A Technical Analysis of the CrowdStrike Global System Failure

——Contemplating "Falcon's Broken Wings"

Antiy Cloud Security Research Center

Antiy CART

Antiy Offensive and Defensive Labs

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

First draft completed: July 19, 2024, 10:35 p.m.
First published time: July 21, 2024, 4:50 a.m.
This version updated: July 23, 2024, 3:20 p.m.

Scan the QR code to get the latest version of the report.

1 Basic Situation and Impact of the Incident

Starting at noon on July 19, 2024, Beijing time, users in many parts of the world reported on social platforms such as X (formerly Twitter), Facebook, and Weibo that computers using Microsoft systems had blue screens, and business systems in at least 20 countries in industries such as transportation, finance, medical care, and retail or public services were affected. The reason is that a large number of hosts using the Windows operating system of CrowdStrike's terminal security products have experienced system crash failures, namely "Blue Screen of Death" (BSOD), causing the computer system to fail to operate normally. The faulty terminals are not limited to desktop terminals, but cover a large number of servers and cloud nodes, including causing the interruption of several important Microsoft and AWS cloud services and tenant services. Moreover, the relevant hosts will automatically enter the blue screen state after restarting, **forming a repeated crash closed loop**. This incident is the most widespread information system catastrophic event in the world this year, and it is also the largest-scale security disaster event caused by security products themselves. The consequences of the incident far exceed the historical security incidents caused by security products such as the Symantec mistakenly killing the Chinese version of Windows in 2007, which caused the system blue screen incident. At 19:00 Beijing time on July 19, a mixed analysis team composed of personnel from the Cloud Security Center, Security Research and Emergency Response Center, and Attack and Defense Laboratory of Antiy conducted follow-up analysis, reported the progress of analysis and judgment to the management and emergency departments in a timely manner, developed the CrowdStrike_Crash_Fix emergency response tool to assist users in handling threats, and released this analysis report.

CrowdStrike is one of the major cloud and endpoint security vendors in the United States. It was founded in 2011. In June 2024, its market value was close to $100 billion, making it one of the largest cybersecurity listed companies in the world. Its cloud-native endpoint protection platform, CrowdStrike Falcon, has pioneered multi-tenant, cloud-native, and intelligent security solutions, combining next-generation antivirus software, threat intelligence, endpoint detection and response (EDR), device control, threat intelligence search and IT security operations, incident response, and proactive services. The platform has independent modules for managing system vulnerabilities and mobile terminal detection and response, and also provides 19 cloud modules through a SaaS model across multiple large security markets, including enterprise endpoint security, cloud security, managed security services, security and IT operations, threat intelligence, identity protection, and log management.

CrowdStrike explained that the incorrect configuration update pushed by the company's endpoint security software "Falcon Sensor" had a compatibility issue with the Windows system, causing a blue screen on the computer installed with the security software. Later, the company's representative replied on its customer support platform that the company's engineering department has determined that the problem is related to the "content deployment" function of its product. The incorrect update has been revoked and the matter is being actively investigated.

This is a domino effect incident caused by a widely used security product failure, which caused a large number of host systems to crash and a large number of infrastructure systems to be unable to provide services. The incident caused the interruption of business system services of organizations in at least 20 countries and regions, including the United States, the United Kingdom, Australia, Canada, and Japan, and affected industries or public services such as aviation transportation, medical services, media, banking and financial services, retail, and catering in many parts of the world.

Table 1-1 Affected industries, countries/regions, and relevant institutions

Areas covered	Related organizations
Air Transport	Some airlines in the United States, Australia, the United Kingdom, the Netherlands, India, the Czech Republic, Hungary, Spain, Hong Kong, Switzerland, etc. experienced flight delays or airport service interruptions. Delta Air Lines, American Airlines and Allegiant Air announced the suspension of all flights.
Media Communications	Israel Post, French TV channels TF1, TFX, LCI and Canal+ Group networks, Irish national broadcaster RTÉ, Canadian Broadcasting Corporation, Vodafone Group, phone and internet service provider Bouygues Telecom, and many more.
Transportation	Australian freight train operator Aurizon, West Japan Railway Company, Malaysian railway operator KTMB, British Rail, Australia's Hunter Line and Southern Highlands Line regional trains, etc.
Banking and Financial Services	Royal Bank of Canada, TD Bank, Reserve Bank of India, State Bank of India, DBS Bank of Singapore, Bradesco Bank of Brazil, Westpac Banking Corporation, ANZ Bank, Commonwealth Bank of Canada, Bendigo Bank, etc.
Retail	German supermarket chain Tegut, some McDonald's and Starbucks, Dick's Sporting Goods, British grocery chain Waitrose, New Zealand's Foodstuffs and Woolworths supermarkets, etc.
Medical Services	Memorial Sloan Kettering Cancer Center, the UK National Health Service, two hospitals in Lübeck and Kiel, Germany, some hospitals in North America, etc.
…	…

For more details on the main affected areas, see Appendix II: List of affected organizations .

The incident had little impact on domestic government and enterprise organizations, mainly because CrowdStrike is a product that is banned from sale in mainland China. The main foreign-funded enterprises and some

enterprises using Microsoft data centers in China were affected by the failure. For example, the check-in and check-out services of the Conrad Hotel in Shanghai, which is under the Hilton Hotel Group, were affected.

Of course, this also created obstacles for the team's analytical work.

2 Emergency Response Solutions

2.1 Manually Delete Problematic Files (Original Solution)

CrowdStrike's business support system is highly online. It released a solution on a webpage visible only to registered customers. Non-customers cannot access it, but affected users publicly shared the official solution:

1. Restart Windows to safe mode or recovery mode, or boot with WinPE;
2. Open the "%systemroot%\System32\drivers\CrowdStrike" folder;
3. Delete the files named "C-00000291*.sys" (*represents any character);
4. Restart the system normally.

The following is a more complete description of the incident and the solution. For users in similar environments such as public clouds, you can use the method of "backing up and mounting the disk to a temporary virtual system" in the figure below to handle the error file.

At the same time, for users who use BitLocker volume encryption, they need to prepare the recovery key and then enter the safe mode to operate.

