VENAFI®

// APT41 Perfects Code Signing Abuse to Escalate Supply Chain Attacks

// The Rise of Code Signing as a Major Attack Vector

Extensive research has found that compromised code signing certificates used in supply chain attacks are the primary goal of Chinese threat actors APT41, also known as Winnti Group. Recent analysis shows that this group spent the last decade honing attack methods to compromise code signing keys and certificates in "low value" targets like gaming and adware organizations. These certificates are then used in a wide variety of targeted cyberespionage attacks in the software, hardware, media, healthcare, high-tech and telecommunications sectors.

APT41 attackers are disciplined software developers who recognize that the vulnerabilities in most software build environments are ripe for exploitation. In addition, they have discovered that infiltrating the software build pipelines of software providers is a huge force multiplier in any attack—since successfully compromising commercial software is an extremely efficient way to infiltrate a large number of the software providers' customers. By taking advantage of the lax security controls in software development pipelines and subverting the power of trust in network security models, APT41 has been able to execute attacks using stolen code signing keys and certificates to compromise high-profile targets and remain undetected on their victims' networks for months or, in some cases, years.

Figure 1: Industries targeted by APT41 between 2012-2019, according to FireEye

The research in this white paper shows that code signing keys and certificates are such powerful attack weapons that they now appear to be the primary goal of many APT41 activities. APT41 has spent years patiently building, testing and refining the tactics and techniques required to steal code signing materials, which then become a shared resource for use in targeted attacks by APT41 attackers. These extremely powerful techniques, tactics and protocols are extremely difficult to defend against and leave every organization that uses commercial software at risk.

// Introduction: Code Signing and Threat Actors

Signed code is used to confirm the software publisher's identity to ensure that the code is issued by a trusted software publisher and has not been tampered with, so it's safe to run on your network. Users and security tools typically trust signed code even when the software developer may not be known to them and the certificate used to sign the code comes from an unknown issuer.

Malicious code that uses a legitimate code signing certificate from a trusted developer will not only allow adversaries to execute code on a secured system, but also enable the malicious code to go unnoticed. Attackers will go to many lengths to steal them. Adversaries target developers and development environments where security controls are lax. Once they gain access to these environments, they can pivot into production environments to steal valuable information. If they are able to successfully compromise companies that build commercial software, attackers can also compromise the development pipeline directly by injecting malicious code into legitimate software or corrupting updates in supply chain attacks that also compromise the victim's customers.

What is APT41?

APT41 most likely consists of a superset of groups (see Appendix I) involving several cyberespionage contractors working for the Chinese state while still carrying out criminal, financially motivated activities for profit, likely with some form of implicit approval from officials. Looking at the indicators of compromise and intelligence artifacts, the activities associated with criminal motivations and personal gain can be easily distinguished from the same actor operating in the interest of a nation-state. For that reason, some security vendors have separated the two sets of activities (as in the case of CrowdStrike and Symantec).[1]

// APT41: One Set Strategy, Two Objectives

The cyberespionage activity of APT41 is mostly focused on the theft of source code, software code signing certificates, intellectual property, customer data, internal technology documentation and valuable business information. These same set of activities also facilitate financially-motivated schemes, including ransomware, cryptojacking (abusing compromised systems to mine cryptocurrencies like Bitcoin) and virtual currencies manipulation. The financially motivated activity has primarily focused on the video game and adware industry.

APT41 Tactics, Techniques, and Procedures (TTPs)

Like many cyberespionage groups, APT41 is a sophisticated, creative and well-resourced adversary. However, this group uses highly sophisticated attack methods when they are targeting "low level" targets. In other words, APT41 is unique among China-based threat actors because they leverage specially crafted, non-public malware typically reserved for espionage operations in activities for financial gain, that appear to be outside the scope of state-sponsored missions. This includes the use of Linux rootkits and Master Boot Record (MBR) bootkits on Windows systems to hide their malware and maintain persistence on victim systems—these TTPs are generally reserved for espionage operations.[2]

Initial access:

A preferred way of entry for APT41, is by compromising the supply chain of a commercial software vendor in order to get to their selected targets.

Other common tactics used by APT41 include spear-phishing with malicious attachments to gain access to a target network. Over the past few years, their skills have matured, and they now use multiple exploits for existing vulnerabilities in popular products like Citrix, Cisco and Zoho for initial access, privilege escalation and execution.

Post exploitation:

After compromise, APT41 attempts to spread laterally in the network using stolen credentials and various reconnaissance tools, focusing their efforts on finding code signing certificates. As part of this process, they can compromise hundreds of systems and use dozens of unique pieces of malware including backdoors, credential stealers, keyloggers and rootkits.[3]

The secondary goals of the attackers depend on the victim organization. In gaming-related organizations the group goes after personal or financial gain through manipulation or theft of in-game virtual currencies and attempts to deploy ransomware. With non-gaming victims, they go after intellectual property such as user, technology or clinical data.

