

# APT41

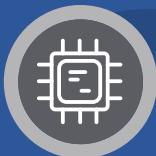


**Double Dragon**  
APT41, a dual espionage and  
cyber crime operation

# Table of Contents

|   |    |
|---|----|
| <b>Overview</b>   | 4  |
| <b>Targeting</b>  | 6  |
| <b>Operations Over Time</b>                                     | 8  |
| <b>Cyber Espionage Activity</b>                                 | 10 |
| Case Study: Healthcare Sector Targeting                         | 12 |
| <b>Financially Motivated Activity</b>                           | 14 |
| Case Study: Video Game Industry Targeting                       | 17 |
| <b>Third-Party Access</b>                                       | 20 |
| <b>History of Supply Chain Compromises</b>                      | 21 |
| December 2014   | 22 |
| March 2017  | 23 |
| July 2017   | 24 |
| June 2018   | 25 |
| July 2018   | 26 |
| <b>Overlaps Between Espionage and Financial Operations</b>      | 27 |
| <b>Attribution</b>  | 30 |
| <b>Status as Potential Contractors</b>                          | 33 |
| <b>Links to Other Known Chinese Espionage Operators</b>         | 34 |
| Certificate Overlap   | 35 |
| Launcher Overlap  | 36 |
| Code Family Overlap   | 36 |
| <b>Use of Code-Signing Certificates</b>                         | 39 |
| <b>Outlook and Implications</b>                                 | 41 |
| <b>Technical Annex: Attack Lifecycle</b>                        | 42 |
| Initial Compromise  | 43 |
| Establish Foothold  | 44 |
| Escalate Privileges   | 45 |
| Internal Reconnaissance   | 45 |
| Lateral Movement  | 46 |
| Maintain Presence   | 47 |
| Complete Mission  | 48 |
| <b>Technical Annex: MITRE ATT&amp;CK Mapping</b>                | 49 |
| <b>Technical Annex: Code-Signing Certificates Used by APT41</b> | 51 |
| <b>Technical Annex: Additional Malware Overlaps</b>             | 52 |
| Background  | 52 |
| HIGHNOON  | 52 |
| HIGHNOON.BIN and HIGHNOON.LITE                                  | 52 |
| HIGHNOON.LINUX and HIGHNOON                                     | 54 |
| CROSSWALK and CROSSWALK.BIN                                     | 54 |
| <b>Technical Annex: Malware Used by APT41</b>                   | 60 |
| <b>Technical Annex: APT41 IOCs</b>                              | 63 |

# Executive Summary



FireEye Threat Intelligence assesses with high confidence that APT41 is a Chinese state-sponsored espionage group that is also conducting financially motivated activity for personal gain.

APT41 espionage operations against the healthcare, high-tech, and telecommunications sectors include establishing and maintaining strategic access, and through mid-2015, the theft of intellectual property.

The group's operations against higher education, travel services, and news/media firms provide some indication that the group also tracks individuals and conducts surveillance.

FireEye Threat Intelligence assesses with high confidence that APT41 carries out an array of financially motivated intrusions, particularly against the video game industry, including stealing source code and digital certificates, virtual currency manipulation, and attempting to deploy ransomware.

APT41 has executed multiple software supply chain compromises, gaining access to software companies to inject malicious code into legitimate files before distributing updates.



# Overview

FireEye Threat Intelligence assesses with high confidence that APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control. Activity traces back to 2012 when individual members of APT41 conducted primarily financially motivated operations focused on the video game industry before expanding into likely state-sponsored activity. This is remarkable because explicit financially motivated targeting is unusual among Chinese state-sponsored threat groups, and evidence suggests these two motivations were balanced concurrently from 2014 onward.



- APT41 is unique among tracked China-based actors in that it leverages non-public malware typically reserved for espionage operations in what appears to be activity that falls outside the scope of state-sponsored missions.
- Based on early observed activity, consistent behavior, and APT41's unusual focus on the video game industry, we believe the group's cyber crime activities are most likely motivated by personal financial gain or hobbyist interests.

This contrasts with the state-sponsored goals that likely drive the group's healthcare, high-tech, and politically related targeting.

- We believe that APT41 is highly sophisticated and innovative. Its history of financially motivated targeting of the video game industry has ultimately supported the group's state-sponsored activity.

- The group's distinct use of supply chain compromises to target select individuals, consistent use of compromised digital certificates, and deployment of bootkits (rare among APT operators), highlight a creative and well-resourced adversary.
- Some of the early operations driven by personal gain used techniques that would later be pivotal in executing supply chain compromises.
- Learning to access video game production environments enabled APT41 to develop the tactics, techniques, and procedures (TTPs) that were later leveraged against software companies to inject malicious code into software updates.

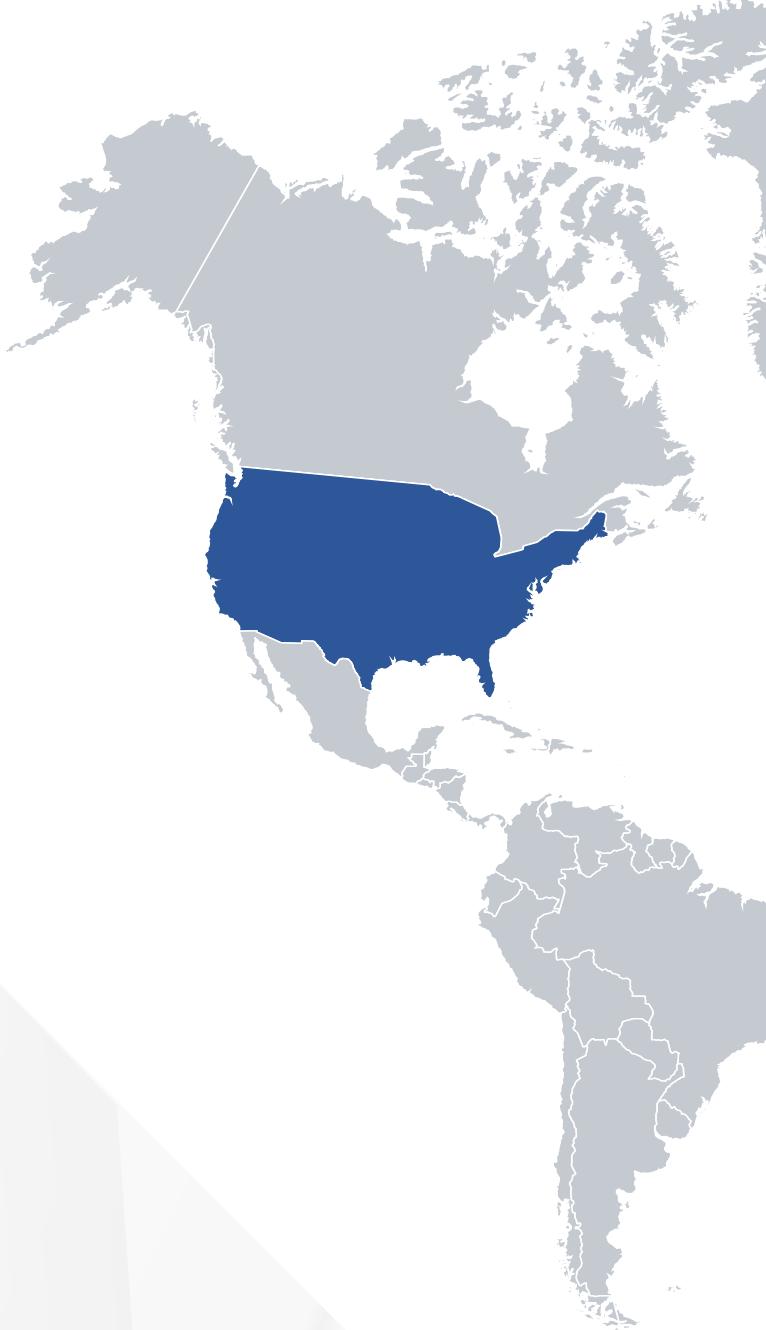
APT41 campaigns include most of the incidents previously attributed in FireEye Threat Intelligence reporting to GREF Team and a number of additional clusters that were previously unnamed.

