Review of Cyberattacks from US Intelligence Agencies

- Based on Global Cybersecurity Communities' Analyses

China Cybersecurity Industry Alliance (CCIA)

April 2023

Contents

Chapter 1. The Start of Cyberwar - An Analysis of the Stuxnet Event

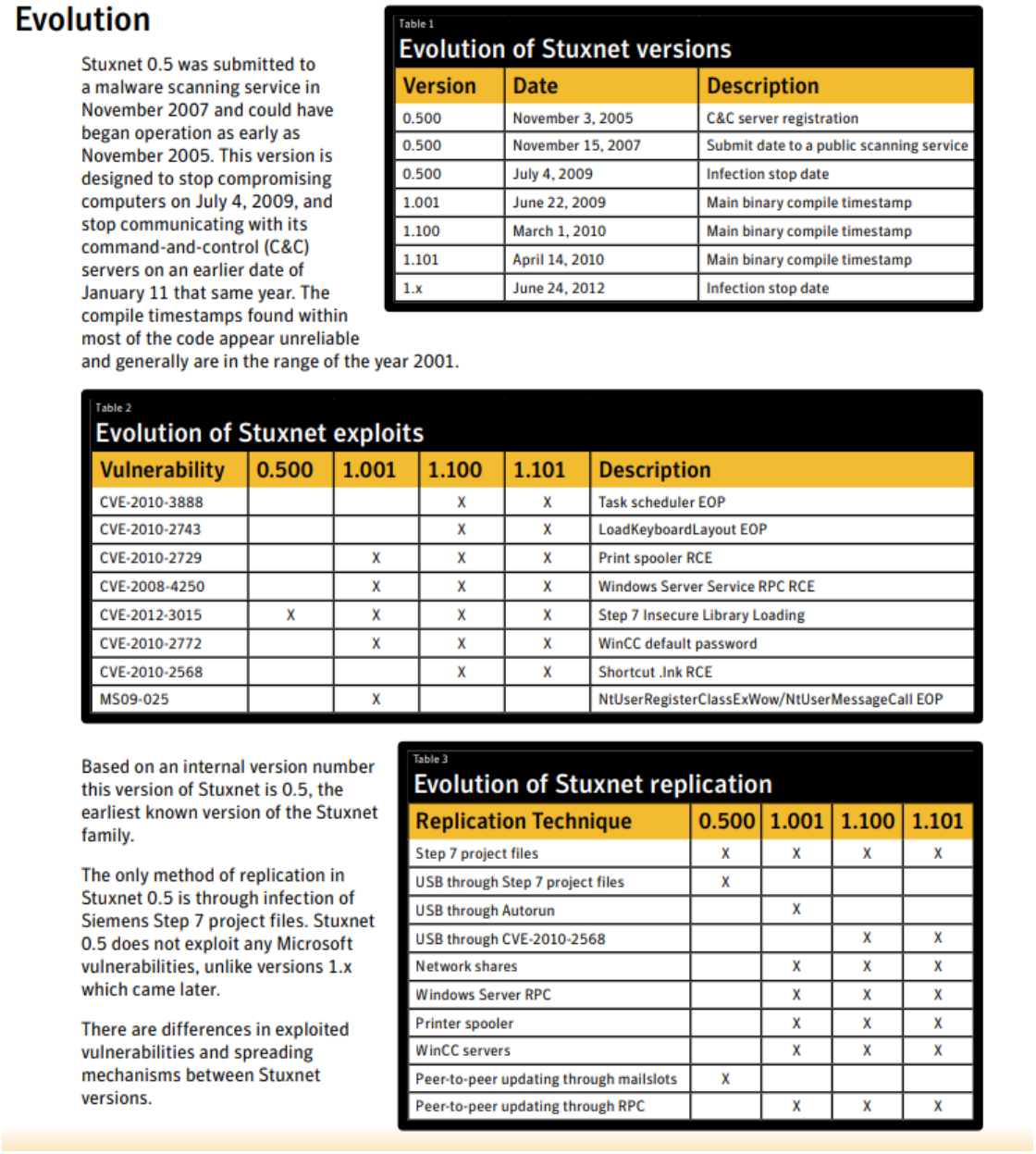
By the end of the 20th century, with the rapid development of information technology, cyberspace had gradually become the "fifth domain" of human society. At the same time, the concerns about the militarization of cyberspace continued to increase all over the world. Fears of cyberwar turned into reality in 2010, when the Stuxnet computer worm attacked Iran's nuclear facilities, indicating the United States opened the Pandora's box.

Event Review

In November 2010, the Iranian government publicly acknowledged an earlier virus attack on its network at the Natanz nuclear facility. According to external analysis, it was the Stuxnet virus that attacked Iran's nuclear facilities, which destroyed nearly a fifth (some say two-thirds) of Iran's centrifuges and infected more than 200,000 computers, leading to the abnormal operation of nearly 1,000 machines. The attack set back Iran's nuclear program by at least two years. The event was later regarded as the beginning of the era of cyberwar, and the prelude to the transformation of the war mode by cyber viruses as a "super destructive weapon."

The Process of Study, Analysis, and Publication

In June 2010, VirusBlokAda, a Belarusian cybersecurity vendor, investigated the computer crash and reboot problem for some Iranian customers. The technicians found a new worm in the computers. According to the characteristic word "stux" appearing in the virus code, the new virus was named Stuxnet. In August 2010, American cybersecurity vendor Symantec pointed out that about 60% of the computers infected by the worm worldwide were in Iran. In September 2010, Symantec disclosed the basic information[1] and infection method of Stuxnet[2], and revealed its attack target. It analyzed the method of the virus infecting Siemens Step 7 project files and the process of infecting programmable logic controller (PLC), and revealed the virus' evolution process from the earlier version 0.5 to other versions in subsequent reports (See Fig. 1-1)[3]:



Evolution

Stuxnet 0.5 was submitted to a malware scanning service in November 2007 and could have began operation as early as November 2005. This version is designed to stop compromising computers on July 4, 2009, and stop communicating with its command-and-control (C&C) servers on an earlier date of January 11 that same year. The compile timestamps found within most of the code appear unreliable and generally are in the range of the year 2001.

Table 1
Evolution of Stuxnet versions

Version	Date	Description
0.500	November 3, 2005	C&C server registration
0.500	November 15, 2007	Submit date to a public scanning service
0.500	July 4, 2009	Infection stop date
1.001	June 22, 2009	Main binary compile timestamp
1.100	March 1, 2010	Main binary compile timestamp
1.101	April 14, 2010	Main binary compile timestamp
1.x	June 24, 2012	Infection stop date

Table 2
Evolution of Stuxnet exploits

Vulnerability	0.500	1.001	1.100	1.101	Description
CVE-2010-3888			X	X	Task scheduler EOP
CVE-2010-2743			X	X	LoadKeyboardLayout EOP
CVE-2010-2729		X	X	X	Print spooler RCE
CVE-2008-4250		X	X	X	Windows Server Service RPC RCE
CVE-2012-3015	X	X	X	X	Step 7 Insecure Library Loading
CVE-2010-2772		X	X	X	WinCC default password
CVE-2010-2568			X	X	Shortcut .lnk RCE
MS09-025		X			NtUserRegisterClassExWow/NtUserMessageCall EOP

Based on an internal version number this version of Stuxnet is 0.5, the earliest known version of the Stuxnet family.

The only method of replication in Stuxnet 0.5 is through infection of Siemens Step 7 project files. Stuxnet 0.5 does not exploit any Microsoft vulnerabilities, unlike versions 1.x which came later.

There are differences in exploited vulnerabilities and spreading mechanisms between Stuxnet versions.

Table 3
Evolution of Stuxnet replication

Replication Technique	0.500	1.001	1.100	1.101
Step 7 project files	X	X	X	X
USB through Step 7 project files	X			
USB through Autorun		X		
USB through CVE-2010-2568			X	X
Network shares		X	X	X
Windows Server RPC		X	X	X
Printer spooler		X	X	X
WinCC servers		X	X	X
Peer-to-peer updating through mailslots	X			
Peer-to-peer updating through RPC		X	X	X

Fig. 1-1 Evolution Process between Different Versions of Stuxnet

In November 2010, Symantec sorted out the process of some cybersecurity vendors' discovery and understanding of Stuxnet (See Tab. 1-1)[4,5]:

Tab. 1-1 Discovery and Cognition of Stuxnet (Symantec)

Time	Event
November 20, 2008	Trojan.Zlob variant found to be using the LNK vulnerability only later identified in Stuxnet.

April 2009	Security magazine Hakin9 releases details of a remote code execution vulnerability in the Printer Spooler service. Later identified as MS10-061.
June 2009	Earliest Stuxnet sample seen. Does not exploit MS10-046. Does not have signed driver files.
January 25, 2010	Stuxnet driver signed with a valid certificate belonging to Realtek Semiconductor Corp.
March 2010	First Stuxnet variant to exploit MS10-046.
June 17, 2010	VirusBlokAda reports W32.Stuxnet (named Rootkit.Tmphider). Reports that it's using a vulnerability in the processing of shortcuts/.lnk files in order to propagate (later identified as MS10-046).
July 13, 2010	Symantec adds detection as W32.Temphid (previously detected as Trojan).
July 16, 2010	Microsoft issues Security Advisory for "Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)" that covers the vulnerability in processing shortcuts/.lnk files. Verisign revokes Realtek Semiconductor Corps certificate.
July 17, 2010	ESET identifies a new Stuxnet driver, this time signed with a certificate from JMicron Technology Corp.
July 19, 2010	Siemens reports that they are investigating reports of malware infecting Siemens WinCC SCADA systems. Symantec renames detection to W32.Stuxnet.
July 20, 2010	Symantec monitors the Stuxnet Command and Control traffic.
July 22, 2010	Verisign revokes the JMicron Technology Corps certificate.
August 2, 2010	Microsoft issues MS10-046, which patches the Windows Shell shortcut vulnerability.
August 6, 2010	Symantec reports how Stuxnet can inject and hide code on a PLC affecting industrial control systems[6].
September 14, 2010	Microsoft releases MS10-061 to patch the Printer Spooler Vulnerability identified by Symantec in August. Microsoft reports two other privilege escalation vulnerabilities identified by Symantec in August.
September 30, 2010	Symantec presents at Virus Bulletin and releases comprehensive analysis of Stuxnet.

Kaspersky, a Russian cybersecurity vendor, has almost the largest number of and the most comprehensive reports of Stuxnet and related viruses in the industry. Kaspersky has published dozens of reports, which comprehensively analyzed the behavior and purpose, attack target, vulnerability exploit, evasion, C2, and especially discussed the LNK vulnerability and signature drive of Stuxnet virus. It also revealed the first five victims of the Stuxnet (See Fig. 1-2)[7]. Kaspersky pointed out that such a complex attack can only be carried out "with nation-state support."

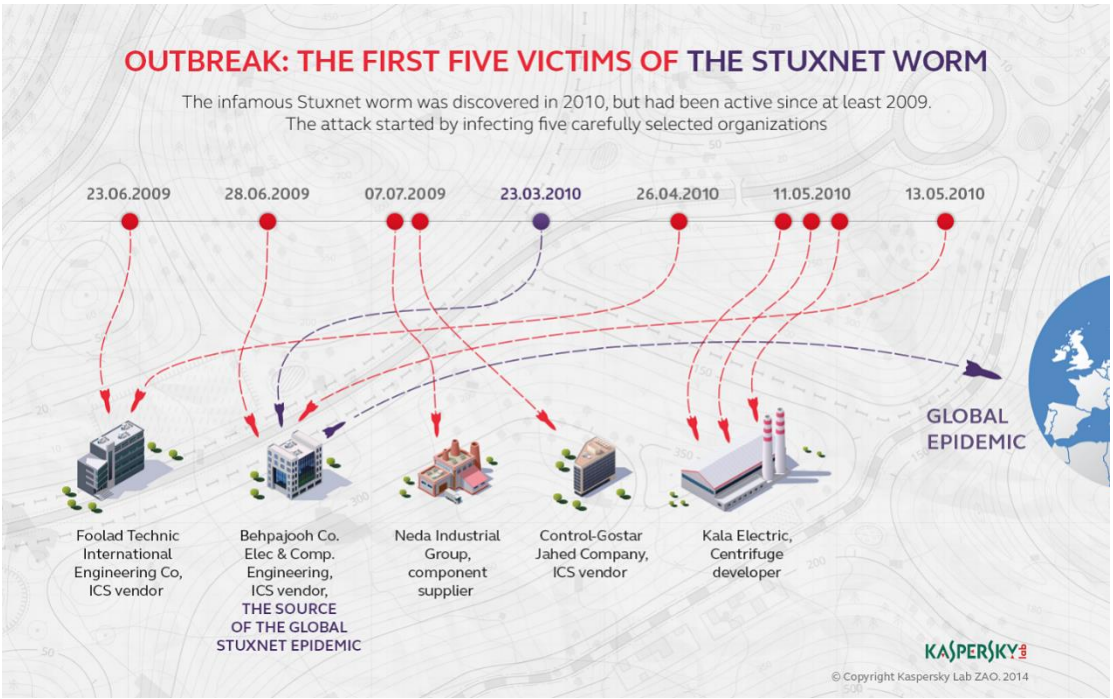


Fig. 1-2 The First Five Victims of Stuxnet Attack

Antiy is one of the earliest Chinese cybersecurity vendors to analyze the Stuxnet and its related viruses. After capturing some samples, Antiy set up a simulation analysis sand table (See Fig. 1-3)[8].

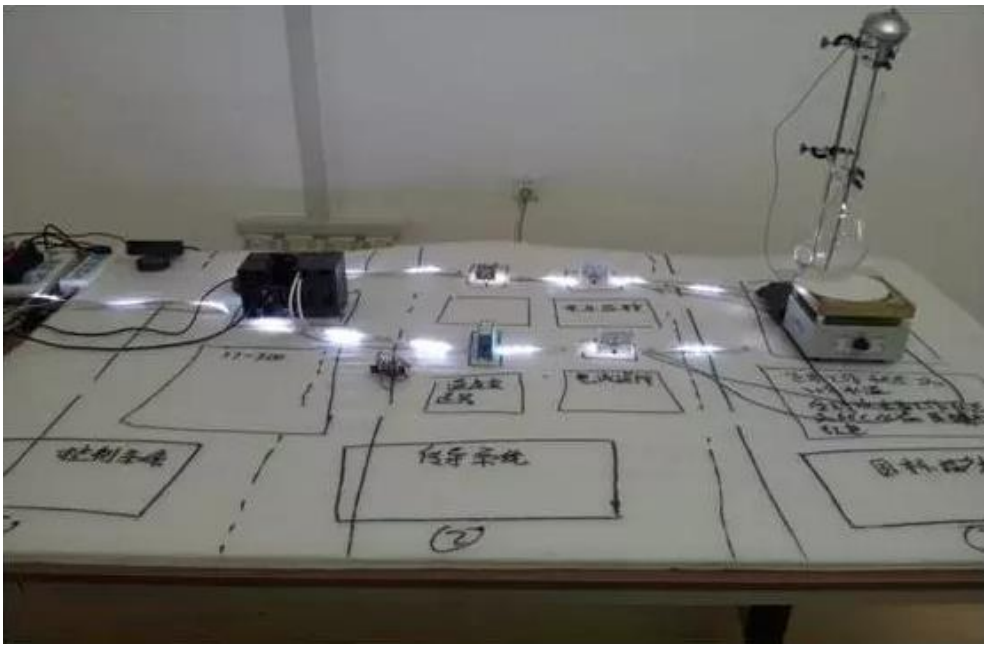
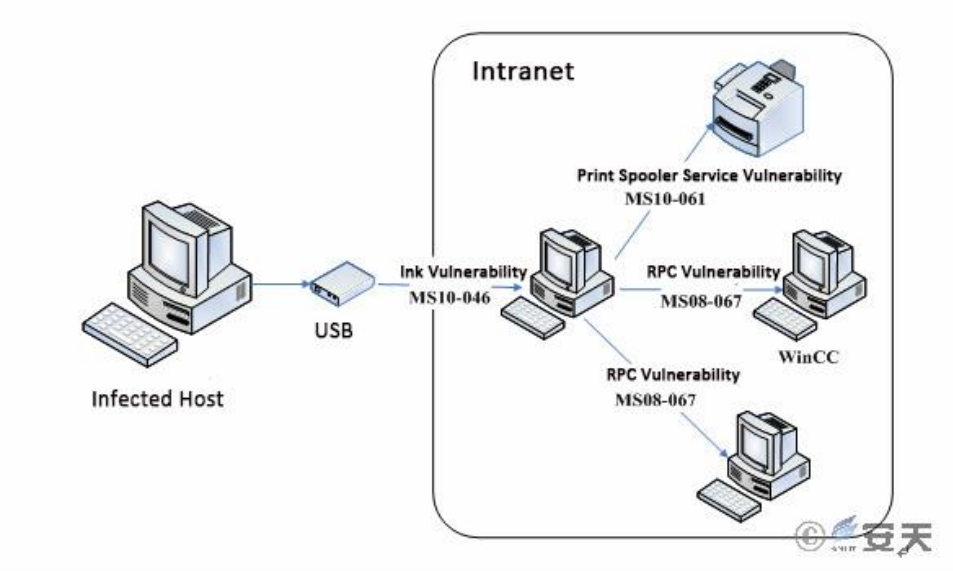


Fig. 1-3 Stuxnet Simulation Analysis Sand Table

On September 27, 2010, Antiy released *对 Stuxnet 蠕虫攻击工业控制系统事件的综合报告* (*Comprehensive Report on Stuxnet Worm Attacks on Industrial Control Systems*)[9], which analyzed the attack process, transmission mode, attack intention, file derivation and the exploited multiple zero-day vulnerabilities of Stuxnet worm. The report also analyzed several zero-day vulnerabilities and summarized the attack characteristics of the worm and provided the solution (See 1-4)[9].



1-4 Transmission Mode of Stuxnet Worm Breaking Through Physical Isolation Environment

In October 2010, Antiy released *对 Stuxnet 蠕虫的后续分析报告* (*The Follow-up Analysis Report on Stuxnet Worm*), which analyzed the technical mechanism of C2 address, update mode and USB transmission condition of the Stuxnet virus (See Fig. 1-5)[10].

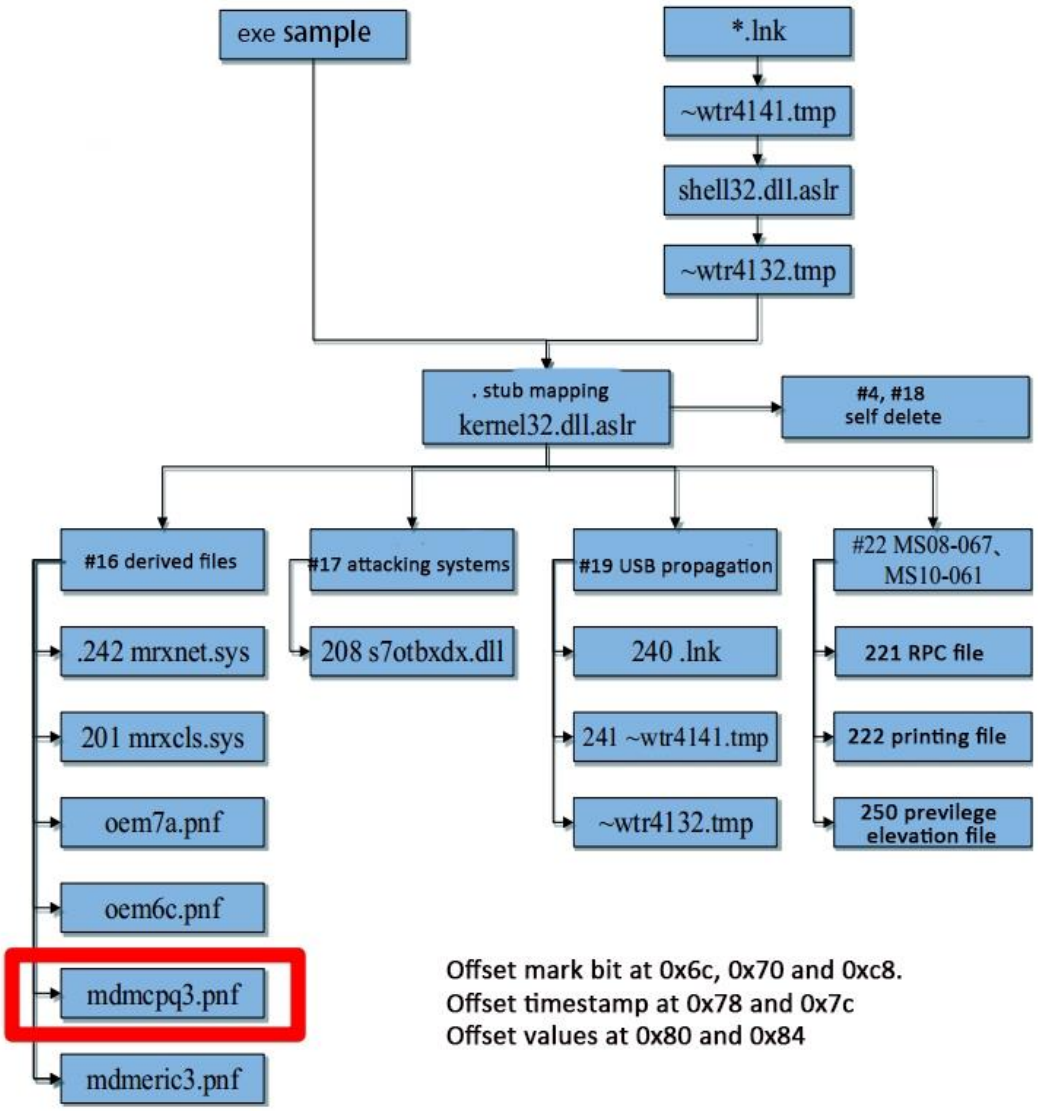


Fig. 1-5 File Release Structure and USB Transmission Logic Diagram of Stuxnet

In January 2012, Antiy released the report *WinCC 之后发生了什么* (*What Happened after WinCC*)[11] , analyzing the impact of the Stuxnet virus attacking the industrial control systems on field devices. Based on the real industrial control system, a possible attack scenario was deduced, and the attack process of the Stuxnet virus on the industrial control system was simulated by setting up environmental replicating (See Fig. 1-6)[11].

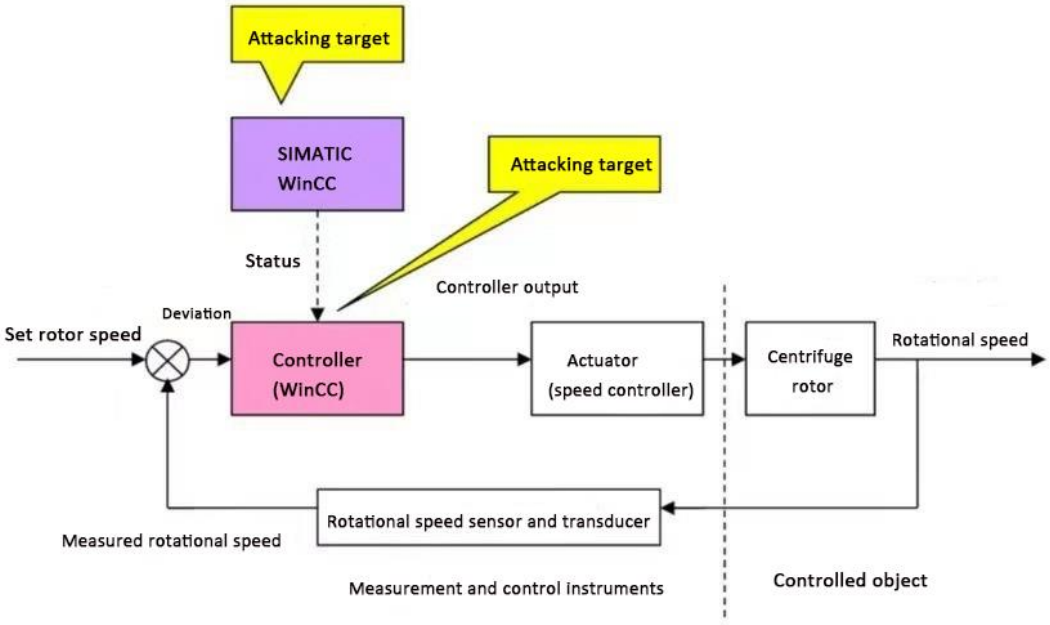


Fig. 1-6 Analysis and Conjecture of Rotation Speed Interference Mechanism

In November 2013, Ralph Langner, a German IT security expert, published two papers successively[12,13], disclosing the research results of his three-year tracking and analysis of Stuxnet, which he described as "history's first field experiment in cyber-physical weapon technology." Calling it "a textbook example of cyber warfare", Langner outlined the specific implementation method and operational flow of how to "create physical destruction by a cyberattack" based on his tracking of and research on two versions of the Stuxnet virus and the attacks.

Summary

Through the comprehensive analysis of cybersecurity vendors and experts, the Stuxnet incident was unveiled in full with a large number of details: it was an intrusion that has undergone long-term planning, preparation and lurking. Using highly complex malware and multiple zero-day vulnerabilities as attack weapons, it targets uranium centrifuges and causes over-pressure to make the centrifuges speed up revolution abnormally, resulting in the destruction of more than 1,000 centrifuges and a significant reduction in uranium enrichment and separation capacity. In the history of information technology development, there were a large number of network viruses and attacks. However, the Stuxnet incident was considered the first cyberattack that had been fully verified technologically, causing damage to the key industrial infrastructure in the real world equivalent to that caused by the traditional physical attacks, and achieving the

preset attack purpose. By staging cyberattacks on other countries' industrial infrastructure, the US opened the Pandora's box of cyberwar. The analyses of the global cybersecurity industry revealed vividly the whole picture of the attack[14]. Unfortunately, however, countries and the cybersecurity industries all over the world at that time mainly focused on the technical risks exposed by the attacks, without fully realizing the threat of cyberspace militarization by the US behind the event. In these analyses, there was no effective and systematic integration of national sovereignty and security perspectives, nor were there international laws and other aspects involved.

References

1. Symantec. *Stuxnet Introduces the First Known Rootkit for Industrial Control Systems*. 2010. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=94b1015b-da22-499a-abff-7f263ee5e490&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
2. Symantec. *Stuxnet P2P component*. 2010. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=12adb5c4-1b6b-41dc-95a5-e6320371a847&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
3. Symantec. *Stuxnet 0.5: The Missing Link*. 2013. https://docs.broadcom.com/doc/stuxnet-missing-link-13-en
4. Symantec. *W32.Stuxnet Dossier*. 2010. https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en
5. Symantec. *Stuxnet: A Breakthrough*. 2010. https://community.broadcom.com/symantecenterprise/viewdocument/Stuxnet-a-breakthrough?CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
6. Symantec. *Exploring Stuxnet's PLC Infection Process*. 2010. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ad4b3d10-b808-414c-b4c3-ae4a2ed85560&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
7. Kaspersky. *Stuxnet: Zero victims.* 2014. https://securelist.com/Stuxnet-zero-victims/67483/
8. *安天. 安天研究人员在安全焦点峰会进行两场主题演讲*. 2016.

https://www.antiy.cn/Market/Meeting/404.html

9. 安天. *对 Stuxnet 蠕虫攻击工业控制系统事件的综合分析报告*. 2010.
https://www.antiy.cn/research/notice&report/research_report/20100927.html
10. 安天. *对 Stuxnet 蠕虫的后续分析报告*. 2010.
https://www.antiy.cn/research/notice&report/research_report/20101011.html
11. 安天. *WinCC 之后发生了什么？——浅析攻击工业控制系统对现场设备的影响过程*.2012
https://www.antiy.cn/research/notice&report/research_report/20120117.html
12. Ralph Langner. *Stuxnet's Secret Twin. Foreign Policy*. 2013.
https://foreignpolicy.com/2013/11/19/Stuxnets-secret-twin/
13. Ralph Langner. *To kill a centrifuge：A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. 2013.
https://www.langner.com/to-kill-a-centrifuge/
14. 肖新光. *Reverse Deception: Organized Cyber Threat Counter-Exploitation (请君入瓮—APT 攻防指南之兵不厌诈) Preface.* 2017.
https://blog.csdn.net/weixin_34403693/article/details/90540185

Chapter 2. The Subsequence of Stuxnet - Follow-up Analysis of Duqu, Flame and Gauss

While Stuxnet was still raging all over the world, more complicated viruses such as Duqu, Flame and Gauss came up one after another. Through in-depth deconstructive analysis, experts in the industry gradually confirmed that these viruses were homologous to Stuxnet, spreading at the same time or even earlier than Stuxnet.