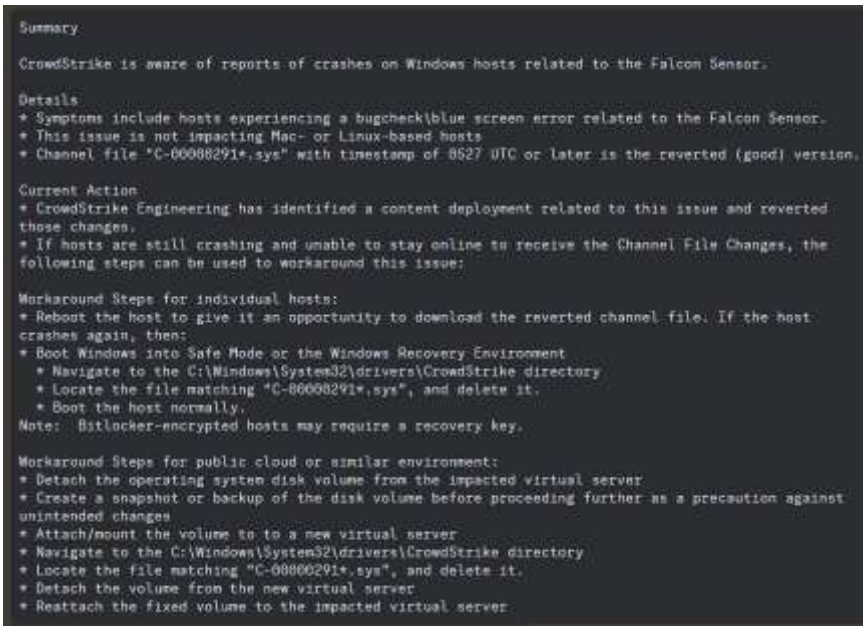

Figure 2-1Event description and solution

2.2 CrowdStrike _Crash_Fix (Released by Antiy)

On the evening of July 19, Antiy CERT released a temporary disposal tool, CrowdStrike _Crash_Fix, which has been uploaded to the Antiy vertical response platform (https://vs2.antiy.cn/) . After Windows is restarted to safe mode or recovery mode, this tool can be used to process abnormal files with one click. According to feedback from affected users, this tool can significantly save the time required for disposal. (The current tool has been updated to version V0.5 , which already supports disposal based on WinPE media boot).

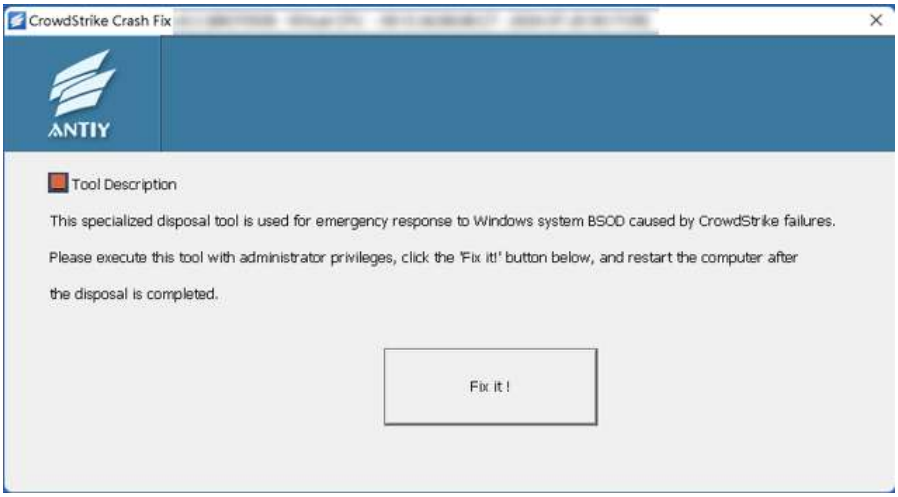

Figure 2-2Antiy temporary solution tool CrowdStrike_Crash_Fix

3 Technical Analysis of Events

3.1 CrowdStrike's Working Mechanism

CrowdStrike Falcon Sensor is a very typical EDR product with kernel (driver) level primary defense. After installation/preinstallation on the Windows platform, the corresponding program files are installed to the directory pointed to by %ProgramFiles%\CrowdStrike, and its driver and important data files are installed to the directory of %SystemRoot%\System32\drivers\CrowdStrike. Its main defense capability comes from multiple system kernel driver modules. Among them, CSBoot.sys is the Early Launch Anti-Malware (ELAM) function module of the Windows operating system (a mechanism that uses Microsoft interfaces to implement security software to load before malicious code to ensure the safety of the boot chain); CSFirmwareAnalysis.sys is the firmware security module; CSAgent.sys is the core function module of the primary protection; cspcm4.sys is the policy analysis module. The order of loading is CSBoot.sys, CSFirmwareAnalysis.sys, CSDeviceControl.sys, CSAgent.sys, and cspcm4.sys.

Table 3-1 List of CrowdStrike's main programs and driver modules

Classification	File name	Description
App	CSFalconService.exe	Main service processes
	CSFalconController.exe	Background control program
	CSFirmwareAnalysisSupportTool.exe	Firmware Analysis Tools
	CSDeviceControlSupportTool.exe	External device control
Drivers and kernel modules	CSBoot.sys	The operating system's Early Launch Anti-Malware (ELAM) feature module protects driver loading
	csfirmwareanaltsis.sys	Firmware Security Module
	cspcm4.sys	The kernel registers the callback interface module to provide a callback interface for CSAgent.sys
	Config.sys	Module for managing policy configuration
	CSAgent.sys	The main functional modules include file filtering, network filtering, and process control
	CSDeviceControl.sys	USB device filter driver

The module CSAgent.sys where the blue screen occurs is its main functional module, which carries dual digital signatures from CrowdStrike and Microsoft. According to the preliminary analysis of Antiy's attack and defense laboratory, it contains functions such as file monitoring, operation monitoring, and network filtering, and is the core

driver of its active defense and host firewall. The basic operating principle is: after the driver is loaded, it first reads the policy configuration, and makes release and blocking operations for file reading and writing, process loading, memory execution, API call, network access and other actions according to the policy; in order to quickly and agilely fight against threats and update protection capabilities in real time, excellent host security software often supports online distribution, dynamic reception, and instant analysis of effective and issued policies, so that configurations can be flexibly changed to handle emergencies without restarting the system. CrowdStrike uses this mechanism. However, since the driver directly calls the system kernel interface , the stability of the module will have a direct impact on the system kernel. It may be due to an improper policy configuration. When parsing and executing the policy, the synchronization mechanism between the system and the system is not properly handled, or the system resources are improperly allocated, causing the system deadlock problem and triggering the blue screen protection .

3.2 Analysis and Speculation on Relevant File Formats and Mechanisms

The error code of the "blue screen" fault in this incident is "PAGE_FAULT_IN_NONPAGED_AREA", and the driver with the error in the blue screen information is "CSAgent.sys". Combined with the official disposal suggestion to delete the "C-00000291*.sys**"** file, it can be clearly determined that **the direct cause of this incident is due to the loading and parsing of the "C-00000291*.sys" file with incorrect settings by** "CSAgent.sys".

