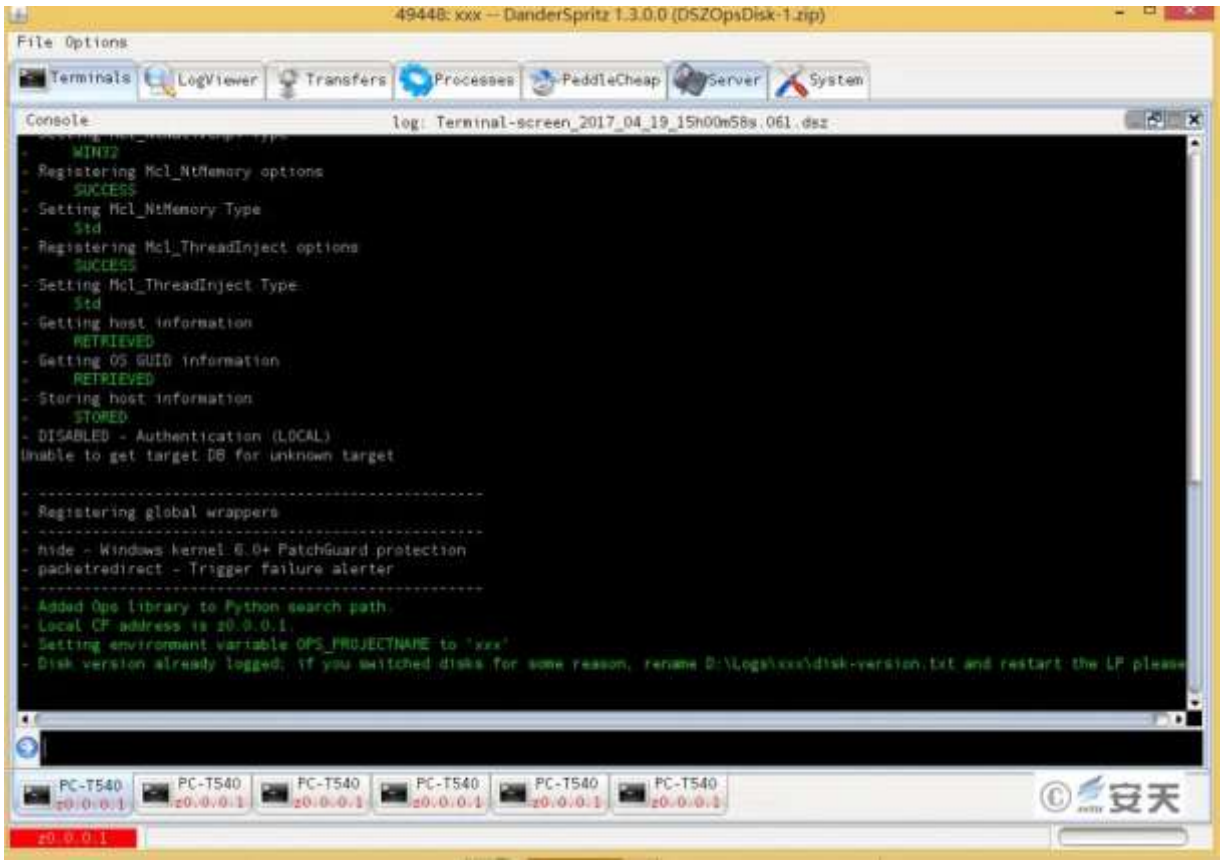

Figure 4 DanderSpritz remote control platform 4

With the help of the DanderSpritz platform, the attacker can control the victim host in all directions, and the specific operation is through the combination of hundreds of plug-ins to complete the corresponding functions. These plug-ins represent an architectural style that, instead of writing a single Trojan horse with a highly complex functionality, breaks the functionality down into small modules that are highly independent, with a granularity that is almost "atomized." If it is simple such as that operation of obtain the system information, it also takes the similar obtain environment variable, language set, network state and so on as an independent small module, which will ensure that the system operation can be fully developed on demand, Thereby maximally ensuring the care and silence of the job.

©Antiy All Rights Reserved. Reprint without loss is welcome

Most of the documents exposed by the "Shadow Broker" are attack plug-ins of the "DanderSpritz" platform. according to the list of released documents, the attack tools and plug-ins are very rich and standardized. Including remote control, vulnerability utilization, backdoor, plug-in, etc. For example, the DanderSpritz _ All _ Find .txt file contains more than 7, 000 lines, of which there are hundreds of plug-ins.