Event Review

On October 14, 2011, a team from Hungarian cybersecurity vendor CrySyS discovered a virus sample very similar to Stuxnet[1], mainly intended to facilitate stealing private information. CrySyS named the virus Duqu because it creates files with the file name prefix "~DQ".

In April 2012, the Iranian Ministry of Petroleum and the National Iranian Oil Company were both attacked by a malware, which was later confirmed to be Flame. By that time, the virus had infected related computer systems in Iran, Lebanon, Syria, Sudan and other Central and North African countries. Security vendors speculated that the Flame could trace back as early as 2007, and it might be released by attackers in March 2010 (to steal commercial intelligence of Iran's oil sector).

In August 2012, Kaspersky discovered that a spy software Gauss specialized in collecting financial information appeared in the Middle East. This new cyber monitoring virus can monitor bank transactions and steal website login information. Thousands of Middle East bank customers' passwords and important data had already been stolen. In the subsequent research of global cybersecurity vendors, Duqu, Flame and Gauss all proved to be related to Stuxnet.

The Process of Study, Analysis, and Publication

1. Duqu

CrySyS Lab was the first to find Duqu virus. On October 14, 2011, CrySyS released a 60-page report *Duqu: A Stuxnet-like Malware Found in the Wild*.[1] The virus was named Duqu for the first time. CrySyS said it was widely used in targeted attacks, and used a digital signature from a Taiwan science and technology company. CrySyS analyzed the main features of Duqu and compared it with Stuxnet, only to find that these two viruses bear striking similarities.

On October 18, 2011, Symantec released a report, which analyzed the global infection situation, installation process and loading logic of Duqu in details, and pointed out that the purpose of Duqu was different from that of Stuxnet. It was mainly used to collect the intelligence data and assets of the targets and to prepare for attacks like Stuxnet (See Fig. 2-1)[2].

Feature	Stuxnet	Duqu
Modular malware	✓	✓
Kernel driver based rootkit	✓	✓ very similar
Valid digital signature on driver	Realtek, JMicron	C-Media
Injection based on A/V list	✓	✓ seems based on Stux.
Imports based on checksum	✓	✓ different alg.
3 Config files, all encrypted, etc.	✓	✓ almost the same
Keylogger module	?	✓
PLC functionality	✓	✗ (different goal)
Infection through local shares	✓	No proof, but seems so
Exploits	✓	?
0-day exploits	✓	?
DLL injection to system processes	✓	✓
DLL with modules as resources	✓ (many)	✓ (one)
RPC communication	✓	✓
RPC control in LAN	✓	?
RPC Based C&C	✓	?
Port 80/443, TLS based C&C	?	✓
Special "magic" keys, e.g. 790522, AE	✓	✓ lots of similar
Virtual file based access to modules	✓	✓
Usage of LZO lib	?	✓ multiple
Visual C++ payload	✓	✓
UPX compressed payload,	✓	✓
Careful error handling	✓	✓
Deactivation timer	✓	✓
Initial Delay	? Some	✓ 15 mins
Configurable starting in safe mode/dbg	✓	✓ (exactly same mech.)

Fig. 2-1 Preliminary Comparison Between Duqu and Stuxnet

Starting from October 20, 2011, Kaspersky successively released 10 analysis reports about Duqu[3-12], deciding that the virus is a highly customizable and universal framework that can work with any number of modules of any kind, and published its homologous sample correlation analysis with Stuxnet and timestamp correlation analysis. In the follow-up research, Kaspersky also revealed that Duqu exploited the font file vulnerability MS11-077 to deliver the document file to launch an attack, and analyzed its C&C servers and the first/second layer C&C addresses. It pointed out that the major feature of Duqu 2.0 was that malware only resided in the memory of the infected machine, leaving no trace in the physical hard disk. Malware will be briefly removed when a machine is restarted, but as long as it is connected to the internal network, malware will be transmitted from another infected machine.

It is worth mentioning that in June 2015, some intelligence agencies used Duqu to attack Kaspersky, with the intention of monitoring and stealing its source code, but the attack behavior was captured and released by Kaspersky. Kaspersky, after a lot of investigation, found that this was another well-organized and precise APT attack, and only state-sponsored team could do it. Kaspersky clearly identified the attackers were the same group behind Duqu, so this attack sample was named "Duqu 2.0" (See Fig. 2-2)[13]. Eugene Kaspersky, co-founder and CEO of Kaspersky, published an analytic article *Why Hacking Kaspersky Lab Was A Silly Thing To Do* on *Forbes* website[13].

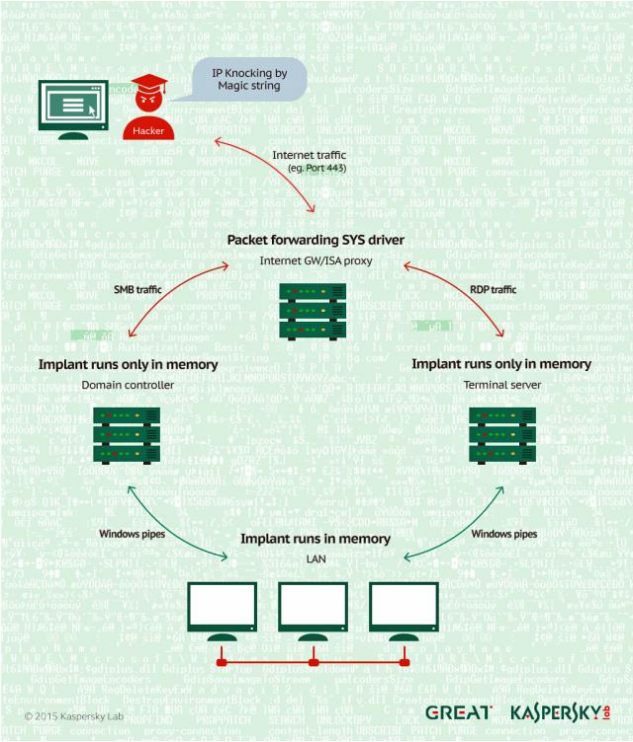


Fig. 2-2 The Attack Process of Duqu 2.0

In May 2012, Antiy published the article *探索 Duqu 木马身世之谜—— Duqu 和 Stuxnet 同源性分析* (*Duqu and Stuxnet Homology Analysis Report*) in the magazine of Programmer[14], analyzing the module structure, compiler architecture and key functions of Duqu. The article pointed out that the structures and functions of Duqu and Stuxnet are similar to some extent. At the same time, when analyzing the decryption keys, anti-tracking methods, and program bugs of Duqu, the researchers found the same logical judgment errors in the samples of Duqu and Stuxnet. According to the coding psychology, it was judged that the two have homology (See Fig. 2-3)[14].

Comparison Object	Duqu Trojan	Stuxnet Worm
Modular functions	Yes	
Ring0 injection mode	PsSetLoadImageNotifyRoutine	
Ring3 injection mode	Hook ntdll.dll	
Injecting system process	Yes	
Resource embedding DLL module	1	Several
Exploiting Microsoft vulnerability	Yes	
Using digital signature	Yes	
RPC communication module	Yes	
Profile decryption key	0xae240682	0x01ae0000
Registry decryption key	0xae240682	
Magic number	0x90.0x05,0x79,0xae	
Determining the existence of bugs in the code based on the running mode	Yes	
Bugs in registry operation code	Yes	
Attacking industrial control system	No	Yes
Driver compilation environment	Microsoft Visual C++6.0	Microsoft Visual C++7.0

Fig. 2-3 Comparison of Duqu and Stuxnet Homologous Key Code Genes

2. Flame

In April 2012, the Iranian Ministry of Petroleum and the National Iranian Oil Company were attacked by malware, which brought the Flame virus into the vision of cybersecurity vendors. Kaspersky considered it as one of the computer viruses with the most complex attack mechanism and the highest threat level ever found[15], and its structural complexity was 20 times more sophisticated than Stuxnet. Alexander Gostev, Kaspersky's chief security expert, said that both the writing mechanism and the attack mechanism of Flame were very complicated. According to the analyses of relevant clues, the appearance of Flame could even be traced back as early as 2007, and it might have been active in some form for 5 to 8 years, or even longer.

Kaspersky pointed out that once infected with Flame, all the information from keyboards, screens, microphones, portable storage devices, networks, Wi-Fi, Bluetooth, USB sticks, and system processes could be collected. The recorded information includes users' webpage browsing history, communication calls, account passwords and keyboard input. It could even use Bluetooth function to steal files from smart phones and tablets connected to infected computers. All information collected could be sent to servers that remotely controlled the viruses (See Fig. 2-4)[15]. Once the data collection task was completed, these viruses could destroy themselves, which was one of the reasons they could lurk for a long time.

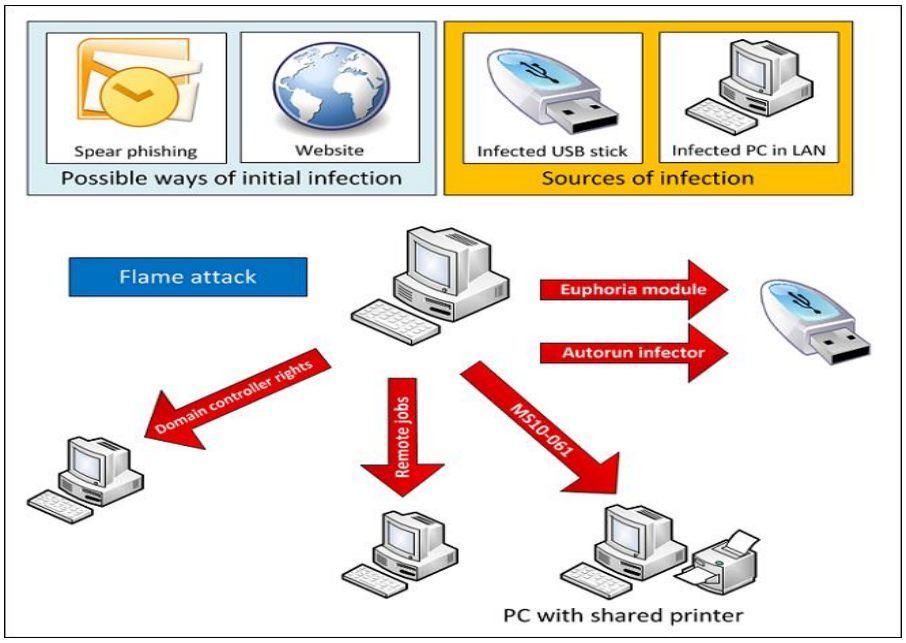


Fig. 2-4 Possible Transmission Routes of Flame

Kaspersky said that Flame used man-in-the-middle attack technology to spread via Microsoft Windows Update. The difference between Flame and Duqu was that Duqu was based on Tilded framework like Stuxnet, while Flame used Flamer framework. Compared with Stuxnet and Duqu, Flame was more intelligent, and its attack target and code composition was quite different. Kaspersky believed that the teams behind the two frameworks shared the source code of at least one module, indicating that they have cooperated for at least one time, and belong to two parallel projects within the same organization. The attack mechanism of Flame is more complicated, and the target has a specific geographical location, which may indicate that the team behind the virus is very likely manipulated by government agencies.

Eugene Kaspersky said in a statement: "Stuxnet and Duqu belonged to a single chain of attacks, which raised cyberwar-related concerns worldwide. The Flame malware looks to be another phase in this war, and it’s important to understand that such cyber weapons can easily be used against any country."

In May 2012, Antiy released a report to analyze the operation logic, transmission mechanism and main module functions of Flame (See Fig. 2-5)[16]. Antiy believes that Flame is a sophisticated componentized Trojan with more modules than Stuxnet. In its vulnerability attack module, there is a USB attack module that has been used by Stuxnet, verifying the homology between the two.

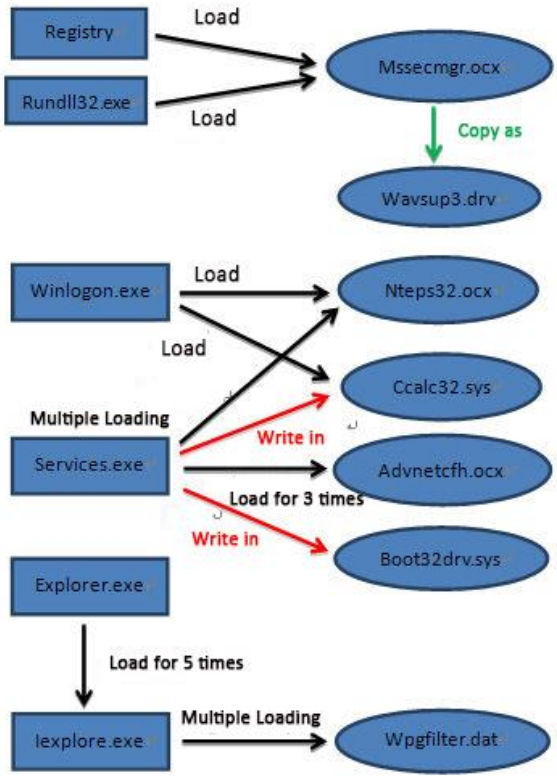


Fig. 2-5 Startup Loading Sequence of Flame's Main Modules

In June 2012, Microsoft released an investigation report[17], pointing out that Flame is mainly used for highly complex and highly targeted attacks. It can extract 1KB samples from files such as PDF, Excel and Word documents, compress and upload the samples to the C2 server, and then the attackers will issue instructions to grab the documents they are interested in. Flame was used to attack those who use Microsoft Windows Update. It bypasses the legitimate Windows Update by setting a forged server. When a computer is connected to the network, the user will see the forged Microsoft Update software, and at this time, Flame is transmitted from the forged server to the computer. Certain technologies used by this virus are used by some low-level attackers for a wider range of attacks.

CrySyS Lab named Flame "sKyWIper" in its research, and believed it was an information stealing malware. Its modular structure combines various communication and attack technologies, and it may have been active for 5 to 8 years, or even longer[18]. In the report, CrySyS analyzed its main modules, storage formats, encryption algorithms, injection mechanisms, and behavior and purpose (See Fig. 2-6)[18], pointing out that sKyWIper may have been developed by a government agency with a large amount of budget and technologies, and may be related to cyberwar activities.

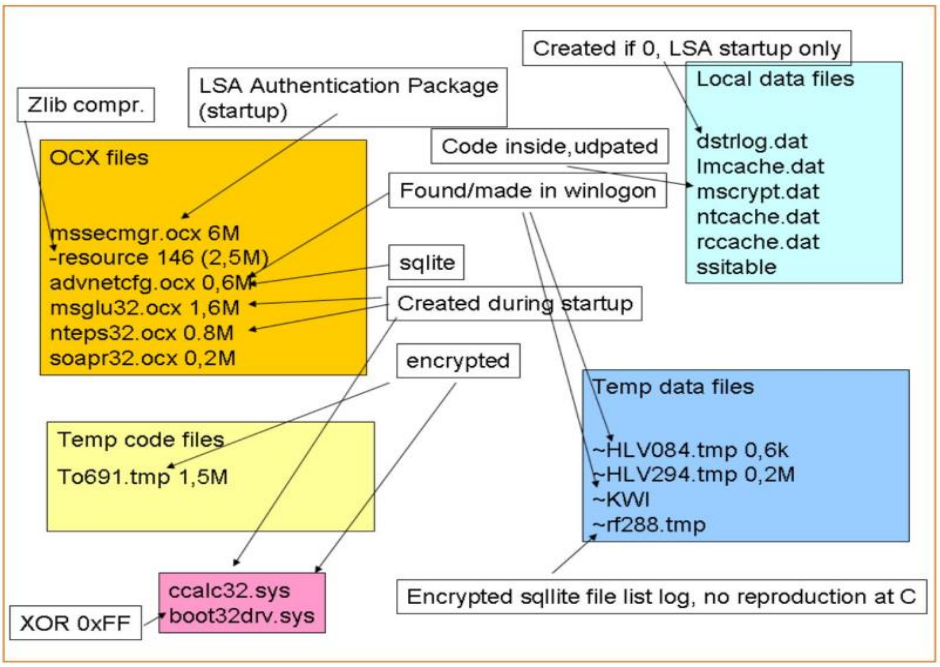


Fig. 2-6 Related Documents of Flame

3. Gauss

In August 2012, Kaspersky discovered the Gauss virus, and considered it as a complicated cyber spyware toolkit developed by the creators of the Flame virus. It is highly modular and supports new functions, and can be deployed remotely by attackers in the form of plug-ins (See Fig. 2-7)[19].

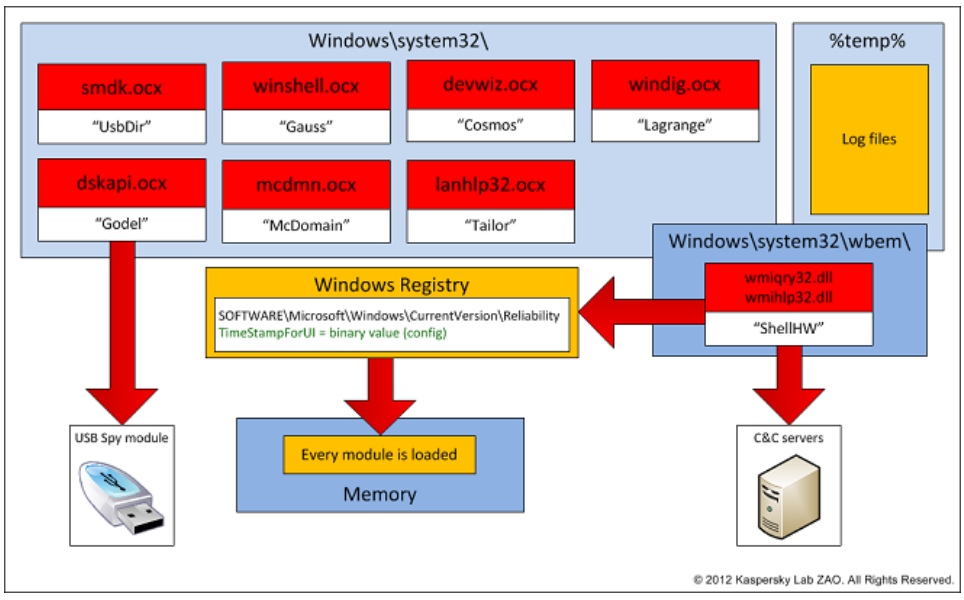


Fig. 2-7 The Architecture of Gauss

Kaspersky said that there is enough evidence to prove that Gauss is closely related to Flame and Stuxnet, and is created by entities related to Stuxnet, Duqu and Flame, while Stuxnet was nation-state sponsored.

After the Stuxnet incident, due to its relatively large scale and many versions, the cybersecurity community had not obtained the complete version and sample collection of Stuxnet for quite a long time. Therefore, some historical questions about Stuxnet remained, such as: why did a highly directional operation show a divergent propagation effect and exist in thousands of samples? Regarding these issues, Antiy released *震网事件的九年再复盘与思考* (*Review and Thinking Nine Years after the Stuxnet Incident*)[20] in 2019. Through continuous research and tracking, Antiy analyzed the characteristics, causes, mechanism of action, and related advanced malware engineering framework of each version of Stuxnet. The correlation between malware used by Stuxnet, Duqu, Flame, Gauss and Equation Group was also analyzed. It is pointed out that the United States has maintained at least two malware frameworks and parallel projects, Tilded and Flamer, and developed the above-mentioned malware. Fanny and Flowershop are also found, based on more clues, to be related to the above malware (See Fig. 2-8)[20].

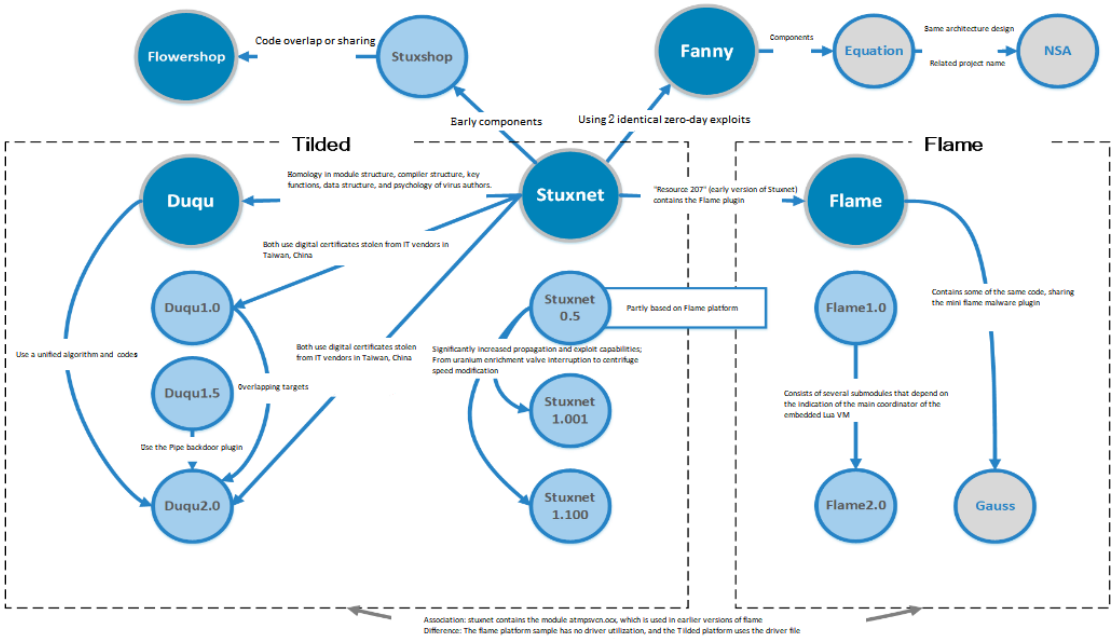


Fig. 2-8 The Relationship Diagram Between Stuxnet and Duqu, Flame, Gauss, Fanny, Flowershop

Summary

The huge harm caused by Stuxnet is based on the long-term operation and information collection of the malware of Flame and Duqu. The Stuxnet series of virus attacks showed that the industrial infrastructure may be fully invaded and infiltrated, and even encounter the risks and serious consequences of battlefield preparations. The sample research of many vendors has confirmed the connection between Duqu, Flame, Gauss and Stuxnet, and basically identified the United States as the culprit behind them.

For the discovery and tracking analysis of Stuxnet and its homologous viruses, global cybersecurity vendors focused more on its complex structure and sophisticated design in the early days. Relevant research was basically based on the analysis of the principles of the vulnerabilities used, the reverse analysis of the samples, and the review of the mechanism of the samples. The attacks were handled purely as technical security threats to prevent, and the analysis always lacked thinking from assignment to operational perspectives, without a deeper understanding of these virus attacks from the political, diplomatic, and social levels.

References

1. CrySyS. *Duqu: A Stuxnet-like malware found in the wild.* 2011. https://www.yumpu.com/en/document/view/17515556/duqu-a-Stuxnet-like-malware-found-in-the-wild-crysys-lab
2. Symantec. *W32.Duqu: The Precursor to the Next Stuxnet.* 2011. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=933c68f1-6ee7-473e-9eb6-6c8459f790f2&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
3. Kaspersky. *The Mystery of Duqu: Part One.* 2011. https://securelist.com/the-mystery-of-duqu-part-one/31177/
4. Kaspersky. *The Mystery of Duqu: Part Two.* 2011. https://securelist.com/the-mystery-of-duqu-part-two/31445/
5. Kaspersky. *The Mystery of Duqu: Part Three.* 2011. https://securelist.com/the-mystery-of-duqu-part-three/31486/
6. Kaspersky. *The Mystery of Duqu: Part Five.* 2011. https://securelist.com/the-mystery-of-duqu-part-five-6/31208/

7. Kaspersky. *The Mystery of Duqu: Part Six (The Command and Control servers).* 2011. https://securelist.com/the-mystery-of-duqu-part-six-the-command-and-control-servers-36/31863/
8. Kaspersky. *Stuxnet/Duqu: The Evolution of Drivers.* 2011. https://securelist.com/Stuxnetduqu-the-evolution-of-drivers/36462/
9. Kaspersky. *The Mystery of the Duqu Framework.* 2012. https://securelist.com/the-mystery-of-the-duqu-framework-6/32086/
10. Kaspersky. *The mystery of Duqu Framework solved.* 2012. https://securelist.com/the-mystery-of-duqu-framework-solved-7/32354/
11. Kaspersky. *The Mystery of Duqu: Part Ten.* 2012. https://securelist.com/the-mystery-of-duqu-part-ten/32668/
12. Kaspersky. *The Mystery of Duqu 2.0: a sophisticated cyberespionage actor returns.* 2015. https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/
13. Eugene Kaspersky. *Why Hacking Kaspersky Lab Was A Silly Thing To Do.* 2015 https://www.forbes.com/sites/eugenekaspersky/2015/06/10/why-hacking-us-was-a-silly-thing-to-do/
14. *安天. 探索 Duqu 木马身世之谜—— Duqu 和 Stuxnet 同源性分析.* 2012. https://antiy.cn/research/notice&report/research_report/261.html
15. Kaspersky. *The Flame: Questions and Answers.* 2012. https://securelist.com/the-flame-questions-and-answers/34344/
16. *安天. Flame 蠕虫样本集分析报告.* 2012. https://www.antiy.cn/research/notice&report/research_report/20120531.html
17. Microsoft. *Flame malware collision attack explained.* 2012. https://msrc-blog.microsoft.com/2012/06/06/flame-malware-collision-attack-explained/
18. CrySyS. *skyWIper (Flame Virus)- Complex cyber-warfare targeted attacks.* 2012. https://www.crysys.hu/publications/files/skywiper.pdf
19. Kaspersky. *Gauss: Nation-state cyber-surveillance meets banking Trojan.* 2012. https://securelist.com/gauss-nation-state-cyber-surveillance-meets-banking-trojan-54/33854/
20. *安天. 震网事件的九年再复盘与思考.* 2019. https://www.antiy.com/response/20190930.html
21. Trend Micro. *DUQU Uses Stuxnet-Like Techniques to Conduct Information Theft.* 2011. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/90/duqu-uses-Stuxnetlike-techniques-to-conduct-information-theft
22. Kaspersky. *The Roof Is on Fire: Tackling Flame's C&C Servers.* 2012

https://securelist.com/the-roof-is-on-fire-tackling-flames-cc-servers/33033/

23. Kaspersky. *'Gadget' in the middle: Flame malware spreading vector identified.* 2012. https://securelist.com/gadget-in-the-middle-flame-malware-spreading-vector-identified/33081/
24. Kaspersky. *Flame: Replication via Windows Update MITM proxy server.* 2012. https://securelist.com/flame-replication-via-windows-update-mitm-proxy-server/33002/
25. Kaspersky. *Back to Stuxnet: the missing link.* 2012. https://securelist.com/back-to-Stuxnet-the-missing-link/33174/
26. Kaspersky. *The Day The Stuxnet Died.* 2012. https://securelist.com/the-day-the-Stuxnet-died/33206/
27. Kaspersky. *Gauss: Abnormal Distribution.* 2012. https://securelist.com/gauss-abnormal-distribution/36620/
28. Kaspersky. *The Mystery of the Encrypted Gauss Payload.* 2012. https://securelist.com/the-mystery-of-the-encrypted-gauss-payload-5/33561/
29. Kaspersky. *What was that Wiper thing?* 2012. https://securelist.com/what-was-that-wiper-thing-48/34088/
30. Kaspersky. *Full Analysis of Flame's Command & Control servers.* 2012. https://securelist.com/full-analysis-of-flames-command-control-servers/34216/
31. Kaspersky. *Stuxnet: Zero victims.* 2014. https://securelist.com/full-analysis-of-flames-command-control-servers/34216/
32. Kaspersky. *Duqu is back: Kaspersky Lab reveals cyberattack on its corporate network that also hit high profile victims in Western countries, the Middle East and Asia.* 2015. https://www.kaspersky.com/about/press-releases/2015_duqu-is-back-kaspersky-lab-reveals-cyberattack-on-its-corporate-network-that-also-hit-high-profile-victims-in-western-countries-the-middle-east-and-asia
33. Kaspersky. *The Duqu 2.0 Technical Details.* 2015. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf
34. Kaspersky. *The Duqu 2.0 persistence module.* 2015. https://securelist.com/the-duqu-2-0-persistence-module/70641/

Chapter 3. Whole Picture of the Super Machine - Follow-up Analysis of the Snowden Incident

Stuxnet, Duqu, and Flame revealed the attack abilities of the US intelligence agencies, but at that time the global security industry's perception of the US attack abilities was still limited to the extremely complex Trojan and the rich zero-day vulnerability reserve. In 2013, the Snowden incident showed that the US cyber intelligence attack capability was such a huge system that it was "far beyond reach." With the gradual release of more documents by Snowden, global cybersecurity vendors had more materials which could be used to analyze the engineering systems and equipment systems of the US intelligence agencies' cyberspace operations, and the whole picture of the US cyberspace super machine was gradually revealed.