In the same directory as CSAgent.sys and other drivers (%Windows%\%System32% \drivers\CrowdStrike), there are multiple files with the first two letters of the file name being " C- " and all with the extension sys. We need to seriously point out that **these C-*.sys -named files are not driver files** . **Some online analyses of this incident also refer to these as system files or driver files, which may be a misinterpretation of the extension**. System files (or driver files) with the extension sys in Windows are PE executable files with the file header |4D 5A|. For example, the crashed CSAgent.sys is a PE file. In the corresponding directory, files with the extension "sys" and the uniform beginning with "C-" should be a type of data file in a custom format. These files all have the file header |AA AA AA AA| and do not have the ability to execute, or at least do not have the ability to execute directly under the system. In the information released by CrowdStrike, these files are called "Channel Files" and are stated to be configuration files of Falcon Sensor, which are used for daily updates of CrowdStrike's defense mechanism. Therefore, it can be basically judged that the relevant files are mainly similar to data files of rules/policies/baselines.

These "channel files" are named in the format of C-xxxxxxxx-00000000-xxxxxxxx.sys. The first character C in the file is presumably the initials of CrowdStrike. There are three Arabic numerals, each 8 bits long. The first numeral

is the channel number, which corresponds to the value at fixed offset 0x6 in the file after conversion to hexadecimal. The second numeral value of all collected files is fixed to 0, so it can only be guessed that it corresponds to the value at fixed offset 0xC (all values are also zero). The third numeral value corresponds to the value at fixed offset 0x10 in the file after conversion to hexadecimal .

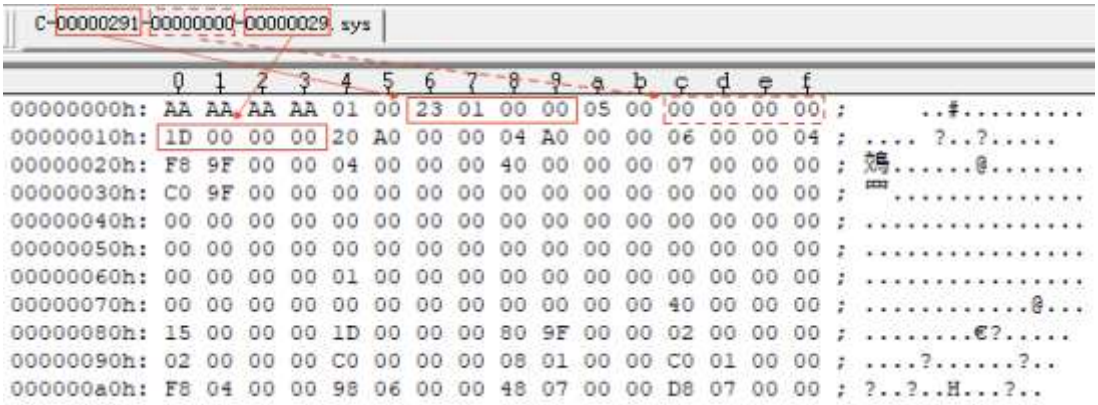

Figure 3-1 The correspondence between the file header of the channel file corresponding to the accident and the value and file name therein

Due to the complex mechanism of related products, the specific functions of these channel files have not yet been determined. Observing the file content, it is determined that the file has undergone a certain encoding transformation, but it does not seem to be encrypted using a grouping algorithm. We analyzed the naming rules of the files and guessed the meaning as follows: the first section of numbers is the channel number, which is the number of its rule/configuration library, and the corresponding value range is set for the rule/configuration classification, the second section is the reserved section, and the third section is the number of times the rule/configuration library is updated (i.e., version).

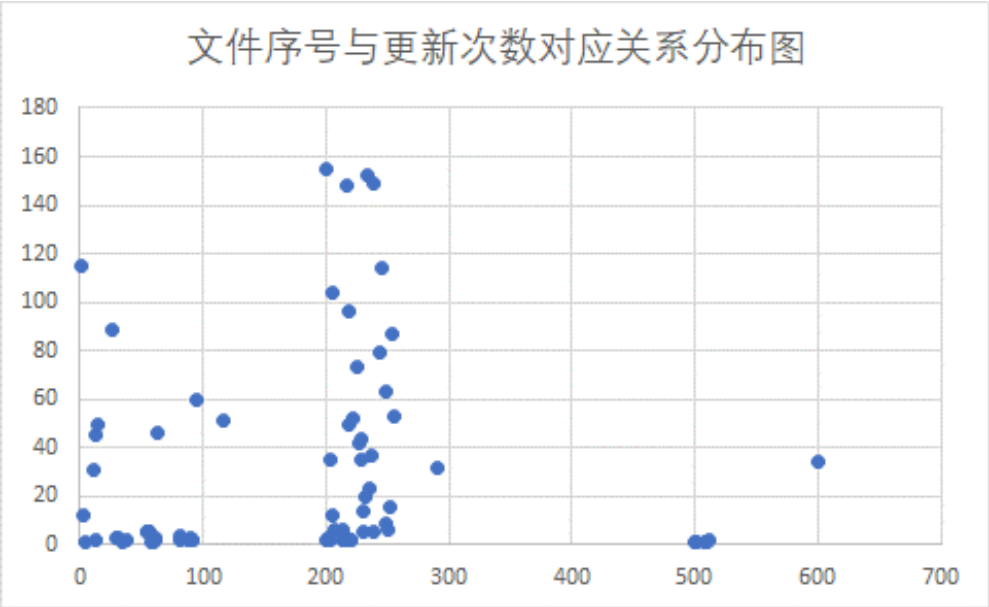

Figure 3-2 C-series file type serial number (guess) and update count (guess) relationship distribution