DanderSpritz

Name	Type	Price
DanderSpritz All	DanderSpritz Everything	250.0 BTC
DanderSpritz Base	DanderSpritz LP Only	25.0 BTC
PC2.2	DanderSpritz RAT	25.0 BTC
ST1.14	DanderSpritz BackDoor	25.0 BTC
LegacyWindowsExploits	DanderSpritz Exploits	25.0 BTC
DaPu	DanderSpritz Plugin	10.0 BTC
Darkskyline	DanderSpritz Plugin	10.0 BTC
DeMi	DanderSpritz Plugin	10.0 BTC
Df	DanderSpritz Plugin	10.0 BTC
DmGz	DanderSpritz Plugin	10.0 BTC
Dsky	DanderSpritz Plugin	10.0 BTC
EP	DanderSpritz Plugin	10.0 BTC
Flav	DanderSpritz Plugin	10.0 BTC
GaTh	DanderSpritz Plugin	10.0 BTC
GeZu	DanderSpritz Plugin	10.0 BTC
GrCl	DanderSpritz Plugin	10.0 BTC
GrDo	DanderSpritz Plugin	10.0 BTC
GROK	DanderSpritz Plugin	10.0 BTC
Pacu	DanderSpritz Plugin	10.0 BTC
Pc	DanderSpritz Plugin	10.0 BTC
Pfre	DanderSpritz Plugin	10.0 BTC
ScRe	DanderSpritz Plugin	10.0 BTC
StLa	DanderSpritz Plugin	10.0 BTC
TeDi	DanderSpritz Plugin	10.0 BTC
UtBu	DanderSpritz Plugin	10.0 BTC
Zbng	DanderSpritz Plugin	10.0 BTC

Figure 5 Screenshot of the attack plug-in for the "DanderSpritz" platform exposed 5

©Antiy All Rights Reserved. Reprint without loss is welcome

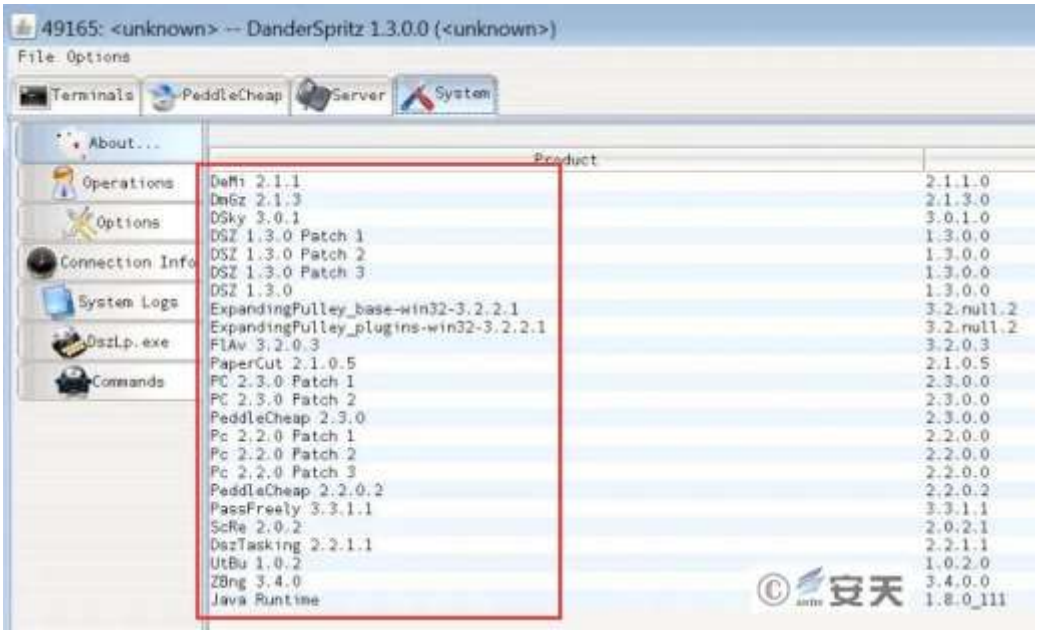

Figure 6 screenshot of the "DanderSpritz" attack platform 6

3 NSA Framework for Research and Development of Cyber Attack Equipment

The US advantage in cyberattack equipment stems from its operational objectives, which attempt to cover all mainstream IT scenarios, and its multi-year continuous investment.

In a follow-up analysis of the Stuxnet in 2011, Antiy suggested the possible homology between the Stuxnet and the virus [2] [3]. Through the comparison of key code structure, key using method and code logic between virus and stuxnet worm, we find a lot of identical or similar code fragments, and prove our conjecture [4]. Antiy's conclusion at that time was that "through the comparison of key code structure, key use method and code logic between virus and stuxnet worm, we found a large number of identical or similar code segments. This indicates that there is a code reuse relationship between the two, or that both are developed based on the same code framework. "But the question of whether the relationship to reuse or the development of the same framework was inconclusive at the time. Combining the later analysis results and progress of other organizations, it can be concluded that at least two malicious code frameworks, namely, Tilded and Flamer, have been maintained by the relevant A2PT attack organizations. Stuxnet, Toxic and Flame, and Gauss are developed based on the Tilded and Flamer frameworks respectively. On June 11, 2012, Kaspersky released a report that the earlier version of the 2009 version of the Stuxnet

