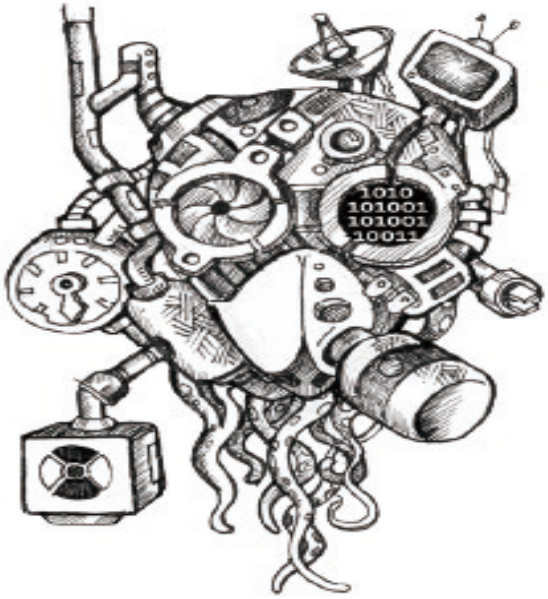
Extracting Defense Principles from Overlooked Details

—— “Reconsidering the 'Stuxnet' Attack 15 Years After Its Exposure

Antiy Security Research and Emergency Response Center

Antiy Strategic Intelligence Center

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



First draft: June 22, 2025

First published: March 02, 2026

Update of this edition: March 02, 2026

Scan to get the latest version

History cannot be assumed, but a retrospective study is needed ——

Background introduction to the report

From February 28, 2026 (Iranian local time), the US-Israeli coalition launched a large-scale joint military operation code-named "Epic Fury" against Iran, bombing and air strikes against a large number of targets in Iran [1]. On the same day, Iran confirmed that Supreme Leader Khamenei was killed in an air strike.

Dan Kane, chairman of the U.S. Joint Chiefs of Staff, said [2] that U.S. Cyber Command and Space Command are "the first actors" to provide "superimposed non-kinetic operational effects" to support the system. He said at a Pentagon press conference: "The coordinated space and network operations have effectively paralyzed the communication and sensor networks in the area of responsibility, and the opponent has lost effective reconnaissance, coordination and counterattack capabilities."

Therefore, we have to look back on the "Stuxnet" attack that was exposed in 2010, which blocked Iran's nuclear development process for a long time. Many people can't help but wonder whether Iran would have become a nuclear power if the cyber attack had not been successfully carried out; if it had become a nuclear power, what would have been the situation in the Middle East, including the global power map; and if Iran had mastered nuclear weapons, whether today's scene would have happened. History cannot be assumed, but it needs to be studied retrospectively. We uphold the position of opposing nuclear proliferation and supporting the peaceful use of nuclear energy, but at the same time we oppose armed intervention and unilateral sanctions. Whether we follow up from the initial analysis or at this time, we hope to present the deep logic of the use of cyberspace forces in war.

In June 2010, the "Stuxnet" virus was exposed. Since July 15, 2010, Antiy has carried out the analysis of "Stuxnetwork", set up a reduction sand table, analyzed its basic principle [3], USB ferry mechanism [4], mechanism of action on WinCC [5] and other contents, and released many analysis reports, and further for flame (Flame)[6], poison (Duqu) and other viruses and Stuxnetwork homology [7] and other issues, for several years of tracking analysis. By 2019, we released "Nine Years of Resuming and Reflections on the Stuxnet Event" [8]. In June 2025, the United States bombed Iran's nuclear facilities, and on the occasion of the 15th anniversary of the exposure of the "Stuxnet" incident, Antiy Emergency Response Center and Antiy Strategic Intelligence Center jointly completed the report of "Reconsidering the 'Stuxnet' Attack 15 Years After Its Exposure". Three series of reports, namely technical, tactical and strategic, decided to be internal results and not made public. We then noticed that on July 22 of the same year,

the US Cybersecurity and Infrastructure Protection Subcommittee also held a hearing on the topic "Full Operation: 15 Years after the 'Stuxnet 'Virus and the Evolution of Cyber Threats to Critical Infrastructure.

On January 6, 2026, in response to the U.S. invasion of Venezuela and the kidnapping of President Maduro and his wife, Antiy released reports such as "Spectrum Speculation and Correlation Analysis of Network Operation Capability Behind the U.S. Army's Invasion of Venezuela" [9]. Under the background of extremely low visibility of the incident, Antiy made a careful deduction and analysis of the relevant incidents from the perspective of capability system evaluation and actor paradigm. Antiy's strategic analysts summed up the characteristics of the Trump administration's new military operation: "Resist the war of great powers and fear the quagmire of interventionism. However, by carrying out" beheading operations "through rapid and relatively low-cost" special operations "and completing the regime change in anti-American countries, we can not only avoid falling into the quagmire of war that may be brought about by the former American interventionism, but also declare the scope of its influence. Under the premise of choosing this more cost-effective way of action in line with the strategic interests of the United States, the Trump administration may be more adventurous than other presidents."

Since the tense situation in Iran this time, there have been voices in the industry that Antiy CERT will continue to follow up. However, after discussion, we decided not to release public technical analysis. Antiy Strategic Intelligence Center plans to talk about some views and judgments in its publication when it plans to create the WeChat Official Account named "Cyber Space Combat Reference".

Regarding the US-Israel bombing of Iran, on the one hand, it is necessary to see that the United States and Israel have achieved part of the preset operational goals based on super intelligence capabilities and repressive strength. From the tactical and technical aspects, it is necessary to attach great importance to and analyze its capabilities. And the application process; but on the other hand, there is no need to exaggerate it as a new myth. For this reason, we decided to make public the technical articles in the three reports of "15 years of rethinking the" Stuxnet attack "last year. Based on the review of the key information that the" Stuxnet "incident did not receive enough attention, the report refined several working principles of network security attack and defense, and also sorted out the" Stuxnet "attack from the perspective of the security capability when the" Stuxnet "incident occurred, it shows that the effectiveness of the attack does not come entirely from the superior ability of the attacker, but also from the lack of ability and indifference of consciousness of the defender. This is a process of thinking about breaking the myth and disenchantment. We hope to bring a voice from the perspective of the network security industry and adhere to long-term strategic determination in the chaotic and complicated information. At the same time, we would like to make it

clear that whether our analysis results are released or not comes from our own judgment and understanding of the responsibility of China's cyber security enterprises, rather than SentinelOne interpretation of "being suppressed" by a peer for us. We also thank Jack Paulson (Jack Poulson) for his public disclosure of the US intelligence contractor's analysis of our portrait, as well as the analogy of our analysis to "WikiLeaks" and the use of Pompeo (Michael R. Pompeo) during his tenure as CIA director, to propose the assassination of Assange (Julian Assange) to give a risk to our personal safety.

We believe that the "resumption" of the "Stuxnet" incident will enable Chinese and international cyber security workers to learn lessons and nutrients from historical coordinates-including a comprehensive understanding of attack activities and technologies, but also about defense laws. Understanding and iteration. To improve our own security capabilities and prepare for future threats.

1 By the myth of the "Stuxnet"

Fifteen years have passed since the Stuxnet incident came to light in 2010. From cyber security confrontation to military history, this is a milestone event that confirms that "cyber attacks can be translated into physical space effects, including local equivalence with fire strikes". This is indeed a milestone event that opened the Internet War Magic Box, but at the same time, it also brought many "myth" labels, and there are also many rumors that are inconsistent with the facts. These are all mixed in the "Stuxnet" incident. In the understanding. So that when people talk about "Stuxnet", they are often not accurately and objectively based on the real technical process, but are talking about a myth that has been constructed. Fifteen years on, Stuxnet has evolved from a real threat to a specimen for study. But the nature of the attack, the logic of defense, and the nature of security that it reveals remain unchanged.

As a model case of "breaking through the physical isolation network", the initial entry process of "Stuxnet" has been misjudged. In 2010, when Antiy CERT first participated in a multi-party discussion on "Stuxnet", the technical personnel of relevant European industrial control manufacturers who participated in the discussion explained how "Stuxnet" penetrated into the intranet of the industrial system. It was possible that a large number of USB disks with "Stuxnet" virus were scattered and dropped near relevant institutions, and then misused and transmitted to the network by personnel. However, some discussants accepted this obviously unreasonable possibility and believed that the entry of "Stuxnet" into the intranet was a probabilistic event of "collision" type of capturing opportunistic windows. However, the actual situation of the attack on the U disk directed by Dutch maintenance engineers, which was exposed only a few years later, is not known.

In the driver of the "Stuxnet" attack, legal digital signature certificates stolen from Realtek and JMicron two Taiwanese manufacturers in China were used to help it bypass the driver signature verification of the Windows system. In addition, in the "Stuxnet" code, there are codes that judge the targeted bypass of the antivirus software process, thus strengthening the targeted penetration influence of the "Stuxnet. The concealment of the "Stuxnet" attack has also been exaggerated. Because it uses Rootkit means to make its key modules land, it cannot be seen in the resource manager, so that it is considered by many people to discover the "Stuxnet" Host activity is very difficult. And because of the complex encryption it uses for its own code and configuration, this impression is also passed on to its network activities, believing that it is difficult to observe and discover during its lateral movement. However, the actual situation may be that no host security software is deployed on some hosts of the target, and the traffic monitoring and

analysis capability of the intranet is not deployed. The biggest legend about "Stuxnet" is that this is an attack based entirely on the combination of 0day vulnerabilities. Therefore, it intensifies a defense cognition, that is, the attention of defending advanced persistent threats is completely focused on the proposition of "unknown vulnerabilities", while ignoring the actual situation and the role of attack payload (execution body).

In fact, the above misjudgments have long been confirmed to be inconsistent with the real situation in a large number of historical analysis and exposure information, including Antiy. However, due to the strong inertia, these real details are blocked in public cognition. Therefore, we would like to emphasize another version of "Stuxnet": it is a masterpiece of cyber attack engineering, but it is not an impeccable and perfect process; it pioneered the attack on industrial control systems, but it is also a myth that is not undefended. The reason why "Stuxnet" can go straight into it is not simply based on the skill of its attack technology, but also because the target system itself is almost undefended except for physical isolation measures.

There are no absolutely safe systems, but there are no completely unsolvable attacks. This is dialectics!

2 About some details that have been revealed but not taken seriously

We have titled this report "Guidelines for Distilling Defense from Neglected Details" in the hope of re-combing and mentioning details that have long been verified and explained in historical analysis, but have been overwhelmed by preconceived and deliberately mythical judgments, in order to re-break those solidified stereotypes.

2.1 Manual directional contact breakthrough-rather than capturing small probability windows

In an attack activity where the mission objective is clear, the attacker has a clear will to attack and abundant resources, and has consumed a lot of engineering and preparation costs, it is of course necessary to capture the operation window. But it is clear that it will not take an opportunistic approach, leading to attacks that may be exposed before they are achieved, but to ensure the success of the penetration. The real reason why "Stuxnet" broke through to the inside of the uranium centrifuge facility network, although from the analysis in 2010, the functional code of USB ferry and internal network lateral movement has been found. However, it was not until 2019 that it was revealed in the media report "Exclusive Disclosure: How Dutch Secret Informer Helped the United States and Israel to Launch a Stuxnet Cyber Attack on Iran (Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran)" [10]. At this time, the "Stuxnet" incident has not been hot enough, resulting in many people still do not understand how the "Stuxnet" penetration is completed.