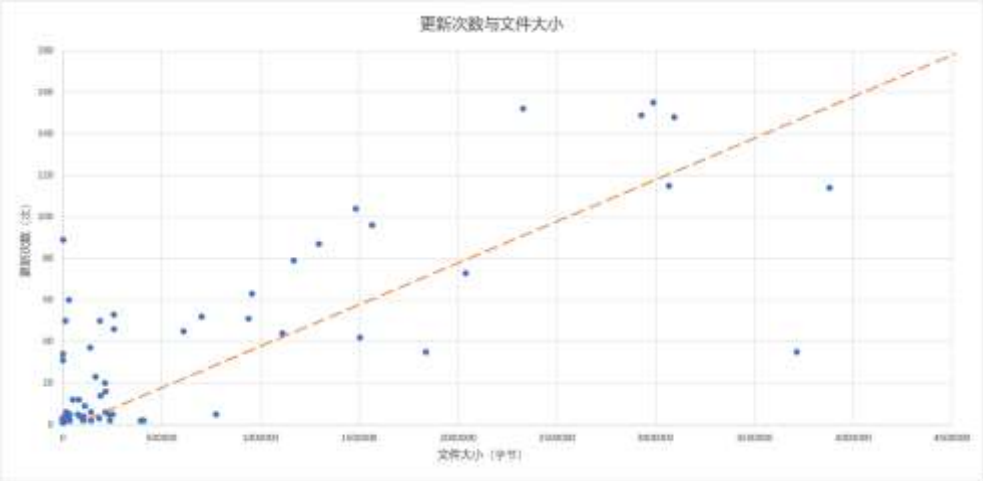

Figure 3-3 Relationship between the number of updates (guessing) and file size of C-series files

Based on the above two statistical analyses, we can see that the pipe numbers are continuously distributed according to the value range. For relatively large files, we guess that the larger the number of updates, the more likely it is that our guess about the file naming rules is valid.

CrowdStrike 's official explanation for the relevant vulnerabilities is:

The files involved this time that start with "C-00000291" and have an extension of ".sys" are configuration files, also known as "Channel Files". These files are Falcon These files are updated several times a day in daily operations based on the daily threat techniques and tactics monitored by CrowdStrike.

The file starts with C, and each "channel file" is assigned a unique number as an identifier. The one affected this

time is 291, and the related files start with "C-00000291-" and use ".sys" as the extension. Although they use the driver file extension, these files are not drivers. 291 channel files control Falcon's "Named Pipes" on Windows. "Named Pipe)" is a common technology, usually used in Windows environment for inter-process communication or inter-system communication.

The file was updated at 04:09 UTC, triggered by a malicious named pipe used in a newly detected cyberattack C2 framework. However, a logic error was triggered during the update, causing the operating system to crash.

Antiy's analysis team further speculated that the 291 file contained detection and rejection rules for attacks related to named pipes, which may target named pipe enumeration, named pipe privilege escalation, named pipe forgery, etc. We are also analyzing whether Microsoft's patch this month is related to the pipe vulnerability, and whether the recently disclosed vulnerability is the origin of this "failed update".

3.3 Efforts to Reproduce and Analyze Related Issues

Since CrowdStrike prohibits downloading related products in mainland China, the analysis team only has the early version of the related software after the incident. Antiy Offense and Defense Laboratory relies on relatively limited resources to obtain the problematic sys files and combine them for analysis. However, due to the limitations of the analysis environment, stable vulnerability reproduction has not been achieved at present.

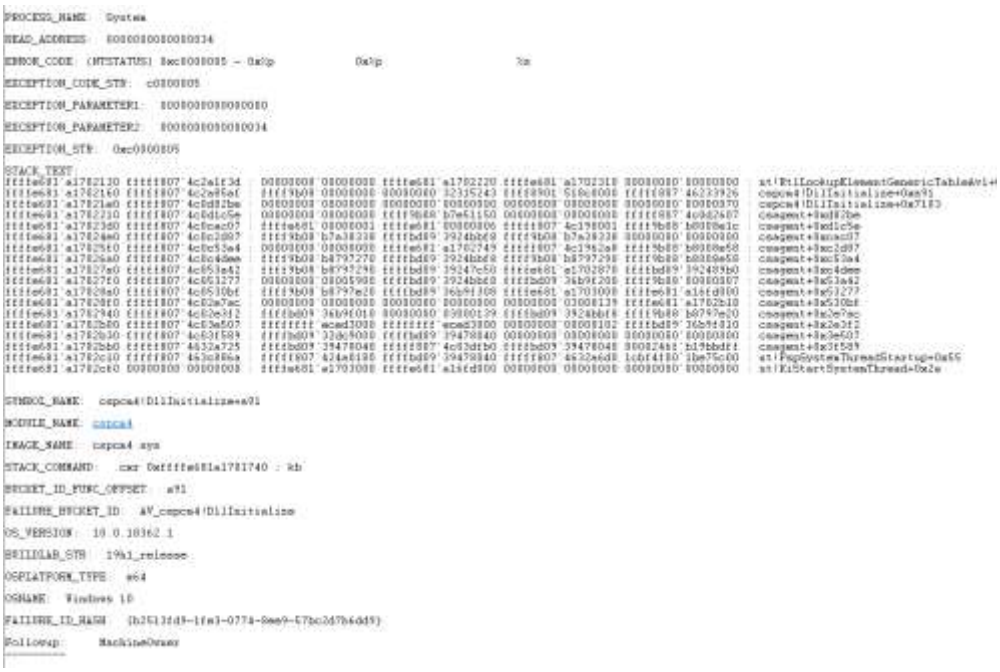

Figure 3-4 Antiy Attack and Defense Lab reproduced the blue screen caused by the CrowdStrike driver not correctly handling system synchronization