Toolset:

APT41 has been observed using at least 46 different code families and tools (See Appendix II). The most relevant tools are highlighted here:

1. **HIGHNOON:** One of APT41's primary weapons; used as a backdoor; includes a loader, dynamic-link library (DLL), and a rootkit; also used often by APT17.
2. **HIGHNOON.BIN:** Modified version of Windows DLL apphelp.dll, used for persistence.
3. **HIGHNOON.LITE:** Standalone, non-persistent version of HIGHNOON, can download and execute memory-resident modules after C2 authentication.
4. **PHOTO:** DLL backdoor that conducts system reconnaissance.
5. **COLDJAVA:** Backdoor that inserts shellcode and Black Coffee variant into the Windows registry.
6. **Black Coffee:** Has multiple capabilities, from reverse shell, file enumeration, and deletion to C2 communication through legitimate websites, and obfuscating traffic.
7. **China Chopper:** Code injection web shell that can execute Microsoft .NET code within HTTP POST commands.
8. **SOGU:** Backdoor.
9. **Jumpall:** Malware dropper which is known to have dropped variants of HIGHNOON, ZXSHELL, and SOGU.
10. **HOMEUNIX:** Launcher for download plugins used by many other Chinese espionage groups such as APT1, APT10, APT17, APT18, and APT20.
11. **LIFEBOAT:** Backdoor, communicates with C2 server via HTTP.
12. **ZXSHELL:** Backdoor.
13. **POTROAST:** Backdoor.
14. **SWEETCANDLE:** Downloader that can download and execute payload from C2 server.[4]

// Modus Operandi: The Anatomy of an APT41 Attack

APT41 specifically targets the production environment of software development companies. Using advanced Tactic, Techniques and Procedures (TTPs) in the exploitation phase of their attack, the group attempts to move laterally within the target's networks to gain access to the production environment, in order to steal source code and digital certificates, which they use in future campaigns. To enable their lateral movement, the group uses cross-platform attacks, moving between operating systems like Windows, Linux and Android.[5]

They then use their access to the production environments to get gain access to higher level targets by compromising the supply chain of the initial victim, injecting malicious code into legitimate commercial software that is then distributed to organizations who use the software. Initial attack targets are commonly software and gaming organizations in United States, Japan, South Korea and China, while later stage high-profile targets tend to be politically motivated or high-value technology organizations.

Who's Really Behind APT41?

Researchers assess with high confidence that APT41 and all the associated groups working under its umbrella are operating on behalf of the Chinese state intelligence apparatus. This assessment is based on months and years of network traffic captures and forensic investigations conducted by security experts over the past decade, the group's TTPs, observed attack infrastructure and links between all the previously published intelligence. Other indicators that have contributed to this assessment also include the reliance on malware used exclusively by Chinese espionage operators, the use of Chinese-language strings within the code, time zone and operational time.[6]

Moreover, APT41's targeting supports China's long-term economic and political goals as well as military development objectives, including research and development of computer components (motherboards, processors, servers), cloud computing technologies, healthcare and pharmaceutical and others.[7]

Some researchers assess with moderate confidence that the group is constituted of contractors tasked by the Chinese government to conduct espionage operations. This assessment is because some of the individuals attributed to the group have advertised their skills and services for hire in the past (see more about the indictment in Appendix III). This, along with the fact that the group is known to be using the same malware in both financial- and espionage-motivated operations, could support this assessment since individuals directly employed by the state are perhaps less likely to use the same attack tools for personal financial gain without scrutiny from the state.[8]

Initial Goal: Stealing Code Signing Keys and Certificates

The theft of code signing keys and certificates appears to be the primary goal of all the different activities operating under the shared goals of the group's umbrella. Malicious files signed with valid digital certificates can circumvent automated scanning or block security controls and bypass Windows group policies that restrict unsigned code from running on the system. Even when detected, malicious files signed by a digital certificate from a trusted vendor or associated business are less likely to be flagged by security controls and draw suspicion from human analysts.

For this reason, stealing private code signing keys and then using them to sign malware and other tools for upcoming attacks against other victims remains the preferred modus operandi of APT41.

The group uses legitimate code signing certificates to sign their malicious code to ensure compatibility with targeted systems and avoid detection because this approach guarantees a successful attack. Most of the digital certificates used by the group have been valid unrevoked certificates stolen from East Asia-based game development studios and were signed very close to the certificate issue date— this strongly suggests that they had access to the private key or build environment of the compromised company.[9]

Researchers from Kaspersky, who were first to report on this group in 2013, believe that all the stolen certificates they found originated all from the same group and that the group must have close contacts with other Chinese threat groups or that they sell the certificates on the black market in China.[10]