In 2007, in order to break through the physical isolation of Iran's Natanz uranium centrifuge facility, the CIA and Israel Mossad instigated a secret infiltration operation, recruiting Dutch Siemens engineer Erik van Sabben to use his legal identity as a cover to implant the initial infection vector of "Stuxnet" virus into the intranet control system with a U disk. A subsequent investigation found that Eric had previously been developed as an informant by the Dutch intelligence agency, but the United States concealed the details of the "Stuxnet" mission from him, and the Dutch intelligence agency did not know the complete plan. The "Stuxnet" attack is the name of the analyst. Its internal mission in the US intelligence agency is code-named "Operation Olympus". Based on years of technical and tactical preparation by the United States and Belgium, it has been approved by two US governments. This artificial penetration link has extremely high tactical value. After the completion of the mission, "Stuxnet" caused the failure of nearly 1,000 uranium enrichment centrifuges in Natanz. Iran initially misjudged the nature of the attack and treated it as a failure without emergency response. In January 2009, Eric was killed in a traffic accident in Sharjah, United Arab Emirates. In the spring of the same year, the U.S. and Israeli technical teams upgraded the "Stuxnet" virus to enable it to have independent transmission capabilities and achieve secondary penetration.

Around 2008, the US NSA has installed a special USB attack device CottonMouth. At present, it can be preliminarily judged that the NSA has the capability of USB automatic insertion and operation in January 2007. Therefore, it is not known whether the carrier device is an ordinary USB device that only copies the "Stuxnet" virus, or an automated triggered attack device similar to the "water viper. Under the premise that the personnel can contact the terminal, although it can realize manual operation, if the equipment with similar CottonMouth is inserted into the U port for a long time, it can not only realize automatic implantation operation. Moreover, it can form a persistence capability based on peripherals. Similar CottonMouth-II can also implement communication at a certain distance (about 13 kilometers in the open area) to build relay nodes for proximity control.

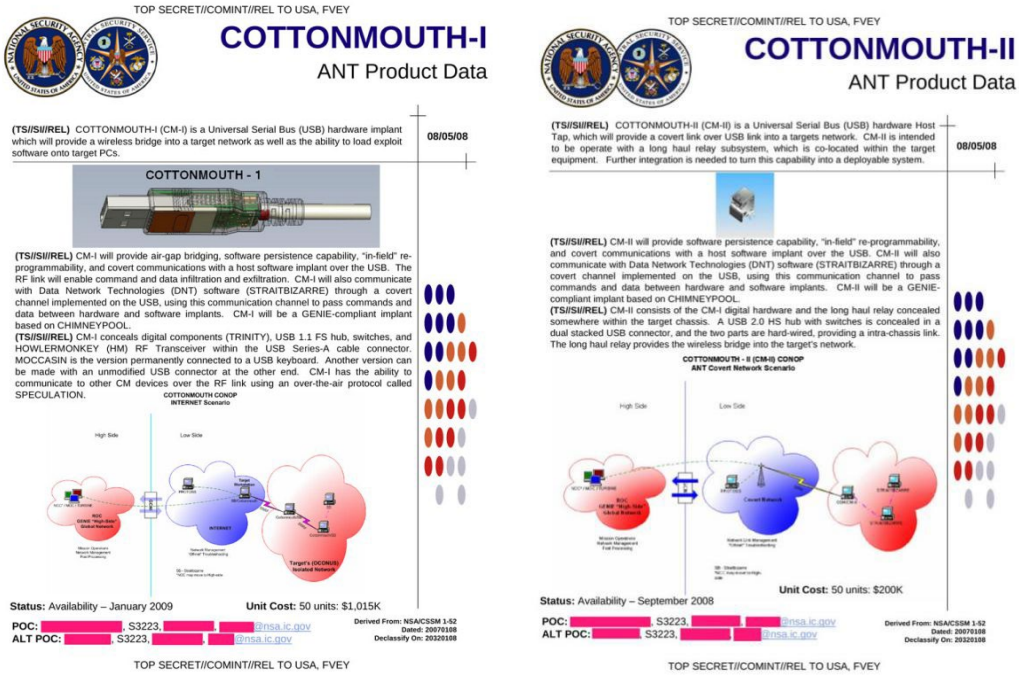


Figure 2-1 U.S. CottonMouth implanted attack equipment based on peripheral (presumably installed around 2008)1

2.2 There are multiple host-visible traces—rather than leaving no trace at all.

"Stuxnet" virus has a variety of defense and evasion capabilities, such as infection condition judgment, regular self-destruction, different operations according to the system installation of security software, Rootkit technology, embezzlement of digital signatures, etc. It can completely bypass the system security mechanism and mainstream security software at that time. However, it is not without flaws by analyzing the behavior traces of the host side and the network side after infection (see the table below). For example, registration driver, injection process, short-term frequent communication in intranet, connection to Internet domain name, file writing of mobile storage device, Hook system API function, etc. are all traces of high-risk behaviors. Even if no direct alarm is given, clues can be found, relevant abnormalities can be found and losses caused by persistent attacks can be reduced through log record retention and regular safe operation. We do not know the specific IT environment in Iran at that time, but from the actual results, Iran did not find the "Stuxnet" virus in time, but let it exist for more than two years from the earliest attack wave.

Table 2-1 "Stuxnetwork" sample after the execution of some typical behavior traces table:1

Type of behavior	Specific content

File Creation	%WinDir%\inf\mdmcpq3.PNF %WinDir%\inf\mdmeric3.PNF %WinDir%\inf\oem6C.PNF %WinDir%\inf\oem7A.PNF %WinDir%\inf\oem7F.pnf %WinDir%\inf\oem7w.pnf %WinDir%\inf\~67.tmp %System%\drivers\mrxcls.sys %System32%\drivers\mrxnet.sys %System%\drivers\usbacc11.sys %System%\drivers\PCIBUS. SYS %System%\comuid.dat %System%\netsimp32.dll %System%\inetpsp.dll %System%\perfg009.dat %WinDir%\msagent\agentsb.dll %WinDir%\msagent\intl\agt0f2e.dll %System%\complnd.dll %System%\dllcache\datacprs.dll %System%\wbem\perfnws.dll %WinDir%\Installer\{6F716D8C-398F-11D3-85E1-005004838609}\places.dat %System%\dssbase.dat %AllUsersProfile%\Application Data\Microsoft\HTML Help\hhorcslt.dat %Temp%\DF419a.tmp %WinDir%\help\winmic.fts Removable Disk\AutoRun.inf Removable Disk\~WTR4141.tmp Removable Disk\~WTR4132.tmp Removable Disk\Copy of Shortcut to.lnk(4 copies)
Registry creation, reading	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNET HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\sbacc11 HKEY_USERS\<SID>\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellRecoveryState
Online behavior	Connect back to C2 server P2P peer-to-peer communication in LAN RPC Remote Execution Vulnerability (MS08-067) Network Attack Exploitation Print Spooler Service Vulnerability (MS10-061) Network Attack Exploitation WinCC Default Password Vulnerability (CVE-2010-2772) Network Attack Exploitation
system behavior	Traversal process Injecting System Processes Hook System API Functions Get system time

After the "Stuxnet" virus infects the host, a large number of files will be generated. Antiy CERT summarizes the path, format, signature and function of the files (see the following table). This includes encrypted configuration files, encrypted modules, but there are also unencrypted DLL, SYS, LNK, etc. In addition to a number of encrypted files, two of the driver (SYS) files have valid digital signatures. These two driver files are the core modules of "Stuxnet" that can persist, avoid detection and self-start. Through these two drivers, the loading of the main module and the hiding of related files are completed. Several DLL files are responsible for P2P networking, C2 communication, USB propagation initial loader, and main module functions. There are also 4 LNK files and 2 DLL files that will be released to the accessed mobile storage device to launch a "ferry" attack using LNK vulnerabilities. "Stuxnet" is a worm-type virus, and its infection in the intranet is very large. The above related file payloads exist in the form of files in the

infected host terminal. Most of these files are not hidden by Rootkit and can be monitored and captured by security software and can be observed by the naked eye. Although the relevant files are unknown to the security software, for such a relatively stable intranet host environment, in fact, combined with effective security operation, traces of relevant attacks can be found, and the victim host can be located and the relevant risks can be disposed of based on clues such as a large number of file increases, blue screen hosts generated, intranet communication, etc.

Table 2-2 Details of landing files after "Stuxnet" infects hosts2

File path name	File format	Signature status	Functionality
%WinDir%\inf\mdmcpq3.pnf	Encrypted hexadecimal	None	Configuration data and host information
%WinDir%\inf\mdmeric3.pnf	Encrypted hexadecimal	None	P2P update configuration data
%WinDir%\inf\oem6C.pnf	Encrypted hexadecimal	None	Log data
%WinDir%\inf\oem7A.pnf	Encrypted hexadecimal	None	Encrypted "Stuxnet" main module
%WinDir%\inf\oem7F.pnf	Encrypted hexadecimal	None	
%WinDir%\inf\oem7w.pnf	Encrypt hexadecimal	None	Encrypted Installation Module
%WinDir%\inf\~67.tmp	Encrypt hexadecimal	None	Encrypted Installation Module
%System%\drivers\mrxcls.sys	BinExecute/Microsoft.SYS	**There is**	Persistence self-starting module
%System32%\drivers\mrxnet.sys	BinExecute/Microsoft.SYS	**There is**	Rootkit hidden module
%System%\drivers\usbacc11.sys	BinExecute/Microsoft.SYS	None	C2 module, P2P module loading driver
%System%\drivers\PCIBUS. SYS	BinExecute/Microsoft.SYS	None	Blue Screen Force Restart Module Caused by Timing
%System%\comuid.dat	Unknown	None	Unknown
%System%\netsimp32.dll	BinExecute/Microsoft.DLL	None	P2P update communication module
%System%\inetpsp.dll	BinExecute/Microsoft.DLL	None	C2 communication module
%System%\perfg009.dat	Unknown	None	Unknown
%WinDir%\msagent\agentsb.dll	BinExecute/Microsoft.DLL	None	P2P update shared files
%WinDir%\msagent\intl\agt0f2e.dll	BinExecute/Microsoft.DLL	None	P2P update shared files
%System%\complnd.dll	BinExecute/Microsoft.DLL	None	P2P update shared files
%System%\dllcache\datacprs.dll	BinExecute/Microsoft.DLL	None	P2P update shared files
%System%\wbem\perfnws.dll	BinExecute/Microsoft.DLL	None	P2P update shared files
%WinDir%\Installer\{6F716D8C-398F-11D3-85E1-005004838609}\places.dat	Unknown	None	P2P update shared files
%System%\dssbase.dat	Unknown	None	Log File
%AllUsersProfile%\Application Data\Microsoft\HTML Help\hhorcslt.dat	Unknown	None	Unknown
%Temp%\DF419a.tmp	Unknown	None	Unknown
%WinDir%\help\winmic.fts	Unknown	None	Step7 Infected Profile
Removable Disk\AutoRun.inf	Text/ISO_IEC.UTF8	None	USB Propagate AutoRun Profile
Removable Disk\~WTR4141.tmp	BinExecute/Microsoft.DLL	**There is**	USB Propagation Initial Loader and Rootkit
Removable Disk\~WTR4132.tmp	BinExecute/Microsoft.DLL	None	Main Module File
Removable Disk\Copy of Shortcut to.lnk (4 copies)	SoftData/Microsoft.LNK	None	USB Propagation Vulnerability Exploit LNK File

2.3 Possible reasons for version evolution — seeking the optimal balance between destructive effectiveness and stealth.

The initial version of the "Stuxnet" sample is not the "worm" Trojan horse form analyzed by the security industry in 2010. This is the 1.x version of "Stuxnet", but its initial release is the 0.5 version. There are obvious differences between the two versions in the mode of transmission, attack mechanism and damage effect.