©Antiy All Rights Reserved. Reprint without loss is welcome

module (called "Resource 207") was actually a Flame plugin. The result is a concatenation of two completely different frameworks, Flamer and Tilded. The malicious code based on these two frameworks has unique skills in infecting target systems and executing major tasks, both of which are used to develop different net-to-air attack equipment. Kaspersky concludes that the teams behind the two frameworks have shared the source code of at least one module, indicating that they have worked as a team at least once, and that they are two parallel projects belonging to the same institution [12]. Based on more clues, you can also string together Fanny and Flowershop with the above events, as shown in Figure 7.[2][0][4]Figure 7 Relationship between Shake-net and Toxic Warp, Flame, Gauss, Fanny, and Flowshop 7

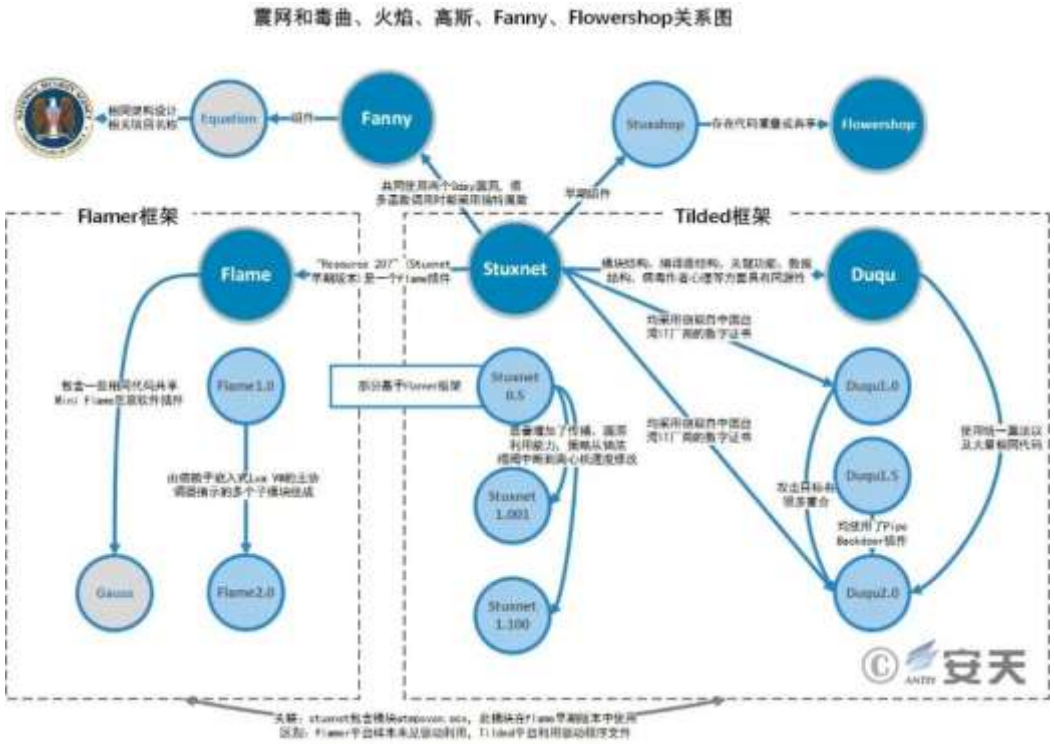

Figure 7 Relationship between Shake-net and Toxic Warp, Flame, Gauss, Fanny, and Flowshop 7

4 Operational Characteristics of US Cyber Attacks

According to the analysis of weapons and attack actions of the US side, we can conclude the following characteristics of the cyberattack operation of the US side:

1. Conduct all-round pre-investigation and information collection. For example, in the Stuxnet incident, the United States went through more than four years of preparation, and before attacking Iran's nuclear facilities, the United States had completely infiltrated Iran's basic industrial institutions. Including equipment manufacturers, suppliers,

©Antiy All Rights Reserved. Reprint without loss is welcome

software developers, and so on, complete research and simulation of Iran's nuclear industry system, the implementation of the final attack only after knowing one's own enemy.

2. Sufficient 0day vulnerability reserves, and saturated multi-vulnerability combination use. For example, in the "Stuxnet" attack, the US used no less than five 0day vulnerabilities; in the attack on SWIFT service providers in the Middle East, the US used no less than seven 0day vulnerabilities. All these can show that the United States has an extremely rich reserve of 0day loopholes, and in its strategic attack activities, the United States uses a saturated combination of multiple loopholes with the idea of "Van Freet's ammo volume."