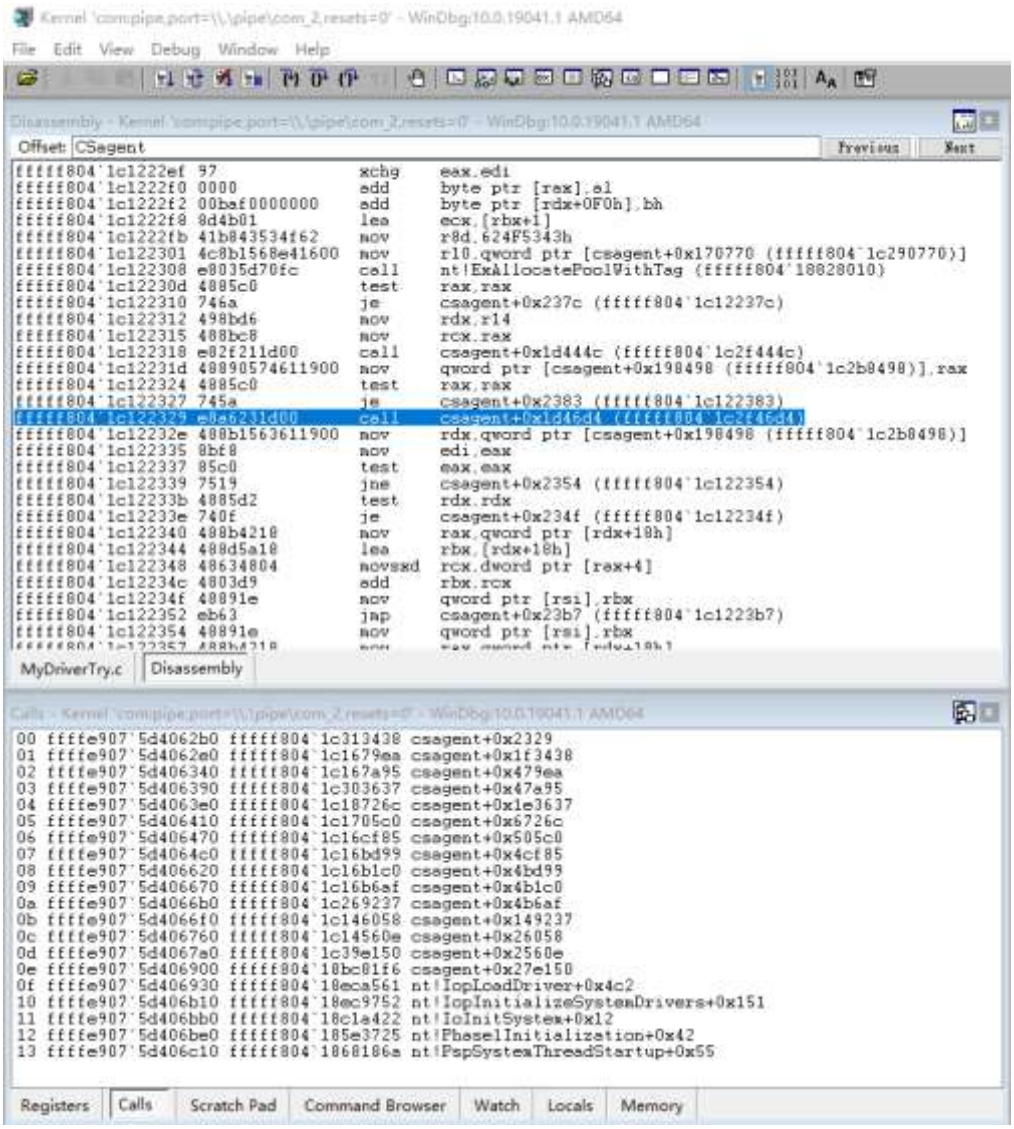

Figure 3-5 Antiy engineers analyze dual-machine debugging of CSAgent module

3.4 Technical Judgment

The direct cause of the incident is already relatively clear. It is a problem with the data configuration file C-00000291*.sys loaded by the CSAgent.sys module of the CrowdStrike product widely installed on a large number of Windows hosts , which leads to a system crash.

Previously, some people doubted whether the problem was caused by Microsoft's patch release, but according to the current public information from all parties. CrowdStrike has admitted that the problem came from the release of a configuration update for named pipes, namely C-*291.sys, at 04:09 UTC on July 19, which immediately caused Windows virtual machines on Microsoft Azure cloud to start experiencing such restart and crash problems. At 05:27 UTC, CrowdStrike revoked this update, and hosts started thereafter will not be affected. Based on the above time process, it can be generally considered that CrowdStrike has confirmed that the incident came from itself.

From the long-term external impression, CrowdStrike has long been facing complex host and workload scenarios, has extensive customer deployment, and its products need to face the strict quality control requirements of Western military and political customers and large international corporate customers. Therefore, its testing and quality control system should be relatively complete, and compatibility testing with the operating system must be its focus. However, it is impossible to verify whether its testing system can reach every rule policy update in a fine-grained manner, and whether it can adhere to strategies such as gray distribution and monitoring/rollback. Is this incident a "black swan" or a "gray rhino". Whether there are still major process problems in its detection and release mechanism, or whether a "black hole-like" time difference has occurred due to specific reasons, we need to wait for more information to be publicly judged. At the same time, we also need to continue to pay attention to and analyze whether this is a clever supply chain prefabricated attack incident.

4 Reflections on the "Falcon's Broken Wings" Incident

1、 **The possibility that the incident originated from a supply chain attack cannot be ruled out, and at least a new threat model is revealed:** although CrowdStrike gave an official explanation for this incident that this was not a network security incident, but a quality accident. However, we still believe that the existing information alone cannot rule out that this was a serious security software supply chain attack. Since security products are often in a key position in the defense system, such as: network boundaries (such as security gateways), real-time monitoring (such as host antivirus and protection software) or above business processes (such as identity authentication), attacks on security software, especially attacks on the supply chain system of security software, may have more serious consequences than attacks on application software or application software supply chains. SolarWinds' supply chain attack shows us the possibility of invading the development environment to establish a downstream lateral movement bridgehead on a large scale, and this incident shows the risk of using the security software supply chain to achieve large-scale collapse and paralysis. This construction can be completely independent of injected code, but can use the security product's parsing mechanism for configuration, library, and data to cause collapse or DoS through parsing errors or process anomalies.

2、 **Facing the security of hosts and workloads is a cornerstone requirement for network security:** This incident is the result of the coupling of CrowdStrike's huge global installed base and the role of the Windows system. But we should not only focus on the accident itself. It is also necessary to see that the threat detection and defense capabilities on the host system side are a rigid link that must be strengthened. The foundation of CrowdStrike's

rapid development is derived from the failure of traditional security boundaries caused by the rise of advanced computing architecture. Security confrontation has shifted from focusing on network detection and interception to defending the enemy outside the city gate to the deep waters where malicious code, hybrid execution body attacks, vulnerability combination exploits and social engineering phishing on the host system side must be fully dealt with. With the widespread use of digital transformation, asset cloudification, ubiquitous access and encryption protocols, traditional access control boundaries or data exchange boundaries such as firewalls and network gates have collapsed completely, and the cornerstone of security is returning to the host system side. System security capabilities need to be extended in cloud hosts, virtualization, and containers along with the extension of modern computing structures, and it is also necessary to further strengthen the security protection of traditional terminals, industrial and dedicated scene workstations, mobile devices, etc. The modern defense system must not only build a defense depth, but also a mesh linkage system. Let the single-point protection capabilities of each host and workload system **form an organization and elasticity**, so that the attacker can be sensed at one point, and their payload and tactics will be quickly captured and converted into intelligence sharing, and quickly form the defense capabilities of other nodes. It is under this general trend that the traditional international Big AV companies continue to maintain their strong presence based on the profound accumulation of malicious code detection and kernel defense. It also enables CrowdStrike to achieve rapid development and rise. The focus of this incident should not only be on the security of security products themselves. Instead, we should pay more attention to the long-standing problem in China, which is the inefficient protection caused by insufficient attention to the construction of security capabilities on the host system side and lack of investment. In some scenarios, in the real scenario, terminal system infection viruses, worms, and macro viruses occur one after another, while the planning is discussing unknown detection, APT protection and artificial intelligence. Some host security products lack reliable malicious code detection capabilities. In order to reduce costs, they generally use the open source anti-virus engine ClamAV, which has seriously insufficient detection capabilities; they even ignore supply chain risks and directly embed foreign anti-virus engines in binary without commercial authorization. Some products lack effective driver protection and blocking mechanisms, and can only collect information through a few Ring3 HOOKs, and basically cannot see hidden attack behaviors. In terms of host configuration reinforcement, many products can only manage dozens of configuration points. In contrast, the security specifications of the US STIG have an average of more than 600 security configuration points for each operating system. In the face of this gap, it is meaningless to start a mocking mode for CrowdStrike. Instead, we should face up to the widespread lack of protection on the host security side. Security protection capabilities