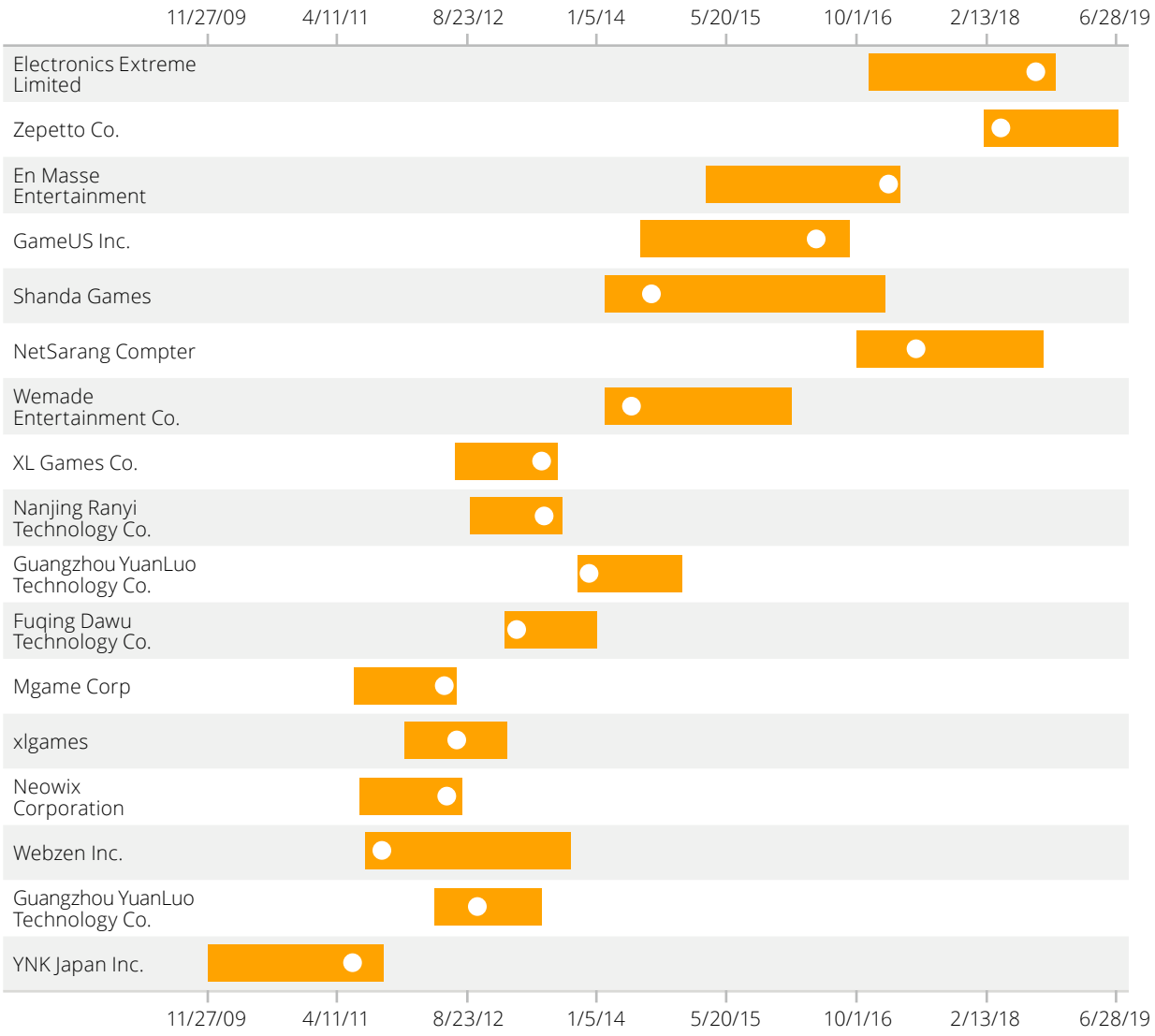


Figure 2: Observed use of code signing certificates from FireEye report

Kaspersky discovered more than a dozen compromised digital certificates which were subsequently used to sign malware deployed in attacks on other higher priority targets.[11]

FireEye researchers noted that in some cases APT41 signed malware samples with digital certificates that were just about to expire, indicating that they were actively managing and prioritizing a library of digital certificates stolen for this purpose.

BlackBerry intelligence researchers also noticed that in 2020 the group has shifted from signing malware with certificates stolen from gaming development companies to signing malware with certificates stolen from adware vendors, resulting in very low detection rates. They believe that this was being done to bypass network defenders by hiding malware within the high volume of innocuous adware alerts large organizations typically receive in any given day.

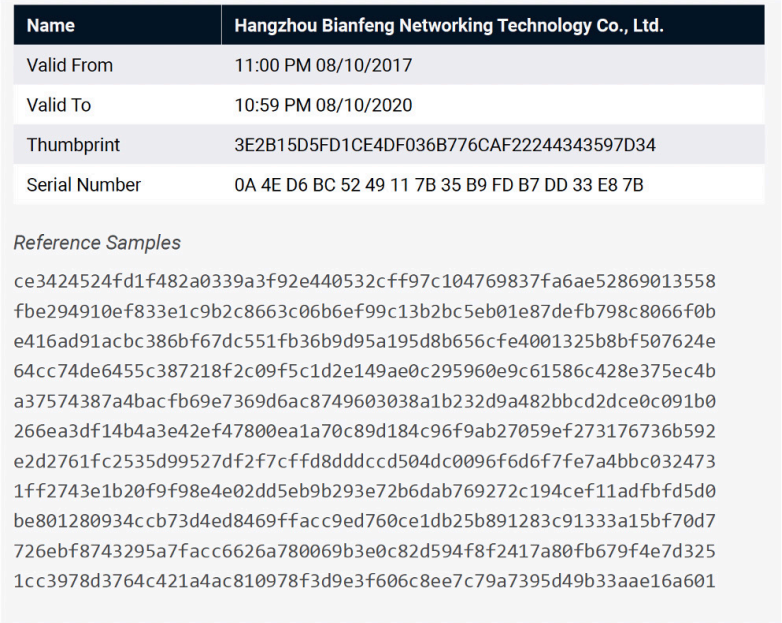
Although using code signing certificates that belong to adware developers seems counterproductive because antivirus vendors would most likely flag it, BlackBerry researchers believe these types of modifications are directly targeting the triage process of incident response and blue team members, who due to alert fatigue, might easily disregard adware alerts.

Which Industries Does Apt41 Target?

The group has been observed targeting the following sectors:

- Software development
- Hardware manufacturers
- Telecommunication
- Media
- Video game
- Non-profit organizations
- Universities
- Think tanks
- Retail
- Travel services
- Virtual currencies
- Healthcare
- Biomedical and pharmaceutical
- Foreign governments
- Aviation
- Pro-democracy politicians and activists

The primary targets for these attacks have been in the United States and east Asia. However, Germany, Indonesia, the Russian Federation, South Korea, China, Sweden, Thailand, Turkey, Japan and Hong Kong have also been targeted as well as organizations in other countries.