3. Super border penetration ability. The United States is rich in vulnerabilities in network firewalls, routers, switches, VPNs and other network equipment, and has complete tools to access control boundaries and network equipment and forward traffic. And this will be used as a relay station to continuously attack the internal network target. For example, in the attack on EastNets, the largest S WIFT service provider in the Middle East, the US broke through the external VPN firewall and the intranet enterprise firewall successively, and installed the traffic forwarding Trojan horse on the firewall.

4. Combination of manpower, electromagnetism and net-air operation. The United States regarded the cyberspace as only one of the channels to achieve secret theft, and the combination of human means and electromagnetic means to achieve the best attack effect. For example, ANT's "Agkistrodon I" is an electromagnetic network-to-air hybrid device that combines USB-based injection and wireless data return mechanisms, with a maximum communication range of up to 8 miles, according to the data.

5. Super-strong breakthrough capability against physical isolation. The United States broke through the physical isolation network by establishing a bridgehead and a second electromagnetic channel with the aid of peripherals and auxiliary signaling devices based on the modes of logistics chain hijacking and bringing in by people. For example, in the Stuxnet attack, according to the relevant information, the personnel of the Dutch intelligence agency enter the scene and connect the USB device with the Stuxnet virus to the isolated internal network to initiate the attack.

6. High modularization of ultra-large-scale malicious code engineer load, high complexity of load frame and loader part against analysis and detection, and only limited collection and persistence of delivery load in early stage, Only when the conditions of remote delivery advanced payload are satisfied can the targeted delivery payload

©Antiy All Rights Reserved. Reprint without loss is welcome

carry out the attack behavior. These characteristics can be seen through the analysis of the structure of the Trojan platform such as DanderSpirit, and the process of attacking EastNets and other targets.

7. Strict local and network encryption, payload configuration data, resources, function encryption against anti-virus and sandbox detection, network communication uses asymmetric encryption. It may also wait for network request activation to combat network-side detection. The widespread use of encryption can be seen from seismic networks to a series of subsequent samples and analyses.

8. Non-file entity technology is widely adopted, and direct memory loading for execution or hidden disk storage space is established. According to the analysis, the United States has basically adopted the memory Trojan horse non-landing technology since at least 2008, and the HASH of the Loader samples of the seismic network changes every time they are landing, which makes the threat intelligence such as the similar file MD5 invalid.

9. Deep covert persistence capability, firmware persistence, firewall and mail gateway persistence. In that case of an attack, a match host is selected, the trojan is written into the hard disk firmware, and the trojan is written into the hard disk firmware even if the us reinstalls the system, Can still be activated again.

10. The payload covers all operating system platforms. So far, samples of various operating system platforms have been found in the US attack, such as Windows, Linux, Solaris, Android, OSX and iOS. This is fully disclosed in Antiy's historical report, "From Equations to Equations."

5 Summary

Network security protection must face up to threats and adversaries, fully realize the severity of the risks and challenges faced by network security, and thoroughly implement the overall national security concept. To safeguard national sovereignty, security and development interests to carry out network security defense work. An in-depth analysis of the organizational structure, support system, attack equipment, operation means, operation system and action characteristics of ultra-high-capacity cyberspace threat actors is an important foundation for our defense work. It is the basic support to build up the objective enemy situation. Build the network security defense work on the basis of correct enemy situation [4], and truly build the dynamic, comprehensive and effective network security defense capability.[4]

©Antiy All Rights Reserved. Reprint without loss is welcome

Appendix I: Antiy continues to analyze the information regarding the US attack organizations and attack incidents.

Antiy has continued to track and analyze US attack organizations and related events, and has released dozens of relevant analysis results since 2010 [5].[0]

In 2010, Antiy released the "Comprehensive Report on the Stuxnet Worm Attack on Industrial Control Systems" [6]. The report analyzes the attack process, propagation mode, attack intention and file derivation of the Stuxnet worm, analyzes several zero-day vulnerabilities it exploits, summarizes the attack characteristics of the worm, and gives a solution. Finally make evaluation and thinking. The report is an early comprehensive report on seismic network analysis by reverse engineering system in China, and an important reference for the domestic public to understand the truth and details of Stuxnet worm attack. In October of the same year, Antiy issued a supplementary analysis report, pointing out that the transmission of seismic network through USB disk is determined by seven groups of configuration data, including time stamps and restrictive conditions, In addition, we analyze that propagation and update of seismic network in local area network by open RPC service, sharing service and remote access WinCC system database, And the behavior of attacking the PLC (Programmable Logic Controller) of the Siemens system by hijacking the DLL, and determining that the PLC code injected by the seismic network can function normally only in a certain specific hardware device, This further indicates that it is extremely targeted.[0]