must be continuously strengthened on the system side, and a minimized security boundary must be built. It is increasingly difficult to achieve defense value by stacking boxes. With advanced computing architecture, the deep integration of system security and threat detection capabilities is the future of security.

3、**Security products, including the development environment and the entire life cycle of security products, need to be highly valued:** Since application software and platforms have higher user visibility and are related to user business continuity, network managers often pay more attention to the update testing and deployment process of application software, especially platform systems. In order to combat threats and the attenuation of capabilities after deployment, security software needs to be upgraded more frequently, such as virus libraries, policy libraries, and vulnerability libraries. Since these upgrades are basically run automatically in the background, they are often blind spots in their own testing and black boxes in customer-side scenarios. Since security products have security functions, they are easy to bring users a sense of trust, but the security functions of security products are not equivalent to the security of the security products themselves. If security vendors do not pay attention to the security of their own products, more functions will bring greater insecurity. But at the same time, it is also recommended that users do not panic about capability upgrades due to this incident and refuse to upgrade. If security software cannot be upgraded in time, relative threats will evolve and monitoring and protection capabilities will rapidly attenuate. This brings a larger window of opportunity for attack breakthroughs, comprehensively improves the success rate of attackers, and causes users to avoid accidental risks while leading to inevitable risks.

4、**Driver-level primary defense is necessary, but it needs to be more reliable, robust and secure:** From the perspective of protection from physical hosts to virtualization, despite such major security incidents, we still firmly believe that driver-level primary defense is necessary. Although security protection based on drivers and kernel modules does have a greater risk of causing system reliability, the security and stability of kernel-level protection should be guaranteed through more automatic and comprehensive testing, rather than throwing the baby out with the bathwater. Without kernel-level primary defense, relying solely on the HOOK and collection points at the Ring3 level, it is not only almost difficult to intercept and block threats, but even impossible to achieve effective threat perception, and may be easily deleted or uninstalled by attackers. Although this type of protection reduces the risk of underlying system failures to a certain extent, it brings the customer scenario into a state where it may be penetrated by attackers at any time. The Agent of system security products should be better modularized, allowing users to choose between underlying protection or lightweight monitoring based on

their defense capabilities and resource utilization, rather than amplifying users' fear of driver-level primary defense and bringing users into a risky situation of weak defense. Of course, we also believe that the design, implementation, and rule operation of driver-level defense must be done with great caution to intercept as many threats as possible before they run, and to avoid entering a memory confrontation state as much as possible. This is also an important guide for our execution body governance philosophy.

5、**Modern computing structures are likely to further migrate from virtualization to containers:** Among workload solutions, virtualization solutions are relatively heavy-loaded, and once underlying security issues occur, they are difficult to repair. For example, even after the public cloud virtual machine in this accident is restarted, it will blue screen again. Because it cannot connect to the remote desktop, it is naturally impossible to recover by entering safe mode. In comparison, the combination of container + canary release can relatively reduce update/deployment failures. It is predicted that after this incident, the process of using container technology for independent workloads will be greatly accelerated, except for data centers and edge clouds. And virtualization support is a good thing for the relatively less than ideal trust-building architecture. But at the same time, traditional endpoint security vendors who simply rely on the security of physical hosts to virtualization to support cloud solutions face new challenges that are difficult to meet container security requirements. Always following the evolution of advanced computing architectures and protecting advanced computing architectures are important guarantees for the long-term success of security vendors.

6、**We have no capital to hope for the best:** American oligarchic capital and politicians have tried their best to repeatedly discredit China on cybersecurity issues, promote the decoupling of China and the United States, and continue to create rifts between the Chinese and American cybersecurity industries, which has made the cybersecurity industry irreversibly move towards camps. In particular, CrowdStrike has repeatedly participated in activities to discredit China, and has also shown indifference and arrogance in the face of this major global event, which makes us have great antipathy towards it. But we still believe that although such a serious incident has occurred, it cannot cover up CrowdStrike's super strength in product development and operation, and it is still one of the best security companies in the world. As a security company that also uses malicious code detection and analysis as its basic capabilities, platform + AI empowerment as its operating support, and host system security as its cornerstone scenario, **Antiy has no capital to gloat over major events that have occurred in international peers, but must regard this incident as a common lesson for the industry**. System security is a product form that is deeply coupled with the protected object, and we will maintain a deeper respect for user

scenarios. For the Chinese cybersecurity industry, this disaster happened outside of us, which does not mean that we have passed the "big test". We can only say that the risks that we really need to deal with are still lurking in the near future. I also believe that colleagues who are engaged in system security are brave enough to actively respond to the huge challenges facing system security and are committed to the research, development, creation and operation of advanced security capabilities. We should not shrink back because of the extremely high stability and reliability requirements of high-level drivers and kernel module defenses, and instead hype concepts such as lightweight agents; we should not avoid the necessary construction costs because it requires huge investment to strengthen our own defense environment and code security throughout the life cycle. We should not be indifferent, self-promoting, or even gloating over other people's misfortunes; for ourselves, we should find our own improvement points from other people's events, and while continuing to improve the security capabilities and protection effects on the system side, continue to strengthen our own security left shift and assist customers in improving the capability distribution operation process. This is the responsibility that responsible cybersecurity companies must bear!

From another perspective, domestic government and enterprise organizations have a huge user base of Windows hosts, **and they were almost unaffected by such a large-scale incident, which shows the great significance of China's network security industry and technological self-reliance.** Although China's network security industry system fell into a state of low-level, oversaturated competition when the market was not fully developed, we will surely grow into a decisive and powerful industrial force in the process of developing new quality productivity.