Name	Hangzhou Bianfeng Networking Technology Co., Ltd.
Valid From	11:00 PM 08/10/2017
Valid To	10:59 PM 08/10/2020
Thumbprint	3E2B15D5FD1CE4DF036B776CAF22244343597D34
Serial Number	0A 4E D6 BC 52 49 11 7B 35 B9 FD B7 DD 33 E8 7B

Reference Samples

```
ce3424524fd1f482a0339a3f92e440532cff97c104769837fa6ae52869013558
fbe294910ef833e1c9b2c8663c06b6ef99c13b2bc5eb01e87defb798c8066f0b
e416ad91acbc386bf67dc551fb36b9d95a195d8b656cfe4001325b8bf507624e
64cc74de6455c387218f2c09f5c1d2e149ae0c295960e9c61586c428e375ec4b
a37574387a4bacfb69e7369d6ac8749603038a1b232d9a482bbcd2dce0c091b0
266ea3df14b4a3e42ef47800ea1a70c89d184c96f9ab27059ef273176736b592
e2d2761fc2535d99527df2f7cffd8dddccd504dc0096f6d6f7fe7a4bbc032473
1ff2743e1b20f9f98e4e02dd5eb9b293e72b6dab769272c194cef11adfbfd5d0
be801280934ccb73d4ed8469ffacc9ed760ce1db25b891283c91333a15bf70d7
726ebf8743295a7facc6626a780069b3e0c82d594f8f2417a80fb679f4e7d325
1cc3978d3764c421a4ac810978f3d9e3f606c8ee7c79a7395d49b33aae16a601
```

Figure 3: Example of a stolen code signing certificate and Windows reference sample from BlackBerry report

It is not clear if every single key and certificate used in APT41's activity was actually stolen by the same group. It's difficult to gauge to what extent APT41 is actively stealing code signing keys and certificates or buying some of them from underground marketplaces or other Chinese counterparts. However, it is clear that using code signing certificates is the preferred modus operandi of the group because it ensures much higher success rates in attacks against high-level targets.

Payload: Engineering Supply Chain Attacks

APT41 does not confine their activities to stealing code signing materials. They also strive to compromise the whole code signing infrastructure and software development environment. Since 2017, the group's operations have included a series of supply chain compromises. They have a long history of carrying out such operations against the video game development industry, but they no longer confine their attacks to this industry.

Once the attackers gain access to the internal network of a commercial software vendor, the group strives to get a foothold in the production environment and insert a backdoor to legitimate server software packages used by hundreds of companies worldwide.

After successfully executing multiple software supply chain compromises, the attackers distributed backdoored software to its third-party customers who were tricked into installing malicious code signed by a legitimate certificate. The second-stage payloads are then deployed to a very specific and limited set of victim systems that are intentionally highly obfuscated to make it harder to pinpoint the identity of the organizations they are targeting.

APT41 is reported to be responsible for several high-profile supply-chain attacks against the software industry which lead to the distribution of trojanized software to more victims:

Timeline

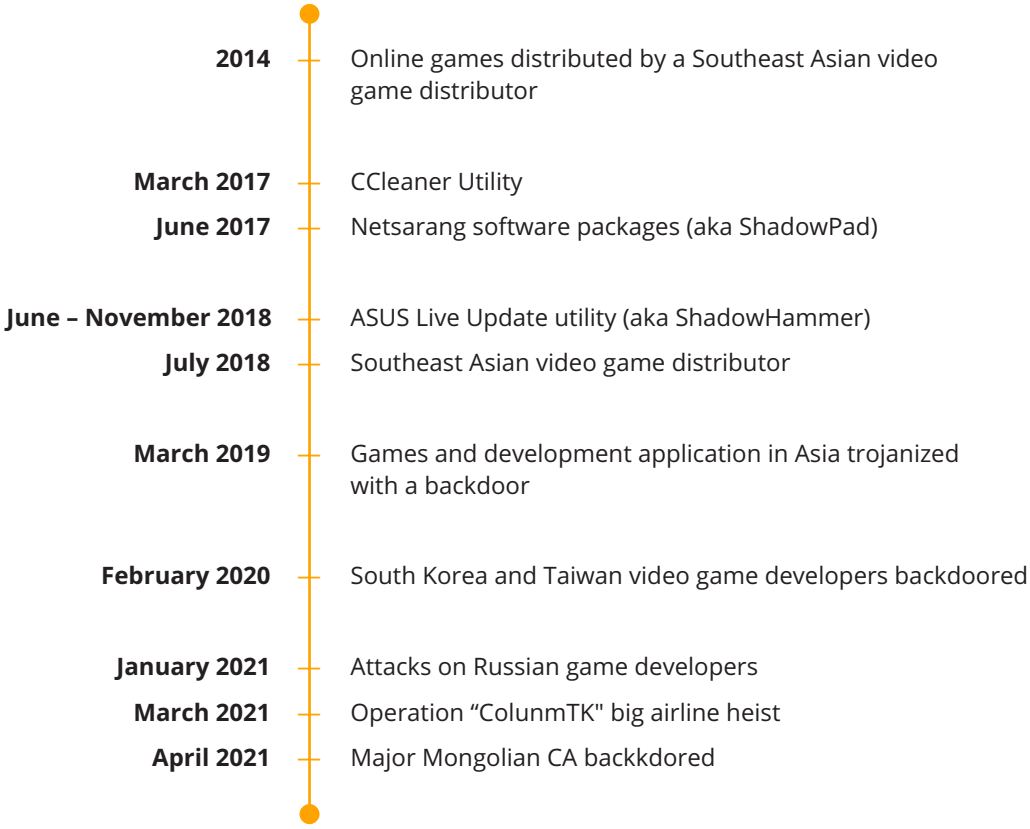


Figure 4: A timeline of reported operations carried out by APT41

// APT41 In Action: Key Supply Chain Attacks

The Gaming Industry: Ground Zero

For over 10 years, APT41 has been consistently focused on the video game industry in what appears to be cybercrime activities motivated by personal financial gain. This contrasts with the state-sponsored goals that drive the group's targeting of other sectors like healthcare, software and other industries.

Some of the early operations used techniques that would later be pivotal in executing supply chain compromises.