Table 2-3 Comparison of Differences between Stuxnetwork 0.5 and Version 1.x3

capacity dimension	0.5 version	1.x version	Description
Concealing ability	1、Multiple module code release on disk 2、No digital signature 3、Some modules cannot be established under the condition of killing soft	1、Module Encrypted Storage 2、With a verifiable digital signature in a sensitive module	The 0.5 version uses a more complex code development platform, but due to its lack of evasion capabilities, it may not be possible to achieve operational purposes in an environment with secure software. The 1.x version bypasses the killing software and completes the task by means of digital signature, module encryption storage, multi-process execution of tasks, etc.
Communication capacity	Stuxnet 0.5 is copied via the Step 7 project archive file. When a removable drive is inserted into an infected system, Stuxnet 0.5 infects Step 7 project archive files with a. s7p or. zip extension on the drive. In addition, the Step 7 project archive files stored on this disk will also be infected.	1. Windows RPC services 2. Windows printing services 3. WinCC SQL Server Service4. Lnk file parsing vulnerability 5. USB Autorun automatic execution function 6. Weak Password Sharing and Propagation	0.5 version of the targeted dissemination, dissemination capacity is limited, but highly targeted The 1.0 version uses a combination of multiple vulnerabilities to spread, which is not highly targeted, but has a very strong ability to infect.
destructive capacity	To modify the status of the valves supplying uranium hexafluoride gas to the enriched uranium centrifuges. This can close the uranium transfer valve, resulting in a blockage of uranium flow and damage to the centrifuge and its associated systems.	By quickly adjusting the speed of the centrifuge, to achieve the purpose of destroying the centrifuge	The 0.5 version uses overpressure to destroy the centrifuge, and the time from infection to destruction of the centrifuge is shorter. The 1.0 version uses the method of adjusting the speed to destroy the centrifuge and shorten its life, which can be adjusted for a longer time.

Then, what is the root of version evolution? From the perspective of action and effectiveness, it is more likely that there are two original versions that follow the IT operation adjustment of the Iranian environment, and have become invalid after achieving the initial effect. Including Iran's expansion of new centrifuge facilities in many places,

the scope of its initial operation cannot be covered, and it needs to be followed up by means with more communication and penetration capabilities.

At the same time, there may be the following reasons for the version differences:

From the balance of damage effect and concealment, the 0.5 version of the attack may have a greater risk of exposure. The International Atomic Energy Agency (IAEA) verification report shows that between December 2009 and January 2010, about 2000 centrifuges at Iran's Natanz nuclear facility were replaced-this anomaly is partly the result of overpressure caused by the "Stuxnet" cascading through valves. However, this batch damage pattern may also gradually be exposed in the event analysis zeroing. The 1.x version destroys the analysis effect of uranium by modifying the rotation speed, and at the same time realizes more fine wear and damage to the centrifuge through the change of rotation speed, which may be an important driving force for the evolution of the version.

Adaptation of target environment: The centrifuge system and related key PC nodes and software conditions of Iran's nuclear facilities are also changing, and attackers need to constantly adjust their attack strategies to cope with changes in the target environment. From the perspective of version iteration, "Stuxnet" has experienced multiple versions such as 0.500, 1.001, 1.100, 1.101, etc. This frequent version update may reflect the attacker's continuous optimization process for different environments. The 1.x version has wider platform compatibility than the 0.5 version, which may be the result of the attacker's adaptation to different Siemens WinCC versions.

The evolution of propagation may reflect the attackers' quest for tactical flexibility. The 0.5 version relies heavily on human contact, which has obvious limitations-once the intelligence line is exposed or there is a problem with the landing personnel, the attack will stall. The 1.x version adopts more diversified communication methods, which can be infiltrated indirectly by infecting supplier technicians, and can also use LNK vulnerabilities (CVE-2010-2568) and print service vulnerabilities (CVE-2010-2729) to move the network horizontally. The transformation of this mode of communication has greatly reduced the dependence on a single source of intelligence. As for the large-scale spread of version 1.x-the reason for infecting more than 45000 networks around the world, Antiy has done more analysis on this in "Nine Years of Re-evaluation and Thinking of Stuxnet Event", which will not be repeated here.

2.4 Exploit multiple known vulnerabilities-not all 0day

Since the version of "Stuxnet" that was initially concerned and discovered by the industry is a 1.001 version that uses multiple vulnerabilities to move horizontally and spread through the network, the attention of "Stuxnet" has focused on the 0day vulnerability. However, in fact, the initial release version 0.5, which caused the damage to the batch of centrifuges, not only did not use the 0day vulnerability, but also did not use the vulnerability to carry out attacks. It is a group of complex malicious code executions with certain infection propagation attributes. Version 1.001 of the virus uses multiple vulnerabilities for rights raising, dissemination and execution, but Antiy CERT can show by comparing the relationship between sample compilation time and vulnerability disclosure time that version 1.001 uses both 5 0day vulnerabilities and 3 Nday vulnerabilities (MS08-067, MS10-061 and MS09-025 respectively, MS10-061 of which was disclosed by Microsoft in September 2010, however, the actual vulnerability was disclosed in Hakin9 magazine in April 2009, so the vulnerability can also be considered as Nday vulnerability). MS08-067 of these vulnerabilities were well-known at the time and had a major impact on computers around the world that year. Judging from the version change of "Stuxnet", there are deletion vulnerabilities and other propagation modules in the subsequent version of 1.X, but the MS08-067 has been retained in all versions of 1.X. It is more likely that the attack organization has already figured out Iran's nuclear industry system environment, has no attack detection capability deployment for vulnerability exploitation, and knows that its physically isolated intranet system has not updated the system patch, and has no basic governance for weak password network sharing (weak password sharing propagation module is also used in all versions of 1.X).

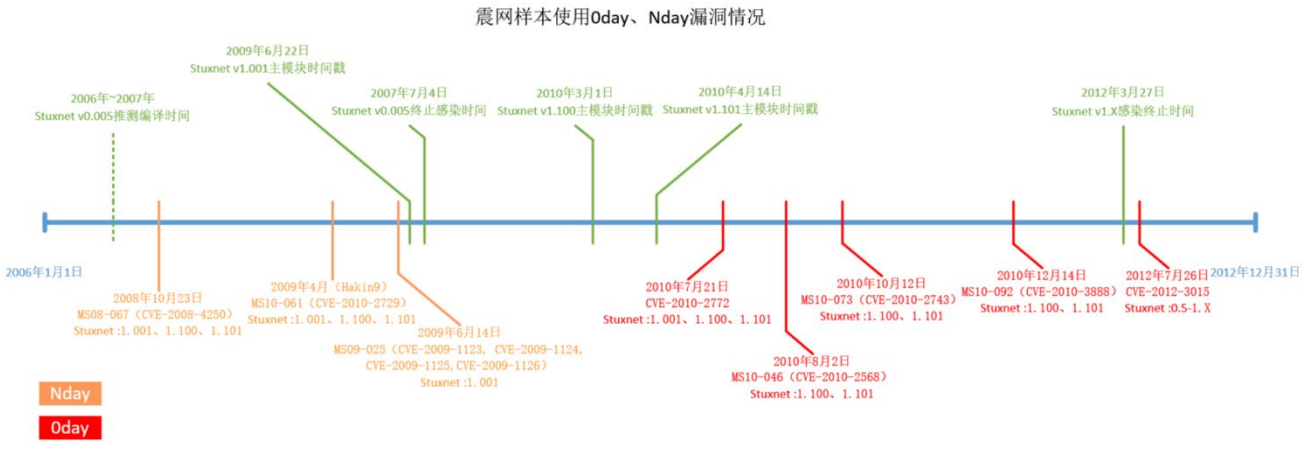


Figure 2-2 "Stuxnet" sample uses 0day and 1day vulnerabilities.2

Table 2-4 List of vulnerabilities used by Stuxnet4

CVE Number	MS Number	Vulnerability can prove weaponization time	Vulnerability exposure time	Whether 0day	Vulnerability Type	Service/Port
CVE-2008-4250	MS08-067	2009/6/22	2008/10/23	No	Remote Code Execution Vulnerability	Windows RPC Services/445
CVE-2010-2729	MS10-061	2009/6/22	2009/4	No	Remote code execution vulnerability	Windows Printer Services/139, 445
CVE-2009-1123	MS09-025	2009/6/22	2009/6/14	No	Windows Kernel Empty Vulnerability	/
CVE-2009-1124	MS09-025	2009/6/22	2009/6/14	No	Windows Kernel Empty Vulnerability	/
CVE-2009-1125	MS09-025	2009/6/22	2009/6/14	No	Windows Kernel Empty Vulnerability	/
CVE-2009-1126	MS09-025	2009/6/22	2009/6/14	No	Windows kernel privilege escalation vulnerability	/
CVE-2010-2772		2009/6/22	2010/7/21	Yes	WinCC Default SQL Authentication Vulnerability	SQL Server Service/1433
CVE-2010-2568	MS10-046	2010/3/1	2010/8/2	Yes	Remote Code Execution Vulnerability	/
CVE-2010-2743	MS10-073	2010/3/1	2010/10/12	Yes	Windows kernel privilege escalation vulnerability	/
CVE-2010-3888	MS10-092	2010/3/1	2010/12/14	Yes	Task Scheduler Right Vulnerability	/
CVE-2012-3015		2006-2007	2012/7/26	Yes	DLL Load Arbitrary Code Execution Vulnerability	/

2.5 Embezzlement of certificate signatures-a supply chain security link that has not received enough attention.

"Stuxnetwork" embezzled the certificate signature certificate, is the focus of the analysis of the parties at that time. But how to deal with this type of attack from the entire supply chain system has been ignored to some extent.