# Targeting

Like other Chinese espionage operators, APT41 targets industries in a manner generally aligned with China's Five-Year economic development plans. However, some campaigns attributed to APT41 indicate that the group is also deployed to gather intelligence ahead of imminent events, such as mergers and acquisitions (M&A) and political events. Directly targeted verticals include:

- Healthcare: including medical devices and diagnostics
- High-tech: including semiconductors, advanced computer hardware, battery technology, and electric vehicles
- Media: including news organizations
- Pharmaceuticals
- Retail
- Software companies: which were compromised in supply chain operations potentially affecting large numbers of victims
- Telecoms
- Travel services
- Education
- Video games: including development studios, distributors/publishers, and activities enabling supply chain compromises
- Virtual currencies: including in-game currencies, cryptocurrencies, and related services

APT41 has targeted organizations in 14 countries (and Hong Kong) over seven years, including: France, India, Italy, Japan, Myanmar, the Netherlands, Singapore, South Korea, South Africa, Switzerland, Thailand, Turkey, the United Kingdom, and the United States (Figure 1). APT41 espionage operations against entities in these countries follow targeting of verticals consistent with Chinese national policy priorities.



**Figure 1:**

Countries and industries targeted directly by APT41.

**Industries Targeted**

Automotive

Financial

Pharmaceuticals

Business Services

Healthcare

Retail

Cryptocurrency

High-Tech

Telecommunications

Education

Intergovernmental

Travel

Energy

Media and Entertainment

# Operations Over Time

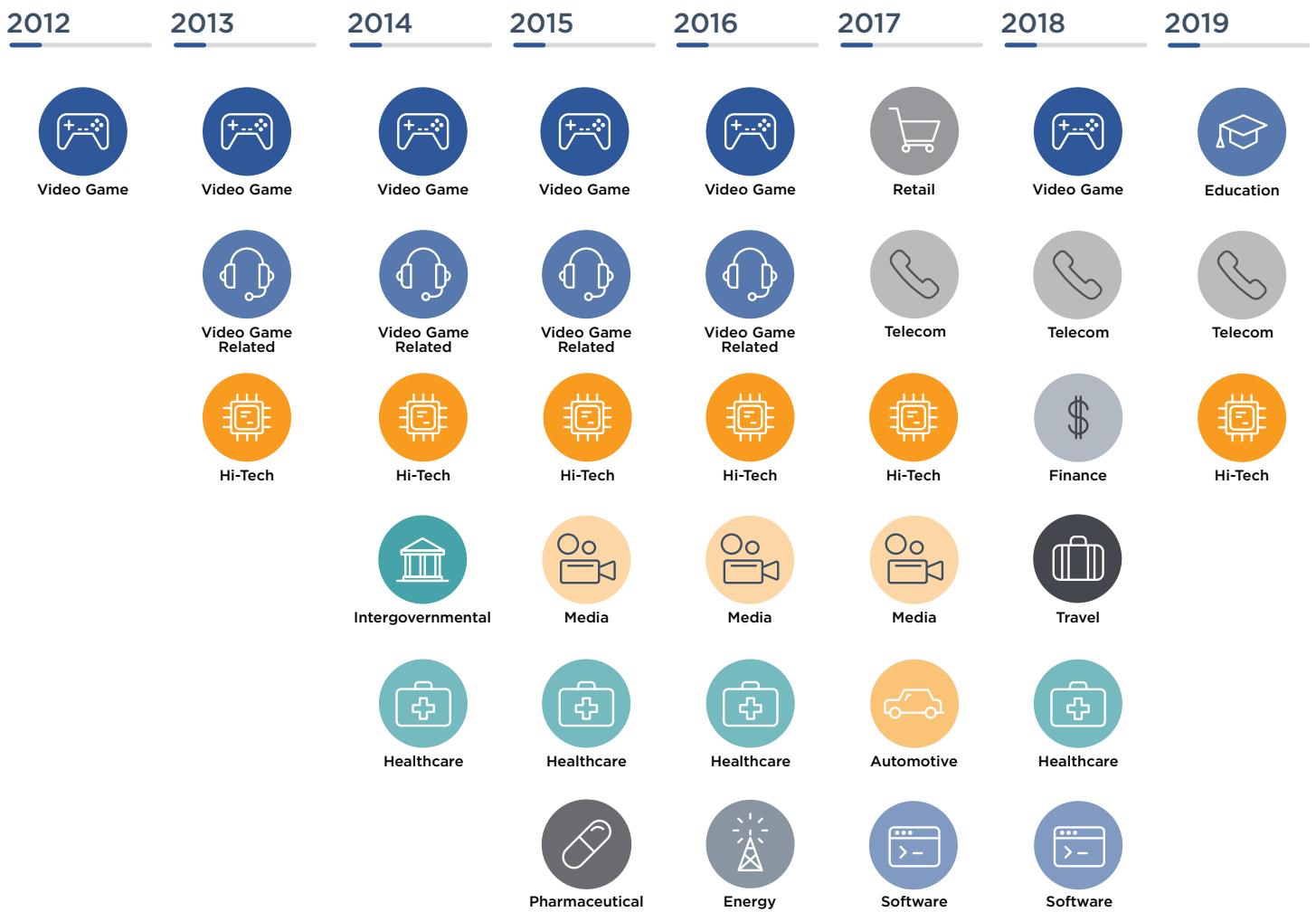
The duality of APT41's state-sponsored activity and its own cyber crime operations is demonstrated in the group's simultaneous operations. Throughout the group's observable history, APT41 has consistently run its own financially motivated campaigns concurrently with espionage operations. In contrast, APT41 espionage targeting has changed significantly over time, suggesting shifts in assigned missions or new contracts to complete. A breakdown of industries targeted by APT41 over time can be found in Figure 2.

- We believe that like other Chinese espionage operators, APT41 has moved toward strategic intelligence collection and establishing access, but away from direct intellectual property theft. This shift, however, has not affected the group's consistent interest in targeting the video game industry for financially motivated reasons.
  - We have not observed evidence of IP theft since late 2015.
  - In 2014, APT41 was observed carrying out espionage campaigns concurrently with financially motivated intrusions, demonstrating that they could balance different objectives simultaneously.
- Espionage operations occurred while the group was still carrying out financially motivated campaigns, including longer-term intrusions, which typically extended for more than a year.
  - In one instance, APT41 was attempting to steal data from a healthcare target while also attempting to deploy ransomware at a video game studio.
- Compromising organizations in different sectors concurrently provides some indication that they are fulfilling specific assigned tasks.
  - Campaigns have expanded into additional industries including telecoms, the automotive sector, higher education, and travel services.
  - In 2015, we observed a time period in which eight organizations in six different industries were compromised simultaneously.
- Since 2017, APT41's activities have included a series of supply chain compromises. The operation injects malware into legitimate server software packages used by hundreds of companies worldwide but limits deployment of additional payloads to select targets.