Milestones:

"'Winnti'—More Than Just a Game"

The first reports of this activity appeared in a report by Kaspersky in 2013, who had been investigating the group's activity since 2011. The report showed that the group had already been active for several years and specialized in targeting the online video game industry. Even then, the group mostly focused on stealing source code and digital certificates of legitimate software vendors, in addition to getting access to production gaming servers and new intellectual property including conceptual ideas, design and more.[12]

"Double Dragon—APT41, A Dual Espionage and Cybercrime Operation"

In 2019, FireEye published a report describing APT41's latest cyberespionage activities and the array of financially motivated intrusions against the video game industry in particular. This report also outlines TTPs which included stealing of source code and digital certificates, virtual currency manipulation and attempts to deploy ransomware.

In the same report, FireEye gave other examples of how APT41 used their successful experiences compromising the software development supply chain in the gaming industry to target other software companies. In these compromises, the attacker's objective was to inject malicious code into legitimate files before it was distributed the software customers.[13]

"Connecting The Dots—Exposing the Arsenal and Methods of the Winnti Group"

The same year, ESET published a new report on the group with additional examples of financial gain activity against video game companies, which included backdooring games and other software with cryptomining tools.

In their report, ESET reported strong links between APT41 (Winnti) and high-profile attacks against CCleaner, Asus, and Netsarang.[14]

"No 'Game Over' For the Winnti Group"

One year later, in 2020, ESET reported that APT41 (Winnti Group) was targeting several MMO (Massively Multiplayer Online) video gaming companies based in South Korea and Taiwan. Their research showed that APT41 managed to compromise their victims' software build environment and compromise the supply chain by injecting malicious code into the game executables. In other cases, the game servers themselves were compromised, which allowed the attackers to manipulate in-game currencies for financial gain.[15]

"Higaisa Or Winnti? Apt41 Backdoors, Old And New"

In 2021, Positive Technologies reported APT41's attacks targeting the gaming industry had expanded to game developers based in St. Petersburg, Russia as well. The attack targeted two different game developers using TTPs associated with the group, including the use of stolen code signing keys and certificates.[16]

Targeting the video game industry—for financial gain and individual targeting—has ultimately empowered the group's state-sponsored activity, because it has enabled APT41 to develop and master the TTPs that were subsequently used in attacks against high-profile companies with the objective of contaminating their supply chain and injecting malicious code into software updates.[17]

Ccleaner & Shadowpad: Compromised Software Build Server

Reports suggest that APT41 is responsible for the compromise of the widely used computer utility software for Windows CCleaner (previously Piriform; now owned by Avast). The attack, uncovered by Morphisec in 2017, was a multi-stage campaign that targeted Piriform's build server (outside of Avast infrastructure) and altered a compiler's library to include malicious code. The payload was injected during compilation on Piriform's build server, then signed through the legitimate signing process and distributed to 2.27 million users. The trojanized version was available for a month before it was detected and patched.[18]

The first stage of the malware was designed to collect non-sensitive information from CCleaner customers to identify the compromised machine and download a second stage binary to a selected group of victims. The second stage payload was delivered to just 40 devices out of the millions of devices infected, making it a highly targeted attack. The second stage binary ultimately delivered the infamous backdoor dubbed ShadowPad. The targeted companies were: Samsung, Sony, Asus, Intel, VMWare, O2, Singtel, Gauselmann, Dyn, Chunghwa and Fujitsu.[19]

ASUS Liveupdate & Operation Shadowhammer: Malware Delivered Through Software Updates

In January 2019, Kaspersky researchers discovered a sophisticated supply chain attack which they dubbed Operation ShadowHammer that involved Taiwan-based tech giant ASUS and its Live Update Utility. The backdoored ASUS binaries were signed with ASUS legitimate certificates ("ASUSTeK Computer Inc."), which means that either that ASUS production environment or signing infrastructure was compromised by the attacker or that they were able to get control of ASUS signing materials. In either case, the fact that the binaries were signed with a legitimate ASUS certificate allowed the attackers to appear legitimate and remain undetected for a long period of time.[20]

At least half a million users have downloaded and installed a backdoored version of the application, but the second stage payload was delivered to a specific, unknown pool of users, who were identified by their network adapters' MAC addresses. Kaspersky was able to identify at least 600 different MAC addresses from the samples they collected but didn't disclose any specific victims.

FireEye and ESET reportedly have evidence suggesting that at least one telecom company was one of the intended targets during the ASUS compromise, which is consistent with APT41's espionage targeting over the past few years.[21]

Airline Heist & Operation Colunmtk: From Supply Chain Attack To Data Breach

In March 2021, SITA, an international provider of IT services for the air transport industry worldwide, confirmed it had suffered a security incident.[22] In the following month, several of SITA's customers, including Air India Singapore Airlines and Malaysia Airlines, reported that they had suffered from data breaches as well, suggesting that this was another supply chain attack.

Group-IB, who investigated the incident with Air India, confirmed with moderate confidence that the actor behind the attack was APT41.[23]

Mongolian CA: Targeting The Source of Legitimate Certificates

In April 2021, Avast discovered another supply chain attack on a major East Asian certificate authority (CA) in Mongolia called MonPass. The researchers discovered that a MonPass installer downloaded from the official website had been backdoored with Cobalt Strike binaries. The backdoored client was available for download from February 8, 2021 until March 3, 2021 and was delivered to all MonPass users that downloaded it.