Event Review

On June 5, 2013, the British newspaper, *The Guardian*, exposed the order secretly issued by the US court on April 25, 2013. The order requires that, from the day on until July 19, the US telecommunications giant Verizon must hand over the call records of millions of users to the US National Security Agency (NSA) every day, including international long-distance call records[1]. According to the report, the specific data required by the NSA includes the number of calls, call duration, call time, etc., but the contents of the calls are not covered. At the same time, Verizon was required to keep the whole process strictly confidential. The next day, the whistleblower, CIA intelligence officer Snowden, revealed a secret NSA program code-named PRISM, exposing 9 international Internet giants including Microsoft, Yahoo, Google and Apple to cooperate with the US government to secretly monitor information such as call records, emails, videos, and photos. The program even invaded the network equipment of multiple countries including Germany and South Korea. The subsequent series of leaked documents jointly exposed that the monitoring and network intrusion operations had been implemented by the US government for a long time.

Some neutral media around the world continued to follow up and expose the surveillance operations of US intelligence agencies[2-4]. In October 2013, *The Guardian* published an article *Attacking Tor: How the NSA Targets Users' Online Anonymity*[2], which revealed that the NSA used vulnerability development technology and Internet monitoring technology to launch network attacks on Tor users by exploiting

vulnerabilities in their Firefox browser to obtain information and intelligence. The specific operation was to identify Tor users on the Internet through powerful Internet monitoring, and redirect these users to a group of secret network servers (code-named FoxAcid), thereby infecting their computers.

In June 2014, British technology media The Register published an article, *NSA: Inside the FIVE-EYED VAMPIRE SQUID of the Internet*, saying that Snowden's leaked documents show that the NSA and the "Five Eyes" partners have established a secret monitoring and control network around the world, covering global communication and computer security organizations and companies. The safety of the Internet as a common communication medium has been completely broken, and the damage to IT security has been deliberate and continuous[3].

The Process of Study, Analysis, and Publication

In July 2013, the chief technology officer of Antiy wrote an article *斯诺登效应的前因解读* (*Interpretation of the Antecedents of the Snowden Effect*) in the Communications of the CCF[5], pointing out that the incident was not simply a matter of monitoring and privacy leakage, but deeply involved in many aspects of the current global order, diplomacy, intelligence and domestic affairs. Antiy believed the Snowden incident mainly exposed: 1. The PRISM project, as an integral part of the network intelligence system of the NSA, mainly used the interfaces provided by major Internet companies in the United States for data retrieval, query and collection; 2. Most mainstream IT companies in the United States, such as Google, Microsoft, Apple and Facebook, are related to this project; 3. The Office of Tailored Access Operations (TAO) affiliated to the NSA had been attacking China for 15 years, with its related actions assisted by Cisco (See Fig. 3-1)[5].

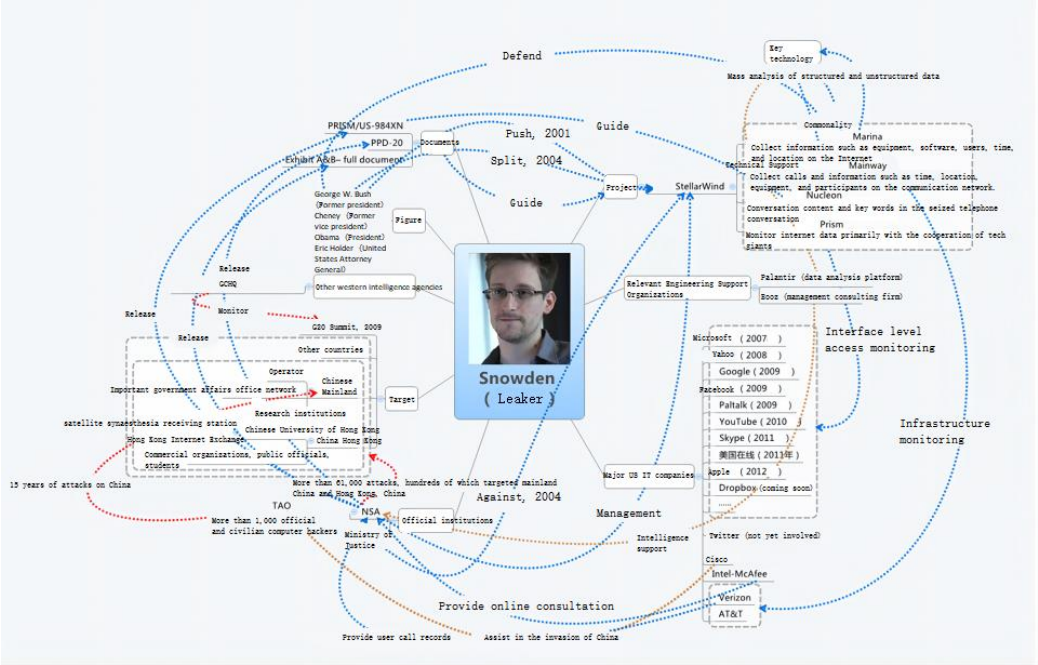


Fig. 3-1 Relational Diagram of Information Related to the Snowden Incident

The documents exposed by Snowden revealed that in 2004, the US government launched the STELLARWIND program to conduct large-scale intelligence collection and monitoring. Later, due to legal and other issues, STELLARWIND was split into projects such as PRISM, MAINWAY, MARINA and NUCLEON, which were taken over by the NSA. Antiy released a series of articles in December 2017 and had an in-depth analysis of the STELLARWIND program (See Fig. 3-2) [6].

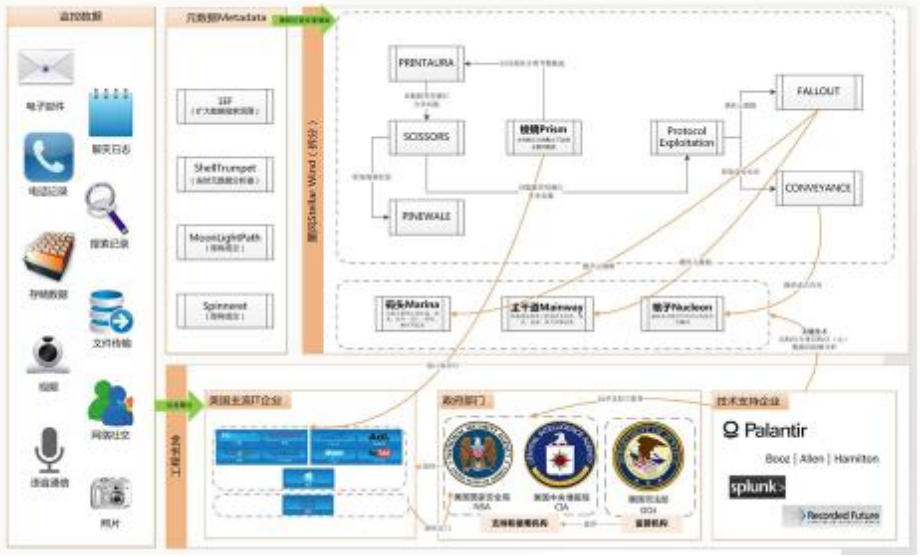


Fig. 3-2 STELLARWIND Program Structure Analysis

The articles from Antiy pointed out that, according to the documents leaked by Snowden, the United States had carried out a large number of cyber intelligence eavesdropping programs, with PRISM a typical one. The United States had obtained various types of network intelligence through monitoring of large submarine optical cables, monitoring of key special areas, computer network exploitation (CNE), satellite monitoring, and third-party intelligence sharing, so as to grasp a whole picture of global targets and form a more accurate target positioning. This capability laid the foundation for the United States to gain all-round advantages in cyberspace security defense and countermeasures, deterrence, and attacks.

Based on the intelligence acquisition capability covering the whole world, the United States has established an offensive capability support system represented by TURBULENCE. Through the relevant capability modules such as passive signal intelligence acquisition, active signal intelligence acquisition, mission logic control, intelligence diffusion and aggregation, and directional positioning, a complete cyberspace intelligence cycle was realized. Combined with offensive and defensive capability modules such as TUTELAGE and QUANTUM, the United States further realized active defensive and offensive operations in cyberspace driven by intelligence (See Fig. 3-3 and Fig. 3-4)[6].

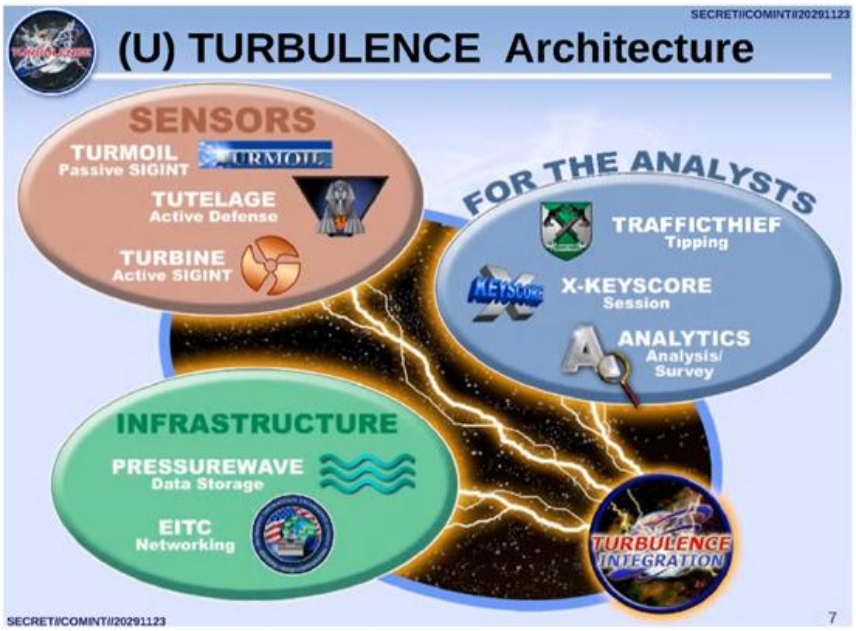


Fig. 3-3 TURBULENCE Architecture

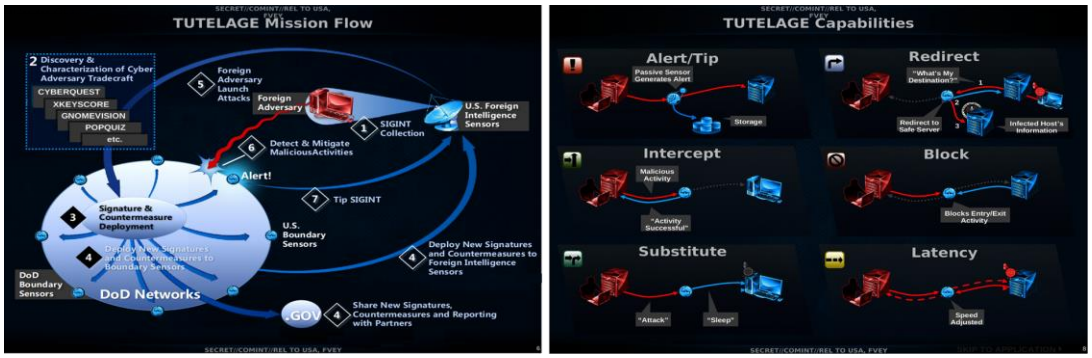


Fig. 3-4 TUTELAGE System Task Flow

In 2022, 360 0Kee Team released a report, revealing that the NSA had launched indiscriminate attacks against global targets for more than 10 years. 360 0Kee Team analyzed the QUANTUM attack system, FOXACID zero-day vulnerability attack platform, VALIDATOR and UNITEDRAKE backdoor, and pointed out that the number of infected organizations worldwide may reach millions (See Fig. 3-5)[7].

Fig. 3-5 Path and Intent of Cyberattack Weapons of US National Security Agency

Especially for the QUANTUM system, 360 0Kee Team conducted a detailed technical analysis from the perspective of attack technology, attack modules, application scenarios and attack implementation process (See Fig. 3-6)[8]. Combined with the real cases discovered, it fully confirms the details of the NSA's large-scale indiscriminate cyberattacks against Internet users around the world.

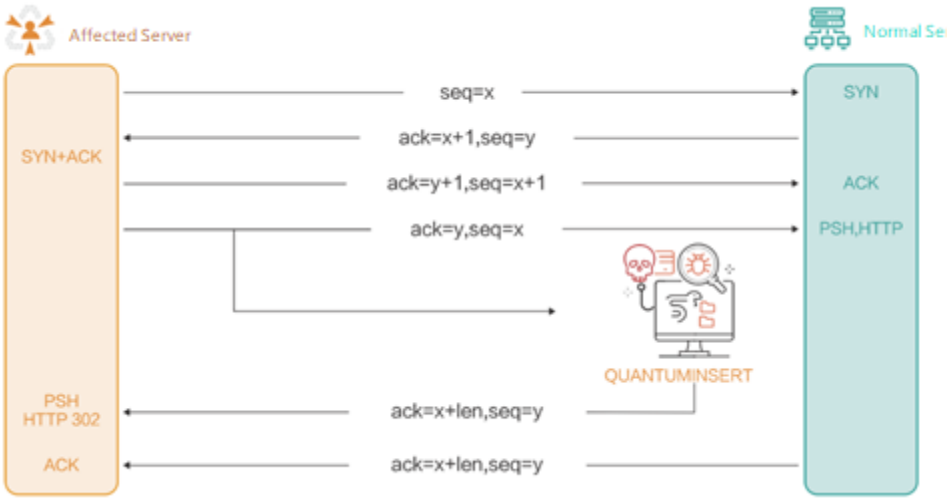


Fig. 3-6 QUANTUM Injection Attack Process

Summary

Through the documents leaked by Snowden, global cybersecurity vendors have gradually realized the capability system of the US to carry out operations in cyberspace. Studies have shown that based on a complex organizational system, huge personnel scale and abundant security budget, the United States has established a complete engineering system to support cyberspace operations through the construction of a series of large-scale engineering systems. Based on this, the United States has integrated cyberspace capabilities such as intelligence acquisition, active defense, offensive operations, and related support links into its overall national capability.

At the same time, the United States has the tradition of putting national security first. With the development of its national strength, the United States gradually regards its global surveillance and intelligence eavesdropping operation capabilities as the cornerstone of its global interests and hegemony, and uses all kinds of cyber intelligence acquired to form its "innate advantages" in cyberspace operations. Eavesdropping on submarine optical cables and operators, in particular, gives the United States an unparalleled advantage in signal acquisition and intelligence gathering in terms of concealment and anti-traceability. The strong systematic capability of operations combined with the hegemonic concealment and anti-traceability advantage has helped build the US cyberspace abilities that are far beyond reach.

With the publication of the documents leaked by Snowden, the perspective of the cybersecurity community has gradually risen from the tactics, techniques, and

procedures (TTPs) to the strategic level, and the whole picture of the cyberspace super machine has gradually been revealed.

References

1. The Guardian. *NSA collecting phone records of millions of Verizon customers daily.* 2013. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
2. The Guardian. *Attacking Tor: how the NSA targets users' online anonymity.* 2013. https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity
3. The Register. *NSA: Inside the FIVE-EYED VAMPIRE SQUID of the INTERNET.* 2014. https://www.theregister.com/2014/06/05/how_the_interenet_was_broken/
4. 明镜周刊. *"Vorwärtsverteidigung" mit QFIRE.* 2013. https://www.spiegel.de/fotostrecke/qfire-die-vorwaertsverteidigng-der-nsa-fotostrecke-105358.html
5. 肖新光. *斯诺登效应的前因解读. 中国计算机学会通讯.* 2013（7）. https://www.antiy.cn/doc/market/201307.pdf
6. 安天. *“美国网络空间攻击与主动防御能力解析”系列文章 12 篇. 网信军民融合.* 2017(12)-2018(11). https://mp.weixin.qq.com/s/PnaYXZ9snK6fv_lgCFszDw
7. 360. *网络战序幕：美国国安局 NSA（APT-C-40）对全球发起长达十余年无差别攻击.* 2022. https://mp.weixin.qq.com/s/jHjzky8xIaEuocHzbWjFSA
8. 360. *Quantum（量子）攻击系统–美国国家安全局"APT-C-40"黑客组织高端网络攻击武器技术分析报告（一）.* 2022. https://mp.weixin.qq.com/s/lzf16Fchfv1fMG3IExq7XA

Chapter 4. Rumors of Backdoors - How the US Pollutes Standards for Encryption Communication

There have been widespread doubts and speculations in the cybersecurity community about whether the US has embedded backdoors in basic IT products. In August 1999, Andrew Fernandes, chief scientist at Canada's Cryptonym Corp., discovered a key named "_NSAKey" in the Windows system CryptoAPI (encryption interface)[1], which reminded people of the NSA. Despite Microsoft's explanation, the cybersecurity community remained suspicious, and has since begun to look for backdoors reserved by the US.

In early September 2013, a number of American and British media outlets reported that the NSA had hidden a backdoor in the SP 800-90A standard released by the National Institute of Standards and Technology (NIST). The reports confirmed rumors that had long circulated in the cybersecurity community. Since then, thanks to the continuous efforts of the cybersecurity industry and academia, this suspicion has been gradually proved. With further digging into Snowden documents, the NSA's long-term systematic manipulation of the cryptographic system and its global surveillance by exploiting the vulnerabilities of encryption standard have been exposed, and its actions have undermined global trust in network technology. It also had a great impact on the ecological environment of global international relations.

Event Review

In early September 2013, *The New York Times*, the non-profit online news website ProPublica.org, and *The Guardian* respectively reported the NSA's long-term sabotage activities on encryption technology, as exposed by Snowden documents. The reports directly confirmed a speculation circulated in the security industry since 2007, that in the special publication SP 800-90 (renamed SP 800-90A after 2012) *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, officially released by NIST in 2006, one of the four recommended Deterministic Random Bit Generator (DRBG) algorithms, Dual_EC_DRBG, indeed had a backdoor. What shocked and upset the world was that this algorithm, computationally inefficient (compared with the other three) and flawed, had become the standard because of the NSA's carefully orchestrated global surveillance ambitions.

The cryptographic encryption system is designed based on a one-time encryption mechanism, and it relies on a high-quality random number generation mechanism. It can even be said that the random number mechanism is the foundation of modern encryption technology. If the random number generation mechanism is tampered with, the entire cryptographic protocol will be easily broken.

Doubts from Academia

In 2007, at the International Cryptography Annual Conference (Crypto 2007), cryptographers Niels Ferguson and Dan Shumow from Microsoft analyzed the possibility that Dual_EC_DRBG could be implanted with a backdoor from a technical perspective. The logic of the argument is that several constants in the standards used to define the algorithmic elliptic curve do not explain their origin. If these constants are specially chosen, and the algorithm designer has the data used to choose them, then all future "random" sequences generated by the algorithm can be extrapolated by obtaining only the first 32 bytes of the random sequences generated by the algorithm (See Fig. 4-1) [2].

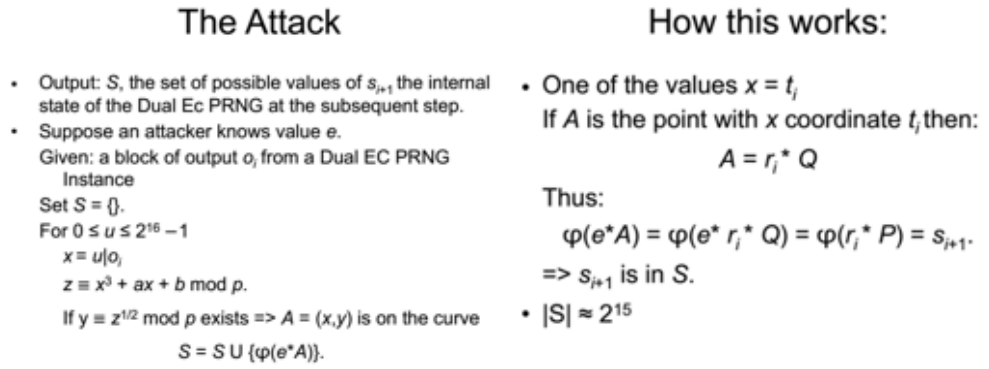


Fig. 4-1 Exploitation Principle of Dual_EC_DRBG Vulnerability

But cryptographers can't prove whether the algorithm designer has saved the relevant data for some purpose, so the discussion of this algorithm is limited to "vulnerabilities." It was not until 2013 that *The New York Times* and others confirmed this speculation.

Confirmation

"Cryptographers have long suspected that the agency planted vulnerabilities in a standard adopted in 2006 by the National Institute of Standards and Technology and

later by the International Organization for Standardization, which has 163 countries as members," reported the article *NSA Able to Foil Basic Safeguards of Privacy on Web* by *The New York Times* on September 6, 2013[3]. "Classified NSA memos appear to confirm that the fatal weakness, discovered by two Microsoft cryptographers in 2007, was engineered by the agency. The NSA developed the standard and aggressively put it into the international group, privately calling the effort a 'strategic challenge'."

This activity is part of the SIGINT Enabling Project, which receives an annual grant of $250-300 million to "actively engage the US and foreign IT industries to covertly influence and/or overtly utilize the design of commercial products." One of the goals in the agency's 2013 budget request was to "influence policies, standards and specifications for commercial public key technologies" (See Fig. 4-2 and Fig. 4-3)[4].

TOP SECRET//SI/TK//NOFORN

(U) COMPUTER NETWORK OPERATIONS
(U) SIGINT ENABLING

This Exhibit is SECRET//NOFORN									
	FY 2011[1] Actual	FY 2012 Enacted			FY 2013 Request			FY 2012 — FY 2013	
		Base	OCO	Total	Base	OCO	Total	Change	% Change
Funding ($M)	298.6	275.4	—	275.4	254.9	—	254.9	-20.4	-7
Civilian FTE	144	143	—	143	141	—	141	-2	-1
Civilian Positions	144	143	—	143	141	—	141	-2	-1
Military Positions	—	—	—	—	—	—	—	—	—

[1]Includes enacted OCO funding. Totals may not add due to rounding.

Fig. 4-2 NSA SIGINT ENABLING Project Budget

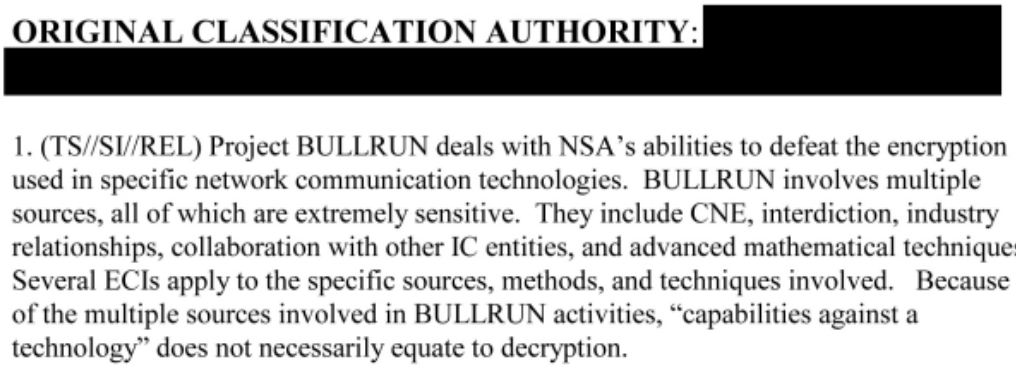
(U) Project Description

(TS//SI//NF) The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint, etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact. In this way, the SIGINT Enabling approach uses commercial technology and insight to manage the increasing cost and technical challenges of discovering and successfully exploiting systems of interest within the ever-more integrated and security-focused global communications environment.

Fig. 4-3 NSA SIGINT ENABLING Project Description

On September 5, 2013, *The Guardian* published an article named *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*[5], reporting the BULLRUN program[4] used by the NSA to crack Internet encryption technology. The program was first exposed in documents leaked by Snowden. "Project BULLRUN deals with the NSA's abilities to defeat the encryption used in specific network communication

technologies. BULLRUN involves multiple sources, all of which are extremely sensitive." The NSA is capable of cracking widely used online protocols, including HTTPS, Voice over IP, and Secure Sockets Layer (SSL), among others. The leaked documents also show that the NSA's Commercial Solutions Center "leverages sensitive, cooperative relationships with specific industry partners" to insert vulnerabilities into Internet security products (See Fig. 4-4)[4].



ORIGINAL CLASSIFICATION AUTHORITY: [redacted]

1. (TS//SI//REL) Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple sources, all of which are extremely sensitive. They include CNE, interdiction, industry relationships, collaboration with other IC entities, and advanced mathematical techniques. Several ECIs apply to the specific sources, methods, and techniques involved. Because of the multiple sources involved in BULLRUN activities, "capabilities against a technology" does not necessarily equate to decryption.

Fig. 4-4 NSA BULLRUN Program Description

These reports immediately aroused great concerns in the global security industry, and various studies and investigations into the NSA's manipulation of passwords and global security have since been launched. On December 27, 2013, Jacob Appelbaum, the former core programmer of The Onion Router (Tor) project, displayed a set of leaked PPT documents at the 30th Chaos Communication Conference (30C3), which contained programs and Trojans developed by the NSA to exploit vulnerabilities in various network products. The products include servers, routers, firewalls and mobile devices from DELL, HP, Juniper, CISCO and etc. Appelbaum said he suspected that the NSA had worked with some of these companies, and the disclosures were intended to allow the companies themselves to clarify whether they were complicit or victims of the NSA under the pressure of exposure.

In September 2013, American cryptographer Matthew Green published a blog post: *A Few Thoughts on Cryptographic Engineering*, in which he pointed out that the NSA "has been doing some very bad things. At a combined cost of $250 million per year, they include [6]:

1. Tampering with national standards (NIST is specifically mentioned) to promote weak, or otherwise vulnerable cryptography.

2. Influencing standards committees to weaken protocols.
3. Working with hardware and software vendors to weaken encryption and random number generators.
4. Attacking the encryption used by the next generation of 4G phones.

…

All of these programs go by different code names, but the NSA's decryption program goes by the name BULLRUN."