©Antiy All Rights Reserved. Reprint without loss is welcome

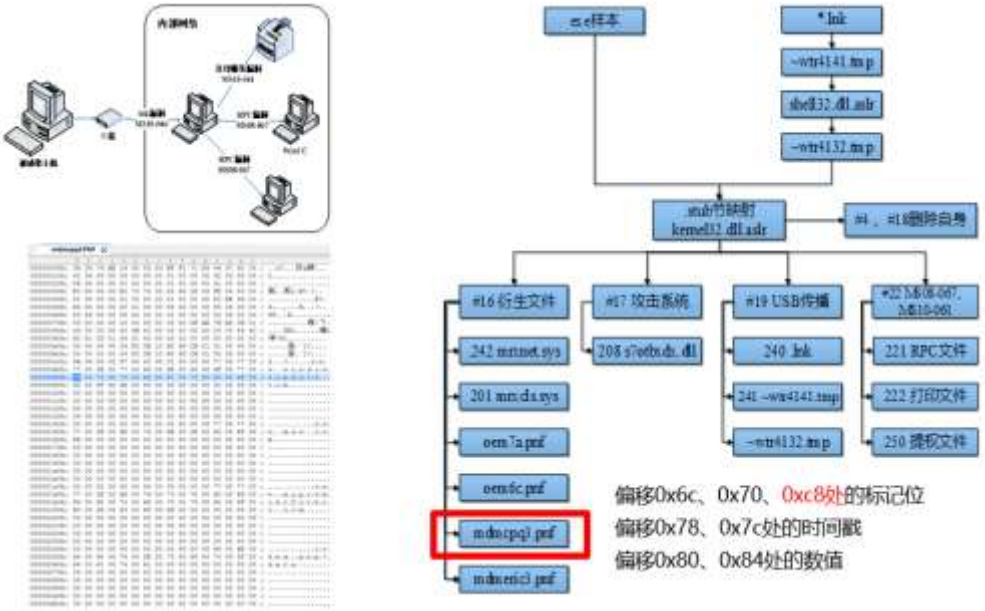

Figure 8 Analysis of seismic network module and analysis of ferry mechanism 8

In September 2011, Antiy released the Homology Analysis Report of Duqu and Stuxnet [6], in which the module structure, compiler architecture and key functions of the Duqu virus were analyzed. It is found that the structure and function of Duqu and Stuxnet are similar to each other, and in the analysis of Duqu's decryption key, anti-tracing method and program BUG, the author's coding psychology is similar to that of Stuxnet. Based on the same logic errors found in the samples of Duqu and Stuxnet, the homology of the two was judged by the method of coding psychology, and the analysis report on the homology of Duqu and Stuxnet was published. And in the "Programmer" magazine published the related article.[0]

In January 2012, Antiy Microelectronics and Embedded Security R & D Center issued a report "What Happened After WinCC" [6], speculating on the possible attack scenario mechanism of Stuxnet: Suppose the centrifuge speed is automatically controlled by PID algorithm. If that worm attack WinCC and modifies the relevant parameter of the PID algorithm in the database, the rotation speed of the centrifuge will change, and even the automatic control of the rotation speed of the centrifuge will fail, otherwise the separation power and the separation coefficient of the centrifuge will decrease. Failure to separate nuclear-grade or weapons-grade uranium-235 (uranium-235 is not high enough).[0]

In July 2012, Antiy published a 100-page "Flame Worm Sample Set Analysis Report" [7], but the analysis only covered less than 5% of the flame virus modules. At the same time, the event also triggered Antiy CERT to this kind of module-by-module stacking type of analysis to reflect.[7]

©Antiy All Rights Reserved. Reprint without loss is welcome

From 2015 to 2017, Antiy published four series of analysis reports on Formula Organization in both Chinese and English. "Trojan Horse to Modify Hard Disk Firmware - Attack Component of the Organization of Equation (EQUATION)" [8], "" Analysis of Encryption Techniques in Some Components of Equation "[9]. "From" Equation "to" Equation Group "- Analysis of High-level Malicious Code by EQUATION Attacks" [10], "Analysis of Equation Organization's EQUATIONDRUG Platform" [11], in a series of reports, In that pap, the mechanism of hard disk firmware reprogramming and the attack module nls _ 933w. dll are analyze in detail, It verifies the ability of ultra-high net-space actors to realize persistence in all sustainable scenarios, and analyzes the local registry data and remote communication data algorithms of the organization, It is pointed out that the organization uses the modified RC symmetric algorithm, gives the complete decryption algorithm, key structure and two-level cipher table, and decrypts the almost dead-angle-free, all-platform attack capability of the organization, Samples of its Linux and Solaris platforms were exclusively declassified around the world, forming a modular block diagram of host operations for an organization of equations, revealing the modular operation mode of ultra-high net-air threat actors. So far, based on the continuous tracking and analysis of Antiy for 4 years, we have found the complete operational capability of the ultra-high-capacity cyberspace threat actor (equation organization).[0][9][10][11]