The important attack technique of "Stuxnet" virus is that the two core driver modules (copy persistence and hide related files) have digital signatures of mainstream manufacturers. It uses the embezzled two normal signatures (see the following figure and table) to put the cloak of "credibility" on its own malicious files, and greatly strengthens its own credibility through signatures, A variety of sensitive behaviors (boot self-start, injection process, Hook system

API) driven by it can bypass the detection of operating system and security software, and can openly perform any operation in the system.

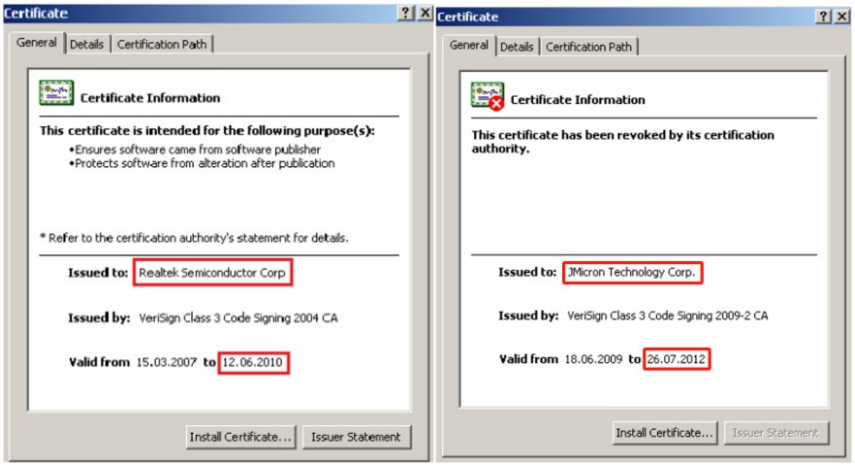


Figure 2-3 Two stolen digital signatures used by Stuxnet [12]3

Table 2-5 Realtek Company Stolen Signature Information5

Field Name	Value
Name	Realtek Semiconductor Corp
Issuer	VeriSign Class 3 Code Signing 2004 CA
Validity period	2007-03-15 00:00:00 to 2010-06-11 23:59:59
Effective use	Code Signing (Code Signing)
signature algorithm	SHA1 with RSA
SHA1 Fingerprint	Kan
MD5 Fingerprint	Kan
SHA256 Fingerprint	E95ABDF0826009D3362EB15715CC269BA400054B042C94866D82C65CAD7316FF
Serial number	5E 6D DC 87 37 50 82 84 58 14 F4 42 D1 D8 2A 25

Table 2-6 JMicron Company Stolen Signature Information6

Field Name	Value
Name	JMicron Technology Corp
Issuer	VeriSign Class 3 Code Signing 2009-2 CA
Validity Period	2009-06-18 00:00:00 to 2012-07-25 23:59:59
Effective uses	Code Signing
Signature algorithm	SHA1 with RSA
SHA1 Fingerprint	F1B6ABBEAD95F2180FBC40142121F399ADAD4F31
MD5 Fingerprint	Kan
SHA256 fingerprint	Kan
Serial number	47 6F 49 F4 C9 59 F6 56 E9 AA 1E B8 7F C5 29 BB

The headquarters of JMicron Technology, the company to which Stuxnet embezzled its signature, was located in the same science park as the RealTek at that time. Coincidentally, after the "Stuxnetwork" incident, a large number of digital certificate embezzlement, hash collision forgery of certificates, digital certificate issuing institutions were invaded to issue false certificates, tampering with the source code to use the original factory signature and other events. The code signature system is an important cornerstone of the software supply chain security system, but it is not enough to ensure the security of the software independently in an open scenario. The security of the certificate

issuing environment of the digital signature itself, the unified management and annulment mechanism of the certificate, the system security of the certificate authority itself, and the security of the certificate user environment should be given standardized management and sufficient attention. At the same time, in the large-scale industrial system, the application of software certificate is bound to be massive, the issuance of software certificate is bound to be discrete, and the signature system is bound to penetrate. Antiy has pointed out many times that in the new PE samples, those with "legal" digital signatures have a high proportion, which will inevitably make it impossible to rely solely on mathematical verification to ensure the safety of the entire software supply chain environment in the host scenario confrontation, and it will inevitably require anti-virus engines and main defense to carry the trusted system to carry the penetration confrontation.

2.6 Traffic features are prominent—rather than silent and unnoticed.

As analyzed in the above section, a large number of vulnerabilities were used in the "Stuxnetwork" attack process, of which 4 were used to break through the physical isolation propagation. One of these vulnerabilities was "ferried" to the isolation network using mobile storage devices, and 3 vulnerabilities were used to propagate in the intranet. "Stuxnet" in the use of these three vulnerabilities to spread, intranet traffic can be observed to produce very significant behavioral anomalies.

To reproduce the dissemination activities of "Stuxnetwork", it uses network sharing to disseminate itself. After establishing a connection with the target, it first sets the target file path, then transmits the file data in clear text, and sends the execution file command after the transmission is completed. Relevant actions have obvious traffic traces. The specific traffic behavior is shown in the following figure.

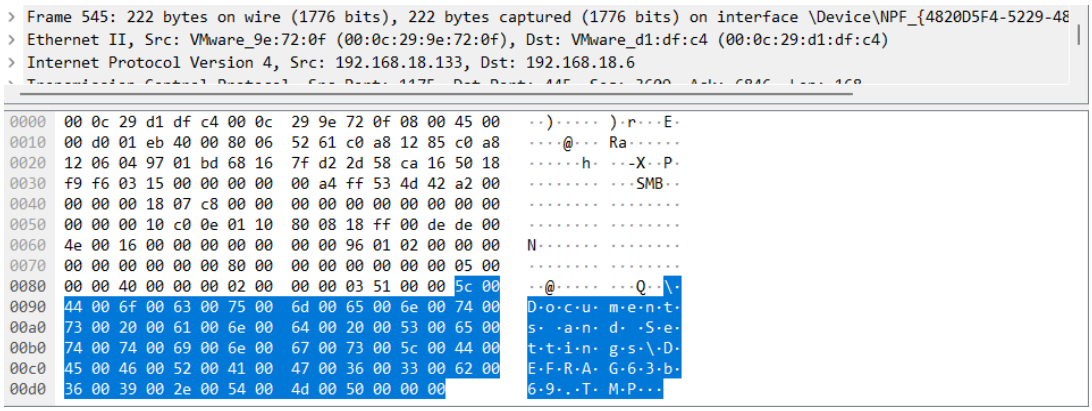


Figure 2-4 "Stuxnet" Set Propagation Target Path: DEFRAG[RANDLNT].tmp(PEEXE File)-4

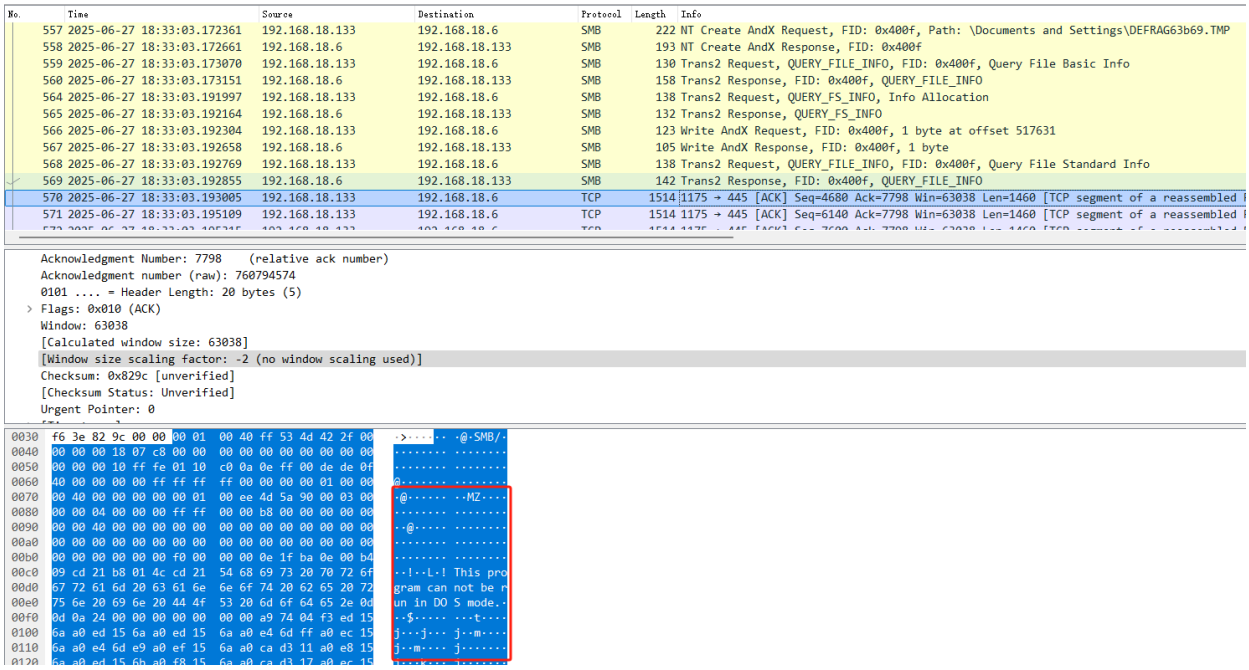


Figure 2-5 "Stuxnet" begins to transmit attack payload to the target host in clear text.-5

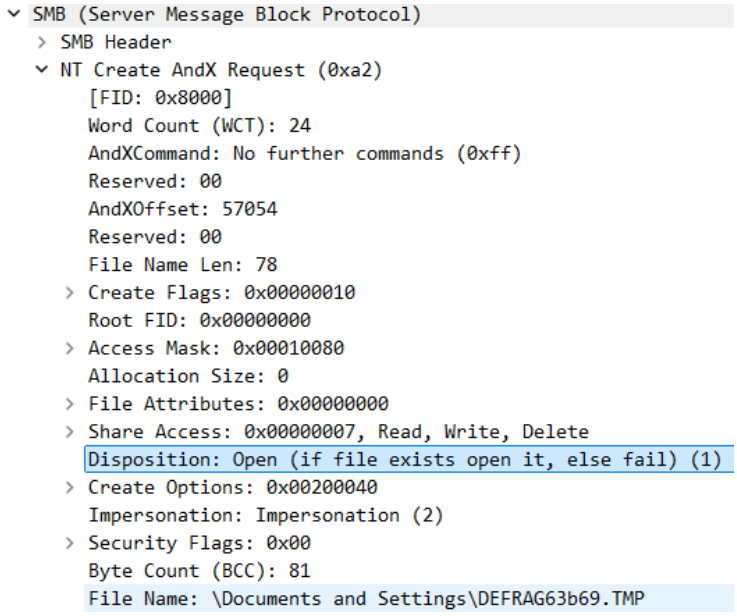


Figure 2-6 "Stuxnet" successfully sends execution commands using network sharing propagation.6

From the above analysis, it can be found that when "Stuxnetwork" uses the network to spread, there are many abnormal situations in the traffic, such as: transmitting PE files, sending execution commands, etc., and it is an observable feature of Ming culture. Therefore, whether it is an intranet or an open network, it should not be monitored because it is isolated, and it should be monitored and recorded by safety protection equipment. As The Langner Group says, Iran should have been aware of these flows, not failed to conduct any tests.