**Figure 2:** Timeline of industries targeted by APT41.

## INDUSTRIES TARGETED BY APT 41



# Cyber Espionage Activity

Observed APT41 targeting is consistent with China's national strategies to move production capabilities upmarket into research and development (R&D)-heavy fields. These initiatives were especially highlighted with "Made in China 2025," a plan announced in 2015 that aims to shift China's economy toward higher value products and services, including pharmaceuticals, semiconductors, and other high-tech industries.

- We assess that the targeting of high-tech firms that produce computer components aligns with Chinese interests in domestically developing high-end technologies as outlined in the **12th** (2011) and **13th** (2016) Five-Year plans, as well as the **Made in China 2025** (2015) initiative.
  - Since 2013, APT41 has targeted organizations involved in the research, development, and sale of computer components used for machine-learning, autonomous vehicles, medical imaging, and the consumer market. The group also targeted companies involved in producing motherboards, processors, and server solutions for enterprises.
  - In April 2013, the group targeted an enterprise cloud-computing provider. Developing domestic cloud-computing technologies was a goal in the 12th Five-Year Plan.
  - In a 2014 compromise, APT41 targeted a European conglomerate and specifically focused on systems physically located in China.
- The timing of multiple intrusions attributed to the group indicate a focused interest in strategic business decisions, including entry into the Chinese market, partnerships/M&A, and expansion into other regional markets.
  - In October 2017, an intrusion into a retailer targeted strategic investment plans at the same time as the firm was beginning to negotiate a partnership with a Chinese company (although this potential deal was not publicized).
  - In spring 2015, APT41 targeted information related to two entities undergoing a merger announced the previous year. This included data related to a senior executive, as well as payroll and communications integration issues.

- Since 2017, APT41 has consistently targeted telecommunications companies, possibly a crucial first step to establish a foothold in targeting a particular region.
  - Targeted telecom companies spanned several countries, and recently identified intrusions were concentrated in countries where we had not identified any prior APT41 activity.
  - APT41 has targeted large telecom companies and their subsidiaries in various locations, demonstrating consistent interest in obtaining access to these targets.
  - The group has also repeatedly targeted call record information at telecom companies, supporting indications of their wider intelligence collection efforts.

In addition to specifically targeting industries of strategic value, we suggest that APT41 is also given more tactical assignments, including reconnaissance and identifying dissidents.

- A hotel was targeted two weeks ahead of a diplomatic visit in which high-ranking Chinese officials stayed there. Personal data within the reservations system was directly accessed, suggesting the group was potentially tasked to reconnoiter the facility.
- We assess with moderate confidence that APT41 gathered intelligence on pro-democracy dissidents in Hong Kong based on the targets and timing of operations.
  - In July and August 2016, APT41 sent spear-phishing emails to Hong Kong media organizations known for pro-democracy editorial content.
  - The timing and targeting of this activity suggests possible interest in the pro-democracy Umbrella Movement candidates who were **running** for seats in Hong Kong's legislative council.
  - A spear-phishing email with the subject-line "help" was later sent to one of the previously targeted organizations in October 2017, coinciding with the **sentencing** of pro-democracy Occupy activists. The ruling placed a five-year ban on the activists from holding public offices in Hong Kong.

- This was the first instance we have observed of APT41 targeting pro-democracy groups in Hong Kong.

APT41 frequently leverages timely news stories as the lure content in their spear-phishing emails, although social engineering content does not always correlate with targeted users or organizations.

- In 2015, APT41 targeted a Japanese media organization with a lure document (Figure 3) titled “中東呼吸器症候群(MERS)の予防,” which translates to “Prevention of Middle East Respiratory Syndrome (MERS).” The fear of respiratory infections and a potential pandemic provide particularly effective lure material against targets in the Asia-Pacific region that had first-hand experience with prior SARS and avian flu outbreaks.

**Figure 3:**

MERS-themed lure document leveraging sexyjapan.ddns.info for C&C (MD5: 5e87b09f9a3f1b728c9797560a38764b).

## 【感染症】中東呼吸器症候群(MERS)の原因・症状・予防法

- [サイトマップ](#)
- [INDEX](#)



- [健康管理](#)
  - 食と健康
  - 運動と健康
  - 睡眠
  - ストレス
  - 肥満・メタボリックシンドローム
  - タバコ・禁煙
  - 疲労回復法
  - 飲酒・アルコール
  - 女性の健康
  - 健康診断・検診・人間ドック
  - 予防接種・ワクチン
  - 放射線・放射能汚染・医療被曝

[もっと見る](#)

- [症状・病気](#)
  - 脳・神経の病気
  - 目の病気
  - 薬・口の病気
  - 耳・鼻・喉の病気
  - 肺・気道の病気
  - 心臓・血管・血液の病気
  - 胃腸の病気
  - 肝臓・すい臓・胆のうの病気
  - 腎臓・膀胱・尿管・尿道の病気
  - 婦人病・女性の病気
  - 不妊症
  - 骨・筋肉・関節の病気
  - 皮膚・爪・髪の病気
  - 痛み・疼痛
  - メンタルヘルス

[もっと見る](#)

- [治療・介護](#)
  - 医療情報・ニュース
  - 病院

**CASE STUDY**

# Healthcare Sector Targeting

APT41 activity aimed at medical device companies and pharmaceuticals is demonstrative of the group's capacity to collect sensitive and highly valuable intellectual property (IP), although we have not observed evidence of IP theft since late 2015. The healthcare sector was targeted in a manner that is highly specific and most likely indicative of focused taskings from sponsoring organizations with a stake in the healthcare market. Targeted information included pharmaceutical development, clinical trial data, and intelligence regarding a medical subsidiary's parent company.





The targeting of these organizations just ahead of the release of products requiring a long R&D cycle can confer a significant market advantage to a competitor. The observed activities are indicative of ongoing efforts to support China's own R&D efforts in support of Made in China 2025.

- Between July 2014 and May 2016, APT41 targeted a medical devices subsidiary of a large corporation.
  - Although APT41 initially targeted the parent company, 30 percent of the victimized hosts were related to a subsidiary specialized in manufacturing medical devices. Password strings and spoofed domains leveraged in the operation signify a narrow tasking to target the subsidiary instead of the parent corporation.
  - We have some indication based on the nature of hosts targeted that APT41 was interested in information technology employees and software used by the medical device subsidiary.

- A keylogger dubbed GEARSHIFT was first deployed at the medical device company. A digital certificate from the victim was compromised and used to sign malware used in an operation against a separate biotech company detailed below.
- A biotech company undergoing acquisition was targeted by APT41 in May 2015. Highly sensitive information about corporate operations, including human resources data, tax information, and acquisition-related documents, were targeted.
  - Clinical trials data of developed drugs, academic data, and R&D funding-related documents were exfiltrated.
  - The time frame, use of the same GEARSHIFT sample, and a digital certificate from the aforementioned medical device company provide some indication that these two campaigns were conducted by the same operator concurrently.
- In 2018, we observed APT41 target a third healthcare company, although their goals during this compromise were unclear.

# Financially Motivated Activity

Unlike other observed Chinese espionage operators, APT41 conducts explicit financially motivated activity, which has included the use of tools that are otherwise exclusively used in campaigns supporting state interests. The late-night to early morning activity of APT41's financially motivated operations suggests that the group primarily conducts these activities outside of their normal day jobs. However, the group compiled malware for use in cyber crime activity even during espionage-focused working hours.