©Antiy All Rights Reserved. Reprint without loss is welcome

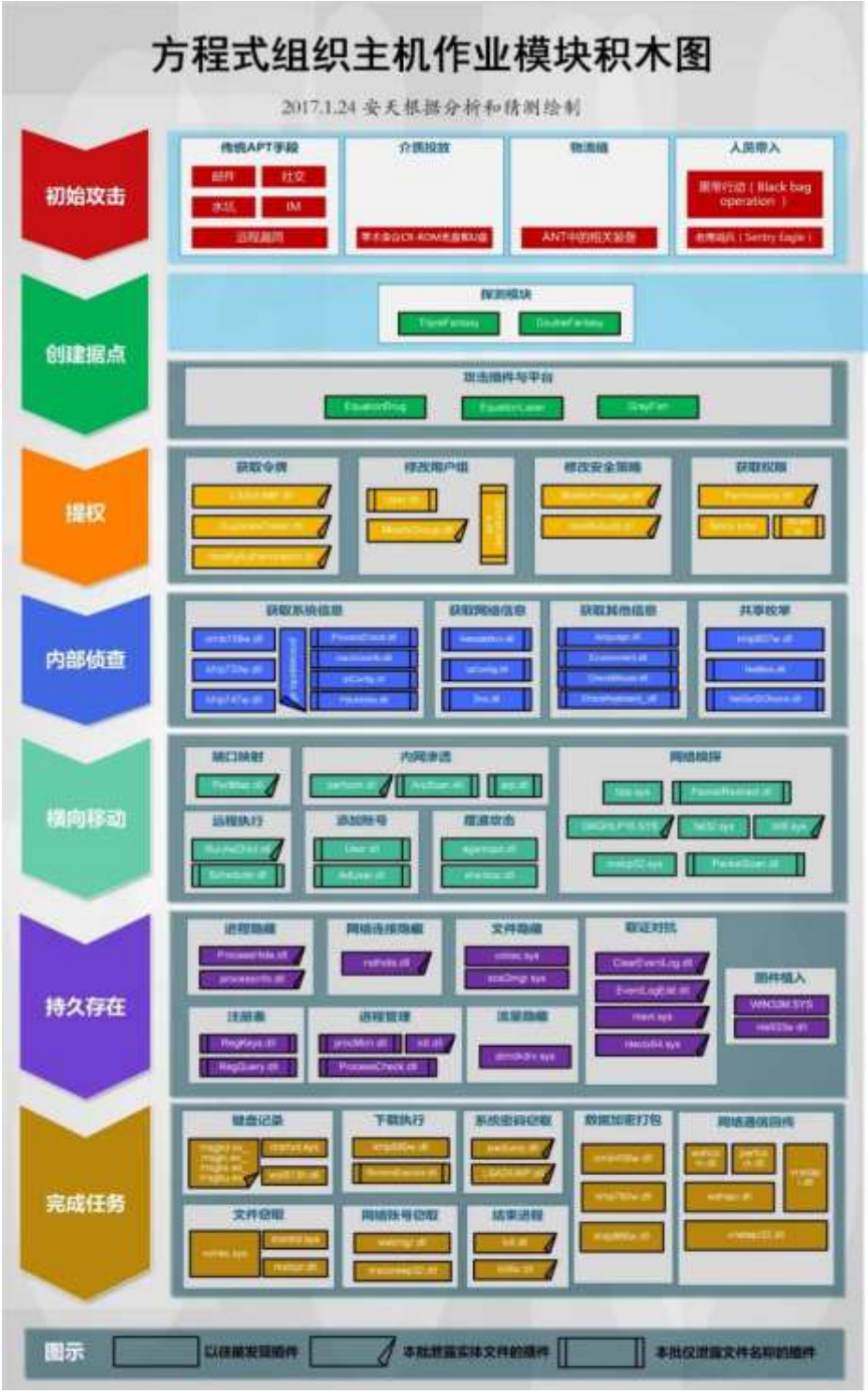

Figure 9 Building block diagram of operation module of equation organization host machine 9

In 2019, Antiy first introduced the process of Formula Group's attack on EastNets, the Middle East financial services agency. This is a new result of Antiy's combination of historical analysis of the Formula Organization with leaked data from the "Shadow Brokers." In the same year, Antiy officially released the Recovering Analysis Report on "Equation Group" Attack on SWIFT Service Provider EastNets [12], which accurately restored the panorama and

©Antiy All Rights Reserved. Reprint without loss is welcome

topology of IT assets affected by the attack. The whole process of the killing chain was completely reappeared, and the weapons used in the operation and the operation process were thoroughly combed and visualized.[12]