2.7 Misconceptions and Misjudgments — Failing to Consider the Possibility of a Cyberattack During Initial Investigation

Unlike today's solidified impression that the personnel level of Iranian institutions has been infiltrated into a sieve, the "Stuxnet" attack occurred during Iran's ascent in an industrialized country, when the degree of infiltration of Iranian personnel by the United States and Israel was much lower. When the centrifuge damage caused by the "Stuxnet" attack first appeared, the Iraqi side did not consider the possibility of being attacked by network intrusion in the investigation, and focused the accident investigation on "internal personnel damage" and domestic equipment quality defects. Two directions.

Of course, there are certain objective reasons for this. At the level of technical investigation, the centrifuge system of Iran's nuclear facilities adopts a mixed supply chain model, which includes not only equipment provided by foreign manufacturers such as the Netherlands, but also domestic equipment and components with unstable quality. Its self-produced centrifuge modules have inherent defects in the manufacturing process and assembly process, resulting in frequent systematic failures. This objective technical background made Iranian technicians initially more inclined to attribute failures to equipment reliability issues than to targeted cyber attacks [14].

According to the BBC report, "in terms of internal investigation, as the number of centrifuge failures continues to rise, Iran's security services have arrested and prosecuted a number of suspected 'nuclear spies, 'and even executed some engineers in an attempt to curb the attack situation through internal rectification". Of course, it cannot be ruled out that the relevant reports may be the Western media's vilification of Iran [15]. However, judging from the implementation of the "Stuxnetwork" attack, there may be the possibility of internal personnel providing internal information for the United States. However, judging from the fact that it requires Dutch operation engineers to implement the launch, it lacks reliable and reliable "internal ghost" support when it initially implements the cyber attack.

It was not until the end of 2009 to 2010 that Iran gradually confirmed the virus attack and realized that there was a major misjudgment in the early emergency response strategy as the results of the reverse analysis of the "Stuxnet" virus by international network security research institutions were made public one after another. When faced with events beyond the scope of cognition, the parties tend to use their existing knowledge and experience to explain anomalies, but it is difficult to effectively enumerate all possibilities and make reasonable judgments to guide the direction of analysis. Such cognitive biases inevitably lead to valuable emergency response windows being missed.

3 Some Deficiency and Regret of Antiy's Historical Analysis Work

After the "Stuxnet" incident, major manufacturers in the global network security industry (including Kaspersky, Symantec, etc.) have all invested in a technical competition for "Stuxnet" analysis. Through continuous attention and in-depth analysis, the whole picture of this super complex network attack is gradually explained. In the analysis of "Stuxnet", Kaspersky, Symantec and other international manufacturers have shown great strategic patience, determination and analytical strength. In the years after the "Stuxnet" event, more and more continuous analysis results and technical blogs were contributed. Antiy itself is also a Chinese security company that has invested resources in this analysis relay and followed up the analysis for a long time. However, while gaining experience, all the work is bound to have shortcomings and lessons. We look back on Antiy's own analysis work, and there are still some regrets and deficiencies, which are worth summarizing.

3.1 A mistake in our historical analysis

In our analysis report released on September 26, 2010, there was a serious error in the illustration of the spread of "Stuxnet", that is, the MS10-061 was illustrated as an attack on the printer, which was actually an attack on the printing service of the Windows system. Due to the large number of "Stuxnetwork" modules, the function is extremely complex, at that time we mainly focused on the "Stuxnetwork" itself sample operation mechanism and other directions, coupled with the team members at that time were mainly malicious code analysis, so at that time did not accurately analyze the specific mechanism of each vulnerability. For the print service exploit vulnerability, the report writer mistakenly thought that this was an attack against a printer, so the target of this exploit was set as a printer on the drawing. This is a serious technical error that attacks the Windows's print service, not the printer. Such an illustration would lead the reader to think that the printer itself was a process target in the "Stuxnet" attack and could serve as a bridgehead for chain diffusion, leading to related cognitive misunderstandings. To our great uneasiness and regret, this error has been passed on to many documents and books because many other domestic analysis reports, reports and publications have quoted and referred to Antiy's report. Although when reflecting on this matter, some colleagues in the industry humorously said that this kind of mistake was an anti-plagiarism secret note left by Antiy in the report, but from our point of view, this is an unforgivable technical mistake. It also reflects that we should face the analysis work with a more rigorous and realistic attitude.

We draw the wrong original image (3-1) and compare it with the updated image (3-2).

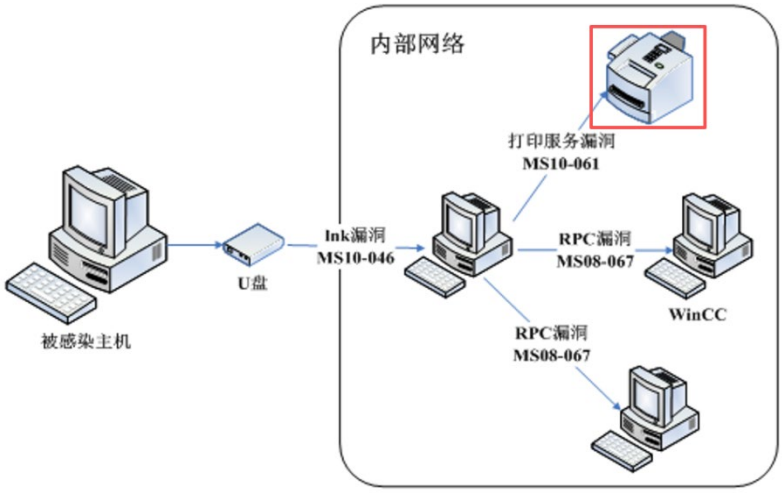


Figure 3-1 Propagation path diagram of "Stuxnet" with serious errors1

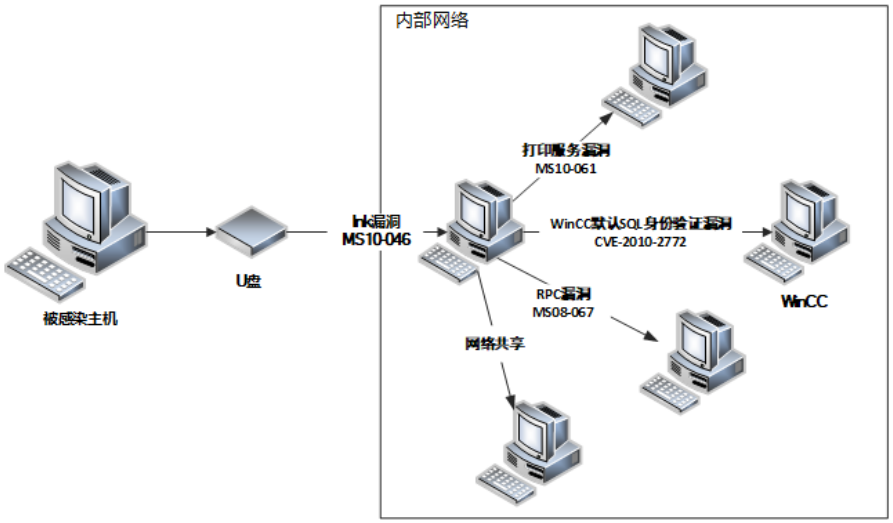


Figure 3-2 Multiple propagation paths of "Stuxnet" (after correction)2

3.2 Missing spectrum of analytical work

For "Stuxnet" and "Stuxnet" homologous associated with the Flame, Duqu, Gauss and other attacks, Antiy history has formed more than ten analysis reports, but looking back at the historical report, the lateral movement of its intranet diffusion, network data analysis is insufficient. Cybersecurity companies, research institutions and individual researchers have contributed dozens of high-quality research articles to this topic. These research literatures cover all aspects of "Stuxnet" from multiple levels. However, looking back at these documents, there are similar problems to Antiy to a certain extent.

Because the "Stuxnet" attack was implemented by relying on highly complex malicious code, the main role of the analysis at that time was naturally the security vendor with deep anti-virus accumulation as the protagonist, but this itself also introduced the method and path dependence of our work as an anti-virus enterprise. The whole analysis work was carried out around the code disassembly analysis of dynamic and static mixture, auxiliary supplement part of its mechanism of action of the complex disk and reduction. From the point of view of the richness of the existing results, the code analysis of the whole module, function, vulnerability exploitation and the mechanism of action is very rich, but the analysis of its horizontal movement and diffusion in the intranet is obviously not enough. Although we have discussed and expanded on why it forms diffusion and propagation in the Nine-Year Re-evaluation and Reflection of the Stuxnetwork Event, the diffusion map that can be formed by the operation law of the horizontal movement of its entire intranet has become a serious defect point in the historical analysis work. Due to various conditions, the relevant analysis has not been effectively extended to the relevant related links, such as the actual situation of the relevant certificate authority embezzled by "Stuxnet", its issuing certificate and issuing environment, why the United States can continue to operate to realize the theft of the certificate, even including whether the location of the certificate theft is in the specific software and hardware enterprise or may be in the issuing authority or the path of certificate issuance, neither has seen a more effective correlation analysis.

3.3 Analysis contest does not really drive the refining of defense laws

Another thing to reflect on is that in this series of analytical work, we have to a certain extent an "analytical competition" mentality with international outstanding companies such as Kaspersky and Symantec.

As one of the earliest safety teams in China to participate in the analysis of "Stuxnet. We have built two versions of the environmental sand table model of "Stuxnet", trying to restore the whole picture of the attack, from the initial infection to the lateral movement, from the payload delivery to the final destruction, each link tries to fill the information gap with technical analysis, including a very fine-grained analysis only on the conditions and control logic of USB ferry. However, the more we analyze, the more we find a reality: "Stuxnet" is not a "virus" or worm or Trojan horse in the traditional sense, but a super software engineering behind it. Its full picture, based on the perspective of reverse analysis, can hardly be fully revealed. This makes the analysis of the "Stuxnet" series inevitably a non-convergent process. Every new analysis may discover new problems, and there will never be a complete answer to all its details. We have invested a lot of manpower and material resources in marathon continuous analysis, which has driven some of the engine detection and defense capabilities. However, there is competition for resources in

analyzing spectrum and capability developing spectrum. When the analysis team spent years tracking the evolution of homology and variation between samples, when researchers repeatedly deliberated on the mechanism of exploitation of a vulnerability, have we ever regarded "analysis" as a substitute for "defense" to some extent?

The sand table model and technical precipitation that we have accumulated in the "Stuxnetwork" analysis are certainly valuable technical achievements. However, the value of these achievements should ultimately be reflected in the methodology that can guide defense practice, rather than just stay at the level of technical research. A deep understanding of the threat of attack, to drive real security progress, is to make the defense system effective against attacks.