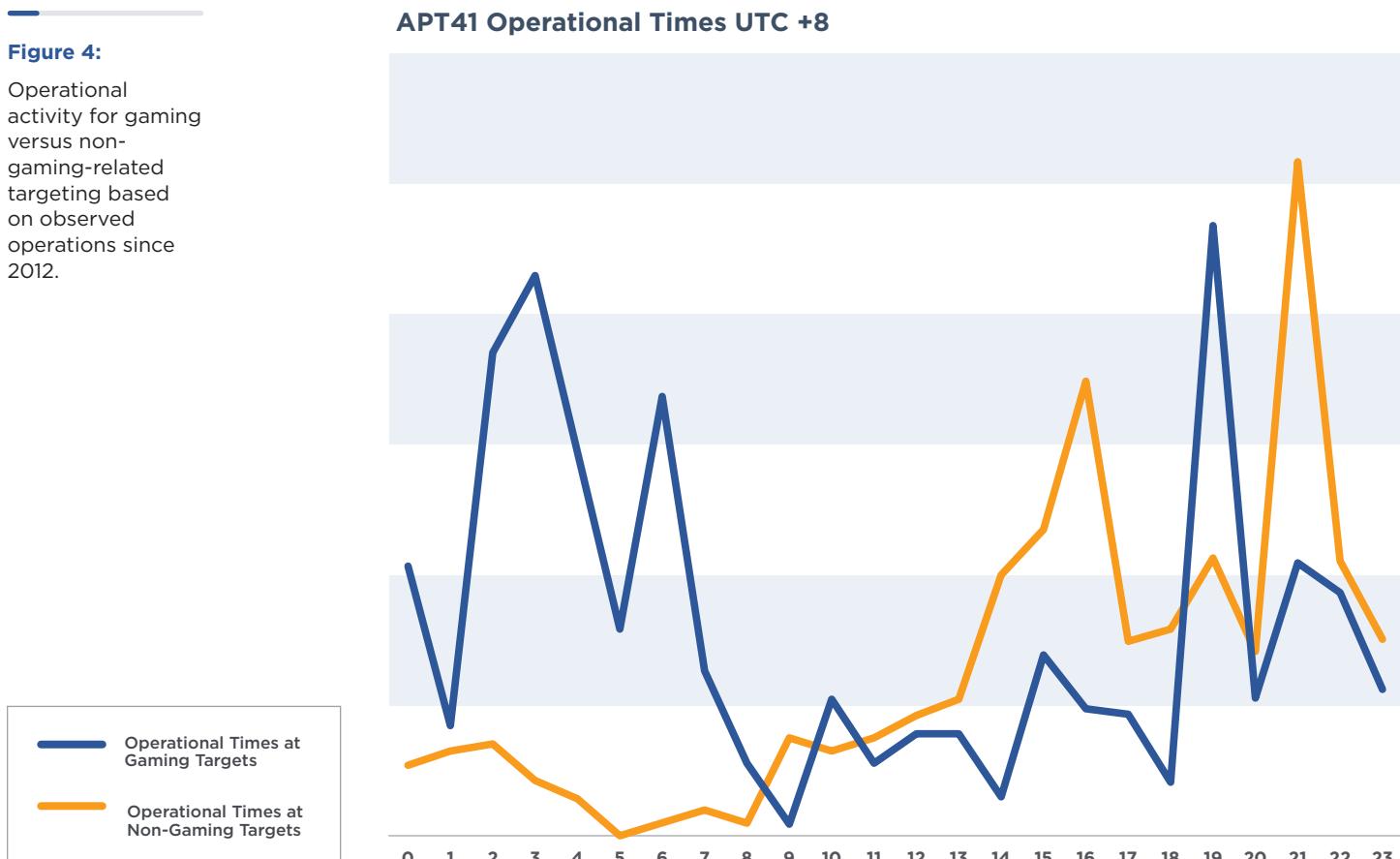
- As demonstrated in Figure 4, operational times for APT41 espionage operations over all observed activity are relatively close to Chinese work hours (in UTC +8, China's time zone).
- In contrast, the group's financially motivated activity targeting the video game industry tends to occur much later in the night.

Operational times at gaming targets are most frequent between 18:00 and 07:00 (UTC +8), providing some indication that the group is moonlighting. Note that this is based on data collected over years and does not represent a daily schedule.

- The typical working hours in China for tech workers is a **"996" work schedule** (9:00 a.m. to 9:00 p.m., six days a week), which is consistent with APT41's operational activity observed over time.
- Operational times at targets not related to video games (and therefore, almost certainly in support of state-sanctioned missions) are more frequent between 14:00 and 22:00 (China Standard Time (CST), UTC +8), closer to conventional working hours (Figure 4).
- Analysis of compile times for all portable executable (PE) files suggests that APT41's average working hours fall between 10:00 to 23:00 (UTC +8), highlighting that the financially motivated activity is most likely extraneous to their espionage operations.
- Compile times for samples used in suspected financial gain missions are skewed toward later in the evening, roughly 19:00 to 00:00 (UTC +8). However, there is significant overlap with the compile times of PE files deployed at espionage targets between 15:00 to 19:00 (UTC +8).

**Figure 4:**

Operational activity for gaming versus non-gaming-related targeting based on observed operations since 2012.



The group has also targeted cryptocurrencies, including at least one case in which there was a connection between cryptocurrency and an online video gaming platform.

- In June 2018, APT41 sent spear-phishing emails using an invitation lure to join a decentralized gaming platform linked to a cryptocurrency service (Figure 5) that had positioned itself as a medium of exchange for online games and gambling sites. The malicious emails were sent from an email address listed with the name Tom

Giardino, which is likely a reference to an employee at Valve, an American video game developer responsible for the software distribution platform Steam and various video games. The body of the email (Figure 6) also mentions gaming offerings. This provides another connection between the targeting of the cryptocurrency organizations and video game targeting.

- In October 2018, the group compiled an instance of XMRig, a Monero cryptocurrency mining tool, demonstrating a continued interest in cryptocurrency.

**Figure 5:**

Screenshot of invitation to join the FairWin online gaming platform.

● Tom Giardino 

项目 (FairWin) 上线申请!

To: [REDACTED]

#### 项目介绍:

FairWin是一个分散的在线游戏平台，确保赢得公平性，因为我们特别的FairChannel保证了准确的RTP费率。该系统基于区块链，这意味着游戏过程是开放的。奖金的支付是自动的，不依赖于组织者。除此之外，我们还提供有趣的大气游戏，带有迷人的图形，可以在任何设备和任何浏览器上运行，这样所有玩家都可以享受这些体验。其他详细内容请参见附件！



FairWin.chm.xz

**Figure 6:**

English translation of invitation to join the FairWin online gaming platform.

From: Tom Giardino <hrsimon59@gmail.com>

Date: <redacted>

Subject: Project (FairWin) online application!

#### Project Introduction:

FairWin is a decentralized online gaming platform.

Be sure to win fairness because our special FairChannel guarantees accurate RTP rates. The system is based on a blockchain, which means that the gameplay process is open. The payment of the bonus is automatic. Not dependent on the organizer. In addition to this, we also offer fun generous games with fascinating graphics. It can be run on any device and any browser so that all players can enjoy these experiences. Please refer to the attachment for other details!