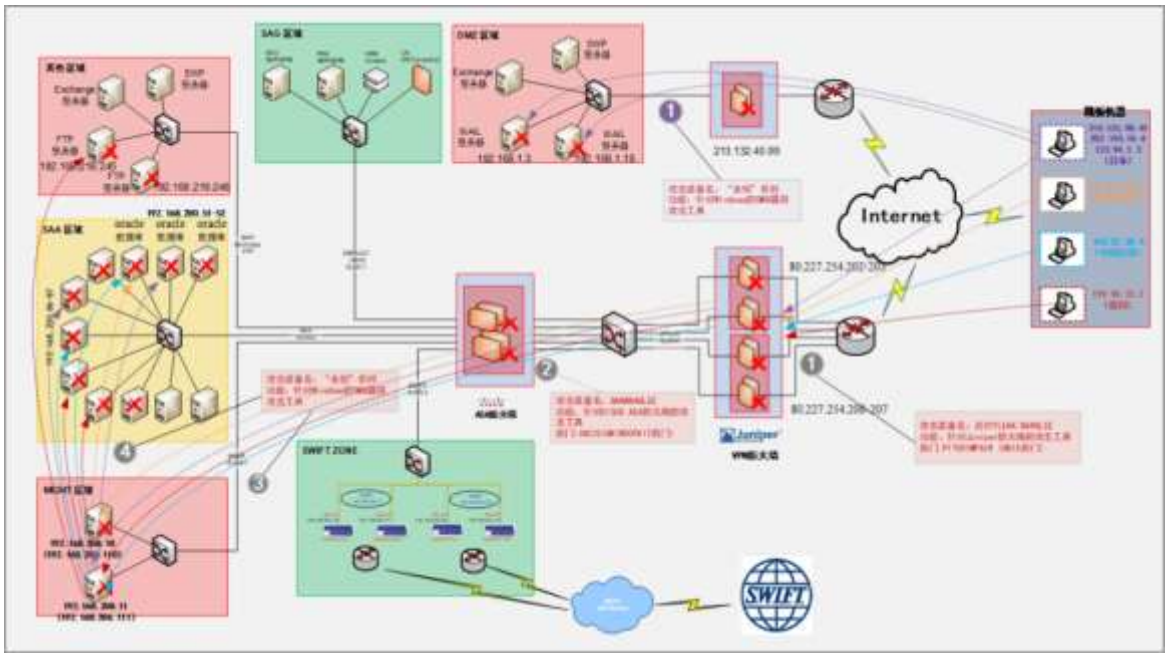

Figure 10 Repeat of the overall attack process of "Equation Organization" on the EastNets network 10

Figure 11 Demonstration of Attack Action Repeated by Antiy Situational Awareness Platform Visualization Component 11

(For details, please see https://www.antiy.cn/video/20190531/lup.mp4)

©Antiy All Rights Reserved. Reprint without loss is welcome

On September 30, 2019, Antiy released a long report entitled "Nine-year Re-evaluation and Thinking of the Stuxnet Incident" [13], in which: Antiy compares the characteristics and mechanism of each version of Seismological Network in detail, and analyzes the correlation between the relevant advanced malicious code engineering framework and the malicious code used by Seismological Network, Poison, Flame and the later-stage equation organization. The complete time axis of seismic network events, the whole structure and operation logic of seismic network, and the reason why there are a lot of samples in seismic network are analyzed. In that pap, the challenge of APT for detection engine and threat intelligence in network security is rethought, How to establish more reliable basic identification capability and response mechanism, more effective support for TTP, more reliable organization of relevant information, more perfect knowledge engineering operation system are considered. In order to deal with the A2PT organization initiated advanced network and air threat.