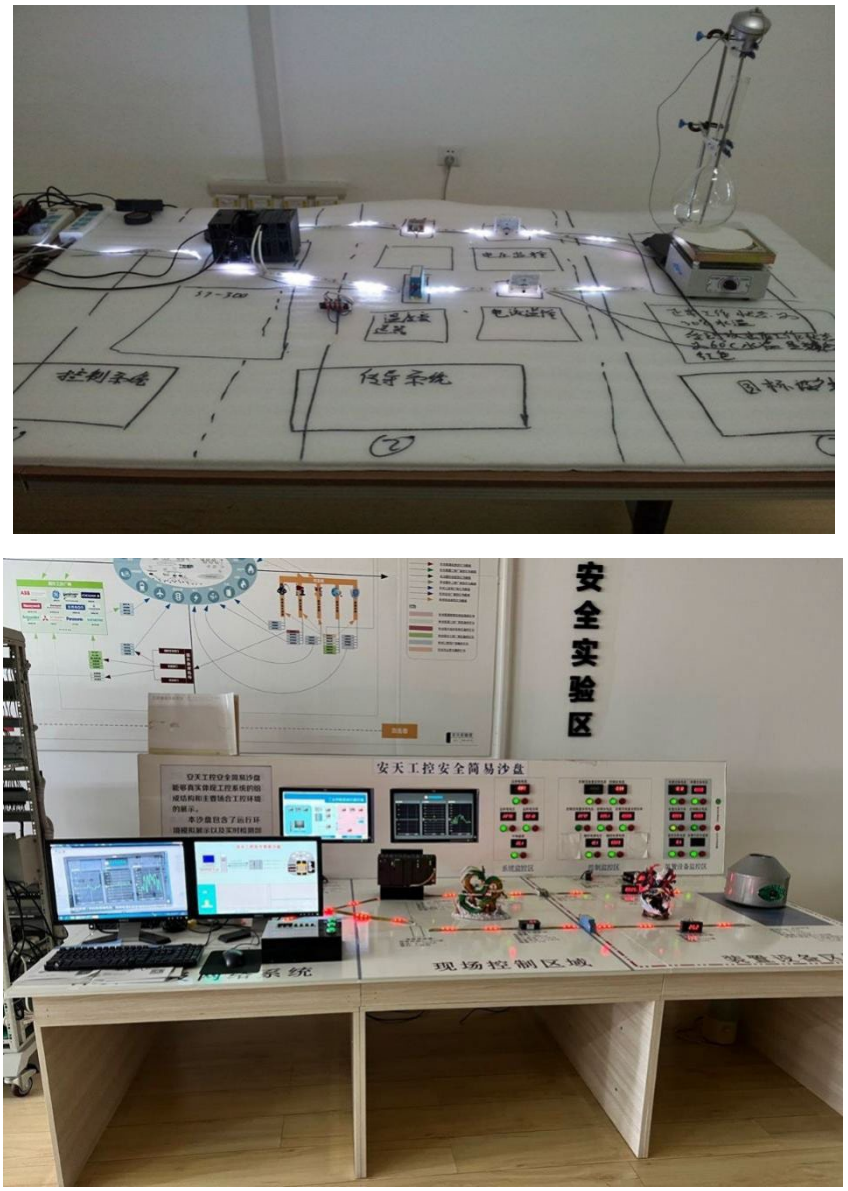


Figure 3-3 Two versions of industrial control sand table used by Antiy for "Stuxnet" analysis.3

Due to the complexity of the "Stuxnet" itself and the focus of global public opinion, the main analysis direction of the "Stuxnet" serves to reveal the details of the sample and attack in greater depth, and the quality of the key details revealed by the main analysis subjects. But how to build a more effective defense from the entire attack process chain, but the lack of high-quality system output. There is no timely drive for the formation of a high-quality, systematic, structured defense framework. Some single-point technologies and methods are exaggerated as "silver bullets" in order to prevent the "Stuxnet" from talking and promoting ".

4 Long-term lessons of the "Stuxnet" incident for network security defense

4.1 Avoidance of "Myth" Attack Activities Lead to Defense Nihilism

The Stuxnet attack itself was indeed an epoch-spanning event. The complete analysis of the mechanism complexity of its malicious code was almost beyond the capabilities of all analysis teams at the time; and the number of vulnerabilities it exploited also reflected the characteristics of using technical resources in a way that Van Fett saturated attacks-These characteristics indeed far exceeded the industry's overall awareness of malicious code and network attacks at the time. It was against this background that the idea that Stuxnet-type attacks were an indefensible "myth" began to spread. It is believed that in the face of such a complex and sophisticated national attack, all kinds of defensive measures are futile-the attacker has unlimited resources and technical capabilities, and the defender can only be "resigned to fate". This view ignores the defensive initiative and initiative, misleads the direction of defense work, and creates a nihilistic dilemma.

The historical analysis and research on "Stuxnet" and the contents of this report just reveal that, as the United States side with absolute supply chain advantages, it also needs to plan and develop attack payloads for a long time, arrange attack kill chains, search for job windows, and precisely implement and manage attack activities in the implementation of attack operations. Even in the background of the "earthquake network", although it is difficult to realize real-time detection and blocking of related attacks, if there are effective security capability deployment and operation and maintenance conditions, it is also an attack that may be detected and blocked in time. A large number of observable behaviors generated during the propagation and operation of "Stuxnet"-abnormal process creation,

suspicious registry modification, communication with external C2 servers-can be captured in systems with perfect detection capabilities. This shows that even if the attack technology is more complex, as long as the trace is left, it may be found and analyzed. And can refine the law of security, adjust the deployment of defense.

The complexity of the "Stuxnet" and the difficulty of analysis reveal, is not the same as the difficulty of defense. The fact that attackers invest significant resources in developing sophisticated attack weapons does not mean that defenders need to fully understand every technical detail of an attack weapon in order to mount an effective defense. Defense is a system deployment that relies on a systematic protection framework to build defense capabilities and form collaborative operation capabilities, especially the implementation of "critical control points" for attack activities. No matter how complex the attack payload is, if it cannot be successfully launched and operated in the target environment, its power cannot be exerted. Secondly, the complexity of the "Stuxnet" is to a large extent to achieve the feasibility of the failure mechanism, rather than simply given to the penetration and the realization of absolute concealment. The attacker needs to accurately understand the centrifuge model, operation logic and working parameters, need to write special payload for Siemens WinCC system and PLC logic controller, and need to design complex attack chain and decision logic to ensure reaching the target. These complexities are the inherent requirements of the attack itself, but from the defense side, these are exactly the "baggage" and burden of the attacker at the confrontation level, this is Antiy CERT's new understanding of "Payload (load, I.e. load)" at the level of attack effectiveness. It is a fundamental logical error to equate the technical complexity of the attack with the difficulty of the defense, and this cognitive bias can lead to ineffective input and self-abandonment by the defender.

For the rejection of real network attack activities, more emphasis should be placed on the load delivery and operation process, rather than on the final constraints on its behavior. Attempting to detect and prevent every possible act of sabotage is desirable, but making it difficult for the attack payload to reach the target environment and gaining access to the target environment makes it impossible for the attack weapon payload to achieve operational coupling-this is the key point of defense.

4.2 We should not only focus on the consequences of paralysis, but also on the threat of long-term concealment.

As a landmark "cyber warfare" event, "Stuxnet" makes people generally believe that the biggest risk of cyber attacks is the destruction of critical infrastructure. There is nothing wrong with the judgment that "causing physical space consequences will lead to greater losses", but "Stuxnet" itself is not a simple cyber attack, but a strike-type

combat operation similar to "withering blade. For example, Lockheed Martin (Lockheed Martin, LMT) researcher Marshall (Michael) put forward the view that "Stuxnet is not APT"-APT attacks pursue long-term latency and concealment to achieve continuous information acquisition, while "Stuxnet" directly caused the destruction of physical facilities and paralyzed, in fact, has constituted a combat operation. Its views have important implications.

The "Stuxnet" incident draws a key difference: the difference between CE/CNE (cyber intelligence operations) and CA/CNA (cyber attack operations). In the Western definition, network intrusion to build connections, continuous information acquisition is called CNE, and only into the physical space impact of the CNA. Once it reaches the CNA stage, it has the characteristics of military combat operations. So, what is the essential difference between these two styles? The key lies in the normalization of the low-intensity confrontation phase, what is the core impact of high-level cyberspace attacks? Is it persistent information and intelligence theft, or the destruction of infrastructure? On this issue, even the U.S. side, which launched the "Stuxnet" attack, has also reflected. On September 13, 2023, the Center for New American Security (CNAS), a US think tank, held a webinar on "Cyber Resilience: Interpreting the US Department of Defense Cyber Strategy in 2023". Dr. John F. Plumb (John F. Plumb) pointed out that they "once believed that the most serious threat to cyberspace was the destruction of key facilities, but later realized that under normal conditions, the greater security risk comes from continuous intelligence acquisition". However, due to the huge sensational effect of "Stuxnet", for a long time, we have simply equated the consequences of high-level cyber attacks with the large-scale destruction of critical infrastructure. This cognitive bias leads to a lack of attention and investment in an equally deadly or even more insidious threat-persistent information and intelligence theft. The harm of this cognitive bias is that in the case of large-scale destruction of key facilities caused by cyber attacks, it is prone to paralysis because there are no events of the same level (or influence) in our country. On the one hand, this may reflect that our key infrastructure network security has a good defense foundation; on the other hand, it also comes from the deterrence of China's strong national strength and military strength, which makes some opponents dare not carry out such activities. But we need to see that this phased "state of peace" can blind us to real threats. This has serious consequences: once the attacker has established a continuous covert control capability, it is only a matter of command and condition triggering. Attackers can master system permissions, remain silent for a long time, continuously collect intelligence, and map asset topology-whether to launch damage depends entirely on the attacker's strategic intentions, and this "uncertainty" itself constitutes a huge "deterrent". More importantly, in high-intensity conflicts and wars, the greater value of network intrusion and intelligence acquisition may not be target damage, but to guide targets for fire strikes, create more favorable strike conditions and assess the effectiveness of strikes.

Thus, in defensive practice, agencies are concerned only with preventing events of apparent consequence: whether there is damage to facilities, whether there is a large-scale power outage, and a serious lack of resources for persistent, hidden deadly threats. This shift in the center of gravity of the defense will result in the consumption of large amounts of resources in the wrong direction. The correct defense idea should be: in the normal network security defense, to prevent intrusion, theft as the main goal, the attacker persistent landing, system control theft, information, intelligence and other data are obtained, as the normal most important and high-level security events. Basic system and data security governance, threat detection and real-time rejection capability building, persistent threat detection and discovery, response process based on baseline enemy thinking, etc. These daily tasks are the key to effectively deal with persistent hidden threats. Effective defense should be able to detect and contain threats when they are still in the hidden and latent stage.