**CASE STUDY**

# Video Game Industry Targeting

A woman with long dark hair is smiling broadly while wearing a white VR headset. Two hands, one from each side, are adjusting the straps of the headset around her head. She is wearing a denim jacket. The background is dark and out of focus.

APT41 continuously returns to targeting the video game sector and seems to have matured its campaigns through lessons learned in operations against the industry. We believe these operations include broadly malicious activity that can enable further operations, such as targeting game source code and compromising digital certificates, while other activities are explicitly financially motivated, such as abusing in-game currency mechanics. APT41 campaigns focused on the video game sector have largely affected studios and distributors in East and Southeast Asia, although global companies based in the United States have also been targeted.



The group leverages many TTPs during the targeting of video game-related organizations, which are likewise employed in their espionage operations.

- Since at least 2012, APT41 has repeatedly gained access to game development environments within affected companies, including online multiplayer networks, as well as targeting of production database administrators.
  - The group is competent in both Linux and Windows environments and can pivot easily between both environments within a single operation, including compromising intermediary servers that provide access to separated Windows and Linux environments.
  - In October 2012, APT41 used captured credentials to compromise a jump server and access a production environment where they deployed a Linux version of PHOTO. Based on the machines targeted, we have some indication that APT41 specifically sought to access production machines used in the development of an upcoming online game.
  - In 2014, APT41 used a variant of SOGU that is capable of connecting to Windows and Linux systems via SSH and Samba/CIFS.
  - APT41 has been observed inserting malicious code into legitimate video game files to distribute malware. In 2018, the group inserted CRACKSHOT malware into game files that were signed with legitimate code-signing certificates, most likely indicating access to the production environment, which facilitated a supply chain compromise.
    - A highly similar incident in 2014 suggests that APT41 (or a closely affiliated actor) has a history of carrying out such operations against the video game industry.
  - APT41's experience gaining access to production environments may have been a precursor to more recent supply chain compromises. The insertion of malware into a build environment for later distribution with legitimate software is a natural extension of the group's earliest activities. Additional details are provided in the section "History of Supply Chain Compromises."

• We have also observed APT41 limitedly deploy rootkits on Linux systems and Master Boot Record (MBR) bootkits, such as ROCKBOOT, on Windows systems to hide their malware and maintain persistence on victim systems. Selective deployment of ROCKBOOT suggests that APT41 reserves more advanced TTPs and malware only for high-value targets.

- Bootkits are a stealthy means of installing malware because the code resides outside of the OS. Because bootkits are initialized prior to the OS and operate in kernel mode, OS applications and security tools may have great difficulty detecting bootkits.
- The use of bootkits among threat actors, however, is rare. It is more common for threat actors to rely on techniques such as DLL search order hijacking or modifying Windows registry keys to achieve persistence.
- The group used the Adore-NG rootkit on older Linux operating systems to hide their Linux backdoor ADORE.XSEC. Note that the Adore-ng rootkit is no longer in development and would likely not run successfully on modern Linux systems, but APT41 deployed this on a legacy game server.

APT41 is well-known for leveraging compromised digital certificates from video game studios to sign malware. The group has abused at least 19 different certificates in this way. Additional details on code-signing certificates are provided in the section "Use of Code Signing Certificates."

- In 2012, APT41 used a code-signing certificate from Mgame, a South Korean game publisher, against other gaming industry entities. The serial number for this certificate was:

01:00:00:00:00:01:30:73:85:f7:02

- A different Mgame digital certificate has been used by several other Chinese operators, including APT17, APT20, and APT31. It is unclear if this certificate was compromised at the same time as the one used by APT41 (or if it was stolen by APT41 and shared with these other groups). The serial number for this certificate was:

**4e:eb:08:05:55:f1:ab:f7:09:bb:a9:ca:e3:2f:13:cd**

APT41 has blatantly engaged in financially motivated activity targeting the video game industry, including manipulating virtual currencies. These activities demonstrate established connections to underground marketplaces and familiarity with monetization and laundering techniques.

- Using its access to a game production environment, in less than three hours the group generated tens of millions of dollars of a popular game's virtual currency. The money was credited to more than 1,000 accounts and most likely sold and laundered in underground markets.
- APT41 has targeted payment services specializing in handling in-game transactions and real money transfer (RMT) purchases.
- In a highly unusual case, APT41 attempted to extort a game company by deploying the Encryptor RaaS

ransomware. We suggest that APT41 sought to target in-game currency but found they could not monetize the specific targeted game, so the group resorted to ransomware to attempt to salvage their efforts and profit from the compromise.

- This ransomware was sold via a Ransomware-as-a-Service (RaaS) operation that was available via a Tor (.onion) website. Users of the ransomware were charged a 20 percent fee for any collected ransom.
- Since this was not the group's typical method of choice for collecting money from a victim environment, it is possible that APT41 turned to a pay-for-service ransomware to avoid having to develop such a tool or set up the associated payment and infrastructure associated with collecting the ransom.
- APT41 attempted to deploy the ransomware through a group policy (GPO) scheduled task. However, the malware was unsuccessfully deployed because of a simple typo.
- Figure 7 shows the ransom note associated with Encryptor RaaS, which contains default messages in both English and German (the instruction links have been redacted). Given that this is the default message, the languages in the note should not be considered when determining actor origin or location.

#### ATTENTION!

The files on your computer have been securely encrypted.  
To get access to your files again, follow the instructions at:

#### ACHTUNG!

Die Dateien auf Ihrem Computer wurden sicher verschlüsselt.  
Um den Zugriff auf Ihre Dateien wiederzuerlangen, folgen Sie der Anleitung auf:

**Figure 7:**  
Screenshot of  
ransomware note.

# Third-Party Access

In multiple instances, APT41 targeted third parties and leveraged this access to target additional victims. APT41's exploitation of third parties varied. In some instances, APT41 moved laterally from one victim environment to another in order to initiate compromise. APT41 has also used credentials compromised in previous operations.

- In 2014, APT41 compromised an online billing/payment service using VPN access between a third-party service provider and the targeted payment service. The payment service was likely targeted because it provided access to multiple gaming companies.
- Although we do not have first-hand evidence of APT41's compromise of TeamViewer, we have observed APT41 use compromised TeamViewer credentials as an entry point at multiple organizations.
  - During a 2017 compromise, APT41 initiated a TeamViewer session and transferred files that were later deleted. Filenames and creation times indicate that these may have been the HIGHNOON backdoor.
  - According to **statements** by a TeamViewer's spokesperson, the company was targeted in fall 2016. The company stated that they conducted a comprehensive security audit of its IT architecture and added additional security measures to help strengthen its security posture.

# History of Supply Chain Compromises

Supply chain compromises are most likely an extension of APT41's tactics used in gaining access to gaming development environments and to other gaming organizations via third-party service providers. Public reports of supply chain compromises linked to APT41 date back to at least 2014, and technical evidence associated with these incidents was used to determine a relationship, if any, with APT41. Our assessment in each of these cases is noted in Table 1.

- As demonstrated in operations targeting the video game industry, APT41 leverages a variety of TTPs to access production environments where they can inject malicious code into legitimate files. The files are signed with valid code-signing certificates and distributed widely to end users.
- Supply chain targeting requires more effort than typically observed mass targeting methods, such as establishing a strategic web compromise (SWC) or conducting large spear-phishing campaigns.