Matthew Green further outlined three ways to break a cryptographic system: 1. attack the cryptography; 2. go after the implementation or add backdoors; 3. access the human side. And he further pointed out that if those standards are credible, then more "breaking" methods will be the latter two.

On December 31, 2013, Belgian freelance security consultant Aris published a blog post *Dual_EC_DRBG Backdoor: A Proof of Concept*[7], which, in combination with the background of the Snowden incident, gave a clear conclusion: "It is quite obvious in light of the recent revelations from Snowden that this weakness was introduced by purpose by the NSA. It is very elegant and leaks its complete internal state in only 32 bytes of output, which is very impressive knowing it takes 32 bytes of input as a seed. It is obviously complete madness to use the reference implementation from NIST …" This is the formal conclusive response of the research community to NIST SP 800-90A after Dan Shumow and Niels Ferguson raised doubts in 2006. This blog post was quickly reprinted and disseminated by ZDNet, Slashdot and other well-known information and news websites.

In 2014, researchers including Stephen Checkoway, then at Johns Hopkins University, technically realized the exploit that two Microsoft cryptographers had previously speculated[8]. They attack and analyze several TLS (Transport Layer Security protocol for providing confidentiality and data integrity between two communicating applications) implementations using Dual_EC_DRBG, including OpenSSL-FIPS, Windows SChannel (Secure TLS communication subsystem) and the RSA BSafe encryption library, and published the results and analysis at the USENIX Security Annual Conference (See Fig. 4-5)[8]. The research shows that using a single CPU or computing cluster, it takes several seconds or tens of seconds to obtain the communication key, demonstrating the destructiveness of the standard: Due to the existence of vulnerabilities, various TLS sessions implemented using Dual_EC_DRBG are insecure.

Attack	Intel Xeon Reference System			16-CPU AMD Cluster
	2^{22} Candidates (s)	Expected Runtime (min)	Expected Cost	Total Runtime (min)
BSAFE-C v1.1	–	0.26	16	0.04*
BSAFE-Java v1.1	75.08*	641	38,500	63.96*
SChannel I	72.58*	619	37,100	62.97*
SChannel II	62.79*	1,760	106,000	182.64*
OpenSSL-fixed I	–	0.04	3	0.02*
OpenSSL-fixed II	–	707	44,200	83.32*
OpenSSL-fixed III	–	$2^k \cdot 707$	$2^k \cdot 44{,}200$	$2^k \cdot 83.32$

Fig. 4-5 The Results of Stephen Checkoway et al. Using the Dual_EC_DRBG Vulnerability to Attack Different TLS Implementations

Research by Stephen Checkoway et al. is disturbingly reminiscent of a December 21, 2013 Reuters report titled *Secret contract tied NSA and security industry pioneer*[9], which states that through a contract of US $10 million, the NSA made encryption technology company RSA use Dual_EC_DRBG as the preferred random data generation algorithm in BSafe to assist relevant agencies in carrying out large-scale surveillance programs.

Aftershock

As *The Guardian* reported in 2013, the NSA's practices have shaken the trust foundation of the entire Internet. The academic and industrial circles' doubts about the security of Internet communications have not diminished over time. To make it worse, the NSA has repeatedly demonstrated its ability to manipulate various communication standards and applications.

In May 2015, the American magazine *Wired* published an article *New Critical Encryption Bug Affects Thousands of Sites*[10], saying that security researchers have newly discovered a key vulnerability Logjam that has existed since the 1990s, allowing attackers to intercept and decrypt secure communications between users and thousands of website/mail servers around the world. "A close reading of published NSA leaks shows that the agency's attacks on VPNs are consistent with having achieved such a break", the researchers wrote in a blog post about the flaw.

In 2015, with the support of the European Commission's ICT Program and the Netherlands Organization for Scientific Research, Daniel Bernstein and others from Eindhoven University of Technology in the Netherlands conducted in-depth research on the NSA's systemic method of systematically manipulating cryptography standards, and published a paper *Dual EC: A Standardized Back Door*[11]. This paper sorts out the

process of the Dual EC algorithm with a backdoor entering the NIST standard, including how professional and academic opinions are systematically ignored. It explains technical aspects of how the backdoor works and how it can be exploited in practical applications, and explores the standardization and patent ecosystem in which the standardized backdoor stayed under the radar. The article pointed out that what is really shocking is the systematic approach of the NSA to weaken encryption standards in an organized way. The Dual EC algorithm with a backdoor has become a standard, which is only the tip of the iceberg of the NSA's systematic activities. This conclusion was quickly confirmed by the Crypto AG incident.

On February 11, 2020, *The Washington Post*, *Zweites Deutsches Fernsehen (ZDF)* and *Schweizer Radio und Fernsehen (SRF)* released a joint investigation report, exposing how the Switzerland-based company Crypto AG was manipulated by the intelligence agencies of the United States and Germany. Crypto AG started out by producing cryptographic equipment for the US Army during World War II. In the mid-1960s, the CIA and the NSA seized the opportunity of Crypto AG's technology upgrade and persuaded the company to produce and sell a new all-electronic encryption machine completely designed by the NSA. In 1967, Crypto AG launched a new generation of electronic encryption machines, whose inner workings were entirely designed by the NSA. Since the 1970s, the CIA and the German Federal Intelligence Service (Bundesnachrichtendienst, BND) have jointly held shares in Crypto AG, secretly controlling the security level of communication encryption equipment sold to more than 120 countries, and stealing the encrypted communication content of governments and enterprise users by intercepting and decoding the encryption program.

In the 1980s, about 40 percent of foreign communications handled by US intelligence officials came from Crypto AG's cryptographic systems, according to intelligence experts. Actual evidence shows that Crypto AG was involved in many major historical events (for example, during the Falklands War, the CIA obtained Argentine military information through Crypto AG and provided it to the UK). In 1993, after BND withdrew from the partnership with the US in Crypto AG, the US acquired all shares held by Germany and continued to control Crypto AG. The CIA continued as the owner of Crypto AG until around 2018. The exposure of this incident shows the ability of the US to obtain intelligence, as well as the interwoven ties between Western technology companies and US intelligence agencies.

Summary

Encryption algorithm is one of the cornerstones of modern cybersecurity technology. Reasonable use of encryption algorithm can ensure the security of network communication. The ability to crack most Internet privacy and encryption technologies, including VPN and HTTPS, suggests the NSA has easy access to most encrypted personal and commercial network communications and online transactions. The NSA eavesdropping and espionage activities on various countries disclosed by Snowden also triggered a global reconsideration and reflection on the US double-faced approach in politics, economy, and diplomacy.

The United States regards the ability to obtain global information and intelligence without blind corners as the basis to support its global interests. It goes further and further in pursuit of global surveillance and control, which not only destroys diplomatic trust between countries, but also causes irreparable backfire to itself. On September 10, 2013, faced with doubts about the encryption standard SP 800-90A, NIST finally issued a statement: "We want to assure the IT cybersecurity community that the transparent, public process used to rigorously vet our standards is still in place. NIST would not deliberately weaken a cryptographic standard. We will continue in our mission to work with the cryptographic community to create the strongest possible encryption standards for the US government and industry at large." NIST also reopened the review period for relevant standards. In 2015, NIST released a revision of SP 800-90A, which removed the Dual_EC_DRBG. However, the trust of industry and academia in NIST has been difficult to restore. Since 2015, several encryption standards and their implementations have been reviewed and analyzed. The hardware vendors involved in the reports are also widely suspected by the public. Whenever bugs or flaws are found in products such as servers and switches mentioned in Appelbaum's exposure documents, the first thing that comes to people’s mind is often a deliberately planted backdoor, rather than a weakness or flaw in the development process.

References

1. Wired. *MS Denies Windows Spy Key.* 1999. https://www.wired.com/1999/09/ms-denies-windows-spy-key/
2. Microsoft. *On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng.* 2007. http://rump2007.cr.yp.to/15-shumow.pdf

3. The New York Times. *NSA Able to Foil Basic Safeguards of Privacy on Web.* 2013. https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html
4. University of Auckland. *Crypto Won't Save You Either.* 2014. https://www.cs.auckland.ac.nz/~pgut001/pubs/crypto_wont_help.pdf
5. The Guardian. *Revealed: how US and UK spy agencies defeat internet privacy and security.* 2013 https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
6. Matthew Green. *A Few Thoughts on Cryptographic Engineering.* 2013. http://blog.cryptographyengineering.com/2013/09/on-nsa.html
7. Aris. *Dual_EC_DRBG Backdoor: a Proof of Concept.* 2013 https://blog.0xbadc0de.be/archives/155
8. Johns Hopkins University. *On the Practical Exploitability of Dual EC in TLS Implementations.* 2014. https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-checkoway.pdf
9. Reuters. *Secret contract tied NSA and security industry pioneer.* 2013. https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220
10. Wired. *New Critical Encryption Bug Affects Thousands of Sites.* 2015. https://www.wired.com/2015/05/new-critical-encryption-bug-affects-thousands-sites/
11. Eindhoven University of Technology. *Dual EC： A Standardized Backdoor.* 2015. https://pure.tue.nl/ws/files/3854147/588733604251427.pdf

Chapter 5. Evidence of Firmware Trojan - The Equation Group Emerged

Firmware is the software written into the hardware, which is embedded deeper than the operating system, loaded even before the operating system. If a virus is written into the firmware, it will be more difficult to be found.

On February 18, 2015, the American media *The Intercept* published an article titled *Researchers Find 'Astonishing' Malware Linked to NSA Spying*[1]. The article disclosed Kaspersky's research results and confirmed that the US used hard disk firmware to realize advanced persistent threat (APT), which shocked the cybersecurity community. As Kaspersky's series of reports gradually exposed the Equation Group from sample evidence, the underlying persistence capability of the NSA became clearer.

Event Review

As early as in January 2014, Darmawan Salihun, a cybersecurity expert specializing in BIOS security, began to publish a series of articles on the InfoSec Institute website, analyzing and exposing NSA BIOS backdoors, such as DEITYBOUNCE and GODSURGE, and called them "God Mode." [2]

From February to March 2015, Kaspersky released a series of reports [3-8], revealing an APT group called Equation Group, already active for nearly 20 years. The group, whose attack complexity and attack skills surpassed all cyberattack groups in history, was behind the Stuxnet and Flame viruses. The Equation Group had infected thousands, or perhaps even tens of thousands of victims in more than 30 countries worldwide, including Iran, Russia, Syria, China, UK, and US. Judging from the self-destruct mechanism used by Equation Group, Kaspersky concluded that the actual number of victims may be even higher.

The Process of Study, Analysis, and Publication

In February 2015, Kaspersky disclosed the global cyber espionage activities of Equation Group for the first time in the world, calling it the most advanced threat actor ever seen. Kaspersky released several detailed analyses [3-8], analyzing many related components of the Equation Group such as DoubleFantasy, EquationLaser, Fanny, EquationDrug, GrayFish and TripleFantasy, especially mentioned the hard disk firmware reprogramming plug-in, EquationDrug and GrayFish attack platform,

explaining the collaborative relationship between the components (See Fig. 5-1) [3]. Kaspersky proved the connection between the Equation Group and Stuxnet, through the fact that two zero-day vulnerabilities exploited by Fanny were later found to be used by Stuxnet in June 2009 and March 2010. In 2016, Kaspersky verified that NSA data leaked by the Shadow Brokers belonged to Equation Group, based on the constant value of the RC algorithm [9].

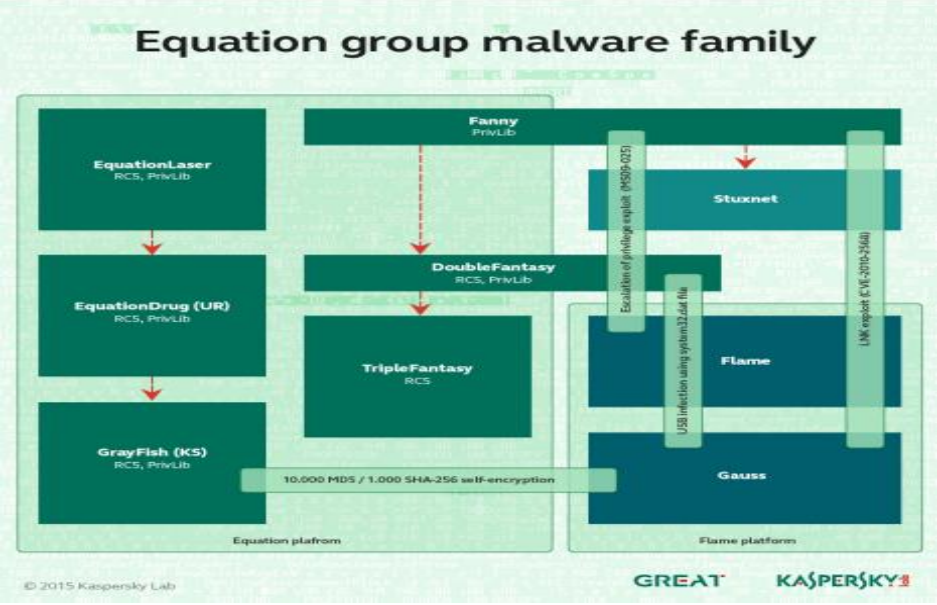


Fig. 5-1 Components of the Equation Group

Kaspersky pointed out that Equation Group implanted persistent attacks on hard disk firmware in high-value targets. Based on the study of samples, there were only a few cases of infection by the hard disk firmware reprogramming module among thousands of victims (See Fig. 5-2) [3], with a hard disk persistence rate of only about 2‰. Therefore, it can be seen that the firmware Trojan of Equation Group is a highly targeted and confidential tactical cyber weapon.

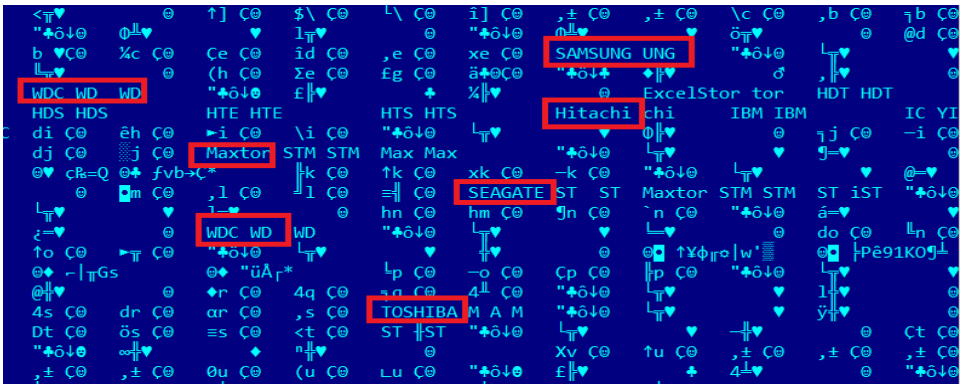


Fig. 5-2 Hard Disk Reprogramming Plug-in Infection Capability

After Kaspersky disclosed the Equation Group, Antiy released two analysis reports of Equation Group on March 5 and April 19, 2015 respectively[10,11]. In the report *修改硬盘固件的木马——探索方程式(EQUATION)组织的攻击组件* (*Trojans that Modify Hard Disk Firmware - Exploring the Attack Components of the Equation Group*), Antiy analyzed the composition structure, correlation, return information, instruction branch, C2 address, and plug-in functions of the main attack platform of Equation Group, and analyzed the attack technology principle of the critical plug-in "hard disk reprogramming" module (See Fig. 5-3)[10].

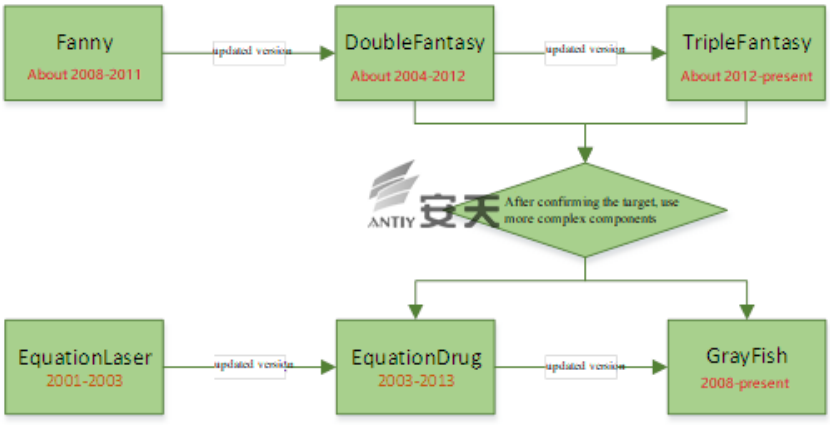


Fig. 5-3 Diagram of the Relationship between the Components of the Equation Group

In the report *方程式（EQUATION）部分组件中的加密技巧分析* (*Analysis of Encryption Techniques in Some Components of EQUATION*), Antiy presented the analysis results of the local configurations and network communication encryption algorithms and keys of the group's multiple components, and published the key structure for industry research and reference (See Fig. 5-4)[11].

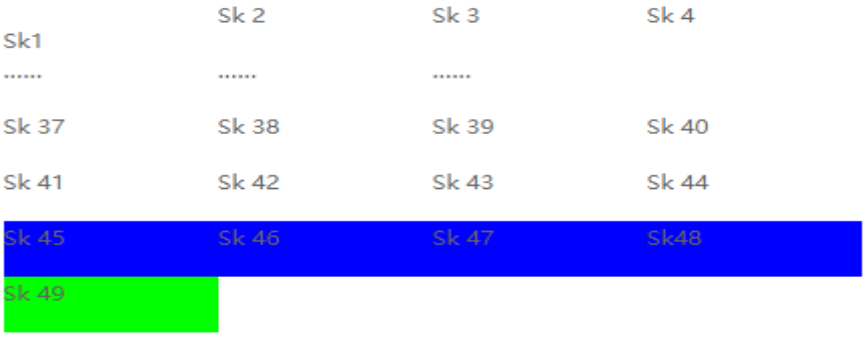


Fig. 5-4 The Equation Group Encryption Algorithm Key Structure Diagram

On February 23, 2022, Chinese cybersecurity company QAX released a report, which revealed the top-tier backdoor Bvp47 of NSA Equation Group, and verified that Bvp47 was a hacking tool belonging to Equation Group through the data leaked by the Shadow Brokers and Snowden (See Fig. 5-5)[12].

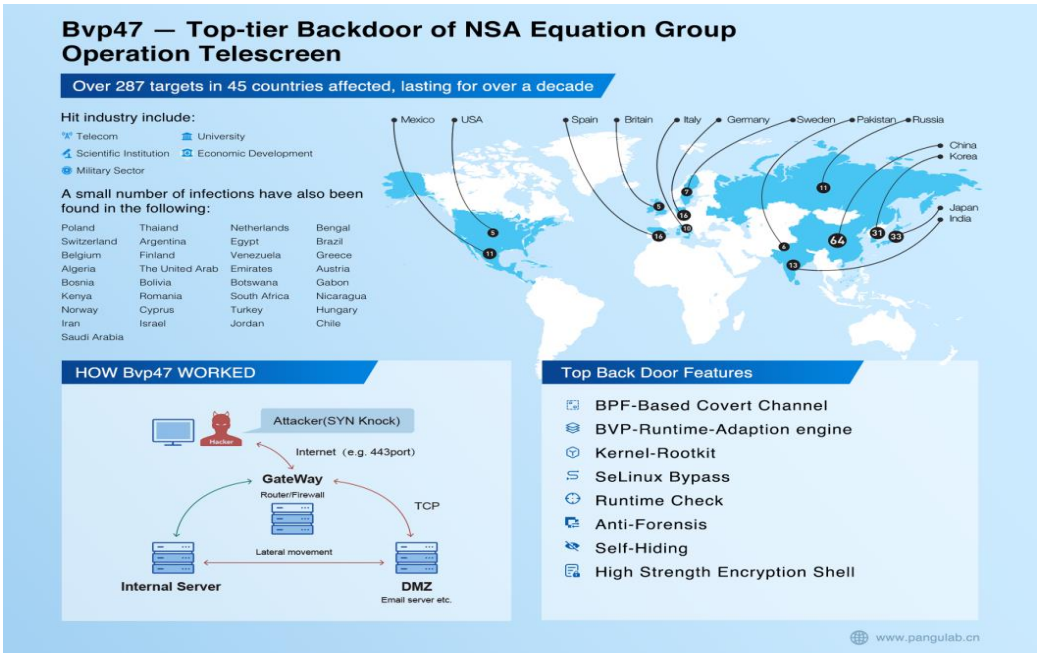


Fig. 5-5 Top-tier Backdoor Bvp47 of NSA Equation Group

After a comprehensive and in-depth technical simulation analysis, QAX reproduced the joint attack scenario of Dewdrops, Suctionchar_Agent and other components such as the Bvp47 backdoor program (See Fig. 5-6)[13].

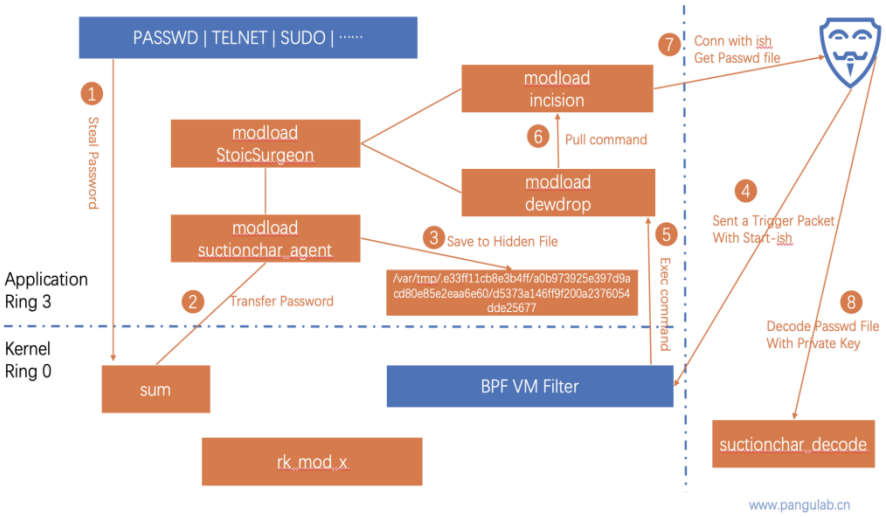


Fig. 5-6 Suctionchar_Agent Attack Scenario

Summary

APT is characterized by longer duration, larger spatial span, and wider resource scheduling capabilities, making it more difficult for security researchers to approach its essence. The top APT groups in the US, represented by the Equation Group, possess a complete and rigorous operating framework and methodology, a large-scale support engineering system and a combination of standardized equipment to conduct strict organizational operations. The pursuit of concealment and anti-traceability in the operation process makes their attacks seem traceless. It is difficult to detect the track of their breaking, existence, influence, continuity and withdrawal from the network environment or system. Consequently, defenders know little about the actual attack tactics, techniques, procedures (TTP) and corresponding tracks of their cyber operations, and are unable to fully understand and interpret information from the perspective of the whole threat framework.

References

1. The Intercept. *Researchers Find 'Astonishing' Malware Linked to NSA Spying.* 2015. https://theintercept.com/2015/02/17/nsa-kaspersky-equation-group-malware/
2. InfoSec Institute. *NSA BIOS Backdoor a.k.a. God Mode Malware Part 1: DEITYBOUNCE*. 2014. https://cysinfo.com/wp-content/uploads/2017/04/Shadow_release_updated.pdf
3. Kaspersky. *Equation Group: Questions and Answers.* 2015.

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf

4. Kaspersky. *Equation: The Death Star of Malware Galaxy.* 2015. https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/
5. Kaspersky. *Equation Group: The Crown Creator of Cyber-Espionage.* 2015. https://www.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage
6. Kaspersky. *A Fanny Equation: "I am your father, Stuxnet".* 2015. https://securelist.com/a-fanny-equation-i-am-your-father-stuxnet/68787/
7. Kaspersky. *Equation Group: from Houston with love.* 2015. https://securelist.com/equation-group-from-houston-with-love/68877/
8. Kaspersky. *Inside the EquationDrug Espionage Platform.* 2015. https://securelist.com/inside-the-equationdrug-espionage-platform/69203/
9. Kaspersky. *The Equation giveaway.* 2016. http://securelist.com/the-equation-giveaway/75812/
10. *安天. 修改硬盘固件的木马 探索方程式（EQUATION）组织的攻击组件.* 2015. https://www.antiy.com/response/EQUATION_ANTIY_REPORT.html
11. *安天. 方程式（EQUATION）部分组件中的加密技巧分析.* 2015. https://www.antiy.com/response/Equation_part_of_the_component_analysis_of_cryptographic_techniques.html
12. *奇安信. Bvp47-美国 NSA 方程式组织的顶级后门.* 2022. https://www.pangulab.cn/post/the_bvp47_a_top-tier_backdoor_of_us_nsa_equation_group/
13. *奇安信. "电幕行动"（Bvp47）技术细节报告（二）——关键组件深度揭秘.* 2022. https://mp.weixin.qq.com/s/YN8AJOrQWcpleV0tqhRGQQ

Chapter 6. Cyberattacks Covering All Platforms - Exposure of Equation Group's Solaris and Linux Samples

At the beginning of 2015, Kaspersky disclosed the cyberattack operations of the US intelligence agency NSA's Equation Group through sample evidence, and speculated that the Equation Group might have the ability to attack all mainstream operating system platforms. After a succession of exposure, virus samples written by the NSA for various platforms were exposed.

Event Review

In 2015, Kaspersky exposed the NSA Equation Group and released a series of analysis reports, suggesting that all the Equation Group related malware Kaspersky have collected so far is designed to work on Microsoft's Windows operating system. However, there are signs that non-Windows malware does exist.

In the Equation Group attack code against various firewalls and network equipment leaked by the Shadow Brokers in August 2016[1], the public connected the Equation Group with the attack equipment system named "ANT" for the first time, and discovered its ability to achieve injection and persistence against firewall products such as Cisco, Juniper, Fortinet, etc. On October 31, 2016, The Hacker News published an article, revealing more documents released by the Shadow Brokers[2], including a partial list of foreign servers infected by Equation Group. The documents showed that most of the affected servers were running Solaris, which is Oracle-owned Unix operating system, while some were running FreeBSD or Linux.

The Process of Study, Analysis, and Publication

In February 2015, Kaspersky released *Equation Group: Questions and Answers*,[3] suggesting that Equation Group may have multi-platform attack ability. Although the samples collected were all designed to work on Microsoft Windows operating system, there are signs that non-Windows malware used by Equation Group does exist. There is evidence that a Mac OS X version of DOUBLEFANTASY also exists.

On November 3, 2016, Antiy released the report *从"方程式"到"方程组"——EQUATION 攻击组织高级恶意代码的全平台能力解析* (*From Equation to Equations - Revealing the Multi-Platform Operational Capability of Equation Group*)[4]. The report analyzed the Equation Group attack samples targeting multiple architectures

and systems (See Fig. 6-1), and was the first report in the world to expose Equation Group's attack abilities against Solaris (SPARC architecture) and Linux system through real samples. The Antiy report unveiled the NSA's all-platform attack ability, and sorted out related information exposed by other parties.