The Avast analysis showed that a public web server hosted by MonPass was breached eight different times with eight different webshells and backdoors. It is possible that this server was the point of infection for the backdoored client.[24]

Although Avast researchers were not able to attribute the attack with an appropriate level of confidence, RecordedFuture noted several overlaps between this attack with previous activity of APT41.[25]

Chinese Antivirus Anvisoft: Distributing Malware as Legitimate Security Software

Apart from using "traditional" supply chain attacks to target individual targets, Brian Krebs reported that APT41 was also using other types of supply chain attacks to deliver malware inside commercial tools the group appears to have created for this purpose. These tools were marketed as legitimate security software utilities, and the underlying malware was exposed by Krebs in a 2012 report, which revealed that an antivirus company named Anvisoft, created by the same individuals charged with being part of APT41, had been "whitelisted" or marked as safe by competing, more established antivirus vendors.

Anvisoft was allegedly based in California and Canada, but the registration records show that it was registered in the high-tech zone of Chengdu in the Sichuan Province of China. A review of Anvisoft's website registration records showed the company's domain originally was created by Tan DaiLin, an infamous Chinese hacker. At first, none of the antivirus products detected it as suspicious or malicious, but in the days that followed Krebs report, several antivirus products began flagging it for delivering at least two trojans designed to steal passwords from various online gaming platforms.[26]

// Conclusion: Protecting Software Development Pipelines

The publicly reported information covered in this paper makes it possible to clearly link the connections between the TTPs used in gaming and adware attacks and those targeting high-profile targets. Researching these operations also clearly shows the evolution of the Chinese intelligence apparatus over the past decade and the growing synergy between attackers motivated by financial gain and those focused on national intelligence goals.

Over the last 10 years, Chinese intelligence has been patiently and persistently developing the capabilities needed to get into production and software development environments of their selected targets. They have repeatedly demonstrated the value and impact of having trusted and legitimate code signing materials and access to software development supply chains and made this a primary objective.

Beyond the threat posed by APT41, their extensive experience has essentially become a blueprint that other state-sponsored attack groups can follow. Their methods demonstrate to other attackers pursuing financially motivated activities how they can successfully move from "lower value" targets to high-profile and well-resourced organizations.

Until every organization improves the security of its software development environments and increases the security controls governing code signing keys and certificates, every organization is at risk.

Code Signing Security Controls: Your Best Defense Against Supply Chain Attacks

Security and development teams may want to use the following controls as a checklist for evaluation of security best practices for software development and build environments:

- **Control-1: Restrict administrative access to CI/CD tools.** Ensure that only authorized persons can make administrative changes to the CI/CD system.
- **Control-2: Only accept commits signed with a developer GPG key.** Require commits to be signed with a developer GPG key helps to increase the burden on the attacker seeking to insert malicious code.
- **Control-3: Automation access keys expire automatically.** Ensure that access to keys used by automation expire periodically to create a shorter window of attack when keys are compromised.

- **Control-4: Reduce automation access to read-only.** CI systems should have read access only to source code repositories following the principle of least privilege access.
- **Control-5: Only dependencies from trusted registries can be used.** Configure the dependency manager so that it only allows connections to an authorized list of registries to keep malicious packages in the public registries from entering the pipeline.
- **Control-6: Any critical or high-severity vulnerability breaks the build.** Use static application security testing (SAST) to identify serious security issues, including poor cryptographic practices, hard-coded credentials and injection vulnerabilities.
- **Control-7: Store artifacts in a repository in development, stage and production.** Repositories for dev, stage and production should be segregated so that role-based access control can ensure least privilege at each stage.
- **Control-8: Validate artifact digest.** Before an artifact is deployed in any environment, its digest should be validated against the artifact in the repository to ensure that it has not been compromised.
- **Control-9: Pull-requests require two reviewers and a passing build to be merged.** Require two code reviews at the time of pull-requests, including one from a developer who is an owner of that code.
- **Control-10: Artifacts in higher repositories are signed.** Require signed artifacts to ensure that untrusted binaries are not deployed to customer environments and allows validating the source of the binaries.
- **Control-11: Available container images don't have high or critical vulnerabilities.** Test the container images into which applications are packaged for deployment for vulnerabilities.
- **Control-12: Validate artifact signatures and digests.** Validate the signature of an artifact against the digest to ensure that it was not tampered with in the repository and that the artifact being deployed is the same one that was tested.
- **Control-13: Scan deployed images in production.** Validate pre-production controls in production to ensure that the prior controls were followed for all software in production.
- **Control-14: Validate Kubernetes resource manifests.** Control and validate Kubernetes resource manifests just as the actual images are.
- **Control-15: Ensure build environments are ephemeral and immutable.** Build environments should be defined in code with automated creation and teardown, and a fresh environment should be created for every build.

Get the full details on these industry-recommended software security controls and the potential exposures they limit at **https://github.com/Venafi/blueprint-securesoftwarepipeline#readme**

Trusted by

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

About Venafi

Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to- machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

To learn more, visit venafi.com

// Appendix I: Naming APT41

When reading the multiple reports on the threat activities operating on behalf of the People's Republic of China (PRC), it can be challenging to understand various discussions about the same group or malware when different names are being used. This is because security and intelligence vendors, and the attackers themselves, use different naming conventions to track and report the same activity—making general attribution more difficult.

Various analyses and the official United States indictment related to the activities referenced in this research reveal overlaps between the multiple groups. In this report, we considered all of these aliases for the same groups and activities based on researchers referenced below:

- APT41 (FireEye, U.S. government)
- Winnti (Kaspersky, ESET, Clearsky)
- Wicked Panda & Wicked Spider (CrowdStrike)
- BARIUM (Microsoft)
- Blackfly & Suckfly (Symantec).

Other aliases also include: Axiom (Novetta) and Group 72 (Cisco Talos).

Notably, various operations attributed to other China-linked threat actor groups, such as APT17 and Ke3chang, have also leveraged malware and backdoors associated with the same group.[27]

Although these groups are all linked through their use of shared goals and attack resources, they all refer to highly sophisticated threat actors acting on behalf of the People's Republic of China (PRC) since as early as 2009. This group is generally known as APT41, but it may actually be a number of linked groups rather than a single discrete entity. Whether they are part of a single group or multiple subgroups is of less importance for the purpose of this report. The relationships between the variety of attacks attributed to them is sufficient to show they were (and likely are) at least in contact with one another.