Although APT41 supply chain compromises affect very large numbers of victims, the group limits follow-on activity to select victims most likely to reduce detection and ensure any additional malware is delivered only to intended victims. Counterintuitively, supply chain operations add an additional layer of obscurity to the group's operations because it is difficult to pinpoint the desired target set.

- In a June 2018 supply chain compromise, APT41 leveraged MAC addresses and C:\ drive volume serial numbers to identify specifically targeted victims for follow-on activity. This significantly obfuscates the targeted sector or victim set; in a typical spear-phishing campaign, for example, desired targeting can be discerned based on recipients' email addresses.

**Table 1.** Supply chain compromises.

| Date                      | Compromised Entities   | FireEye Attribution Assessment                                |
|---------------------------|--|---|
| December 2014             | Online games distributed by a Southeast Asian video game distributor <ul style="list-style-type: none"> <li>Path of Exile</li> <li>League of Legends</li> <li>FIFA Online 3</li> </ul> | Possibly APT41 or a close affiliate                           |
| March 2017                | CCleaner Utility   | Unconfirmed APT41   |
| July 2017                 | Netsarang software packages (aka ShadowPad)  | Confirmed APT41   |
| June 2018 - November 2018 | ASUS Live Update utility (aka ShadowHammer)  | Stage 1 unconfirmed APT41<br>Reported Stage 2 confirmed APT41 |
| July 2018                 | Southeast Asian video game distributor<br>Infestation<br>PointBlank  | Confirmed APT41   |



## December 2014

**In December 2014, installers for three online games published by a Southeast Asian video game distributor were injected with the SOGU backdoor. The installer for these popular games was replaced by a malicious file that dropped the SOGU backdoor along with the normal game installer.**

- The video game distributor operates servers in East and Southeast Asia for some of the most popular online games, including the three games that were compromised: Path of Exile, League of Legends, and FIFA Online 3 (Table 2).

We have observed many similarities between TTPs involved in this compromise and APT41, including:

- Targeting the same victim organization 31 days apart
- Use of code-signing certificates from the same video game-related issuer organizations

- Use of the same malware families (HIGHNOON.BIN, HIGHNOON.LITE, EASYNIGHT, FRONTWHEEL)
- Use of HIGHNOON.BIN samples with the same compile times
- Overlap in domain resolution to the same IP netblock (61.38.186.0/24) during the same time frame in 2012
- Video game-related supply chain targeting

Despite these compelling overlaps, the actors responsible for this compromise leverage additional unique tools not observed with APT41 or any other Chinese espionage group, suggesting that they are either part of APT41 and maintain their own toolset, or a close affiliate of APT41 that shares both tools and taskings.

**Table 2.** 2014 compromised games.

| Game              | File MD5                         | Malware | C&C            |
|-------------------|----------------------------------|---------|----------------|
| Path of Exile     | 72499e9734ea73e1593cf75c3b26cef0 | SOGU    | gs4.playdr2.tw |
| League of Legends | 645925ca66990f8504d9632f7c7b3ae6 | SOGU    | gs4.playdr2.tw |
| FIFA Online 3     | 1b135f38c68cab15ef47dfbcbb7ab7b9 | SOGU    | gs4.playdr2.tw |

## March 2017

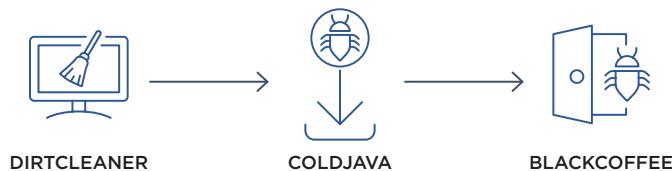
In March 2017, suspected Chinese espionage operators targeted CCleaner, a utility that assists in the removal of unwanted files from a computer. According to the parent company, Avast, the infected CCleaner was downloaded by 2.27 million customers. While we have identified some overlaps between the CCleaner activity and APT41, we do not have enough information to attribute the CCleaner compromise to APT41 at this time.

- Both APT41 and the actors in the CCleaner incident used TeamViewer during initial compromise. According to Avast, the actors used TeamViewer to compromise a developer workstation and used VBScript (x64.vbs) to drop a malicious payload.
- The compromised CCleaner update (which we call DIRTICLEANER) is believed to download a second-stage loader (MD5: 748aa5fcfa2af451c76039faf6a8684d) that contains a 32-bit and 64-bit COLDJAVA DLL payload. The COLDJAVA payload contains shellcode that loads a variant of BLACKCOFFEE (Figure 8).
  - While COLDJAVA has been used by APT41, BLACKCOFFEE has been used by other Chinese cyber espionage groups, including APT17 and APT40. It is possible that COLDJAVA may also be shared between distinct cyber espionage operators.
- Malware samples identified in the CCleaner incident included notable shared design decisions observed in APT41 malware, including the use of domain generation

algorithms (DGA) for C&C, use of dead drop resolvers (**DDR**), and use of shellcode as primary payloads. However, FireEye malware analysis of the compromised CCleaner samples and associated COLDJAVA samples did not reveal shared code with the POISONPLUG and POISONPLUG.SHADOW malware samples used in similar supply chain incidents by APT41.

- DIRTICLEANER uses DGA to generate new C&C domains each month. This is similar to first-stage malware used in the Netsarang compromise described below.
- The BLACKCOFFEE sample reaches out to actor-controlled profiles hosted on legitimate websites to retrieve encoded commands for C&C, a technique known as DDR. The malware parses the content of the websites (listed in Table 3), looking for 12 bytes contained between the tags: "BSM1crOSoft" and "SBM1crOSoft." APT41 POISONPLUG samples have also used DDR for C&C.
- The POISONPLUG and POISONPLUG.SHADOW samples in similar supply chain incidents use a shellcode format that resembles PE files, while the BLACKCOFFEE backdoor that was delivered in the CCleaner compromise uses a traditional PIC blob. Additionally, there is apparent code reuse between observed POISONPLUG and POISONPLUG samples not observed in the CCleaner samples.

**Figure 8:** Malware downloaded by DIRTICLEANER.



**Table 3.** BLACKCOFFEE DDR websites.

| File MD5                         | Legitimate DDR Websites Used for C&C   |
|----------------------------------|--|
| 3ca2a13f646690481dc15d78bac6d829 | <a href="https://github.com/search?q=joinlur&amp;type=Users&amp;utf8=%E2%9C%93">https://github.com/search?q=joinlur&amp;type=Users&amp;utf8=%E2%9C%93</a><br><a href="https://en.search.wordpress.com/?src=organic&amp;q=keepost">https://en.search.wordpress.com/?src=organic&amp;q=keepost</a> |



## July 2017

**In July 2017, APT41 injected malicious code into a software update package maintained by Netsarang and signed it with a legitimate Netsarang certificate in an operation referred to as "ShadowPad" by Kaspersky. The software package is reportedly used by hundreds of companies worldwide.**

- We observed numerous opportunistic infections associated with POISONPLUG.SHADOW spanning 13 countries and a variety of industries, demonstrating the broad impact of this operation. However, we have not observed the associated second-stage at any victim organizations. Open-source reporting indicated one victim was identified in Hong Kong.
- Signing the malicious update with a legitimate NetSarang certificate is consistent with APT41's pattern of using legitimate certificates. In this case, all updates were required to be signed by Netsarang, which means APT41 had to use the code-signing certificate to subvert the update mechanism.