Information	Windows	Linux	Solaris	Oracle-owned Unix	FreeBSD	Mac OS
Antiy The Trojan modifying firmware Exploration in attack components of Equation Group	Analysis of sample payload and hard disk persistence capability					
Antiy Analysis of encryption skills used in Equation Group attack components	Encryption algorithm analysis					
Antiy Revealing the multi-platform loading capability of Equation Group（this report）		Existed. Analysis of related payloads	Analysis of related payloads			
The Hacker News：Shadow Brokers reveals list of Servers Hacked by the NSA			Existed	Existed	Existed	
Kaspersky Equation: The Death Star of Malware Galaxy	Revealing Equation Group					
Kaspersky A Fanny Equation: "I am your father, Stuxnet"	Fanny component analysis					
Kaspersky Equation Group: from Houston with love	Doublefantasy analysis					
Kaspersky EQUATION GROUP: QUESTIONS AND ANSWERS	Equation Group Questions and Answers					Speculation based on network features

Fig. 6-1 Equation Group All-Platform Attack Ability

On January 25, 2017, based on analysis of the Equation Group samples revealed by the Shadow Brokers, Antiy released the report *方程式组织EQUATION DRUG平台解析* (*The Analysis of EQUATION DRUG Platform*)[5]. In this report, Antiy drew a building block diagram of the Equation Group operation module (See Fig. 6-2)[5] and revealed how the United States used refined modules to achieve front and rear field control and delivered malware on demand.

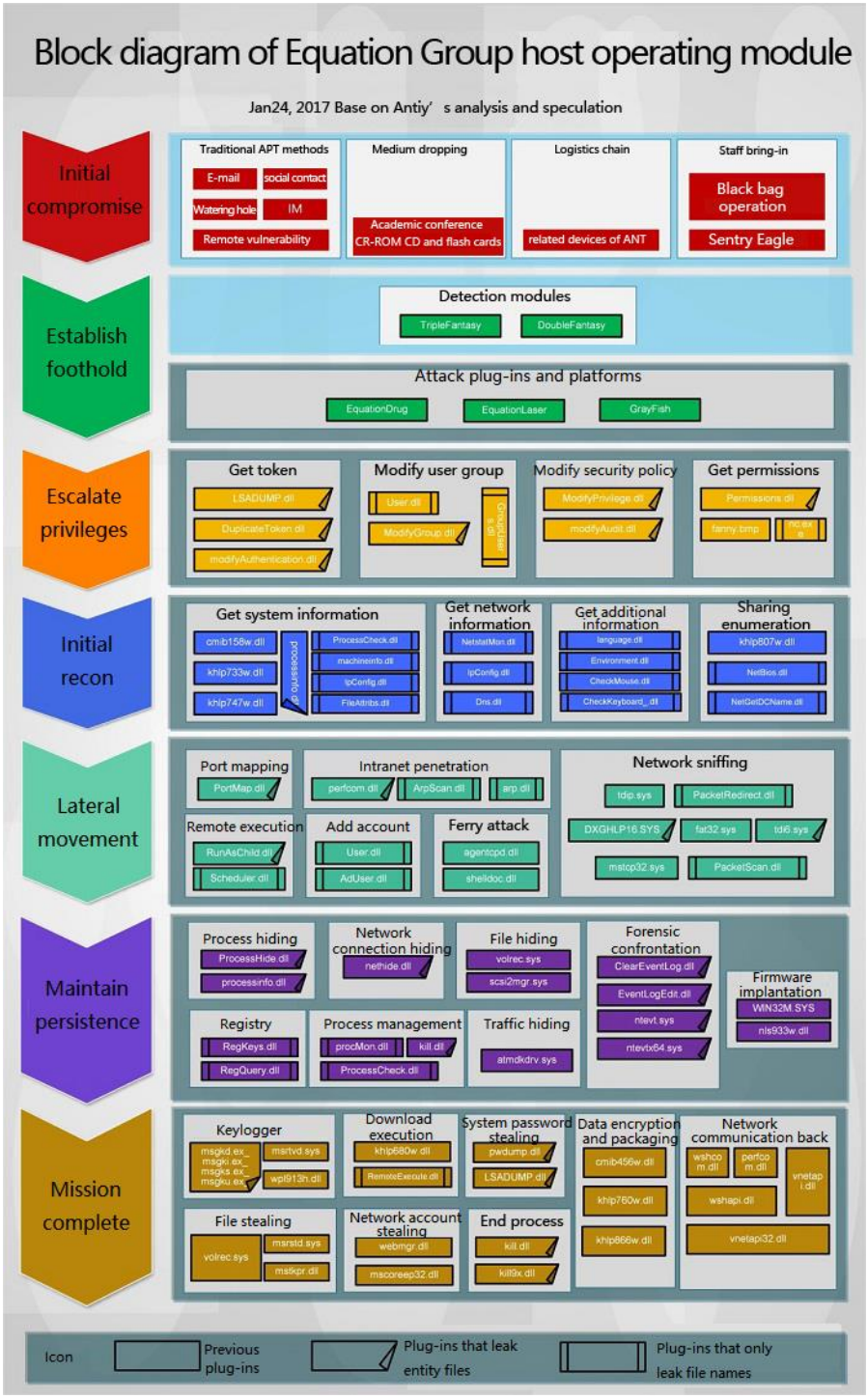


Fig. 6-2 The Equation Group Building Block Diagram of Host Operation Module

We can see that the operation mode of the United States often starts with a memory loader carrying a large number of small DLLs as atomic attack modules, which are transmitted to the front field through an encrypted channel and loaded by the loader, so as to guarantee concealment and reusability.

Summary

Cybersecurity researchers have found that super attack groups seek to extend their payload capabilities to all scenarios where intrusion and persistence can be achieved. In these scenarios, various server operating systems, such as Linux, Solaris and FreeBSD are highly targeted. Based on such research and judgment, cybersecurity vendors have carried out detailed and in-depth tracking research on the super APT Equation Group. The relevant exposed documents of the Shadow Brokers confirmed this judgment. The cybersecurity vendors disclosed part of the analysis of Equation Group samples targeting Solaris platform and Linux platform, analyzed the platform-wide attack ability of Equation Group, and had a further understanding of the US cyber operation capability that is "far beyond reach".

References

1. Cyber Security Review. *Shadow Brokers reveals list of Servers Hacked by the NSA.* 2016. https://www.cybersecurity-review.com/shadow-brokers-reveals-list-of-servers-hacked-by-the-nsa/
2. Hacker News. *Equation Group Cyber Weapons Auction.* 2016. https://news.ycombinator.com/item?id=12290623
3. Kaspersky. Equation Group: Questions and Answers. 2015. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf
4. *安天. 从"方程式"到"方程组"——EQUATION 攻击组织高级恶意代码的全平台能力解析.* 2016. https://www.antiy.com/response/EQUATIONS/EQUATIONS.html
5. *安天. 方程式组织 EQUATION DRUG 平台解析 —方程式组织系列分析报告之四.* 2017. https://www.antiy.com/response/EQUATION_DRUG/EQUATION_DRUG.html

Chapter 7. Leaked Arsenal - Uncontrolled US Cyberweapons Become Tools of Cybercrime

In April 2017, the Shadow Brokers exposed the NSA's cyberweapons in batches, which involved a large number of system-level zero-day exploit tools and advanced backdoor malware. The US lacking of effective control has led to the leakage of "arsenal-level" cyberattack weapons, which has caused great panic among users around the world. One month later, the WannaCry ransomware created a worldwide network disaster only by exploiting the EternalBlue vulnerability in the NSA cyberweapons.

Event Review

The EternalBlue vulnerability was exploited by hackers to carry out a ransomware attack. On May 12, 2017, hackers exploited the EternalBlue vulnerability leaked from the NSA to spread the worm-like ransomware WannaCry, which exploited the SMB vulnerability MS17-010 based on port 445 to infect a large number of Windows computers around the world. Files in the compromised computers were encrypted, and the victims can only unlock and recover files after paying a ransom to the hacker to obtain the key. The WannaCry ransomware virus caused a global Internet disaster. At least 300,000 users from 150 countries were affected, causing a loss of 8 billion US dollars. Many industries such as finance, energy and healthcare were affected with serious crisis management problems. Microsoft released a patch for this vulnerability in March 2017, and the cyberweapons used by the Equation Group and published by the Shadow Brokers on April 14, 2017 contained the exploitation program of this vulnerability. Hackers used this cyberweapon to carry out massive global attacks on all Windows computers that were not patched in time.

This is a serious large-scale cybersecurity incident caused by the proliferation of cyber arsenals.[1] The superpower's unrestrained development of cyber armaments, without strictly performing their custody obligations, has seriously affected the security foundation and trust of the Internet. We can also see from this incident that once high-capability cyberweapons are leaked and out of control, they will quickly transform into a universal attack capability, thereby triggering an avalanche of social risks.

Reactions

On April 16, 2017, China National Vulnerability Database (CNVD), which is under the National Computer Network Emergency Response Technical Team of China (**CNCERT**), issued the *关于加强防范 Windows 操作系统和相关软件漏洞攻击风险的情况公告* (*Announcement on Strengthening the Prevention of Windows Operating System and Related Software Vulnerability Attack Risks*)[2]. A number of vulnerability attack tools related to the SMB service of the Windows operating system disclosed by the Shadow Brokers were notified (See Tab. 7-1)[2], and an early alert of possible large-scale attacks was issued.

Tab. 7-1 Vulnerability Attack Tools with Possible Attacks via Port 445

Tool Name	Main Purpose
ETERNALROMANCE	SMB and NBT vulnerabilities, corresponding to MS17-010 vulnerabilities, targeting ports 139 and 445, impacting Windows XP, Windows 2003, Windows Vista, Windows 7, Windows 8, Windows 2008 and Windows 2008 R2
EMERALDTHREAD	SMB and NETBIOS vulnerabilities, corresponding to MS10-061 vulnerabilities, targeting ports 139 and 445, impacting Windows XP and Windows 2003
EDUCATEDSCHOLAR	SMB service vulnerability, corresponding to MS09-050 vulnerability, target port 445
ERRATICGOPHER	SMBv1 service vulnerability, targeting port 445, impacting Windows XP and Windows server 2003, Windows Vista and later operating systems are not impacted
ETERNALBLUE	SMBv1 and SMBv2 vulnerabilities, corresponding to MS17-010, targeting port 445, impact range: wide, from Windows XP to Windows 2012
ETERNALSYNERGY	SMBv3 vulnerability, corresponding to MS17-010, targeting port 445, impacting Windows8 and Server2012
ETERNALCHAMPION	SMB v2 vulnerability, targeting port 445

After the incident, on May 13, 2017, CNVD issued the *关于重点防范 Windows 操作系统勒索软件攻击的情况公告* (*Announcement on Focusing on Prevention of Ransomware Attacks on Windows Operating System*)[3], which, based on samples

obtained by 360, Antiy and other organizations and related analysis, clarified that the ransomware spread based on port 445 and exploited the SMB service vulnerability (MS17-010). And the overall judgment was that the Shadow Brokers' disclosure of vulnerabilities attack tools led to the attack. According to the CNVD survey, more than 9 million host IPs on the Internet were exposed with port 445, including over 3 million from Chinese mainland. CNCERT monitored ransomware and related cyberattack activities, and advised users to update the released security patches for Windows in time, and protect network boundaries, internal network areas, host assets and data backup.

Shortly after the WannaCry ransomware attack, Kaspersky issued a report, pointing out that EternalBlue[4], the hacking tool used in the attack, was from the NSA's cyber arsenals, and the hacking tool was previously disclosed online by the Shadow Brokers. A weakness in Microsoft Windows operating system has been exploited for massive attacks on those computers.

In January 2017, Antiy released *2016 网络安全威胁的回顾与展望 (The 2016 Threat Annual Report)*[5], pointing out that the proliferation of cyberweapons has comprehensively reduced the attack cost of threat actors, and the resurgence of worms driven by ransom patterns will be inevitable. As predicted, WannaCry broke out and quickly spread worldwide four months after Antiy's report was released. Antiy analyzed the ransomware's use of SMB vulnerability MS17-010 (See Fig. 7-1)[6], and issued reports defining it as "uncontrolled use of arsenal-level attack equipment."[6,7]

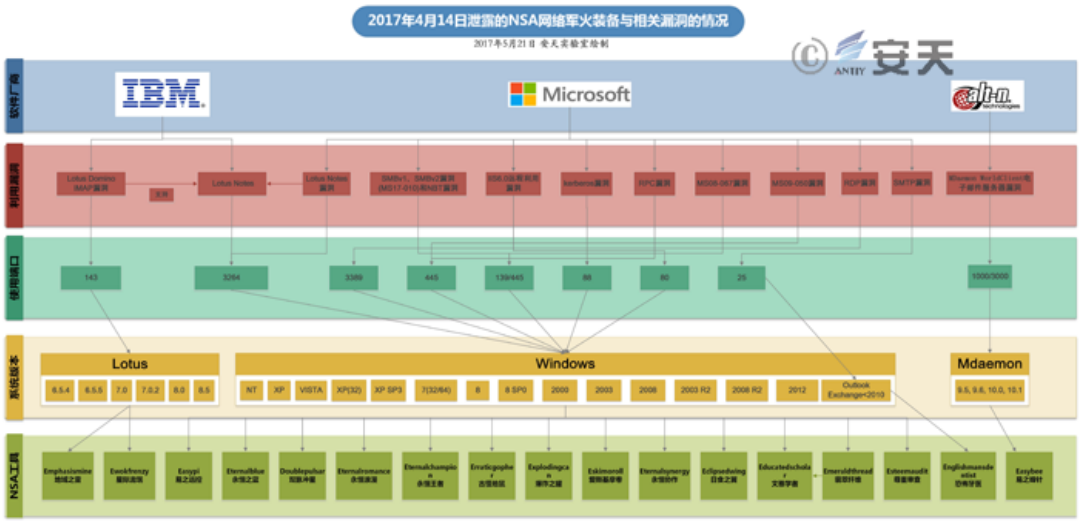


Fig. 7-1 Relationship Between Leaked NSA Cyber Arsenal, Vulnerabilities and System Versions

Given that the WannaCry ransomware only exploits EternalBlue among the exposed cyberweapons, there are other vulnerabilities and tools in the cyber arsenals series exposed by the Shadow Brokers that need attention and protection. On May 22, 2017, Antiy released the *关于系统化应对 NSA 网络军火装备的操作手册* (*Operation Manual on Systematic Response to NSA Cyber Arsenal Equipment*)[6]. Based on the analysis and prediction of WannaCry, Antiy provided the solution process and relevant countermeasures for effectively detecting and defending the current samples and damage mechanism, as well as laying out the possible techniques used by the subsequent ransomware. It reminded users to use standardized process in daily security application and maintenance, integrate security design, passive defense, active defense and threat intelligence, and rely on security products with effective protection capabilities to form the in-depth defense capability.

On May 12, 2017, 360 0Kee Team detected a new ransomware virus spreading rapidly exploiting the EternalBlue vulnerability, and instantly issued an alert calling on the public to install system patches and security software. During the large-scale outbreak of WannaCry, 360 launched a series of solutions after obtaining samples[8].

Summary

Superpowers have a large stockpile of cyberweapons, and once they are stolen or leaked, it is hard to predict the potential threats and impacts. The exposure of the Shadow Brokers has brought to the surface a number of American arsenal-level cyberattack equipment, and these vulnerabilities have been quickly and extensively exploited by other low-level cyber threat actors after the leakage of tools and malware payload, leading to cybersecurity incidents such as the WannaCry outbreak, which profoundly showed the rich reserve and great capability of the US super cyberweapons, as well as the extreme severity of global cybersecurity accidents caused by its leakage and malicious use due to its ineffective control. The EternalBlue vulnerability exploited by WannaCry is just a drop in the ocean of cyberweapons. Although more leaked cyberweapons will not spread unchecked, they may be used by disciplined cyberattack groups in a targeted way and cause as much damage as EternalBlue. Their existence and leakage are more worrying, although they have not received enough attention simply because no widespread harm is done.

References

1. 新华社. *全球网络攻击波及中国 因美国网络武器库泄露*. 2017. http://www.xinhuanet.com//world/2017-05/13/c_1120966771.htm
2. 中国国家信息安全漏洞共享平台（CNVD）. *关于重点防范 Windows 操作系统勒索软件攻击的情况公告*. 2017. https://www.cnvd.org.cn/webinfo/show/4139
3. CNVD. *关于重点防范 Windows 操作系统勒索软件攻击的情况公告*. 2017. https://xjca.miit.gov.cn/zwgk/wlaq/art/2020/art_f77d00b8fb7e4d808f551e0179b9141a.html
4. Kaspersky. *What is WannaCry ransomware?* 2017. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
5. *安天*. *2016 网络安全威胁的回顾与展望*. 2017. https://www.antiy.cn/research/notice&report/research_report/725.html
6. *安天*. *关于系统化应对 NSA 网络军火装备的操作手册*. 2017. https://www.antiy.com/response/Antiy_Wannacry_NSA.html
7. *安天*. *安天针对勒索蠕虫"魔窟"（WannaCry）的深度分析报告*. 2017. https://www.antiy.com/response/wannacry.html
8. 360. *WannaCry 爆发一周年 500 万台电脑惨遭勒索病毒攻击*. 2018. https://www.360.cn/n/10169.html

Chapter 8. Proliferation of Armaments - The US Penetration Testing Platform Becoming a Widely Used Tool for Hackers

Cyber armaments are weapon-level attack platforms, malware, vulnerabilities and their exploitation programs, as well as other tools or components used to facilitate attacks. Now, they mainly include relevant attack tools and support systems developed by intelligence agencies such as the NSA and the CIA, as well as some commercial tools, such as Cobalt Strike and other attack platforms. In recent years, due to the lack of supervision on the automated penetration attack testing platform sold by the United States, the relevant attack platforms have flooded around the world and become the essential tools for attack groups to implement intranet penetration and malicious cyberattacks on a large scale.

Overview

Cobalt Strike is a penetration testing tool first released in June 2012 and created by Raphael Mudge, a former US Air Force security researcher. The commercial version of Cobalt Strike integrates service scanning, automated overflow, multi-mode port monitoring, multiple Trojan generation modes (dll Trojan, memory Trojan, office macro virus, Beacon communication Trojan, etc.), phishing attacks, site cloning, target information acquisition, automatic browser attacks, etc. It can also leverage other well-known tools like Mimikatz, etc. As an efficient penetration testing tool, Cobalt Strike has powerful functions and scalability. It can be well supported from the early stage of payload generation, bait bundling and phishing attack to continuous control and post-penetration after successful payload implantation, covering almost all stages of the attack chain. In recent years, Cobalt Strike has been used by hackers and APT groups to implement real cyberattacks due to the usability and scalability. Attackers use Cobalt Strike to host their C&C servers, and then deploy malware on infected hosts through it. According to a Proofpoint (an American technology security company) study in 2020, 15% of Cobalt Strike campaigns were attributable to known threat actors.

Reactions

On May 27, 2015, Antiy found that in a quasi-APT attack against Chinese government agencies[1], the attacker relied on the Shellcode generated by Cobalt Strike and used

Beacon mode to communicate, realizing the ability to remotely control the target host. Analysts compared the sample module with payload generated by Beacon and found that there were only three differences (See Fig. 8-1)[1]. Based on this, analysts concluded that the sample module was generated by Beacon.

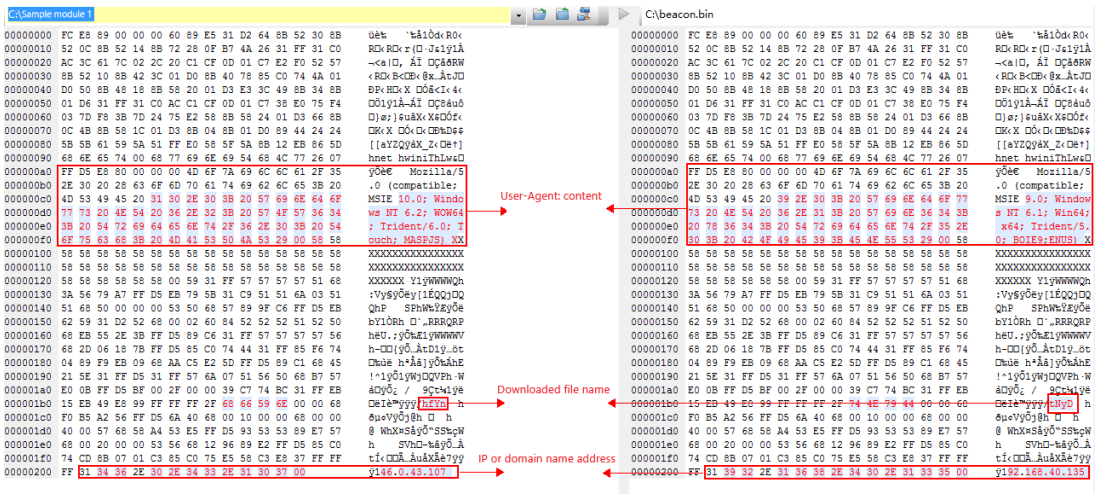


Fig. 8-1 Comparative Analysis of Sample Module and Module Generated by Beacon

At the 2015 China Internet Security Conference (ISC 2015) , Antiy published a public report titled *网络安全中的商业军火* (*Commercial Arsenals in Cybersecurity*)[2]. This report systematically combed the major commercial cyber arsenals such as Regin and Cobalt Strike since the early 21st century, and analyzed their origins with the military cyber capabilities of relevant countries. Taking the commercial attack platform Cobalt Strike as an example, the service and R&D background of its founder, Raphael Mudge, in the US military active and reserve network forces (See Fig. 8-2)[2], clearly reflects the spillover and destructiveness of the US military cyber technology and capability.

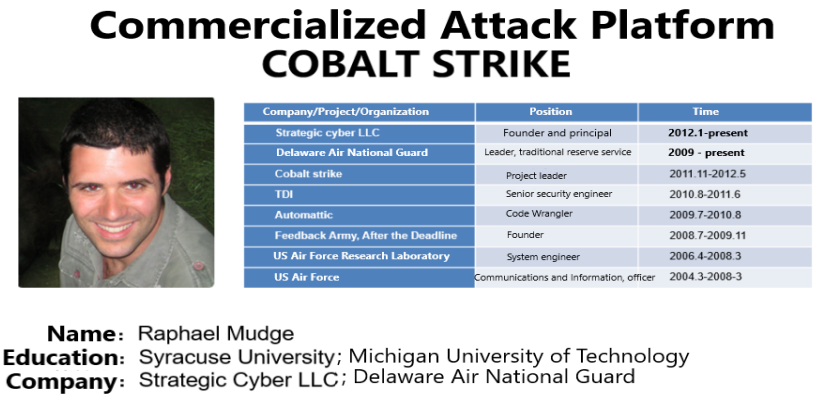


Fig. 8-2 Analysis of Military Background of Cobalt Strike's Founder

A 2020 study by Proofpoint showed that the use of Cobalt Strike by threat actors increased by 161% compared with 2019. About the use of Cobalt Strike in attacks in recent years, the data graph of Proofpoint showed (See Fig. 8-3)[3]: From 2016 to 2017, only a small number of victim organizations were found that attackers have used this tool; a significant increase began in 2018, when Cobalt Strike was implanted in more than 1,000 victim organizations; Cobalt Strike appeared in about 5,000 victim organizations in 2019; in 2020, the number has exceeded 9,000; and in 2021, more than 8,000 organizations became victims of the tool within half a year. Proofpoint pointed out that from 2019 to 2021, 15% of attacks that used Cobalt Strike were linked to known hacking groups.

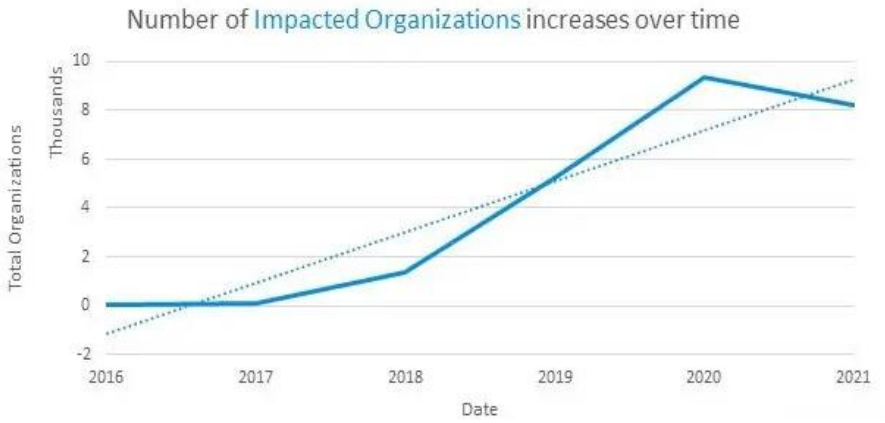


Fig. 8-3 Growth Trend of the Number of Impacted Organizations

The analysis of Sentinelone[4], an American cybersecurity company, shows that: Egregor ransomware is an offshoot of the Sekhmet malware family that has been active since mid-September 2020; the primary distribution method for Egregor is Cobalt Strike; targeted environments are previously compromised through various means (RDP exploit, Phishing) and once the Cobalt Strike beacon payload is established and persistent, it is then utilized to deliver and launch the Egregor payloads.

QAX found that the threat organization Blue Mockingbird exploited the Telerik UI vulnerability (CVE-2019-18935) to compromise the servers to install Cobalt Strike beacon and hijack system resources to mine Monero coins[5]. The analysis indicates that the payload used in attack campaigns is Cobalt Strike beacon, which Blue Mockingbird misused as a legitimate penetration testing tool to execute encoded PowerShell commands. The script uses common AMSI bypass techniques to evade Windows Defender detection, download and load Cobalt Strike DLL into memory.

Summary

Technologies enable the spread of capabilities. Computer technology enables the automation of attack behavior and attack capability, and highly automated commercial attack platforms allow this capability to spread far faster than we expected. Today's superpowers, with the world's top capabilities on both sides of attack and defense, should take more responsibilities for effectively manipulating the proliferation of such weapon-level attack means. However, the fact is that the United States, which has the strongest network technology capability, has not lived up to its stated salvation of "stronger strength, greater responsibility." Instead, based on its strong defense capability, the United States has not effectively restricted and controlled automated attack platforms such as Cobalt Strike, but allowed commercial sales. This has not only brought security risks to cyberspace, but also caused unpredictable potential impact on the security of other countries.

The essence of unilateral deterrence is blackmail. A peaceful and stable world should not be based on the simple winner-take-all model. The confidence of the US, a superpower, should not only come from the absolute victory of cyberwar, but also from the "effective release of security guarantees to other countries and constraints on its own capabilities."[6]

References

1. 安天. 一例针对中国政府机构的准 APT 攻击中所使用的样本分析. 2015. https://www.antiy.com/response/APT-TOCS.html
2. 安天. *网络安全中的商业军火. 中国互联网安全大会（ISC 2015）*. 2015 https://www.antiy.com/presentation/20150929-ISC.pdf
3. Proofpoint. Cobalt Strike: Favorite Tool from APT to Crimeware. 2022. https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware
4. Sentinel Labs. Egregor RaaS Continues the Chaos with Cobalt Strike and Rclone. 2022. https://www.sentinelone.com/labs/egregor-raas-continues-the-chaos-with-cobalt-strike-and-rclone
5. 奇安信. 黑客利用已存在三年之久的 Telerik 漏洞部署 Cobalt Strike. 2022. https://blog.csdn.net/smellycat000/article/details/125342296
6. 新华网. 肖新光：美国凭什么能开启"上帝模式". 2015. http://www.xinhuanet.com/world/2015-09/19/c_128246851.htm

Chapter 9. Exposure of Project CAMBERDADA - Response to the US Monitoring of Cybersecurity Vendors

Faced with the high level of attack capability of the US, the global cybersecurity industry has been competing against the attack campaigns of the US intelligence agencies hidden behind the scenes by analyzing and exposing samples, and upgrading and improving product capabilities. In June 2015, several global media simultaneously disclosed Project CAMBERDADA leaked by Snowden, exposing the evil deeds of the US intelligence monitoring and construction of anti-virus vendors blacklist to the world, which formed a public opinion contest.