Appendix 1: References

[1]. Analysis of the Incident Regarding Symantec's Killing of Chinese Xp System Files, Antiy CERT, 2007

[2]. CrowdStrike Update Pushing Windows Machines Into a BSOD Loop
https://cybersecuritynews.com/CrowdStrike-update-bsod-loop/

[3]. Tech Alert Windows crashes related to Falcon Sensor
https://supportportal.CrowdStrike.com/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19

[4]. BSOD error in latest CrowdStrike update
https://www.reddit.com/r/CrowdStrike/comments/1e6vmkf/comment/ldvwkbn/

Appendix II: List of Affected Organizations

Victim Organization	Industry	Headquarters	Affected Situations
United Airlines	Airline Services	USA	Temporary grounding of all aircraft
Delta Air Lines	Airline Services	USA	Temporary suspension of flight schedule
American Airlines Ground Station	Airline Services	USA	Temporary grounding of all aircraft
Alaska	Emergency Services	USA	Service interruption
Arizona	Emergency Services	USA	Service interruption
911 Services in New Hampshire	Emergency Services	USA	Service interruption
Hospital electronic medical record system	Medical	USA	Massive computer failure
Sky News	Media	U.K.	Suspension
China-Britain Business Council	Media	U.K.	Suspension
Edinburgh Airport	Airport	U.K.	Automatic boarding system failed
Gatwick Airport	Airport	U.K.	Flight delays
NHS services	Health Services	U.K.	Unable to view and manage medical records, fill and manage prescriptions, or schedule appointments
London Stock Exchange	Financial Services	U.K.	Unable to push news updates on its website
Ladbrokes Coral	Retailers	U.K.	
A British railway company	Transportation	U.K.	
Conrad Shanghai	Serve	U.K.	Unable to check in or check out
ABC	Media	Australia	
SBS	Media	Australia	
Seven Network	Media	Australia	
Nine Network	Media	Australia	
Qantas	Airline Services	Australia	
Virgin Australia	Airline Services	Australia	
Jetstar Airways	Airline Services	Australia	
Sydney Airport	Airport	Australia	Affecting the operations of some airlines
Melbourne Airport	Airport	Australia	This affects the check-in procedure. Passengers are advised to consult the relevant airlines.
Woolworths	Supermarket	Australia	Payment system down
Coles	Supermarket	Australia	Payment system down
National Australia Bank	Bank	Australia	Applications Affected
ANZ Bank	Bank	Australia	Applications Affected

Commonwealth Bank	Bank	Australia	Applications Affected
Bendigo Bank	Bank	Australia	Applications Affected
Suncorp	Bank	Australia	Applications Affected
KFC Australia	Food and Beverage	Australia	Payment system down
Self-service checkout system	Retailers	Australia	Payment system down
TD Canada Trust Mobile App	Bank	Canada	
Universal Studios Osaka	Serve	Japan	All systems down
Osaka Mushroom Restaurant	Food and Beverage	Japan	All systems down
McDonald's Japan	Food and Beverage	Japan	All systems down
West Japan Railway Company	Transportation	Japan	Unable to obtain train location information
Train ticket purchase	Transportation	Belgium	Tickets for public transportation cannot be sold
Digital Bulletin	Transportation	Belgium	
JOE	Media	Belgium	
QMusic	Media	Belgium	
Brussels Airport	Airport	Belgium	
Charleroi Airport	Airport	Belgium	
A Belgian bank	Finance	Belgium	
A Belgian postal service	Serve	Belgium	
TF1	TV channels	France	
TFX	TV channels	France	
LCI	TV channels	France	
Canal+	TV channels	France	
Systems for the 2024 Paris Olympics	Application System	France	The issuance of uniforms and certificates was affected, slowing down operations. The certification counter at the press center was closed and security checks could only be done manually to check names.
Air Traffic Control	Transport	Croatia	
Central Health Information System	Medical	Croatia	
Lufthansa	Airline Services	Germany	There is a problem with the "Information and Booking Inquiry" function on the company website
Berlin Airport	Airport	Germany	Some flights are delayed or cancelled
University Hospital of Holstein	Medical	Germany	
Hong Kong International Airport	Airport	Hong Kong Special Administrative Region	Unable to check in automatically, must use manual check-in instead
Cathay Pacific	Airline Services	Hong Kong Special	

		Administrative Region	
Hong Kong Express	Airline Services	Hong Kong Special Administrative Region	
Hong Kong Airlines	Airline Services	Hong Kong Special Administrative Region	
Vistara Airlines	Airline Services	India	IT service disruption
Air India	Airline Services	India	IT service disruption
IndiGo	Airline Services	India	IT service disruption
Alkasa Airlines	Airline Services	India	IT service disruption
SpiceJet	Airline Services	India	IT service disruption
Oracle	IT	India	Device stuck in boot loop and cannot recover
Nokia	IT	India	Device stuck in boot loop and cannot recover
Magen David Adom Hospital: Sheba Hospital	Medical	Israel	Emergency service hotlines affected
Laniado Hospital	Medical	Israel	Increased waiting times and delayed surgery
Rambam Hospital	Medical	Israel	Increased waiting times and delayed surgery
Pharmaceutical companies	Medical	Israel	Complete suspension of production
Israel Post	Serve	Israel	
Railway operator KTMB's ticketing system	Railway Transportation	Malaysia	A technical problem occurred
Transavia Airlines	Airline Services	Netherlands	Service interruption
Royal Airways	Airline Services	Netherlands	Service interruption
Schiphol Airport	Airport	Netherlands	
KNAB Bank	Bank	Netherlands	
ANZ Bank	Finance	New Zealand	
ASB	Finance	New Zealand	
Bank of New Zealand	Finance	New Zealand	
Westpac Banking Corporation	Finance	New Zealand	
Woolworths	Retail Services	New Zealand	Payment system down
Auckland Transport	Transportation	New Zealand	
Christchurch Airport	Airport	New Zealand	
Cebu Pacific flights	Airline Services	the Philippines	Flight delays
Jeju Air	Airline Services	South Korea	
Changi Airport	Airport	Singapore	Service interruption

ENAIRE's Aena	Airline Services	Spain	IT service disruption
Zurich Airport	Airport	Switzerland	No landing allowed
Prague Airport	Airport	Czech Republic	Check-in system interrupted, flight delayed
Amazon	Cloud Services	USA	Internal service systems and companies using AWS services

Appendix 3: Timeline and Summary of Information from All Parties

1. Media Coverage of Developments in the Situation

On July 18, technology media Windows Latest published an article saying that some netizens reported that they encountered errors such as 0x80d02002, 0x800f081f, and 0x80073cf3 many times during the installation of Windows 11's July cumulative update KB5040442. Some netizens also reported that they installed the KB5040442 update three times in a row, and the 0x80d02002 error was reported each time. After the CrowdStrike incident, related information attracted attention, but there is currently no evidence to prove that the two incidents are related.