- Alternatively, it is also possible that APT41 injected malicious code into the package prior to compilation, circumventing the need to steal the code-signing certificate and compile it on their own.
- The first stage of the malware uses DGA, which changes its C&C servers monthly. The use of shifting network infrastructure is most likely intended to add operational robustness and to reduce detection.
- The second-stage shellcode is initialized only after it is activated using a decryption key retrieved from the first-stage DNS communications. This likely allows APT41 to selectively activate the payload on specific victim systems. The second-stage payload contains the default C&C server, notped.com, which overlaps with other APT41 C&C infrastructure. Other reported APT41 domains that may also be related to the second-stage payload can be found in Table 4.

**Table 4.** Reported APT41 domains associated with POISONPLUG.SHADOW.

| Domain             | Associated Malware Family |
|--------------------|---------------------------|
| notped.com         | POISONPLUG.SHADOW         |
| dnsogle.com        | SOGU                      |
| operatingbox.com   | POISONPLUG                |
| paniesx.com        | Unknown                   |
| techniciantext.com | Unknown                   |



## June 2018

In June 2018, a utility used to update ASUS computers was compromised in an operation dubbed “**ShadowHammer**” by Kaspersky. Open-source reporting indicated that more than 50,000 systems installed the malicious update, yet the malware was only designed to execute and retrieve second-stage malware on a designated list of approximately 600 systems, demonstrating this was a targeted campaign. Public reporting on the incident noted that many of the targeted MAC addresses were associated with wireless adapters from various vendors, partially indicating the operation’s targeting strategy.

- Although we have limited visibility into the intended targets of this operation, we observed one of the whitelisted MAC addresses on a system at a telecom company.
- Kaspersky’s analysis of the infected machines revealed that a POISONPLUG backdoor was installed as a result of the malicious update. While we have been unable to attribute the DAYJOB malware used in the incident to APT41 due to an inability to independently confirm this

sequence of events, we confirm the reported stage-two POISONPLUG backdoor is attributed to APT41, contained several gaming references, and was likely used to target the gaming industry.

- The POISONPLUG sample (MD5: 37e100dd8b2ad8b301b130c2bca3f1ea) attempts to connect to a Google document that was created under the same name and email address (Tom Giardino and hrsimon59@gmail.com) that was used to target the cryptocurrency organization. It also attempts to connect to a Steam community page (Table 5).
- The POISONPLUG payload uses DDR and parses the Google document for a C&C command. The Steam community page is likely used as a fallback mechanism.
- FireEye malware analysis of the POISONPLUG sample indicates the malware is likely designed to run only one system with a C: drive volume serial number of 0xc25cff4c.
- Additional POISONPLUG samples located in Table 6 also leverage Google Document and Steam Community Pages for C&C.

**Table 5.** “ShadowHammer” stage-two POISONPLUG sample.

| File MD5                         | C&C Domain   |
|----------------------------------|--|
| 37e100dd8b2ad8b301b130c2bca3f1ea | <a href="https://docs.google.com/document/d/1iQwnF3ibWPZ6-95VHrRAPrL6u_UT_K7X-rQrB7xt95k">https://docs.google.com/document/d/1iQwnF3ibWPZ6-95VHrRAPrL6u_UT_K7X-rQrB7xt95k</a><br><a href="https://steamcommunity.com/id/oswal053">https://steamcommunity.com/id/oswal053</a> |

**Table 6.** POISONPLUG samples leveraging dead drop resolving.

| File MD5                         | C&C Domain   |
|----------------------------------|--|
| 557ff68798c71652db8a85596a4bab72 | <a href="https://docs.google.com/document/d/1KJ_RJRtkKhcuJjXOCKtEOLuwH3sRi72PUhtfuknycRc">https://docs.google.com/document/d/1KJ_RJRtkKhcuJjXOCKtEOLuwH3sRi72PUhtfuknycRc</a>  |
| ff8d92dfbcda572ef97c142017eec658 | <a href="https://docs.google.com/document/d/1TkTC3fHUvEBsBurZIGw7Kf5YsPjblpahl1FksRDCuTo">https://docs.google.com/document/d/1TkTC3fHUvEBsBurZIGw7Kf5YsPjblpahl1FksRDCuTo</a><br><a href="https://steamcommunity.com/id/119887132">https://steamcommunity.com/id/119887132</a> |
| b0877494d36fab1f9f4219c3defbf19  | <a href="https://docs.google.com/document/d/1iQwnF3ibWPZ6-95VHrRAPrL6u_UT_K7X-rQrB7xt95k">https://docs.google.com/document/d/1iQwnF3ibWPZ6-95VHrRAPrL6u_UT_K7X-rQrB7xt95k</a>  |
| ffd0f34739c1568797891b9961111464 | <a href="https://docs.google.com/document/d/1ICySd5ZNGj9Jz8pigZsuv8lciusYKqOq0Rpe2E0zgmU">https://docs.google.com/document/d/1ICySd5ZNGj9Jz8pigZsuv8lciusYKqOq0Rpe2E0zgmU</a><br><a href="https://steamcommunity.com/id/869406565">https://steamcommunity.com/id/869406565</a> |



## July 2018

**Beginning in July 2018, APT41 appeared to have directly targeted several East and Southeast Asia-based video game developers and distributors to inject legitimate executables with the CRACKSHOT backdoor.**

- Like other high-profile supply chain compromises attributed to APT41, these incidents included the incorporation of malicious code into legitimate executables and the signing of these files using legitimate digital certificates from the same compromised organization.

- APT41 used a C&C domain that masquerades as Xigncode, bugcheck.xigncodeservice.com, in the compromise of the video game PointBlank. Ironically, Xigncode is a service intended to prevent hacking and cheating in online games.
- We attribute these compromises (also reported by both **ESET** and **Kaspersky**) to APT41 based on the unique use of the CRACKSHOT backdoor and tactics consistent with APT41 operations. A list of related indicators is in Table 7.

**Table 7.** Video games industry targeting in July 2018.

| Targeted Game / Platform            | MD5 Hashes   | Malware   | C&C Domain          |
|-------------------------------------|--|-----------|---------------------|
| Southeast Asian video game platform | 04fb0ccf3ef309b1cd587f609ab0e81e   | CRACKSHOT | gxxservice.com      |
| Infestation game                    | fcfab508663d9ce519b51f767e902806   | CRACKSHOT | infestexe.com       |
| PointBlank game                     | 0b2e07205245697a749e422238f9f785<br>272537bbd2a8e2a2c3938dc31f0d2461<br>dd792f9185860e1464b4346254b2101b | CRACKSHOT | xigncodeservice.com |