Event Review

On June 22, 2015, the website Free Snowden exposed an NSA document *An Easy Win: Using SIGINT to Learn about New Viruses* with the words "TOP SECRET" (See Fig. 9-1)[1], revealing project CAMBERDADA implemented by intelligence agencies of the United States and the United Kingdom. The project mainly uses the traffic acquisition ability of the US in the invasion of global operators to monitor the communications between anti-virus vendors (such as Kaspersky) and users, so as to obtain new virus samples and other information. According to the cover of the document, the Project probably began in 2007. The Information Assurance Directorate (IAD) and the National Threat Operations Center (NTOC) participated in the project.

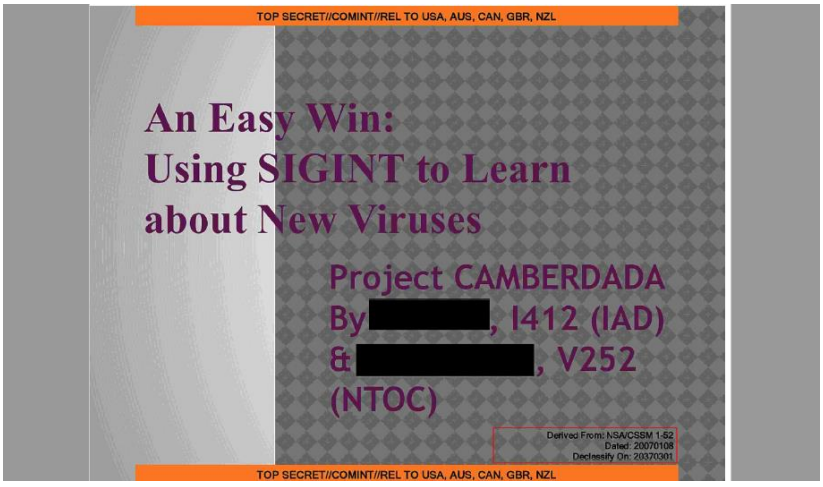


Fig. 9-1 Document Cover of Project CAMBERDADA

Subsequent targets of the project include 23 global key cybersecurity vendors from 16 countries in Europe and Asia, including Chinese security vendor Antiy (See Fig. 9-2)[1].

Fig. 9-2 More Monitoring Target Vendors Listed in CAMBERDADA besides Kaspersky

Reactions

On June 22, when Snowden exposed Project CAMBERDADA, some Western media simultaneously reported this event[2-5].

According to an article published on the website *The Intercept*[2], Project CAMBERDADA showed that the NSA has been systematically spying on software from Kaspersky and other anti-virus vendors since 2008. The NSA made full use of the monitoring capability of the US targeting global networks, with Kaspersky and other cybersecurity vendors as its main targets, monitored and obtained the emails sent by global users to anti-virus vendors, extracted virus samples and other information, intended to analyze, contain, and use these samples, and analyzed whether the security vendors have found and mastered their cyberattack weapons.

According to the article *US and British Spies Antivirus Companies* published on *Wired*[3], Project CAMBERDADA describes a systematic software reverse engineering activity designed to detect software vulnerabilities by monitoring security vendors, so as to help intelligence agencies bypass the software. According to documents leaked by Snowden, the NSA's Signal Intelligence Center screened 10 out of hundreds of thousands of malicious files sent to Kaspersky everyday for analysis. After that, the NSA analysts checked the response of Kaspersky anti-virus software to these malicious files to ensure that they have not been included in the detection. NSA hackers modified those malware for their own use and regularly checked to see whether Kaspersky has listed them in its virus library.

The associate editor at *Forbes* also wrote an article titled *NSA Spied On Non-American Anti-Virus Companies* in the magazine on June 22[4]. British and American intelligence agencies have spied on anti-virus companies and probed their software for weaknesses, as the snoops sought to enhance their offensive surveillance techniques. This was predictable given previous revelations around the extensive hacking capabilities at the GCHQ and the NSA. Anti-virus software has been given high access to computers, making it a good target which intelligence agencies were also working hard to crack them. McAfee and Symantec, the US anti-virus leaders, and Sophos, the best-known UK anti-virus vendor, are excluded from the list. All three have many former government employees and have close working relationships with intelligence and law enforcement agencies. Obviously, this is a blacklist of security vendors beyond the US-led Five Eyes (the US, the UK, Canada, Australia and New Zealand), and that have the ability to detect and contain the US intelligence campaigns.

According to China's Xinhua News Agency, the anti-virus vendors under surveillance told the US media that the relevant reports were disturbing[6].

ESET, a security vendor from Slovakia, said that all enterprises in the information security industry should join forces to fight any attempt to weaken security products. "Our first priority is always to protect our users, products and systems from any intrusion, no matter where it comes from."

Kaspersky's spokesperson said that security vendors should work together to safeguard user privacy and Internet privacy rights, thwart large-scale surveillance and make the world safer.

AVG Technologies from the Czech Republic said that the recently passed USA Freedom Act of 2015 imposes new restrictions on national monitoring, which is a positive move to ensure the safety and security of users, but rebuilding confidence in the digital ecosystem requires a long-term effort.

All the enterprises above were confident in their security products and their products had not been compromised.

Antiy, which was listed as the target, released the report *对相关媒体报道"中企曾被美国情报机构攻击"涉及我司的两点声明* (*Two Statements Concerning Our Company Reported by Relevant Media that "Chinese Enterprises were Attacked by US Intelligence Agencies"*)[7], pointing out that the means disclosed in the leaked documents are mainly the relevant intelligence agencies monitoring the public network channel to obtain the emails reported by users to vendors, rather than attacks on security vendors'

own network systems and products. More importantly, the release of this monitoring target list will further split the global security industry which has already seen cracks and suspicions.

Summary

The United States directly uses global cybersecurity vendors to assist its cyber capabilities through espionage operations. Kaspersky has analyzed in its report that the intrusion was intended to learn anti-virus software[8].

The US CAMBERDADA obtains a large number of virus samples by monitoring global cybersecurity vendors. However, the samples submitted by users to vendors are often those that can bypass vendors' detection. The NSA obtains these samples and then submits them to TAO for reuse, including modifying the sample configuration and converting them into usable attack weapons. At the same time, the NSA determines the processing capacity of a vendor through the submission time of relevant samples and the subsequent response, so that it can better plan actions to bypass detection[9,10].

The purpose of the CAMBERDADA is to capture samples reported by global users to anti-virus vendors, provide reusable sample resources for TAO, and monitor the processing capacity of anti-virus vendors and whether they let off some malware samples.

The US intelligence agencies regard the international anti-virus and security vendors outside their own countries as the stumbling block to their global attacks and surveillance campaigns. At the same time, the US also interacts subtly with the security vendors in their own countries, and forcibly divides the anti-virus and security vendors into different camps. In addition to Kaspersky from Russia, its subsequent targets also include Bitdefender from Romania, Avira from Germany, and Antiy from China. However, major anti-virus vendors in Five Eyes countries (such as the United States and the United Kingdom) such as Symantec, McAfee, Trend Micro and Sophos are not included in the list. It may indicate that the relevant intelligence agencies of the UK and the US have direct interaction and communication channels with the security vendors, without having to resort to surveillance.

This action of the United States intelligence agency is to forcibly divide the anti-virus and security vendors into different camps, which will inevitably lead to the disappearance of the security industry cooperation and emergency coordination mechanism that has been formed difficultly between various countries, and will also

significantly damage the basic trust of users from other countries around the world in the US security vendors.

References

1. Snowden Archive. *An Easy Win: Using SIGINT to Learn about New Viruses.* 2015. https://edwardsnowden.com/wp-content/uploads/2015/06/project-camberdada.pdf
2. The Intercept. *Project CAMBERDADA-NSA.* 2015. https://theintercept.com/document/2015/06/22/project-camberdada-nsa/
3. Wired. *US and British Spies Targeted Antivirus Companies.* 2015. https://www.wired.com/2015/06/us-british-spies-targeted-antivirus-companies/
4. Forbes. *NSA Spied On Non-American Anti-Virus Companies.*2015. https://www.forbes.com/sites/thomasbrewster/2015/06/22/foreign-av-companies-targeted-by-nsa/?sh=3b7081495b8c
5. RT. *NSA, GCHQ targeted Kaspersky, other cybersecurity companies–Snowden docs.*2015. https://www.rt.com/usa/268891-nsa-gchq-software-kaspersky/
6. 新华社. *综述：多国网络安全厂商抨击美英监听计划*. 2015. http://news.xinhuanet.com/world/2015-06/25/c_1115727217.htm
7. *安天. 对相关媒体报道"中企曾被美国情报机构攻击"涉及我司的两点声明*. 2015. https://www.antiy.com/press/20150625.html
8. Eugene Kaspersky. *Why Hacking Kaspersky Lab Was A Silly Thing To Do*. 2015. https://www.forbes.com/sites/eugenekaspersky/2015/06/10/why-hacking-us-was-a-silly-thing-to-do/
9. 至顶网. *"棱镜"无死角美监视计划涵盖全球反病毒厂商*. 2015. http://security.zhiding.cn/security_zone/2015/0624/3055909.shtml
10. *安全牛. NSA 监控全球反病毒厂商 英美除外*. 2015. https://www.aqniu.com/vendor/8284.html

Chapter 10. Broken Window Effect - Iterative Analysis of Leaked Data from Shadow Brokers and WikiLeaks

Edward Snowden's exposure of PRISM revealed to the world the vast cyber intelligence system and capability of the United States for the first time. From 2016 to 2017, the Shadow Brokers and WikiLeaks further unveiled the cyber arsenals of the two major intelligence agencies of the United States, the NSA and the CIA. Through these events, the cybersecurity community has gained a general understanding of the United States' systemic capability and comprehensive layout in cyberspace, rather than the tactical level of understanding gained through specific incidents and sample codes as before. In the first two years, the cybersecurity community gradually understood the framework of the US cyberattack ability through systematic analysis of the leaked files, and marveled at its comprehensive scale and extensive coverage. Since then, the cybersecurity community has continuously discovered and re-understood the US attack weapons and systems in real cyberattacks, and the understanding of the US cyberattack system has become increasingly comprehensive.

Event Review

From August 2016 to April 2017, the Shadow Brokers successively exposed the NSA's cyber weapons and equipment, including attack equipment against cybersecurity devices, the attacking list of global servers, hacking information of SWIFT, the FuzzBunch (FB) vulnerability attack platform, and the DanderSpritz (DSZ) remote control platform, claiming that the attack equipment was related to Equation Group. According to relevant analysis and data, these attack equipment was developed by the United States several years ago, including a large number of system-level zero-day vulnerability exploitation tools and advanced backdoor programs, which revealed the vulnerability reserve capability and attack technology level of the United States.

On March 7, 2017, WikiLeaks exposed 8,761 secret files alleged to be related to cyberattack campaigns of the CIA, including 7,818 web pages and 943 attachments. The leaked files contain the document information of a huge attack equipment library, which covers a wide range of platforms, including not only Windows, Linux, iOS, Android and other common operating systems, but also smart TVs, vehicle smart systems, routers and other network node units and smart devices.

The Process of Study, Analysis, and Publication

From 2016 to 2018, global cybersecurity academia and industry communities were shocked and began to sort out and analyze the leaked data. According to the materials exposed by the Shadow Brokers, they sorted out three core modules in NSA cyber operation system represented by FB, Operation Center (OC) and DSZ. The Vault 7 exposed by WikiLeaks contains 15 tools (toolsets) and five frameworks for CIA cyber operations, which have also been comprehensively sorted out.

In April 2017, Cysinfo analyzed the files leaked by the Shadow Brokers. FuzzBunch (FB) is a modular exploit framework (See Fig. 10-1)[1], whose core functionalities are done by various plugins which are divided into five categories. Of particular concern is 17 zero-day exploits under its "Special" and "Exploit" categories, most of them are related to SMB zero-day vulnerabilities in Windows operating system. A patch from Microsoft released in March 2017 had fixed these vulnerabilities. In addition, there are also exploits for IBM Lotus Domino platform, Microsoft IIS, IMAP, RDP, etc.

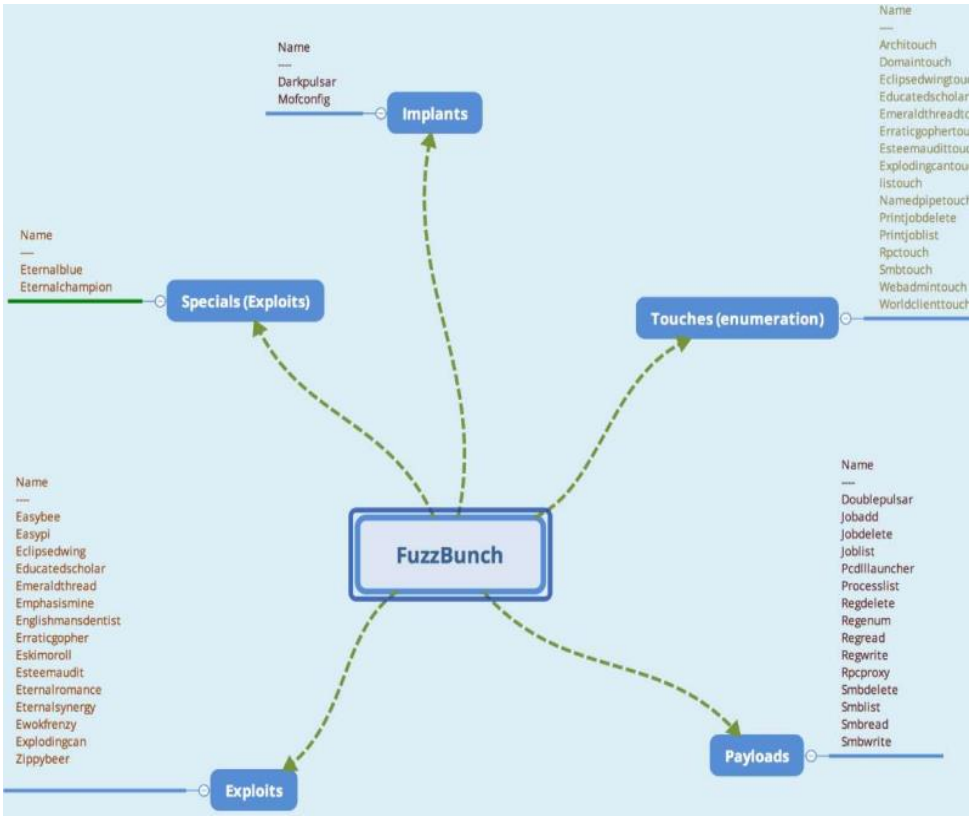


Fig. 10-1 FuzzBunch Components

Cysinfo said that Operation Center (OC) is a fully weaponized all-in-one post-exploitation tool framework (See Fig. 10-2)[1], which is used to control the compromised

machine. Operation Center is capable of deploying various types of remote monitoring tools, manipulating and redirecting network packet, collecting user sensitive information, and disabling security products. PeddleCheap, the core plugin of OC, provides flexible user interface for attackers and loads attack payloads such as DSZ.

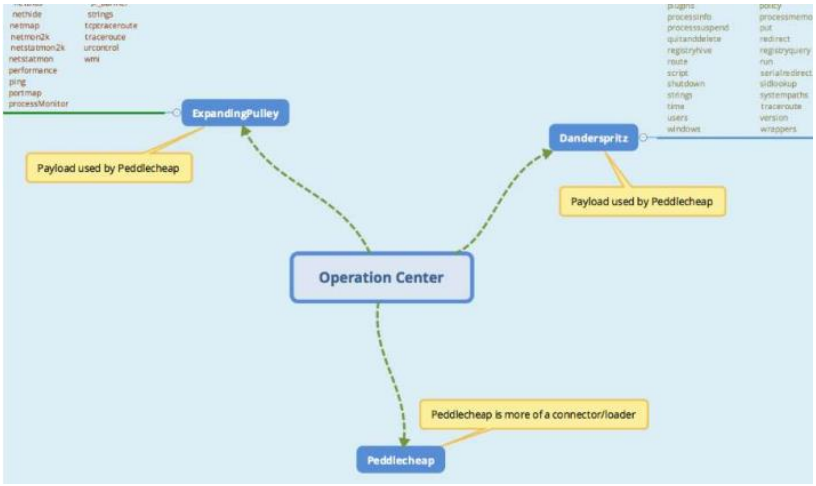


Fig. 10-2 Operation Center Components

The complexity of OC suggests the effort of many years and significant investment of resources. Comments in the code indicate that OC's development dates back to around 2006. Clocksvc.exe is one of the payloads of OC, whose returned IP address belong to Stony Brook Branch of the State University of New York (See Fig. 10-3)[1], a top university in North America, which proved that its development was supported by academic resources.

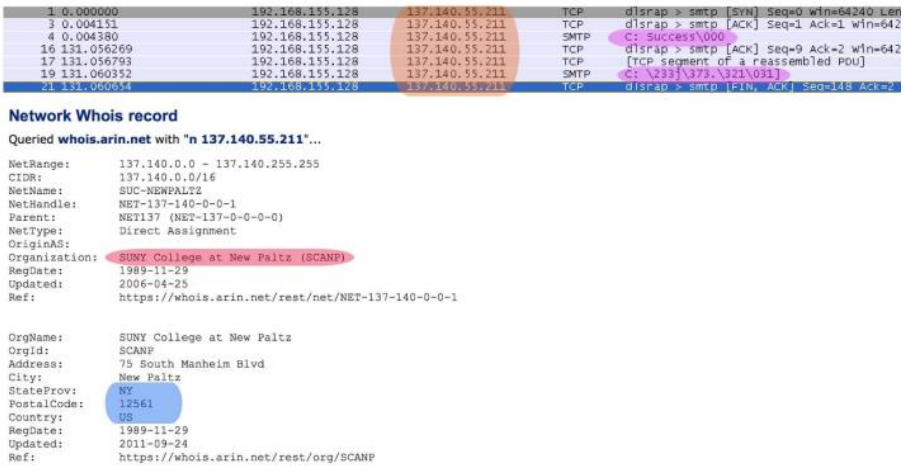


Fig. 10-3 IP Analysis of Clocksvc.exe

More surprisingly, according to Trend Micro's analysis[2], clocksvc.exe (called Tildeb by Trend Micro) is a memory implant that attacks Windows NT 4.0 and Microsoft Exchange Server (See Fig. 10-4)[2], dating back to even earlier than 2006. Its compilation timestamp is October 3, 2000!

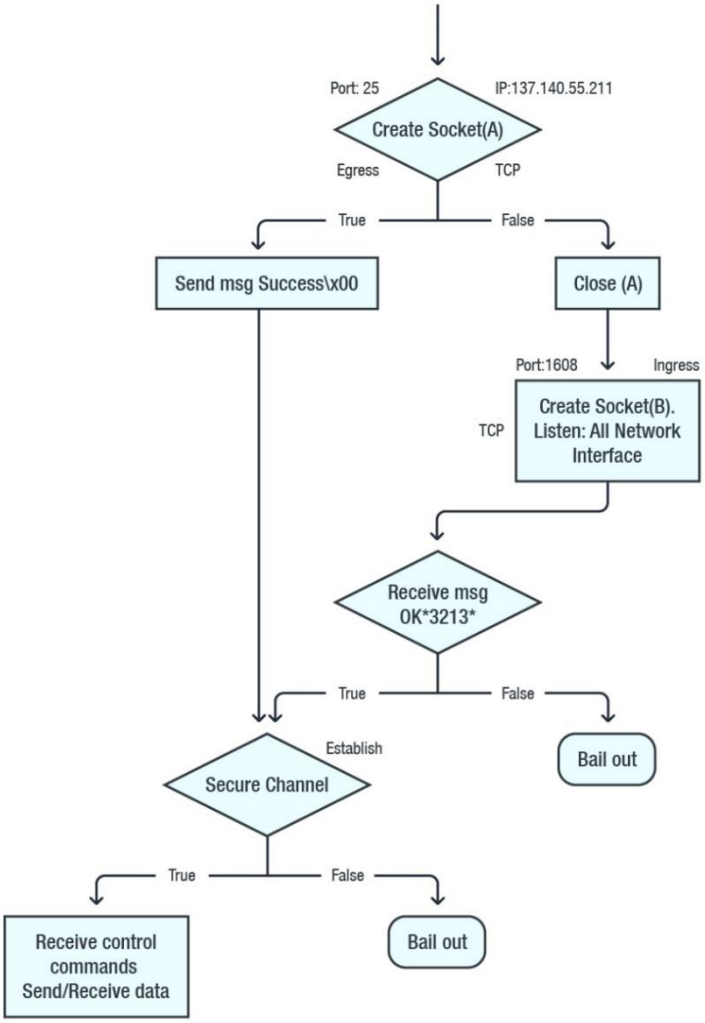


Fig. 10-4 How Tildeb Establishes a Successful Connection

From 2017 to 2018, Antiy conducted in-depth and systematic analysis of the attack equipment and documents leaked by Snowden, the Shadow Brokers and Wikileaks. Since December 2017, Antiy has published a series of reports titled *美国网络空间攻击与主动防御能力解析 (Analysis of US Cyberattack and Active Defense Capability)* for 12 issues in the journal *网信军民融合(Civil-Military Integration on Cyberspace)*[3]. These reports systematically sort out the US cyber offensive and defensive ability from

the perspectives of intelligence cycle, offensive ability support, attack equipment and active defense, and clearly show the US cybersecurity capability system.

In these reports, Antiy points out that the United States has built a formalized, all-platform, full-capability cyberattack equipment system. Attack targets cover various types of IT equipment such as personal hosts, servers, network devices, security devices and mobile smart devices, as well as Windows, Linux, MacOS, Android and other operating systems. Its functions cover reconnaissance, physical isolation breakthrough, intranet lateral movement, persistent residence, supply chain and logistics chain penetration, remote control and other parts.

In October 2018, Kaspersky conducted an in-depth analysis of DarkPulsar in the post-exploitation framework DSZ[4]. DSZ consists of multiple plugins, which can be loaded by PeddleCheap in OC. It is used to control compromised machines, gather intelligence, exploit vulnerabilities and examine already controlled machines. By analyzing the administrative module and several constants that are used to encrypt the traffic between the C&C and the implant, Kaspersky found the mysterious DarkPulsar backdoor, including both 32-bit and 64-bit versions, infecting Windows 2003/2008 Server. Kaspersky traced about 50 victims in Russia, Iran and Egypt, involving fields like nuclear power, telecommunications, IT and aerospace. Advanced abilities for persistence and stealthiness of DarkPulsar (such as encapsulating its traffic into legitimate protocols and bypassing password protection to pass authentication) shows that its developers are highly professional. The developers of DarkPulsar have not skimped on resources when developing persistence mechanisms, including disabling the NTLM protocol security function to bypass the requirement of entering a valid username and password during authentication, indicating that DarkPulsar is aimed at targets with long-term monitoring and controlling value.

In 2021, Israeli security vendor Checkpoint released a report that thoroughly analyzed the DoubleFeature component in DSZ[5]. DSZ is very modular and contains a wide variety of tools for persistence, reconnaissance, lateral movement, bypassing anti-virus engines, and other such shady activities. DoubleFeature can effectively function as a diagnostic tool for the victim machine, because it can evaluate which tools in DSZ can be deployed on the victim machine. For deployed tools, such as UnitedRake (UR), a remote access tool for Windows, DoubleFeature enables monitoring and logging. UR is the tool that Kaspersky dubbed EquationDrug in their original report, which also shows that DSZ (as well as FB and OC) is a large toolset of Equation Group.

In March 2022, China's 360 0Kee Team released a report on APT-C-40[6], an attack group originating from the NSA. According to the report, the analysis of the collected data shows that the group started to attack a series of industry leading companies in China as early as 2010, involving a number of key network management servers and terminals. The attack activities are connected with the implementation time of a certain NSA cyberwar plan. The report pointed out that the US cyberattacks are indiscriminate attacks, which can hijack the normal web browsing traffic of any Internet user in any region of the world. Governments, the financial industry, scientific research institutes, telecom operators, and education, military, aerospace, medical and other industries, as well as important sensitive units and groups in China were targeted.

In April 2017, Symantec analyzed the Vault 7 data leaked by WikiLeaks and found that the espionage tools and equipment described in it could link a threat group called Longhorn to at least 40 recent cyberattacks in 16 countries in Europe, Asia and Africa, because "the tools used by Longhorn closely follow development timelines and technical specifications laid out in documents disclosed by WikiLeaks."[7] According to the analysis, Longhorn has been active since at least 2011. It is a highly complex and sophisticated organization that uses a large amount of zero-day vulnerabilities and sophisticated malware to carry out targeted attacks against key industries, including finance, energy, telecommunications, education and aerospace.

In 2020, China's 360 0Kee Team revealed the 11-year-long network penetration attacks by the US CIA attack group (APT-C-39) on key areas in China, including the aerospace industry, scientific research institutions, oil industry, large Internet companies and government agencies[8]. According to 360 reports, through the study of the Vault 7 network weapon information leaked by WikiLeaks, a series of long-term targeted attacks on China's key areas were discovered. These attacks can be traced back as early as September 2008, and continued until around June 2019, mainly targeting Beijing, as well as Guangdong, Zhejiang and other provinces. The 360 0Kee Team made an in-depth analysis of five relevant evidences, for example, the APT-C-39 group has repeatedly used Fluxwire, Grasshopper and other exclusive CIA cyber weapons to carry out cyberattacks on Chinese targets, and reliably proved that the APT-C-39 group belongs to the CIA. The analysis of APT-C-39 activity shows that the CIA's Vault 7 cyber arsenal poses a serious threat to global cybersecurity.

In March 2022, China's National Computer Virus Emergency Response Center (CVERC) officially released an analysis report on the NOPEN Trojan used by the NSA[9].

Once the Trojan is implanted into the victim's computer, it will become a lurker, opening the vault door to the attacker at any time, and all kinds of confidential data and sensitive information can be exposed. Evidence shows that the Trojan has controlled a large amount of Internet devices and stolen a large scale of user privacy data.

Summary

The Shadow Brokers documents revealed more than 287 targets in 45 countries, including Russia, Japan, Spain, Germany, Italy, etc., over a period of more than a decade. NOPEN, which was leaked by the Shadow Brokers, was one of 41 cyberweapons used by the NSA in the recently revealed attack on China's Northwestern Polytechnical University[10]. Seven years later, the huge cyber arsenal iceberg of the NSA and the CIA still needs to be discovered and recognized by the security field.

References

1. InfoSec Institute. *NSA BIOS Backdoor a.k.a. God Mode Malware Part 1: DEITYBOUNCE.* 2014. https://cysinfo.com/wp-content/uploads/2017/04/Shadow_release_updated.pdf
2. Trend Micro. *Tildeb: Analyzing the 18-year-old Implant from the Shadow Brokers' Leak.*2017. https://documents.trendmicro.com/assets/tech-brief-tildeb-analyzing-the-18-year-old-implant-from-the-shadow-brokers-leak.pdf
3. *安天.“美国网络空间攻击与主动防御能力解析”系列文章 12 篇. 网信军民融合.* 2017(12)-2018(11). https://mp.weixin.qq.com/s/PnaYXZ9snK6fv_lgCFszDw
4. Kaspersky. DarkPulsar. 2018. https://securelist.com/darkpulsar/88199/
5. Check Point. *A Deep Dive into DoubleFeature, Equation Group's Post-Exploitation Dashboard*. 2021. https://research.checkpoint.com/2021/a-deep-dive-into-doublefeature-equation-groups-post-exploitation-dashboard/
6. 360. *网络战序幕：美国国安局 NSA（APT-C-40）对全球发起长达十余年无差别攻击.* 2022. https://mp.weixin.qq.com/s/jHjzky8xIaEuocHzbWjFSA
7. Symantec. *Longhorn Tools Used Cyberespionage Group Linked Vault 7.* 2017. https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7

8. 360. *披露美国中央情报局 CIA 攻击组织（APT-C-39）对中国关键领域长达十一年的网络渗透攻击*. 2020.
https://mp.weixin.qq.com/s/IfnVrmcUInr0OBF7I1m4Wg
9. CVERC. *"NOPEN"远控木马分析报告*. 2022.
https://www.cverc.org.cn/head/zhaiyao/news20220314-nopen.htm
10. 安天. 从 NOPEN 远控木马浮出水面看美国网络攻击装备体系. 2022.
https://mp.weixin.qq.com/s/J2L-Czapzi3Vj5dzOpGzjA

Chapter 11. The First Complete Traceability - The Complete Process of the Equation Group Attacking Middle East Technical Facilities

Before 2017, although the global cybersecurity had some analysis of the US, it remained at the level of sample analysis, except for the analysis of the mechanism and process of the Stuxnet incident due to the active exposure of the US. The Shadow Brokers' revelations in 2017 provided the cybersecurity with the possibility of linking the results of the analysis. Antiy and other vendors combined all kinds of information clues exposed with the long-term accumulation of research results, and were able to initially restore the process of a cyberattack by Equation Group of the United States.