Starting at approximately 21:56 UTC on July 18, some Azure customers experienced service outages in the central U.S., involving management operations, connectivity, and availability failures for multiple services. After the CrowdStrike incident, related information attracted attention. However, Microsoft stated that the incident had nothing to do with CrowdStrike.

On July 19, 04:09 UTC (12:09 Beijing time), CrowdStrike released a sensor configuration update for Windows systems. This configuration update is part of the Falcon platform protection mechanism. This update triggered a logic error, causing a blue screen of death on the affected system. At 06:48 UTC, Google Compute Engine also reported this issue. The sensor configuration update that caused the system crash was fixed at 13:27 UTC on July 19.

On July 19, Microsoft said: "We are aware of an issue affecting virtual machines running Windows Client and Windows Server running CrowdStrike's Falcon software, which may experience a bug check (BSOD, blue screen of death) and get stuck in a restart state. We estimate that the impact began around 19:00 UTC (Universal Standard Time) on July 18."

On July 19, the Federal Aviation Administration (FAA) issued an alert stating that American Airlines, United Airlines and Delta Airlines have requested the FAA to implement a global grounding of all flights. The FAA asked air traffic controllers to inform pilots that the airlines are currently experiencing communication problems.

On the morning of July 19, CrowdStrike founder and CEO George Kurtz said in an interview with NBC's "Today" program: "We deeply apologize for the impact on customers, visitors and everyone else affected, including our company itself." In addition, Kurtz said that many customers have restarted their systems to resume operations, but some systems that cannot be automatically restored may take some time, and the company will ensure that every customer's system can be fully restored.

On the afternoon of July 19, the Hong Kong Airport Authority said that due to a Microsoft system failure, the affected airlines at the airport had to switch to manual check-in procedures, and flight operations were not affected for the time being. The affected airlines switched to manual check-in procedures and activated the emergency response mechanism to follow up, calling on passengers to leave enough time.

At 17:45 on July 19, George Kurtz responded on social media X: "CrowdStrike is actively working with customers affected by a flaw found in a single content update for Windows hosts. Mac and Linux hosts are not affected. This is not a security incident or a cyber attack. The issue has been identified, isolated, and a fix has been deployed. "

On the evening of July 19, Microsoft said the root cause had been resolved. The official account Microsoft 365 Status posted on the X (original Twitter) platform: "The root cause has been fixed, but residual effects continue to affect some Microsoft 365 applications and services. We are taking additional mitigation measures to help."

2. Relevant Expert Opinions

The Guardian quoted Troy Hunt, a well-known cybersecurity consultant, as saying that this could be "the largest IT failure in history." "I don't think it's too early to draw a conclusion: this will be the largest IT failure in history," he wrote on the social media platform X (original Twitter). "This is basically what we all worried about with the Y2K problem, except that it really happened this time."

Dan Ives , an analyst at Wedbush Securities, believes that this incident will have a significant negative impact on CrowdStrike and may give its competitors the opportunity to gain more market share. "This is obviously a major blow to CrowdStrike, and it must take effective measures in the coming weeks and months to restore the trust of its customers and the market."

Industry network security experts analyzed that the blue screen failure was most likely caused by an erroneous program in the antivirus software, which caused a program error in the Windows system, thereby triggering the self-protection mechanism of the Windows system.

"The widespread computer crashes show how reliant the world's technology systems are on software from a handful of companies, including Microsoft and CrowdStrike," said Marie Vasek, assistant professor at the University College London's computer science department. "The problem here is that Microsoft is the standard software that everyone uses, and the vulnerability in CrowdStrike was deployed into every system."

Elon Musk said on social media that he would delete all CrowdStrike software from all Tesla systems, and attached an AI-generated picture of a "CrowdStrike computer room on fire." He then added, "Unfortunately, many of our suppliers and logistics companies are using it."

Australian Home Affairs Minister Clare O'Neill issued a statement saying, "The company has informed us that most issues should be resolved through the fixes they provide, but given the scale and nature of this incident, it may take some time to resolve. All levels of government are closely involved and the focus is on bringing together affected parties and ensuring that the government develops a solution as quickly as possible. We will provide further updates as necessary."

3. Interference Information Analysis

After the incident, a web user posted a post and a video claiming that he was a new employee of CrowdStrike on the day of the incident and the mastermind behind the incident. He also claimed that he was fired because of the incident. The post has been viewed more than 10 million times within a few hours, which shows the wide impact of this "blue screen" incident. However, the information related to the user shows that its authenticity is very low, and its identity as a CrowdStrike employee is also likely to be fake. It is possible that he is a funny blogger like Onion News.

Figure 0-1Posts and replies from people claiming to be CrowdStrike employees

For example, some users discovered that this person was likely to deliberately create "fake news" based on his historical personal profile.

Figure 0-2The falsification clues of this person pretending to be a CrowdStrike employee

Appendix IV: Institutions Involved in the Preparation of This Report

Department	Introduction
 Antiy Cloud Security Center	Responsible for the product development and product marketing support of UWP family cloud security products such as host security, container security, and micro-isolation, as well as security research and security rules/model production in cloud scenarios. The department totem is a white swan, which means to have lofty aspirations, constantly challenge oneself, and climb to the top.
 Antiy CERT	Responsible for the continuous capture, tracking, and analysis of threat events and actors such as APT attacks, targeted ransomware attacks, and black and gray industry crimes, promoting the transformation of threat analysis results into the detection and defense capabilities of Antiy Engine and production services, and transforming the judgment of threat events and trends into knowledge results for the government and the public to understand threat activities. Support Antiy security services and other scenarios for in-depth security analysis needs. The department totem is the Northeast Leopard, which has a keen sense of smell, is fierce and sturdy, acts quickly, and wins every battle.
 Antiy Attack and Defense Labs	Affiliated to Antiy Security Service Center, it supports the red-blue confrontation and vulnerability library support work, and supports the improvement of the security capabilities of related production line products through capability operation and security research. Responsible for the aggregation and reuse of the company's existing product security capability-related rules and test samples to form a virtuous closed loop, responsible for attack and defense research to improve attack and defense capabilities and vulnerability mining support capabilities. At present, the department reuses the Antiy Service Center's department totem woodpecker, which is diligent and meticulous, guards the deep forest and environment, cares for every leaf, and does not let a pest go.

Appendix V: 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.