4.3 APT attacks are costly, and the defense side needs to invest more in security.

In our previous study of Stuxnet, we introduced a relevant comparison between Stuxnet attacks and Operation Babylon to show that cyber attacks are a low-cost means when equivalent effects can be achieved. However, the concept of low cost of cyber attacks is compared to the physical cost and social impact cost of implementing firepower strikes, and cyber attacks themselves need to be supported by large-scale costs.

Stuxnet attacks, for example, require a high-level team of architects and development engineers to write highly complex malicious code. The formation of multiple high-level vulnerability exploitation tools requires vulnerability analysis and mining research capabilities, or collection and procurement from relevant channels. In particular, due to the final effect on the actual physical equipment of the centrifuge, and the use of two ways to adjust the valve pressure and adjust the speed, it is necessary to build a relevant physical environment, the formation of a whole set of highly realistic industrial control range to carry out the corresponding verification. All these indicate that high-level network attacks require huge costs.

From the perspective of security defense, facing a high level of persistent network attacks is bound to be a cost confrontation. From the perspective of physical space, the cost of defenders is usually several times that of attackers. This is because the defense needs to cover all possible attack surfaces, and the attacker only needs to choose a weak point to break through-this asymmetry is also present in cyberspace, if not more prominent.

It is difficult to imagine that a security system driven by price wars or even free of charge can effectively defend against such attacks formed through long-term planning and high cost preparation. The value of a security product is

not in the price tag, but in whether it can actually reduce risk. If a cheap security system cannot effectively detect and block attacks, then its "cheap" is actually costly, and even its "security product insecurity" itself constitutes a security risk.

High-quality defense requires investment, including its own security planning, continuous security operations, and the procurement of high-quality security products and services. These all require continuous investment of funds and resources. Security is never a one-time investment, but an ongoing process. The thinking that security is simply regarded as a "cost center" rather than a "guaranteed investment" is an important reason for the lack of security budget. When the security budget is repeatedly compressed, when the security team is regarded as a "spending department" rather than a "value-creating department", the decline in defense capabilities is almost an inevitable result.

Recognizing the high cost and long-cycle readiness of APT attacks helps us to evaluate the need for security investment more rationally. Real security is not "compliance", but needs to be based on one's own enemy situation and match the threat level. When opponents invest heavily in research and development attacks, security investment must also reach the corresponding level-this is not "over-investment", but "peer-to-peer checks and balances".

Network attack and defense confrontation is also an asymmetric "arms race". In this competition, it can not be considered that the outcome can be determined by the amount of investment, but the lack of investment will inevitably lead to innate passivity.

4.4 Effective defense must be a combination of civil, material and technical defense.

An important revelation from the "Stuxnet" incident is that the threat actors faced by high-value targets often launch compound attacks in a combination of people, things and technology. Single-dimensional techniques, especially those that rely solely on cyberspace, are not enough to deal with this composite attack-a lesson that has been repeated in the field of network security. Judging from the process of the "earthquake net" attack, the attacker used various dimensions: in the human dimension, the target node was directly reached through the operation and maintenance personnel; At the object level, the target shooting range was constructed, mobile devices were used as load carriers, and complex attack loads were used. At the technical level, highly complex malicious codes were developed and used. Corresponding to this attack, the defense system must also be multi-dimensional. No single-dimensional defense-no matter how technologically advanced-can effectively counter such a three-dimensional attack.

Pure technical means are limited. No matter how advanced security products are, it is difficult to prevent insiders from being bought; no matter how perfect the network intrusion detection mechanism is, it is difficult to prevent the physical intervention of personnel; no matter how strict access control is, it is difficult to prevent the security risks in the upstream of the supply chain. Technical means can solve technical problems, but they cannot solve the problems of people and management.

People are both the biggest dynamic element and the biggest risk board. Our current civil air defense system is built more on the basis of preventing errors and accidents and incorrect operations, rather than on the basis of limiting enemy thinking. No matter how strict security training is to build a mechanism based on intelligence confrontation and limit response, it cannot completely eliminate the possibility of personnel infiltration. No matter how perfect the audit system is, malicious acts carefully disguised cannot be found; no amount of high-frequency system security checks can prevent insiders from bypassing the prescribed process. In the face of state-level attackers, this passive, exemption-led civil air defense system is clearly not enough.

There are also vulnerabilities in physical security. No matter how strong the computer room is, it can't stop the authorized maintenance personnel. No matter how strict the entrance guard is, it can't prevent the internal personnel who have been bought. No matter how perfect the equipment inspection is, it can't find the carefully hidden hardware back door. In the "Stuxnet" incident, the attacker implanted the virus into the target system through physical contact, which shows that any omission of physical defense may become the entrance of the attack.

Therefore, the combination of civil air defense, physical defense and technical defense is the basic premise of building a complete defense system. These three dimensions are not simply superimposed, but to form an organic whole that supports and compensates for each other. Technical means can make up for the lack of personnel and physical management, the safety awareness of personnel can reduce the risk that technical means can not cover, and physical security measures can provide basic guarantee for technology and personnel management.

4.5 Physical isolation is effective, superstitious isolation is extremely harmful, and complete isolation is impossible.

In the entire development of informatization and applications, physical isolation has long played a key role as a very important compliance management tool. But at the same time, because of its disadvantages of blocking information connection and affecting work efficiency, it is often deeply criticized.

"Stuxnet" itself proves that the physical isolation defense line can be crossed and invaded, but it also reflects the effectiveness of physical isolation (including strict personnel access management) as a security means itself, which can improve the difficulty of attack implementation. If physical isolation does not work, there is no "Stuxnetwork" attackers need to buy the relevant personnel to carry out the proximity operation. But the historical condition under which physical isolation can be effective is that cyberspace, as an artificial space, exists on the basis of physical facilities. In the "Stuxnetwork" era, the form of information assets is more clearly distributed according to the internal and external network, and the internal network assets are carried within the physical boundaries of the organization. Therefore, based on the discontinuity of physical isolation means, it can effectively restrict the network space connection, so as to play a certain role in the attack. But clearly, it is only one of the necessary means against high-value defense targets. Based on what has been pointed out in the previous article, "Stuxnet" is not as unnoticed as in the legend. There are major observable anomalies on the network traffic side or in the host link. The problem faced by the attacked party is that it believes that physical isolation has formed a solid line of defense, thus failing to build an effective security mechanism in the intranet, forming security protection and related observation capabilities on the host, and failing to repair the system's patch vulnerabilities in time, resulting in the physical isolation being broken through and allowed to run amok and achieve operational effectiveness.

At present, we must face up to the increasingly huge modern information infrastructure, especially the digital evolution in the era of artificial intelligence, including industrial systems, which inevitably rely on efficient information exchange, supply chain supply and personnel interaction, which has formed a multi-point open related system. Physical isolation may not constrain all attack activity, but it itself creates a blockage to the closure of security responsiveness and the distribution of security enablement. Therefore, how to integrate physical isolation into the effectiveness-oriented defense capability framework, effectively play the role of physical isolation in the core scene, and reduce the impact of physical isolation on the closed-loop disposal and capability distribution of security response capabilities, and eliminate the psychological paralysis caused by physical isolation is a problem that we must solve at present.

4.6 Defense cornerstones should first be built around endpoints, not sloppy ability generalization

The "Stuxnet" attack reveals the attack risks that modern industrial systems can encounter. Related events have undoubtedly driven the improvement of my country's defense capabilities in industrial systems, and to a certain extent

promoted the development of industrial control security-related technologies and products. The process has created a number of new "boxes".

After combing through the series of attacks started by "Stuxnet", we still find that the overall attack focus of most advanced network attacks is still around key computing nodes (PCs, servers, intelligent terminals, or other workloads). Therefore, the overall defense cornerstone should be built on the host system and workload side, thus making it a minimized security boundary, realize system environment shaping governance, threat detection engine deployment, active defense and rejection capability construction, comprehensive data collection and aggregation to support linkage analysis and response disposal related support. In fact, what we see is that in the whole capacity layout, the system security protection of the end, cloud host and workload has not been taken as the main direction of investment in the industrial development. Anti-virus software, host security software, workload security, etc. have been the hardest hit by insufficient security budget because they are pure software Agent forms. The resources of security defense are generalized and diluted in the super-long list of various box-type products, and the fantasy is to rely on security gateways or network gates to defend the enemy outside the city gate. However, in fact, network attacks can easily penetrate this box-stacked defense and reach the final terminal in encrypted traffic under the common end-to-end form of application. In terms of security defense, there is a more illusory expectation that the superposition of "artificial intelligence" can be grasped at once. When the threat cannot be visible through the deployment of security capabilities, nor can it effectively implement the defensive actions of the target asset in a fine-grained manner, the security AI will become a "brain in a vat" with neither effective sensory input nor action hands and feet ".

Therefore, defense investment needs to be systematically combed around the real attack paradigm and tactical targeting, rather than simply generalizing domain capability investment. It is necessary to minimize protection from the system to the running object based on the security boundary, and rely on artificial intelligence empowerment, relying on the operating system, to build an elastic and adaptive intelligent security defense line.

4.7 Network attacks need to be a mandatory option for abnormal event risk screening and integrated into the process.

In the modern industrial system, production safety has always been a key element. All walks of life have established a sound quality management and accident disposal process. This system has been tested in long-term practice and formed a scientific evolution system. However, the basic idea of this quality process system was formed

in an era when there was no cyber attack. Its original intention was to deal with traditional risks such as equipment failure, operation error and material defect, and did not take cyber attack into consideration. This means that when there is an abnormality in the production process, the quality management system will follow the established path analysis-check the status of the equipment, review the operation record-but rarely consider "whether there is a cyber attack" in the first place ". However, the process system of network threat response investigation is more in the information department and has not yet been integrated with the quality system.

Cyber attacks have penetrated into the hinterland of industrial control systems. If network security simply pursues independent closed loop, it will form two sets of mechanism problems in the whole industrial scene. Cybersecurity teams and quality management departments are fragmented and lack effective collaboration. In this process, a more reasonable solution is to be able to incorporate the possibility that network intrusion is a higher risk into the traditional quality management and zeroing system as a priority in the process of related abnormal events. Only in this way can we quickly enter the correct global branch after encountering network intrusion. At the same time, eliminating the interference items of network attacks in real quality accidents can also make the original process run better.

Incorporating network intrusion into the necessary option and priority of safe production and accident investigation is to raise the original risk awareness that is biased towards internalization to a comprehensive threat awareness. It does not mean to change the existing quality management system, but to add a new dimension of thinking on the basis of the existing system, so that the quality process is more complete.

4.8 The attack does not necessarily exploit vulnerabilities, and do not fantasize about the existence of a complex system without vulnerabilities.

When discussing cybersecurity attacks, a common misconception is that attacks necessarily rely on exploits. This view holds that attacks cannot succeed without vulnerabilities-vulnerabilities are a necessary prerequisite for attacks.

The attacker achieves the effect by completing a chain of processes-from initial access to permission acquisition, from lateral movement to target achievement. In this chain, the exploit is only one of the means that can be used, not the means that must be used. The vulnerability of the attacked target will bring opportunities for the attacker, but it is not a prerequisite for the successful implementation of the attack.