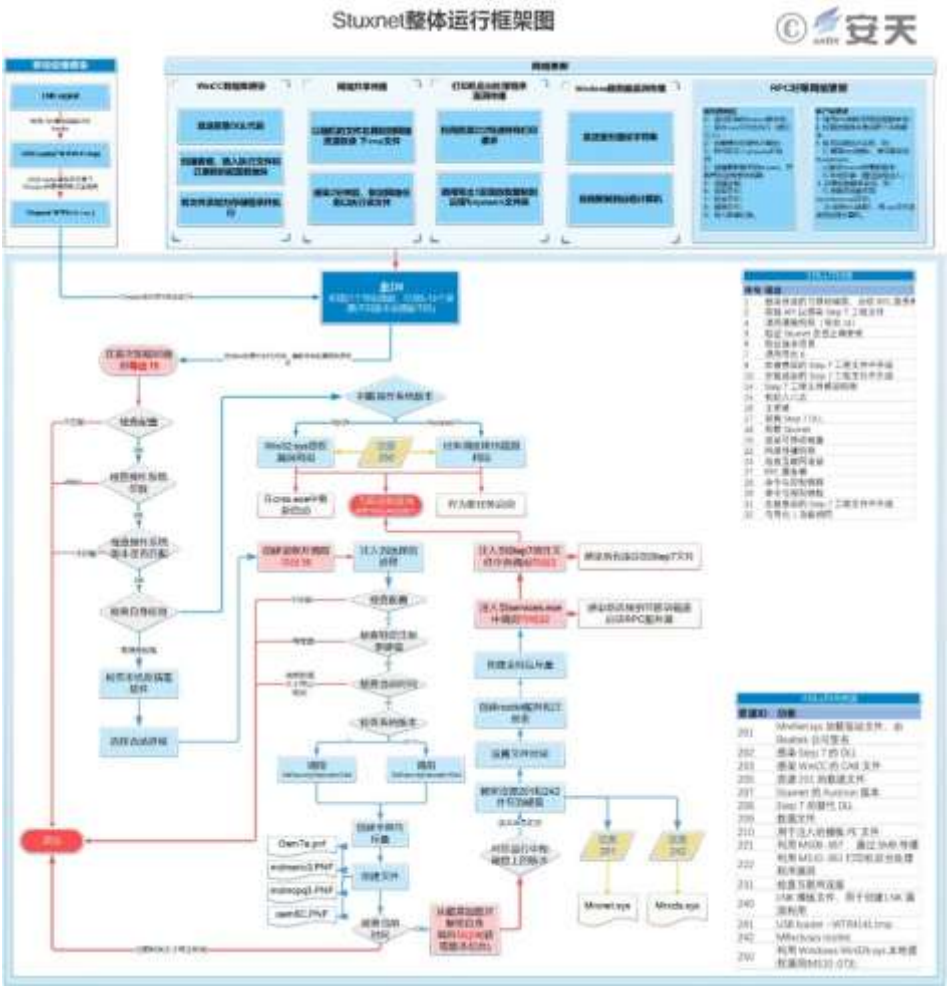

Figure 12 Frame diagram of seismic network overall operation 12

©Antiy All Rights Reserved. Reprint without loss is welcome

Appendix II: Reference

[1] Antiy: "Formula Organization" Attack SWIFT Service Provider EastNets Event Re-offer Analysis Report
https://www.antiy.com/response/20190601.html

[2] Antiy: Exploring the Mystery of the Life of Duqu Trojan Horse - - Homology Analysis of Duqu and Stuxnet
http://blog.sina.com.cn/s/blog_64a6dc1501016sed.html

[3] Antiy: A Study on the Homology of Duqu Virus and Stuxnet Worm and A Collection of Articles on Industrial Control System Security

[4] Antiy: The Application of the Concept of Enemy Situation in Cyberspace Security
https://mp.weixin.qq.com/s/5_izfLmdvVaiTQbt1sHxgQ

[5] Antiy: A Review of Antiy's Series Analysis of "Ultra-High-Capability Cyberspace Threat Activists.
https://www.antiy.cn/research/notice&report/research_report/20210722.html

[6] Antiy: Comprehensive Analysis Report on the Stuxnet Worm Attack on Industrial Control Systems
https://www.antiy.com/response/stuxnet/Report_on_the_Worm_Stuxnet_Attack.html
Antiy: What Happened After WinCC - - Antiy Technical Article Compilation (5) Industrial Control Safety Volume

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

[8] Antiy: Modify the hard disk firmware of the Trojan Horse Exploration Equation (EQUATION) organization of the attack component
https://www.antiy.com/response/EQUATION_ANTIY_REPORT.html
https://www.antiy.net/p/a-trojan-that-can-modify-the-hard-disk-firmware/

[9] Antiy: Analysis of Encryption Techniques in Partial Components of Equation
https://www.antiy.com/response/Equation_part_of_the_component_analysis_of_cryptographic_techniques.html
https://www.antiy.net/p/analysis-on-the-encryption-techniques-of-equation-components/

[10] Antiy: From equation to "equation set" EQUATION Attack Organization High-level Malicious Code Full-platform Capability Resolution
https://www.antiy.com/response/EQUATION_DRUG/EQUATION_DRUG.html

©Antiy All Rights Reserved. Reprint without loss is welcome

https://www.antiy.net/p/the-analysis-of-equation-drug-the-fourth-analysis-report-of-equation-group/

[11] Antiy: Analysis of Equation Organization's EQUATIONDRUG Platform
https://www.antiy.cn/research/notice&report/research_report/646.html

[12] Antiy: "Formula Organization" Attack SWIFT Service Provider EastNets Event Re-offer Analysis Report
https://www.antiy.com/response/20190601.html

[13] Antiy: A Nine-year Re-evaluation of the Earthquake Network Event
https://www.antiy.com/response/20190930.html

Appendix III: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

©Antiy All Rights Reserved. Reprint without loss is welcome

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.

©Antiy All Rights Reserved. Reprint without loss is welcome