// Appendix II: APT41 Code Families and Tools

APT41 has been observed using at least 46 different code families and tools, including:

- 9002 RAT
- AceHash
- ADORE.XSEC
- ASPXSpy
- Barlaiy
- BIOPASS RAT
- BlackCoffee
- Certutil
- China Chopper
- Cobalt Strike
- COLDJAVA
- Crackshot
- CrossWalk
- DEADEYE
- Derusbi
- DIRTCLEANER
- EasyNight
- Empire
- GearShift
- Gh0st RAT
- HDRoot
- HIGHNOON
- HIGHNOTE
- HKDOOR
- HOMEUNIX
- Jumpall
- LATELUNCH
- LIFEBOAT
- Lowkey
- MessageTap
- Meterpreter
- Mimikatz
- njRAT
- NTDSDump
- PACMAN
- PipeMon
- PlugX
- POTROAST
- PHOTO
- Pwdump
- RedXOR
- ROCKBOOT
- SAGEHIRE
- ShadowHammer
- ShadowPad,
- Winnti
- Skip-2.0
- Sogu
- Speculoos
- SWEETCANDLE
- TERA
- TIDYELF
- WIDETONE
- WINTERLOVE
- xDll
- XDOOR
- XMRig
- ZXShell
- Living off the Land.[28]

// Appendix III: APT41 Indictment

In August 2019 and again in August 2020, a federal grand jury in Washington, D.C., charged seven men with hundreds of cyberattacks against organizations in the U.S. and other countries in Asia and Europe. These attacks targeted software development companies, computer hardware manufacturers, telecommunications providers, social media companies, video game companies, non-profit organizations, universities, think tanks and foreign governments, as well as pro-democracy politicians and activists in Hong Kong.

Two of the individuals are Malaysian businessmen Wong Ong Hua and Ling Yang Ching, who were charged with conspiring with other two Chinese individuals to profit from these cyberattacks, specifically those targeting the video game industry in the United States and abroad.[29]

The five Chinese men—ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang and JIANG Lizhi—were identified as part of the APT41 group involved in several intrusions.

Figure 5: The five Chinese men charged by U.S. government for cybercrime and cyberespionage intrusions being part of APT41; from the FBI most wanted report

According to the indictments, the individuals were based in Chengdu, Sichuan and worked in a company called Chengdu 404, describing itself as a network security specialist and claiming to employ a team of white hat hackers who perform penetration testing along with "offensive" and "defensive" security operations.[30] Jiang was said to have a "working relationship" with the Chinese Ministry of State Security. If this is true, it would provide him and his associates with a degree of state protection.[31]

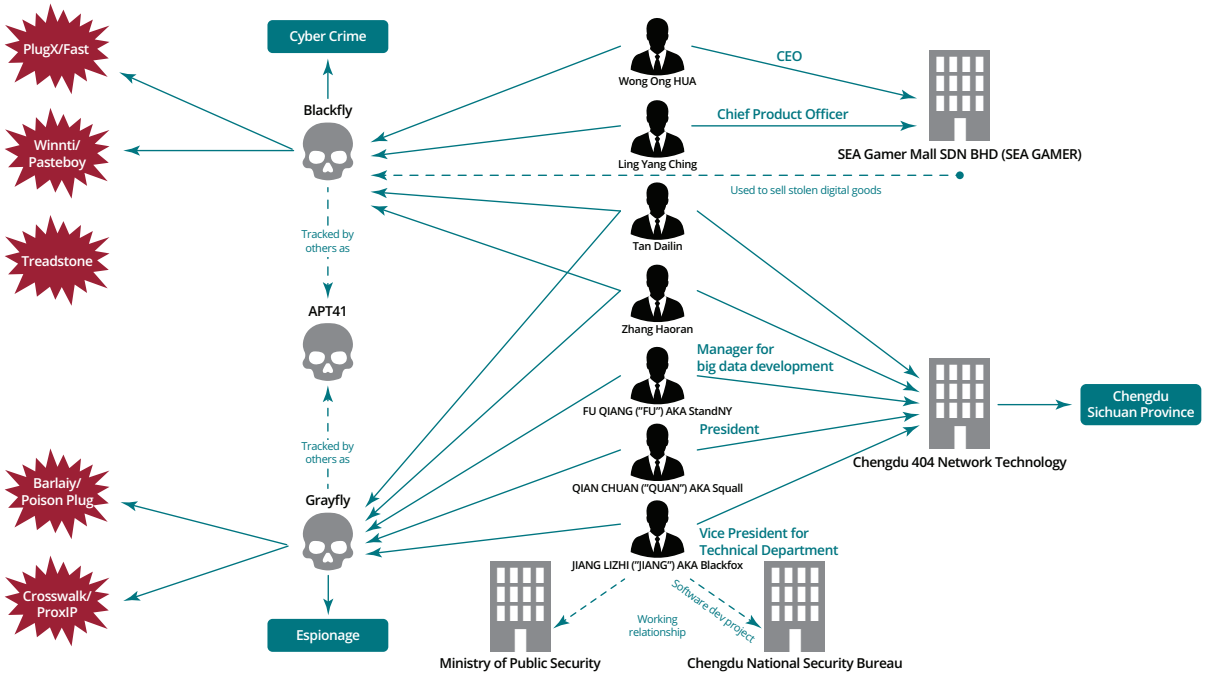


Figure 6: Alleged links between indicted men provided by U.S. prosecutors from Symantec report

APT41's activity seems to be divided to two sub-groups, one lead by Tan Dailin aka Rose (AKA "凋凌玫瑰") and Zhang Haoran and the other one by Jiang Lizhi (AKA "BlackFox") and Chengdu 404 Network Technology Co. Ltd.