Event Review

On April 14, 2017, the relevant data of the US cyberattack disclosed by the Shadow Brokers contained a folder named SWIFT, which fully exposed two cyberattack actions "JEEPFILEA_MARKET" and "JEEPFILEA_POWDER" of Equation Group against SWIFT financial service providers and partners[1,2]. JEEPFLEA_MARKET was an attack launched against EastNets, the largest SWIFT service provider in the Middle East, from July 2012 to September 2013. The action successfully stole thousands of employee accounts, host information, login credentials, and administrator accounts from EastNets in Belgium, Jordan, Egypt, and the United Arab Emirates. The JEEPFLEA_POWDER attack which targeted BCG (Business Computer Group), a partner of EastNets in Latin America and the Caribbean, was unsuccessful.

The Process of Study, Analysis, and Publication

In June 2019, Antiy released a review analysis report titled *方程式组织攻击 SWIFT 服务提供商 EastNets 事件复盘分析报告* (*Analysis Report on the Event of the Attack on the SWIFT Service Provider EastNets by the Equation Group*)[3,4]. In this report, based on the correlation analysis between the leaked information of the Shadow Brokers and historical capture analysis results, Antiy completely reviewed Equation Group's attack on EastNets, the largest SWIFT financial service provider in the Middle East, and restored its attack mid-point, operation path, equipment application, tactical process, scene environment and operation consequences. The report analyzed the targeted assets in detail, such as network equipment and cybersecurity equipment information,

management server information, application server information and SWIFT business server information, drew the network topology diagram (See Fig. 11-1)[3], and sorted out the brand and model information of each asset, security vulnerability information and the name of the corresponding attack weapons used by the attackers.

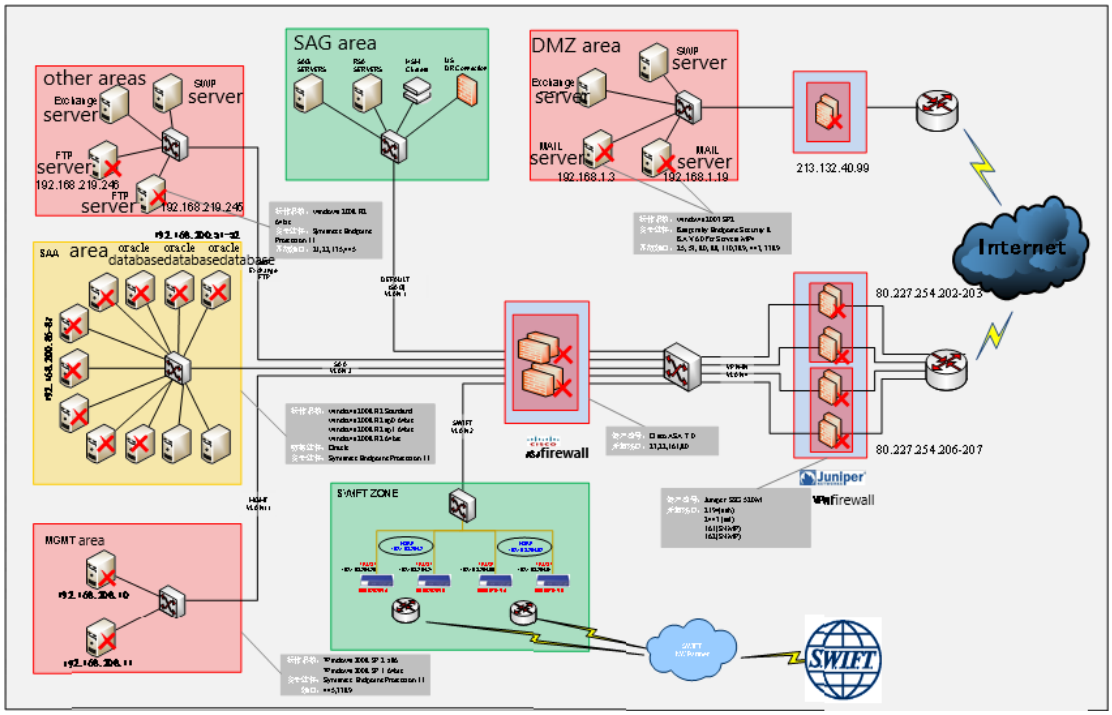


Fig. 11-1 Topology Diagram of the Attacked Asset Profile

The report summarized the information of the attack equipment used by the US in this operation, and classified them as vulnerability exploitation tools and platforms, persistent implanted weapons, and control backdoors according to the functional purposes. It also described weapon functions, applicable scenarios and associated vulnerabilities (See Fig. 11-2)[3], pointing out that the US had the attack capability covering the whole platform and the whole system and held a large number of zero-day vulnerability reserves.

Attack Equipment	Vulnerability Number	Targeted Devices and Functions
Unknown device A	CVE-2015-7755	Unknown device A is a vulnerability attack device for Juniper ScreenOS (the operating system used by Juniper SSG and NetScreen firewall products). When logging in to Juniper firewall through SSH and Telnet, there is an identity authentication bypass vulnerability.
EPICBANANA	CVE-2016-6367	EPICBANANA is a vulnerability attack device for the command-line interface (CLI) parser in Cisco ASA and PIX devices;
EXTRABACON	CVE-2016-6366	EXTRABACON exploits the SNMP service (port 161, 162) for Cisco ASA devices;
ENTERNALCHAMPION	CVE-2017-0146	ENTERNALCHAMPION (Eternal Champion) is a series of "eternal" vulnerability attack device for Windows Server 2008 SP1 x86, etc., using Windows SMBv1 remote code execution vulnerability;
ETERNALSYNERGY	CVE-2017-0146	ETERNALSYNERGY (Eternal Collaboration) is a series of "eternal" vulnerability attack device for Windows 8, etc., using Windows' SMBv1 remote code execution vulnerability;
ETERNALBLUE	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148	ETERNALBLUE (Eternal Blue) is a series of "eternal" vulnerability attack device for Windows 7/8/XP, etc., using Windows' SMBv1 remote code execution vulnerability;
ETERNALROMANCE	CVE-2017-0143	ETERNALROMANCE (Eternal Romance) is a series of "eternal" vulnerability attack device for Windows XP, Vista 7, Windows Server 2003/2008/2008 R2, etc., using the SMBv1 remote code execution vulnerability of all Windows platforms;
EXPLODINGCAN	CVE-2017-7269	EXPLODINGCAN (Exploding Tank) is an attack device that exploits the IIS6.0 webDAV vulnerability;

Fig. 11-2 List of Vulnerability Exploitation Tools Used to Attack EastNets

The report also estimated the attack path (See Fig. 11-3)[3]: the attacker launched the attack from four mid-points of the Internet, successively penetrated two layers of firewalls (VPN firewall, ASA firewall), and prefabricated Rootkit in the firewall. After that, the attackers got into the intranet system through multiple zero-day vulnerabilities and obtained the control of multiple business servers. Finally, through relevant SQL statements, the attackers obtained account names, passwords, transaction track and other relevant information that interested them from the Oracle server.

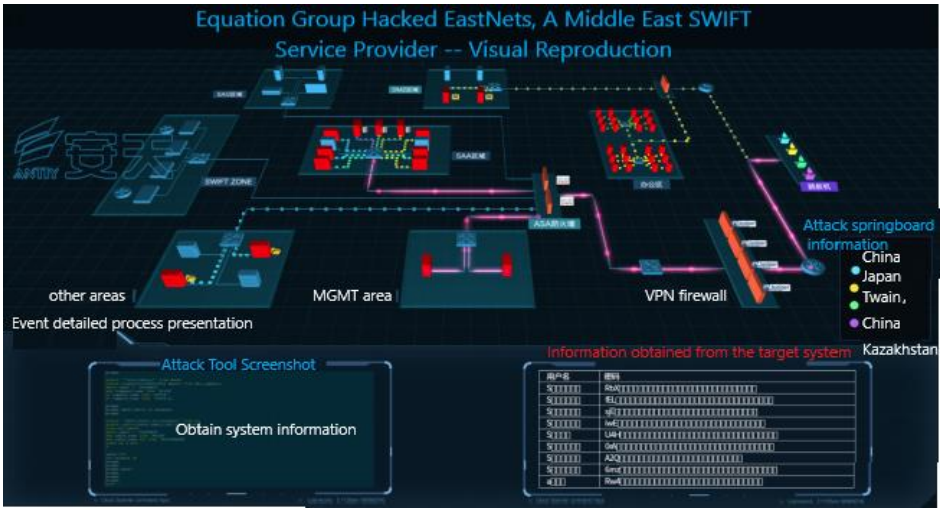


Fig. 11-3 Equation Group's Intrusion into EastNets

In this report, Antiy referred to NOPEN Trojan, a standardized cyberattack device of the NSA. In the 2022 cyberattack on China's Northwestern Polytechnical University, the NSA used the Trojan to take control of the university's border server.

Summary

Faced with the oppression of the far beyond reach super network operation ability of the US, security vendors have initially achieved a complete review of US Equation Group attack event through years of persistent tracking and accumulation, combined with the documents leaked by the Shadow Brokers. In the confrontation with the US, the global cybersecurity vendors are also growing.

The revelation of the Shadow Brokers brought to light a batch of American attack equipment. On the one hand, the leak of these exploit tools and malware payloads can be widely exploited by other low-level cyber threat actors, resulting in WannaCry worm outbreak and other cybersecurity incidents. On the other hand, security researchers can use the information to analyze the overall picture of attack activities of top APT groups from the perspective of a complete threat framework.

References

1. Bleeping Computer. *Shadow Brokers Release New Files Revealing Windows Exploits, SWIFT Attacks.* 2017. https://www.bleepingcomputer.com/news/security/shadow-brokers-release-new-files-revealing-windows-exploits-swift-attacks/
2. The Times of Israel. *Hacked files suggest NSA penetrated SWIFT, Mideast banks.* 2017. https://www.timesofisrael.com/hacked-files-suggest-nsa-penetrated-swift-mideast-banks/
3. *安天. 方程式组织攻击 SWIFT 服务提供商 EastNets 事件复盘分析报告*. 2019. https://www.antiy.com/response/20190601.html
4. *新华社. 对美国网络攻击目标泛化的隐忧.*2019. https://baijiahao.baidu.com/s?id=1636198876284800319&wfr=spider&for=pc

Chapter 12. The US Manipulation of Cyberspace Security Revealed by International Forums

Since the Stuxnet incident was discovered in 2010, the cybersecurity community has increasingly recognized the reckless manipulation and destruction of cybersecurity by the US, and has exposed network behaviors, intentions and activities of the US through international conferences, forums and other communication activities. However, as a country with advantages in cybersecurity technology, the US has not assumed its due responsibilities as a major partner, but has taken advantage of its voice in cyberspace to disrupt and suppress normal international exchanges and obstruct the dissemination and sharing of information by withdrawing reports abruptly.

Sudden Withdrawal of Reports

In 2014, the Black Hat conference withdrew the report *You Don't Have to Be the NSA to Break Tor: Deanonymizing Users on a Budget* by cybersecurity researcher Alexander Volynkin from Carnegie Mellon University. This unusual withdrawal (See Fig. 12-1) led to widespread discussion and suspicion immediately, suggesting that the report was withdrawn under US government pressure[1].

Fig. 12-1 Comments of Black Hat USA 2014 on Withdrawing Report

Despite the US government's various tactics to interfere with cooperation and communication in the cybersecurity field, global cybersecurity enterprises and academia with a spirit of cooperation and sharing remain committed to sharing and openness to promote the development of security in global cyberspace.

Global Security Vendors' Efforts at International Conferences and Forums

In 2012, Carey Nachenberg, vice president and chief architect of Symantec, gave a presentation at the CSIAC Science Forum at Stanford University titled *How a Computer Virus Foiled Iran's Nuclear Program*, revealing Stuxnet's amazing spread, defense evasion and other technical means and its powerful destructive power. In the analysis of transmission mechanisms, he pointed out that seven different software vulnerabilities (backdoors) were used to enable Stuxnet virus to spread across the network, six of which were previously unknown (See Fig. 12-2)[2].

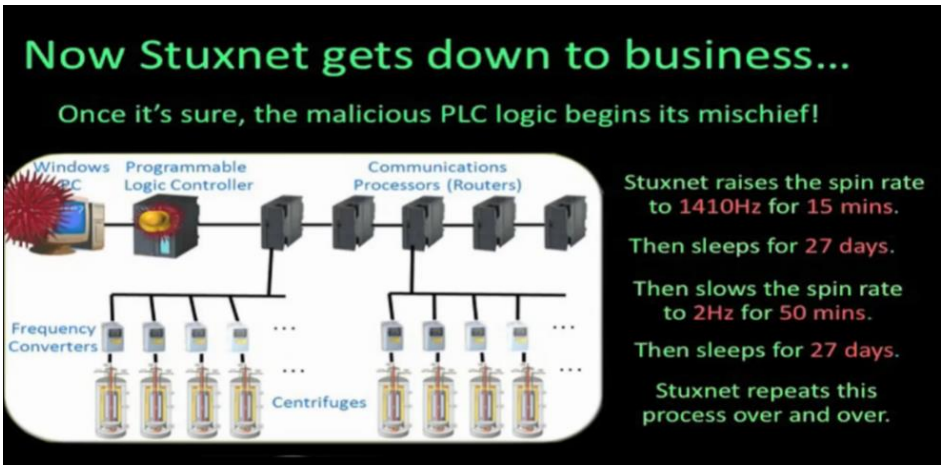


Fig. 12-2 Carey Nachenberg's Analysis of Stuxnet's Destruction Process

On December 27, 2013, Jacob Appelbaum, former core programmer of the Tor Program, presented a set of leaked PPT documents at the 30th Chaos Communications Congress (30C3), which contained exploitable vulnerabilities of servers, routers, firewalls, mobile devices, as well as the corresponding exploits and Trojans (See Fig. 12-3)[3]. The products involved include DELL servers, HP servers, Juniper Netscreen and SSG firewalls, Huawei Eudemon firewalls, Huawei routers, CISCO firewalls, iPhones and Windows Mobile. It also included some general Trojans and specialized hardware, including hard drive firmware Trojans executed through BOOTKIT, BIOSKIT, USB injection and wireless bridge devices, wireless software implantation tools for Windows XP, pseudo-GSM base stations, SIM card SMS implantation tools for iPhones, and for Windows Mobile implant tools, spy phones to collect information, etc.

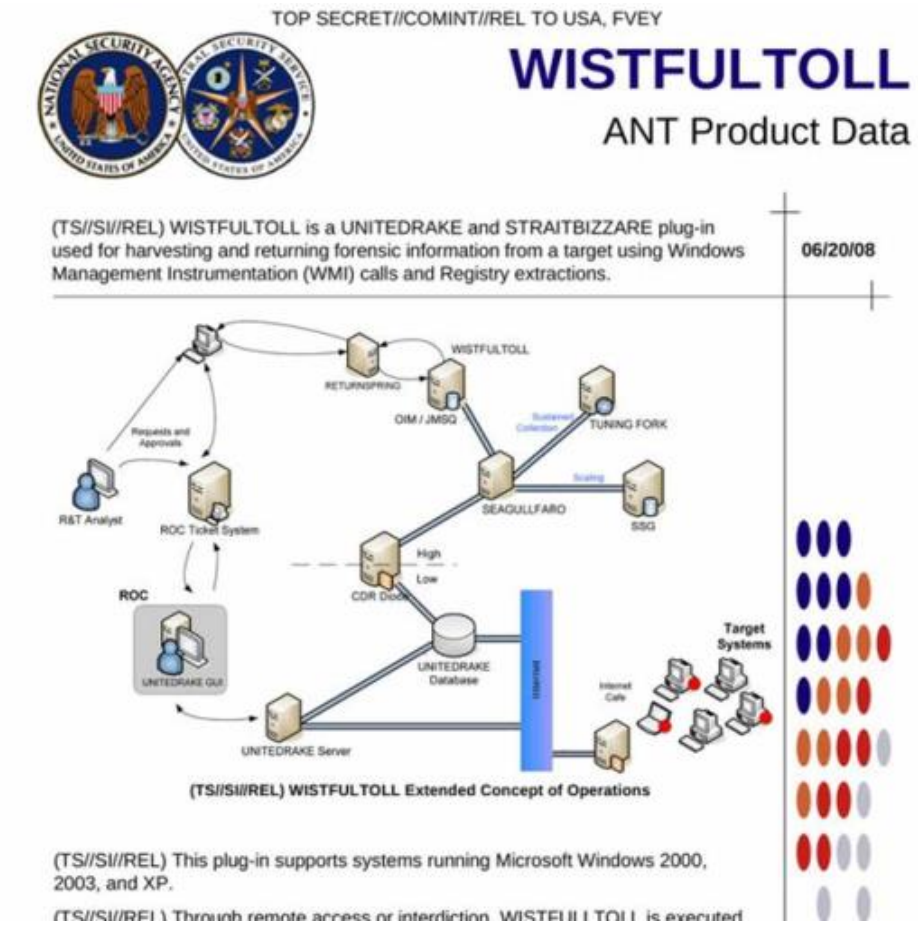


Fig. 12-3 NSA Network Tool WISTFULTOLL Exposed by Appelbaum

In 2014, the US media website *The Intercept* revealed a number of documents leaked by Snowden about covert online operations shared by the Government Communications Headquarters (GCHQ), the NSA, and other agencies from Five Eyes (FVEY) countries, which showed how these agencies manipulate and distort online contents to undermine the integrity of the Internet. Researcher Brian Bartholomew and other researchers from Kaspersky presented a report titled *Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks* at the 2016 Virus Bulletin Conference (VB 2016), further analyzing the multiple deception tactics used in US cyber operations[4].

In 2015, the German magazine *Der Spiegel* (The Mirror) revealed the NSA's "The Fourth Party" intelligence-gathering techniques and programs in cyberspace leaked by Snowden, which were used to obtain intelligence or conduct cyberattacks more covertly by hacking into (and exploiting) third-party cyber infrastructure. Based on this intelligence and their in-depth analysis of several cybersecurity incidents, Juan Andres Guerrero-Sannde and other researchers from Kaspersky released a report titled *Walking*

in Your Enemy's Shadow: When Fourth-Party Collection Becomes Attribution Hell at the 2017 Virus Bulletin Conference (VB 2017)[5], analyzing the stealthy and highly sophisticated nature of this attack technique. For example, an unknown APT group (named ScarCruft by Kaspersky) used websites compromised by DarkHotel, a known APT group, to conduct targeted attacks against companies and individuals in Russia, China, and Korean-speaking countries using tactics, techniques, and procedures similar to DarkHotel (See Fig. 12-4)[5]. The report pointed out that such actions, which only well-resourced intelligence agencies conduct, not only exceed the threat intelligence capabilities of traditional cybersecurity vendors, but also destroy the ecology of threat intelligence.

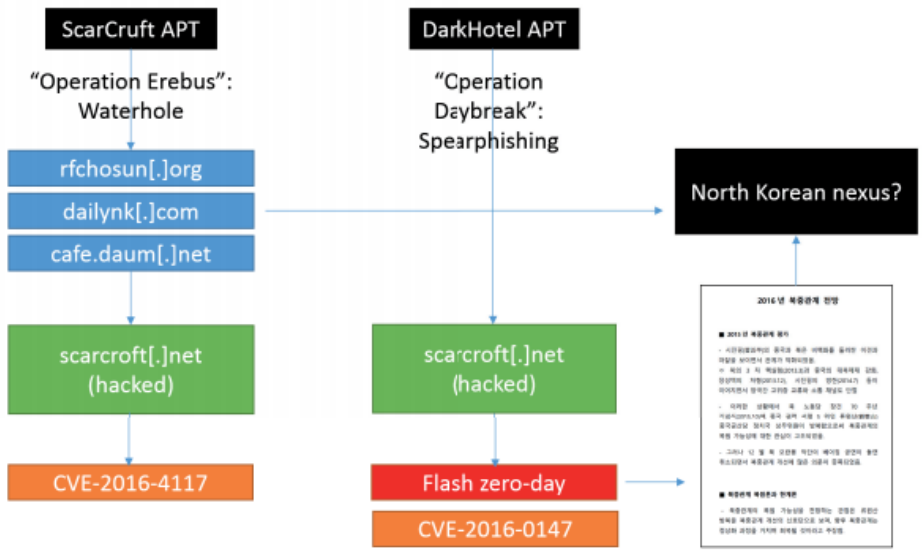


Fig. 12-4 Diagrammatic Representation of the APT ScarCruft Attacks

In 2016, Jason Healey, a senior researcher from the School of International and Public Affairs at Columbia University, published an article titled *The US Government and Zero-day Vulnerabilities* in the Journal of International Affairs, providing an in-depth analysis of the evolution of the US Vulnerability Equities Process (VEP) from 2008 to 2016. It also provided a cautious estimate of the current (2016) number of zero-day vulnerability munitions the United States was likely to possess (See Fig. 12-5)[6].

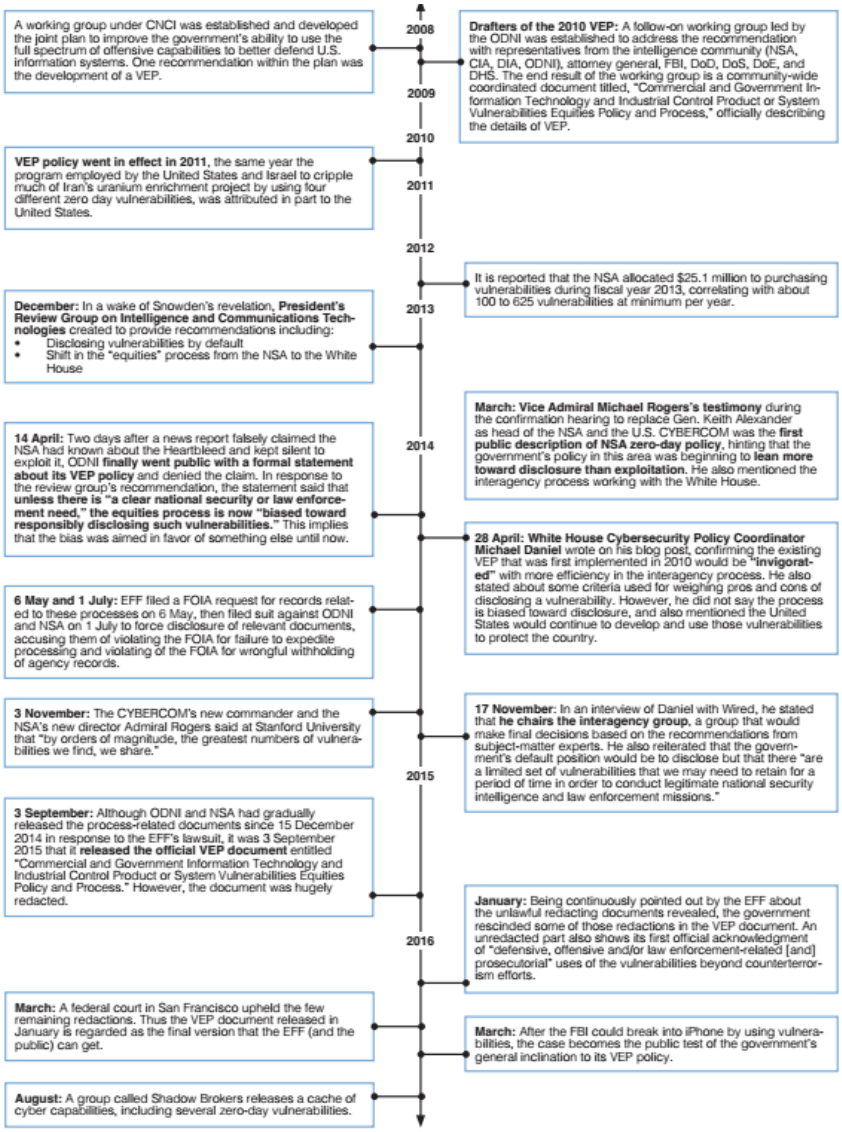


Fig. 12-5 Timeline of VEP Policy

Chinese cybersecurity experts and security vendors have been active in exploring the disruption of the cybersecurity order by national-level cyber threats.

On June 11, 2013, professor Shen Yi from the School of International Relations and Public Affairs of Fudan University in China delivered a report titled *从三叶草到棱镜门——监控与美国网络安全战* (*From Clover to PRISM: Surveillance and the US Cybersecurity Strategy*) at the seminar *新时代网络威胁之路研讨会* (*The Path of Cyber Threats in the New Era*)[7], which made a historical review of the US national surveillance behavior. Through the systematic analysis of Clover Operation (1945-1975), a representative case of intelligence surveillance since the 1940s, to the PRISM program in the early 21st century, this paper summarizes the complex factors behind American surveillance and its impact and harm on global cybersecurity.

In June 2015, the China Anti-Virus Conference was held in Tianjin, Antiy released the report *A^2PT 与"准 APT"事件中的攻击武器* (*A^2PT and Attack Weapons in the Quasi-APT Event*), which for the first time referred to the cyberattack as the A^2PT attack (i.e. Advanced APT Attack) (See Fig. 12-6)[8].

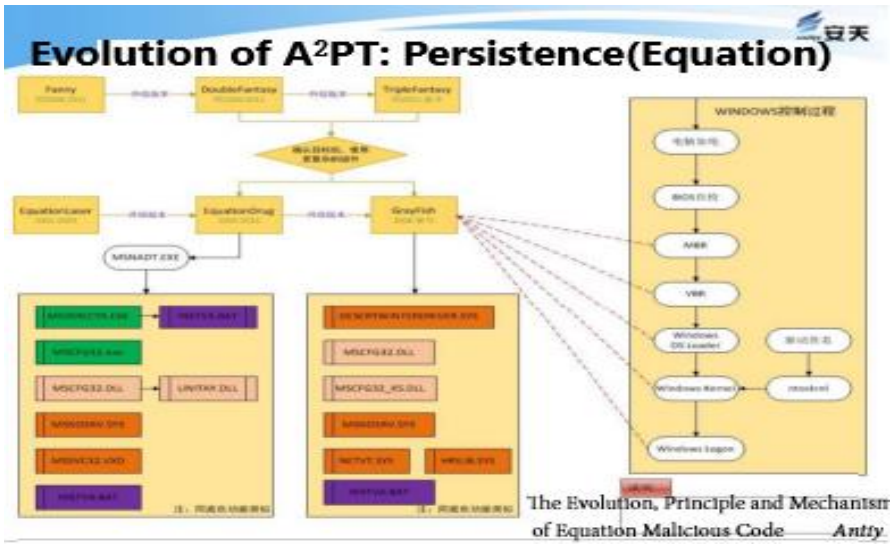


Fig. 12-6 The Report of the China Anti-Virus Conference Reveals the Principle and Structure of Equation Group

In 2016, Antiy gave a presentation at the China and Russia Cyberspace Development and Security Forum titled *The Panda's Scar*, particularly analyzing several APT attacks against China. In particular, it revealed the attacks by the US Equation Group on critical Chinese basic industrial enterprises and summarized their characteristics and capabilities (See Fig. 12-7)[9].