Attackers can directly deliver attack payloads based on user actions. User credentials can be obtained through social engineering; Devices can be directly inserted through physical contact; Backdoors can be implanted through supply chain pollution; Insiders can also be bribed through threats and inducements-none of these attacks rely on traditional exploits. Vulnerabilities are only a choice for an attacker in a particular scenario, not an inevitable choice. From a defensive point of view, the existence of a vulnerability does not equate to the success of an attack. Even if a vulnerability exists, if the attack payload cannot be successfully delivered to the target environment, cannot run properly on the target system, and cannot break through various security detection mechanisms-then the "value" of the vulnerability cannot be realized. This seems simple, but is often overlooked.

Antiy previously pointed out in the study of execution body and operation confrontation: the premise of network attack is the availability of the target system, not the vulnerability (including vulnerabilities). The vast majority of network attacks are the isomorphic behavior of system operation and processing, not the vulnerability utilization behavior. Vulnerabilities (including vulnerabilities) provide one-way availability and behavioral concealment for attackers, and of course they should be focused on. Attacks need to be mitigated by curbing vulnerability, but there is no illusion that they can be eradicated by the demise of vulnerability.

Vulnerabilities are not weapons, they are an attribute of defense targets. Vulnerability exploitation codes and tools are weapons, and their number accounts for only a small proportion of malicious code attack weapons. Self-healing of vulnerabilities and mitigation and prevention of exploits, which are related but not homogeneous defensive actions. Therefore, the focus of defense should focus on the discovery and repair of vulnerabilities, but it should not be used as the whole defense, let alone the illusion of exhaustive discovery of vulnerabilities to ensure "absolute" security. Security defense is not only an internalized self-improvement process, but also an external interaction/engagement process with threat behavior. In the deployment of detection and defense capabilities, regardless of whether there is a vulnerability, it is necessary to ensure that the attack payload is difficult to successfully deliver and run. Including effective application software and supply chain entrance management, strengthen the terminal protection ability and malicious code detection ability, strengthen the network monitoring ability to find abnormal communication, strengthen the behavior analysis ability to identify suspicious activities, etc.-these measures are directly aimed at all aspects of the attack chain to defend. That doesn't mean that bug fixes aren't important-they certainly are. But we shouldn't rely solely on bug fixes for security. In addition to the exploitation of vulnerabilities, the delivery and operation of attack payloads such as malicious code is a necessary key link in the

attack. It is important to pay attention to the detection and blocking of loads and the discovery and repair of vulnerabilities, even more important in some scenarios. Expect our views to make defenders value and think.

4.9 "Known" and "unknown" are not the main perspective of threat response and may be interference items

From the perspective of Stuxnet's use of multiple 0day vulnerabilities, the so-called "known" and "unknown" is not an effective concept of defense-oriented capabilities. This concept tends to bring more confusion than clarity in practice. "Known" and "unknown" itself is a relative concept. It is based on the specific detection and response capabilities of the attacked target as a frame of reference, and is affected by itself and the security capability provider, and there is no unified measurement.

Vulnerability exposure is not the same as getting the attention and fixes of defense agencies. Vulnerabilities that are made public but not patched in time are a more convenient entry point for attackers-a fact that is often overlooked: regardless of whether the vulnerability is exposed or not, as long as the target system has a vulnerability and has not been patched, the attacker can exploit it. Still further, exposure is not meant to be detectable, nor is detectable meant to be defensible. After the vulnerability is made public, if the defender does not update the detection rules or lacks an effective response mechanism, the vulnerability is still available to the attacker. Therefore, the effectiveness of defending against exploits does not depend on whether the vulnerability is exposed or has a CVE number, but on whether the vulnerability exists in the current scenario, whether it has been patched, and whether its exploitation can be effectively prevented.

From the perspective of malicious code defense, there are huge differences in the back-end perception, collection, analysis, and feature engineering operation capabilities of malicious samples from different anti-virus companies, as well as the pre-processing, detection capabilities and update frequency of engines. Because the capture is not consistent, the efficiency of the analysis process is not consistent, and the detection mechanism is not consistent. Whether a malicious code is "known" malicious code or "unknown" malicious code for a vendor is determined by the vendor's own capabilities, and there is no uniform standard. For more security companies, they do not have independent malicious code collection and analysis and engine capabilities, and their product detection and identification capabilities depend on the third-party engine capabilities they use. All these mean that even for the same malicious code sample, there will be differences in its "known", "unknown", detectable and preventable among different security vendors and products. Detected malicious code, if the lack of effective disposal capabilities, the

detection itself has no practical value. However, when the product is placed in a specific user scenario, it is related to whether the user's usage strategy and configuration are updated in time.

Therefore, the "knowledge" and "line" issues in the confrontation are defined from the security protection operation level of the specific asset scenario and the product capabilities of the corresponding security vendor enterprises, at this level, there is never a unified "known" and "unknown" evaluation criteria. Too much emphasis on "known" and "unknown" is actually a kind of "taking knowledge instead of action". Without effective and sustained attention, follow-up and investment, unmanaged "known" vulnerabilities are more effective attack portals, and undetectable "malicious code" is a lower-cost attack weapon. Malicious code infections that have occurred are precisely proof of insufficient system protection capabilities. These basic facts are often ignored. Therefore, ignoring the governance of known vulnerabilities and malicious code, and fantasizing about solving all problems once and for all through an emerging set of innovative mechanisms is a way of looking for "silver bullet" thinking. Such unrealistic thinking is not uncommon in defense scenarios and the security industry. Known does not mean that the protection has been done, and unknown does not mean that it cannot be defended. The real security practice should be: priority must be given to the classification and classification of known vulnerabilities, and priority must be given to the response and zero attribution of malicious code infection events that have occurred. Whether the vulnerability is known or unknown, whether the malicious code is exposed, continue to build detection and defense capabilities. The key is not whether the risks and threats are "known", but whether effective governance is implemented and defense is effective. This is the simple and correct truth.

4.10 Defensive war operations require a war mindset

Looking back on the "Stuxnetwork" attack, it should be pointed out that although the "Stuxnetwork" is used as a representative of the APT incident, according to the US definition of CNE/CE (cyber intelligence operations) and CNA/CA (cyber attack operations), the "Stuxnetwork" is a CNA/CA war operation based on APT means.

From an operational perspective, CNE (Cyber Intelligence Operations) places more emphasis on covert and continuous intelligence acquisition, with the core objectives of long-term lurking, intelligence gathering, and maintaining access-APT (Advanced Persistent Threat) activities are more of the CNE spectrum. However, the goal of "Stuxnet" is to transform the irreversible impact on physical space, causing substantial damage to Iran's nuclear facilities. What war action pursues is to achieve by violent means to bend the opponent to his own will, and to achieve the established goal of killing and destroying physical and social space. Unlike intelligence operations, war operations

have fewer "rules" and "bottom lines"-the attacker can use all necessary means to achieve the intended operational objectives. "Stuxnet" is the product of this logic: it is a combat operation based on cyber intelligence and espionage capabilities.

This means that we cannot examine the "Stuxnet" incident only from the perspective of network attack and defense, and we cannot build a defense system only from the thinking of preventing technical attacks. To deal with war operations, we first need the thinking of war. This is the key reason why we have written "Tactics" and "Strategy" while completing this series of reports "Technical.

We are convinced that:

To crave war is to perish; to neglect war is to risk peril.

Appendix 1: References

[1] Xinhua News Agency. Israel attacks Iran near the office of Iran's supreme leader.(2026-2-28) https://www.news.cn/20260228/fcf17e0d48754f9b827234de6e5e09e1/c.html

[2] Intelligence firms watch for uptick in Iran cyber activity after US, Israel strikes.(2026.3-2) https://www.nextgov.com/cybersecurity/2026/03/how-cyber-command-contributed-operation-epic-fury-against-iran/411818/

[3] An Tian. A comprehensive analysis report on Stuxnet worm attacks on industrial control systems [R/OL]. (2010-9-27) https://www.antiy.com/response/stuxnet/Report_on_the_Worm_Stuxnet_Attack.html

[4] Antiy. Follow-up analysis report on Stuxnet worms [R/OL]. (2010-10-11) https://www.antiy.cn/research/notice&report/research_report/20101011.html

[5] What happened after WinCC? -- Analysis of the Impact of Attacking Industrial Control System on Field Devices [R/OL]. (2012-1-17) https://www.antiy.cn/research/notice&report/research_report/20120117.html

[6] An Tian. Flame Worm Sample Set Analysis Report [R/OL]. (May 31, 2012) https://www.antiy.com/response/flame/Analysis_on_the_Flame.html

[7] Antiy. Explore the Mystery of Duqu Trojan Horse's Life [R/OL]. (September 23, 2013) https://www.antiy.cn/research/notice&report/research_report/261.html

[8] An Tian. Nine-Year Resuming and Thinking of "Stuxnet" Event [R/OL]. (2019-9-30)
https://www.antiy.com/response/20190930.html

[9] Antiy. Speculation and Correlation Analysis of Network Operation Capability Spectrum Behind US Army Invasion of Venezuela [R/OL]. (2026-1-6)
https://www.antiy.com/response/US_military_cyber_ops_in_Venezuela_spectrum_speculation-analysis.html

[10] Yahoo.Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran(2019.9)
https://www.yahoo.com/news/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html

[11] IO. Operation Stuxnet: the cyber attack that changed warfare forever.(2024.11-15)
https://ioplus.nl/en/posts/operation-stuxnet-the-cyber-attack-that-changed-warfare-forever

[12] ESET.Stuxnet Under the Microscope[R/OL]. (2011.1)
https://web-assets.esetstatic.com/wls/en/papers/white-papers/Stuxnet_Under_the_Microscope.pdf

[13] langner.To Kill a Centrifuge[R/OL]. (2013.11)
https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

[14] isis-online. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? [R/OL].(2010.12)
https://isis-online.org/isis-reports/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

[15] BBC.Iran arrests 'nuclear spies' accused of cyber attacks.(2010.10)
https://www.bbc.com/news/world-middle-east-11459468

[16] Virtual Event | Cyber Resiliency: Discussing the 2023 DoD Cyber Strategy.(2023.9.23)
https://www.cnas.org/events/virtual-event-cyber-resiliency-discussing-the-2023-dod-cyber-strategy

[17] Encyclopedia of Antivirus. Worm/Win32.Stuxnet
https://www.virusview.net/malware/Worm/Win32/Stuxnet

[18] Sans.Why Stuxnet Isn't APT. (2011.3.4)
https://digital-forensics.sans.org/blog/2011/03/24/digital-forensics-stuxnet-apt

[19] Symantec.W32.Stuxnet[R/OL].(2010.7)
https://docs.broadcom.com/docs/security-response-w32-stuxnet-dossier-11-enhttps://www.symantec.com/security-center/writeup/2010-071400-3123-99

[20] Antiy. The industrial control system security from the homology of Duqu virus and Stuxnet worm
Antiy Technical Articles Compilation (V) Industrial Control Volume

Appendix 2: About Antiy

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

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

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

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

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