Rose and Zhang Haoran from Chengdu 404 were coworkers between 2011 and 2017. Based on SentinelOne research and other reports, Rose and other individuals, have been active since at least 2005 as part of NCPH hacking group offering services for hire, including software cracking, malware development and penetration testing.[32]

Resources

- https://www.hhs.gov/sites/default/files/apt41.pdf
- https://www.aha.org/system/files/media/file/2020/11/hc3-threat-briefing-tlp-white-chinese-state-sponsored-cyber-activity-november-19-2020.pdf
- https://threatmodel.venafi.com/software/VS0008/
- https://threatmodel.venafi.com/groups/VG0006/
- https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=APT%2041
- https://assets.sentinelone.com/c/Shadowpad?x=P42eqA
- https://attack.mitre.org/groups/G0044/
- https://attack.mitre.org/groups/G0096/
- https://blog.group-ib.com/colunmtk_apt41
- https://blogs.blackberry.com/en/2020/04/decade-of-the-rats
- https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/
- https://en.wikipedia.org/wiki/Double_Dragon_(hacking_group)#Espionage_Activity
- https://github.com/401trg/detections/raw/master/pdfs/20180503_Burning_Umbrella.pdf
- https://krebsonsecurity.com/2020/09/chinese-antivirus-firm-was-part-of-apt41-supply-chain-attack/
- https://krebsonsecurity.com/tag/winnti/
- https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf
- https://mk0resourcesinf5fwsf.kinstacdn.com/wp-content/uploads/2021/03/flash_china_apt_actors.pdf
- https://quointelligence.eu/2020/04/winnti-group-insights-from-the-past/
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt41-indictments-china-espionage
- https://unit42.paloaltonetworks.com/apt41-using-new-speculoos-backdoor-to-target-organizations-globally/
- https://www.aha.org/system/files/media/file/2020/11/hc3-threat-briefing-tlp-white-chinese-state-sponsored-cyber-activity-november-19-2020.pdf
- https://www.bleepingcomputer.com/news/security/chinese-cyberspies-appear-to-be-preparing-supply-chain-attacks/
- https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html
- https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html
- https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html
- https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html
- https://www.govinfo.gov/content/pkg/CHRG-115hhrg31386/html/CHRG-115hhrg31386.htm
- https://www.intezer.com/blog/malware-analysis/new-linux-backdoor-redxor-likely-operated-by-chinese-nation-state-actor/
- https://www.intezer.com/blog/research/evidence-aurora-operation-still-active-supply-chain-attack-through-ccleaner/
- https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer
- https://www.justice.gov/opa/press-release/file/1295981/download
- https://www.justice.gov/opa/press-release/file/1317206/download
- https://www.justice.gov/opa/press-release/file/1317211/download
- https://www.justice.gov/opa/press-release/file/1317216/download
- https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/shadowpad-new-activity-from-the-winnti-group/
- https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/#id3
- https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/
- https://www.recordedfuture.com/redecho-targeting-indian-power-sector/
- https://www.welivesecurity.com/2019/03/11/gaming-industry-scope-attackers-asia/
- https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/
- https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/
- https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/
- https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf

References

1. https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-july-wicked-spider/; https://adversary.crowdstrike.com/en-US/adversary/wicked-panda/?L=109
2. https://content.fireeye.com/apt-41/rpt-apt41
3. https://www.fireeye.com/current-threats/apt-groups.html
4. https://www.hhs.gov/sites/default/files/apt41.pdf
5. https://blogs.blackberry.com/en/2020/04/decade-of-the-rats
6. https://vx-underground.org/archive/APTs/2018/2018.05.03/Burning%20Umbrella.pdf ; https://content.fireeye.com/apt-41/rpt-apt41/
7. https://www.hhs.gov/sites/default/files/apt41.pdf
8. https://content.fireeye.com/apt-41/rpt-apt41
9. https://content.fireeye.com/apt-41/rpt-apt41/
10. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf
11. https://blogs.blackberry.com/en/2020/04/decade-of-the-rats ; https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf
12. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134508/winnti-more-than-just-a-game-130410.pdf
13. https://content.fireeye.com/apt-41/rpt-apt41
14. https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf
15. https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/
16. https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/#id3
17. https://content.fireeye.com/apt-41/rpt-apt41
18. https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf ; https://published-prd.lanyonevents.com/published/rsaus18/sessionsFiles/8739/HTA-T10_CCleaner%20APT%20Attack-A%20Technical%20Look%20Inside.pdf
19. https://www.wired.com/story/ccleaner-malware-targeted-tech-firms/
20. https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/ ; https://securelist.com/operation-shadowhammer/89992/
21. https://www.reuters.com/article/us-china-cyber-moonlighters/chinese-government-hackers-suspected-of-moonlighting-for-profit-idUSKCN1UX1JE ; https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf
22. https://www.sita.aero/pressroom/news-releases/sita-statement-about-security-incident/
23. https://blog.group-ib.com/colunmtk_apt41
24. https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/
25. https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/
26. https://krebsonsecurity.com/2020/09/chinese-antivirus-firm-was-part-of-apt41-supply-chain-attack/
27. https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf
28. https://www.hhs.gov/sites/default/files/apt41.pdf ; https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=APT%2041&n=1 ; https://attack.mitre.org/groups/G0096/
29. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer
30. https://www.justice.gov/opa/press-release/file/1317206/download
31. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer ; https://www.fbi.gov/wanted/cyber/apt-41-group
32. https://assets.sentinelone.com/c/Shadowpad?x=P42eqA