Fig. 12-7 Technical Report "The Panda's Scars" in 2016 China and Russia Cyberspace Development and Security Forum

In 2019, Orange Tsai and Meh Chang, researchers at Taiwan security company DevCore in China, presented *Infiltrating Corporate Intranet Like NSA* at Black Hat, demonstrating how to use techniques of the NSA (such as Equation Group) that have been exposed, pre-auth RCE exploits Fortinet and Pulse Secure SSL VPNs to break into the intranets with (relative) ease (See Fig. 12-8)[10].

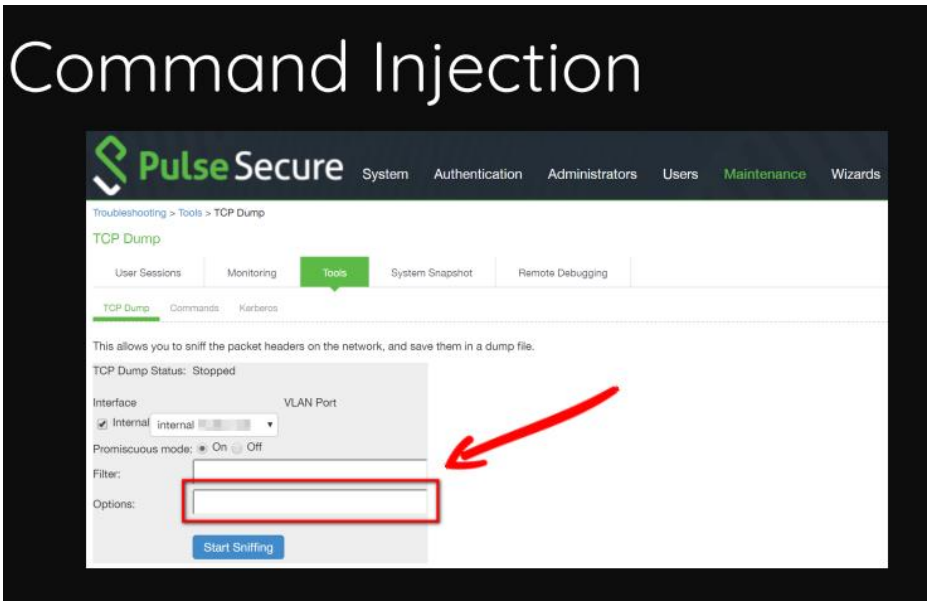


Fig. 12-8 Command Injection After Exploiting the Pulse Secure Vulnerability Shown by Tsai

The report pointed out that SSL VPN is widely used by companies of all sizes to connect the intranets to the public network, and the VPN vendors in the market are relatively concentrated. Therefore, the NSA has long been devoting to discover and exploit vulnerabilities.

Summary

Global cybersecurity challenges are becoming increasingly serious. Only by upholding the spirit of openness and cooperation can all countries build and share a secure cyberspace. International forums are important space for business and academic exchanges.

Over the past decade, through the unremitting efforts of a wide range of security vendors and academics in various international forums, American ambitions and behaviors to manipulate and interfere in cybersecurity by technological advantages have been increasingly exposed and recognized, and encouraged more vendors and academics to do follow-up research.

References

1. BlackHat. A Schedule Update. 2014. https://www.blackhat.com/latestintel/07212014-a-schedule-update.html
2. Symantec. *How a Computer Virus Foiled Iran's Nuclear Program.* 2012. https://cisac.fsi.stanford.edu/multimedia/forensic-dissection-Stuxnet
3. ZDNET. *Top NSA hacks of our computers.* 2014. https://www.zdnet.com/pictures/top-nsa-hacks-of-our-computers/
4. Kaspersky. *Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks.* 2016. https://www.virusbulletin.com/virusbulletin/2016/11/vb2016-paper-wave-your-false-flags-deception-tactics-muddying-attribution-targeted-attacks
5. Kaspersky. *Walking in Your Enemy's Shadow: When Fourth-Party Collection Becomes Attribution Hell.* 2017. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07170728/Guerrero-Saade-Raiu-VB2017.pdf
6. Columbia University. *The US Government and 0-day Vulnerabilities.* 2016. https://jia.sipa.columia.edu/sites/default/files/attachments/Healey%20VEP.pdf
7. 沈逸. *从三叶草到棱镜门——监控与美国网络安全战略.新时代网络威胁之路研讨会.* 2013.
8. 安天. *A²PT 与准 APT 事件中的攻击武器. 中国反病毒大会.* 2015
9. Antiy. *The Panda's Scar—The APT Attacks against China.* 2016. https://www.antiy.com/response/20200304.html
10. DevCore. *Infiltrating Corporate Intranet Like NSA.* 2019. https://i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-Like-NSA.pdf

Chapter 13. Restriction and Suppression - The US Generalized the Concept of Security to Sanction Other Countries' Cybersecurity Vendors

In recent years, in order to maintain its political hegemony, economic interests, and superior military technology and capabilities and at the same time suppress other countries' well-known cybersecurity vendors with technical competitiveness, the US has generalized the concept of national security and regarded it as a panacea to contain its opponents. The panacea is used whenever necessary, even at the expense of disrupting the international order and market rules, or of the interests of consumers around the world, including the US.

Banning Software Products from Kaspersky

Kaspersky, a well-known cybersecurity company, is the target of the United States' key all-round crackdown. It is not only the No.1 target of the NSA's Project CAMBERDADA, but also the cybersecurity vendor whose products are banned. On September 13, 2017, claiming that Kaspersky could threaten the security of US federal information systems, the US Department of Homeland Security requested all federal agencies to identify Kaspersky software products used in their information systems within 30 days and uninstall them within 90 days. Retailers such as Best Buy in the US have also taken Kaspersky products off their shelves. Under the Trump administration, the Department of Commerce was allowed to restrict American companies from trading with foreign adversary countries in the areas of Internet, telecommunications and technology. In the case of Kaspersky, the US Department of Commerce has the authority to prohibit US citizens from using or purchasing its software, or to prohibit users from downloading software updates through regulations in the Federal Register. In 2022, the US government further strengthened the national security review of Kaspersky's software products, claiming that its software products, as anti-virus software with access to computer systems, could steal sensitive information or even tamper with content from American computers.

Containing the Development of Chinese Enterprises with Entity List

With the rapid development of Internet technology in China, more Chinese companies are showing strong competitive power in the global market, posing a challenge to the long-standing network hegemony of the US. Since Obama took office, the US government has increasingly attached importance to cybersecurity increasingly seriously, and taken increasingly tough protectionist measures in the name of "national security" and "economic security". It is well known that the US Department of Commerce has repeatedly used the "open conspiracy" tactic of constantly including Chinese Internet technology companies with the strength of their own innovative technology in the Entity List of sanctions.

The Entity List of the US Department of Commerce is a blacklist that restricts the trade of adversaries in the US. The reason why the adversaries are included in the list is that the US believes that the technology and capabilities possessed by other parties have posed sufficient threat to US overseas interests and national interests. Since ZTE was sanctioned in 2018, maintaining "national security" has been the excuse for the US to add a number of Chinese technology companies to its Entity List. Among the Chinese companies and agencies added to the list on May 22, 2020, Qihoo 360 was the first cybersecurity company to be added in the list, with the reason of "there is a risk of purchasing related items for China's military end use."[1] On October 5, 2022, in accordance with Section 1260H of The National Defense Authorization Act for Fiscal Year 2021, the US Department of Defense released the second list of Chinese Military Companies (CMC) entity list operating in the US. Chinese cybersecurity companies Beijing Knownsec Information Technology Co. and Qihoo 360 were on the list[2]. There are no specific sanctions for companies on the CMC list, but according to the US Department of the Treasury, the CMC list is a "prohibited list", meaning that investments are prohibited or restricted.

Pressuring Foreign Cybersecurity Vendors Exposing US Attacks

In June 2015, Edwardsnowden.com revealed an internal document *An Easy Win: Using SIGINT to Learn about New Viruses*,[3] introducing the Project CAMBERDADA which has been implemented by the relevant intelligence agencies of the US and the UK since

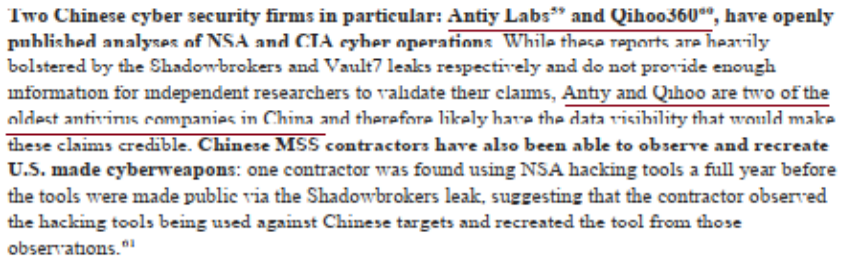
2007. The program mainly monitors the communication between famous anti-virus companies such as Kaspersky and their users, in order to obtain new virus samples and other information. The document also listed more targets (More Targets) that were planned to be monitored, covering 23 anti-virus vendors, including Chinese security vendor Antiy.

On December 22, 2016, NetScout, an American company mainly engaged in network monitoring and management, released an article to distort and smear China Cyberspace Security Association, arguing that since Chinese cybersecurity vendor Antiy, like Kaspersky, published an Equation Group APT related disclosure, Antiy is the spokesperson of "China's anti-APT" (See Fig. 13-1)[4].

Fig. 13-1 Analysis of US NetScout on Antiy and Other Chinese Companies

On February 17, 2022, the US-China Economic and Security Review Committee (USCC) of the US Congress held the second hearing of the 2022 Annual Report[5], with the theme of *China's Cyberspace Capability: Cyberwar, Espionage, and the Impact on the United States*. The report focused on the field of cybersecurity and assessed China's cyber capability and its impact on the security and interests of the United States. The cybersecurity experts attending the hearing believed that China has a mature large-scale defense capability that can detect the Western cyberspace operations. The hearing singled out two Chinese cybersecurity companies, Antiy and Qihoo 360, because they publicly released their analyses of the cyberspace operations of the NSA and the CIA. The US experts pointed out that Antiy and Qihoo 360 are the two of the oldest anti-virus companies in China, and the information they released can make the public more convinced (See Fig. 13-2)[5]. It can be seen that the US has a clear understanding of

China's capability-based cybersecurity vendors, and has always been focusing on and analyzing their potential threats to the US and the challenges the US may face. In the future, there may be more restrictive measures for similar enterprises.



Two Chinese cyber security firms in particular: Antiy Labs[59] and Qihoo360[60], have openly published analyses of NSA and CIA cyber operations. While these reports are heavily bolstered by the Shadowbrokers and Vault7 leaks respectively and do not provide enough information for independent researchers to validate their claims, Antiy and Qihoo are two of the oldest antivirus companies in China and therefore likely have the data visibility that would make these claims credible. **Chinese MSS contractors have also been able to observe and recreate U.S. made cyberweapons**: one contractor was found using NSA hacking tools a full year before the tools were made public via the Shadowbrokers leak, suggesting that the contractor observed the hacking tools being used against Chinese targets and recreated the tool from those observations.[61]

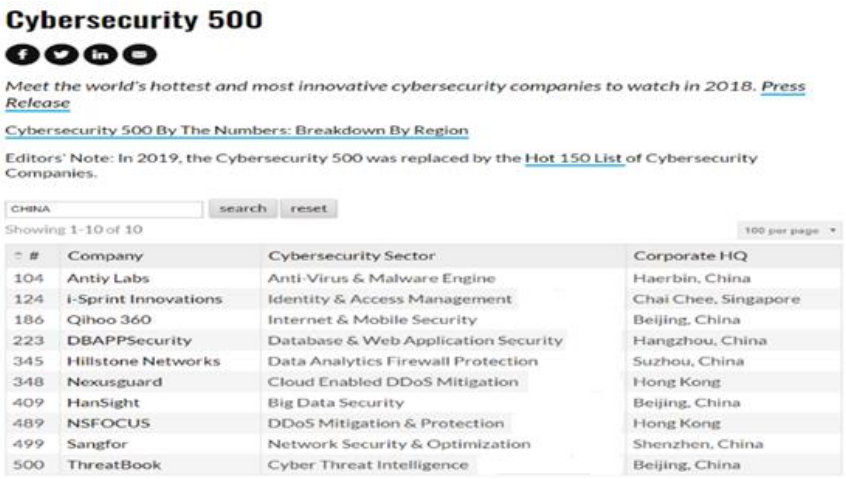
Fig. 13-2 The Hearing of the US Congress Focused on Antiy and Qihoo 360

Special Treatment and Suppression on Chinese Cybersecurity Vendors

With the technological development of Chinese Internet technology enterprises, the international popularity and influence of some Chinese cybersecurity enterprises are gradually developing. Cybersecurity Ventures is a world-renowned investment consulting agency, mainly engaged in cybersecurity market research and information collection, focusing on startups and emerging companies in the cybersecurity industry. Cybersecurity Ventures' ranking of the Top 500 Cybersecurity Innovative Companies is an independent assessment of thousands of cybersecurity vendors around the world, all of which it claims are "the hottest and most innovative"[6]. Before 2019, in the list of the Top 500 Cybersecurity Companies released by Cybersecurity Ventures, Chinese cybersecurity vendors, such as Antiy, Hillstone Networks, DBAppSecurity and Qihoo 360, had all been listed (See Fig. 13-3[6] and 13-4[7]). There were nearly 300 American enterprises on the list, while there were no more than 10 Chinese enterprises, which can't truly reflect the capabilities of China's cybersecurity industry.

vendor	specialty
95. Antiy Labs	anti-virus engine & solution
142. Hillstone Networks	data analytics firewall protection
314. DBAppSecurity	web application & database security
412. Vkansee	fingerprint sensors for mobile security

Fig. 13-3 Chinese Vendors Listed in the 2015 Top 500 Cybersecurity Companies of Cybersecurity Ventures (Partial)



Cybersecurity 500

Meet the world's hottest and most innovative cybersecurity companies to watch in 2018. Press Release

Cybersecurity 500 By The Numbers: Breakdown By Region

Editors' Note: In 2019, the Cybersecurity 500 was replaced by the Hot 150 List of Cybersecurity Companies.

CHINA search reset

Showing 1-10 of 10 100 per page

#	Company	Cybersecurity Sector	Corporate HQ
104	Antiy Labs	Anti-Virus & Malware Engine	Haerbin, China
124	i-Sprint Innovations	Identity & Access Management	Chai Chee, Singapore
186	Qihoo 360	Internet & Mobile Security	Beijing, China
223	DBAPPSecurity	Database & Web Application Security	Hangzhou, China
345	Hillstone Networks	Data Analytics Firewall Protection	Suzhou, China
348	Nexusguard	Cloud Enabled DDoS Mitigation	Hong Kong
409	HanSight	Big Data Security	Beijing, China
489	NSFOCUS	DDoS Mitigation & Protection	Hong Kong
499	Sangfor	Network Security & Optimization	Shenzhen, China
500	ThreatBook	Cyber Threat Intelligence	Beijing, China

Fig. 13-4 Chinese Vendors Listed in the 2018 Top 500 Cybersecurity Companies of Cybersecurity Ventures (Partial)

Since 2019, Cybersecurity Ventures has replaced its Top 500 Cybersecurity Companies list with the Hot 150 Cybersecurity Companies list, all of which are European and American vendors, while China's cybersecurity enterprises are separately ranked[8]. In September 2020, Cybersecurity Ventures released the list of China's Most Popular and Innovative Cybersecurity Companies, including 20 enterprises, such as Antiy, Qihoo 360, QAX, Hillstone Networks, DBAppSecurity, SANGFOR and ThreatBook[9]. In a hearing held on February 17, 2022, by the USCC[5], *China's Cyberspace Capability: Cyberwar, Espionage and the Impact on the United States,*[5] experts said that "China's private business entities are heavily involved in China's cyberspace operations," and explicitly suggested that "the Congress could not just name and humiliate them, instead, it requires the Ministry of Commerce or the Ministry of Finance to separately list Chinese entities related to cyber operations in the list of entities and sanctions, thereby imposing costs on these Chinese cyberspace threat organizations." The expert's comments on China's cybersecurity industry were based on the list of China's most popular and innovative cybersecurity companies released by Cybersecurity Ventures[10].

Summary

In recent years, the hegemony and superiority established by the United States based on its own technical strength and market capacity have been severely challenged. In order to contain rivals in an all-round way as soon as possible, the US government has chosen to abuse the tool of "national security concept" as a "universal glue" to reinforce various barriers, and consolidate its leading position in the global Internet market by

attacking and restraining competitors. At the same time, the US has linked cybersecurity with economic, trade, science and technology, ideology and other issues as a favorable excuse for launching trade wars and science and technology wars, making cybersecurity issues unprecedentedly generalized and politicized. The implementation of the protectionist strategy under the cover of security issues and the suppression and containment of security enterprises outside the United States and the Five-Eye Alliance may temporarily maintain the hegemony and interests of the United States, but its unilateralism featuring "American First" will ultimately damage its national credibility and long-term development.

References

1. Department of Commerce. *Commerce Department to Add Two Dozen Chinese Companies with Ties to WMD and Military Activities to the Entity List.* 2020. https://2017-2021.commerce.gov/news/press-releases/2020/05/commerce-department-add-two-dozen-chinese-companies-ties-wmd-and.html
2. DoD. *DoD Releases List of Peoples Republic of China Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021.* 2022. https://www.defense.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/
3. Snowden Archive. An Easy Win: Using SIGINT to Learn about New Viruses. 2015. https://edwardsnowden.com/wp-content/uploads/2015/06/project-camberdada.pdf
4. NETSCOUT ASERT Team. *Non-Government Organization in Support of Government Hopes.* 2016. https://www.netscout.com/blog/asert/non-government-organization-support-government-hopes
5. USCC. *China's Cyber Capabilities: Cyberwar, Espionage, and Implications for the United States.* 2022. https://www.uscc.gov/sites/default/files/2022-2/February_17_2022_Hearing_Transcript.pdf
6. CRN. *The full cybersecurity 500 list.* 2015. https://www.crn.com.au/news/the-full-cybersecurity-500-list-401442
7. Cybersecurity Ventures. *Cybersecurity 500 by the Numbers: Breakdown by Region.* 2018. https://cybersecurityventures.com/cybersecurity-500-by-the-numbers-breakdown-by-region/
8. Cybercrime Magazine. *"China Cybersecurity Companies,"* 2018. https://cybersecurityventures.com/china-cybersecurity-companies/
9. Cybersecurity Ventures. *China Cybersecurity Companies.* 2020.

https://cybersecurityventures.com/china-cybersecurity-companies/

10. Cybersecurity Ventures. *The Hot 150 Cybersecurity Companies to Watch in 2021*. 2021. https://cybersecurityventures.com/cybersecurity-500/

Conclusion

The NSA, the CIA and other US intelligence agencies, as well as the Cyber Mission Forces led by USCYBERCOM have the largest cyberattack teams in the world, the largest supporting engineering system and the standardized attack arsenal, and the most powerful capabilities of vulnerability collection, mining and analysis, along with the reserve of related resources, supporting the most dangerous and active global cyber operations. The United States has built dozens of large-scale intelligence operation engineering systems, such as TURBULENCE, PRISM, MARINA, and MAINWAY, acquiring the ability to obtain global data. At the same time, by taking the advantages of the standard setting and the supply chain, backdoors were embedded in the encryption standard to carry out long-term systemic control and manipulation of the encryption system. In order to gain intelligence advantages, the United States uses all means, legal and illegal, legitimate and illegitimate, white and dark.

Cyber operations initiated by the United States have become the most serious threat to global cybersecurity, with its equipment system covering all scenarios, vulnerability exploitation tools and malware payloads covering all platforms, and persistent capability covering all links. The United States puts its own hegemony above the sovereign security of other countries. It wantonly launched cyberattacks, which seriously threatened the security of other countries, undermined people's trust in network technology, and even caused great damages to the global political and diplomatic environment. The exposure of the United States cyber behavior has also undermined the trustworthiness of American products and services around the world.

Today, countries around the world can fully find out all of these, thanks to not only the revelations of Snowden and the Shadow Brokers, but also the results of long-term follow-up and analysis by the global cybersecurity community, including enterprises, universities, research organizations and individuals. The history of analyzing and exposing the activities of US intelligence agencies over the past decade has been a long and complex process.

At first, what we can find is only the toes from the devil's footprints. The analysis of viruses, such as Stuxnet, Duqu and Flame, by global security vendors was basically based on the analysis of vulnerability theory, reverse analysis of samples and repeated analysis of sample action mechanism. Gradually, all evidence pointed to the homologous correlation of all these viruses, and to the same dark sources behind these

incidents - US intelligence agencies. However, the analysis lacked more profound systematic thinking, and still took APT attack and even A^2PT attack as a kind of technical threat.

Snowden, the Shadow Brokers and WikiLeaks exposed the US intelligence agencies' vicious practices, such as global surveillance, indiscriminate cyberattacks and the contamination and manipulation of encrypted communications standards. Based on these valuable data clues and follow-up research of the global cybersecurity industries, the US super cyberspace operation capabilities have been completely exposed.

To write this report, the China Cybersecurity Industry Alliance (CCIA) has collected nearly 1,000 research reports from dozens of cybersecurity vendors, universities and individuals. CCIA realizes that it is due to the tireless efforts of so many institutions and people, the invisible devil of the US cyber behaviors becomes visible. Chinese famous writer Lu Xun said: "The history of human bloody war is just like the formation of coal. A large amount of wood was used, but the result was only a small piece." Each and every organization, institution, individual that contributes in this process deserves respect.

During the long and arduous study and analysis process, the attitude and status of global cybersecurity industry has changed dramatically. American cybersecurity vendors, such as Symantec and McAfee, which had made thorough and in-depth analysis of Stuxnet, now kept silent about the cyberattacks launched by the United States. The European anti-virus industry was once prosperous, but now local large enterprises are withering due to the penetration of US mergers and acquisitions. Only Kaspersky still supports the European cybersecurity industry lonely under huge pressure. Although facing escalating pressure, China's cybersecurity enterprises and industry are becoming bigger and stronger.

Global cyberspace is now at strategic crossroads. To be locked in the dark unipolar world or to help construct a brand-new world of cyberspace community of shared future, this is a historical choice facing the global cybersecurity industry.

Appendix: Chronicle of Relevant Events

[2007]

In August, cybersecurity researchers Dan Shumow and Niels Ferguson released *NIST SP800-90 The Possibility of a Backdoor in the Dual_EC_DRBG*.

[2010]

In August, Symantec released *Stuxnet's the First Known Industrial Control System Rootkit*.

In September, Antiy released *Comprehensive Report on Stuxnet Worm Attacks on Industrial Control Systems*.

In October, Symantec released *The W32.Stuxnet Dossier*.

[2011]

In October, Hungary's CrySyS released *Duqu: A Stuxnet-like Malware Found in the Wild*.

[2012]

In May, Kaspersky released *The Flame: Questions and Answers*.

In May, CrySyS released *sKyWIper: A Complex Malware for Targeted Attacks*.

In August, Kaspersky released *Gauss: Anomalous Distribution*.

[2013]

On June 5, British newspaper the Guardian exposed the NSA surveillance event.

On June 6, Snowden exposed the NSA's PRISM Program.

On September 5, the Guardian reported on *How American and British Spy Agencies Defeated Internet Privacy and Security*.

On September 6, The New York Times reported *NSA Can Deceive Basic Online Privacy Protection.*

On September 10, NIST restarted the review of the SP 800-90A Standard.

In November, the US government banned cybersecurity experts from attending the Information Security Forum (ISF2013) held in China.

In November, Ralph Langner, a German IT expert, published *Stuxnet's Secret Twin* on the *Foreign Policy*.

In November, Ralph Langner released *To kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*.

On December 21, the Reuters reported *The Secret Contract Connecting the NSA and the Security Industry Pioneer*.

On December 27, former Tor core programmer Jacob Appelbaum exposed parts of the NSA's "spy tool library" at the 30th Chaos Communications Conference.

[2014]

In January, InfoSec released *Part 1 of the NSA BIOS Backdoor, Known as God Mode Malware: DEITYBOUNCE*.

[2015]

In February, WikiLeaks published *How the Equation Group Goes Evil? How Do We Avoid Being Attacked?*

In February, Kaspersky released *The Equation Group: Q&A*, *Equation: The Death Star of Malware Galaxy*.

In March, Antiy released *The Trojan that Modify Hard Disk Firmware - Exploring the Attack Components of the Equation Group*.

In April, Antiy released *Analysis of Encryption Techniques in Some Components of EQUATION*.

In June, Snowden revealed the internal document of the NSA, *Easy Victory: Using SIGINT to Learn about New Viruses.*

In June, Kaspersky released *Technical Details of DUQU 2.0* .

On June 22, US media The Intercept and Forbes simultaneously exposed the NSA's Project CAMBERDADA.

On June 24, NIST released the SP 800-90A revised version, which removed the Dual_EC_DRBG.

In July, *Dual EC: Standardized Backdoor* was released by the Eindhoven University of Technology in the Netherlands.

[2016]

In August, the Shadow Brokers exposed the cyberattack equipment of the NSA's Equation Group.

In August, the Hacker News reported *The Cyber Arms Auction of the Equation Group*.

In November, Antiy released *From Equation to Equations - Revealing the Multi-Platform Operational Capability of Equation Group.*

In October, the Cybersecurity Review published *The Shadow Brokers Reveals a List of Servers Hacked by the NSA*.

[2017]

On March 7, WikiLeaks released Vault 7, revealing secret documents of CIA cyberattack weapons.

On April 14, the Shadow Brokers released *Partial Tool File for the Equation Group*.

On April 16, the China National Vulnerability Database (CNVD) released *The Announcement on Strengthening Prevention of Attack Risks of Windows Operating System and Related Software Vulnerabilities*.

In September, US Department of Homeland Security required all federal agency information systems to ban software products from Kaspersky.

[2018]

From December 2017 to November 2018, Antiy published a series of 12 articles titled *The Analysis of US Cyberspace Attack and Active Defense Capability* in the journal *Civil-Military Integration on Cyberspace*.

In October, Kaspersky conducted an in-depth analysis of DarkPulsar in the use of post-frame DanderSpritz.

[2019]

In June, Antiy released *The Review Analysis Report on the Equation Group Attacking SWIFT Service Provider EastNets*.

In September, Antiy released *Nine Years Review and Thinking of the Stuxnet Incident*.

[2020]

On February 11, the Washington Post and other media exposed that Crypto AG, a Swiss encryption device vendor, was manipulated by American and German intelligence agencies.

On May 22, the US Department of Commerce added 24 Chinese companies, including Qihoo 360, to its entity list.

[2022]

On February 17, the US Senate held a hearing on *China's Cyberspace Capability: Cyberwar, Espionage, and the Impact on the United States*, pointing out two Chinese cybersecurity vendors, Antiy and Qihoo 360.

On February 23, QAX released *Bvp47 - Top-level Backdoor of the NSA's Equation of the US*.

On March 2, 360 released *Prologue to the cyberwar: NSA (APT-C-40) Launched Undifferentiated Attacks on the Whole World for More than a Decade.*

On March 15, Antiy released *From the Remote Control Trojan 'NOPEN' to See the Surface of the United States Cyberattack Equipment System*.

On September 5, China's National Computer Virus Emergency Response Center (CVERC) issued *The Investigation Report on the Cyberattack of Northwestern Polytechnical University by the US NSA (I)*.

On September 27, CVERC issued *The Investigation Report on the Cyberattack of Northwestern Polytechnical University by the US NSA (II)*.

On October 5, the US Department of Defense released the list of the second batch of *Chinese Military-related Companies (CMC) Operating in the US*, with Beijing Knownsec Information Technology Co., Ltd. and Qihoo 360 on the list.