# Overlaps Between Espionage and Financial Operations

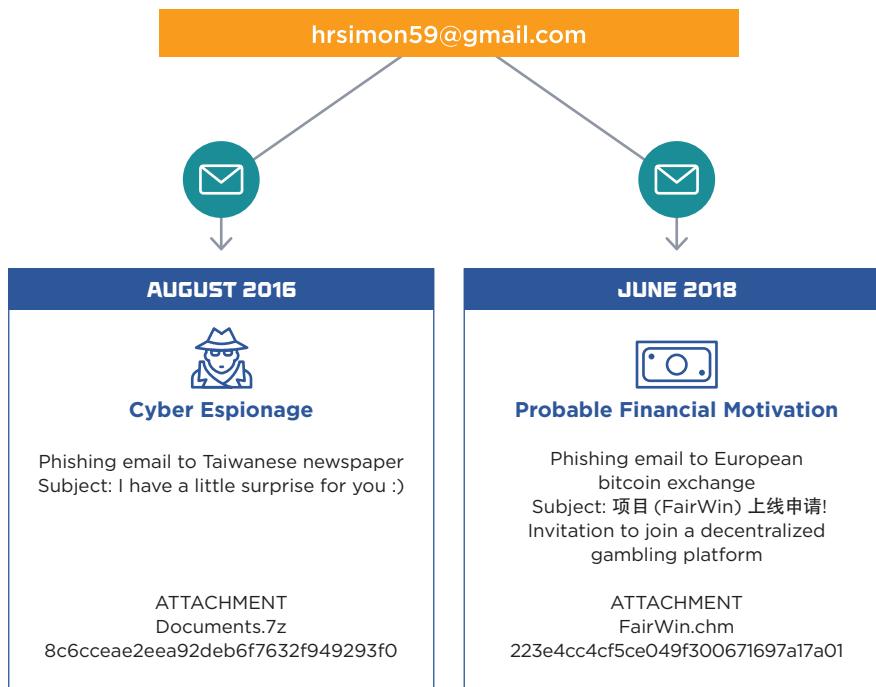
Identified overlaps across various incidents attributed to APT41 demonstrate the group's dual nature. Figure 9 and Figure 10 illustrate crossover between espionage and financially motivated activity, as well as technical similarities in tools used across both types of operations.

- The email address hrsimon59@gmail.com was used to send spear-phishing emails to a Taiwanese newspaper with the subject lure "I have a little surprise for you :)" in an espionage campaign in August 2016 (Figure 9).
- The same email address was later used to target a cryptocurrency exchange in June 2018, demonstrating email reuse between espionage operations and financially motivated activity.

- The lure used to target the cryptocurrency exchange (displayed in Figure 5 and translated in Figure 6) referenced an online gaming platform, tying the cryptocurrency targeting to APT41's focus on video game-related targeting.
- As depicted in Figure 10, hrsimon59@gmail.com was used to create a Google document being used as a POISONPLUG (MD5: 37e100dd8b2ad8b301b130c2bca3f1ea) C&C. As previously mentioned, this sample also connected to a Steam page.

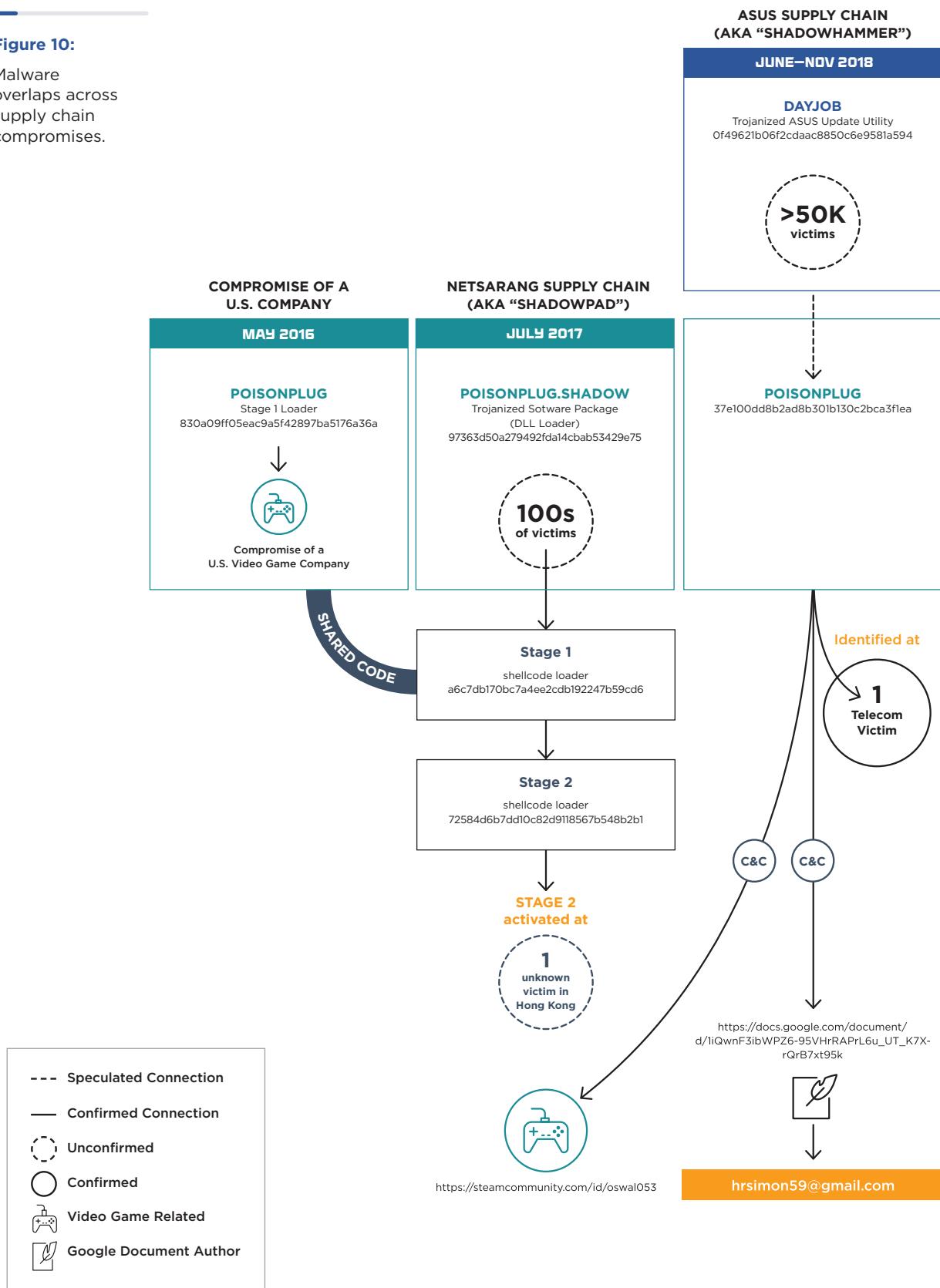
**Figure 9:**

Email overlaps between espionage and financial activity.



**Figure 10:**

Malware overlaps across supply chain compromises.



**Figure 11:**

POISONPLUG  
API hashing (MD5:  
830a09ff05eac9a5  
f42897ba5176a36a).

|                 |       |                     |
|-----------------|-------|---------------------|
| seg000:00010246 | movzx | edi, byte ptr [eax] |
| seg000:00010249 | ror   | esi, 8              |
| seg000:0001024C | or    | edi, 20h            |
| seg000:0001024F | add   | esi, edi            |
| seg000:00010251 | add   | eax, 2              |
| seg000:00010254 | xor   | esi, 7C35D9A3H      |
| seg000:0001025A | cmp   | [eax], dx           |
| seg000:0001025D | jnz   | short loc_10246     |
| seg000:0001025F | cmp   | esi, 0FD5B1261h     |

**Figure 12:**

POISONPLUG.  
SHADOW API  
hashing (MD5:  
a6c7db170bc7a4  
ee2cdb192247b5  
9cd6).

|                              |       |                     |
|------------------------------|-------|---------------------|
| g000:0000F55C 0F B6 0E       | movzx | ecx, byte ptr [esi] |
| g000:0000F55F 8B 45 F4       | mov   | eax, [ebp-0Ch]      |
| g000:0000F562 C1 C8 08       | ror   | eax, 8              |
| g000:0000F565 83 C9 20       | or    | ecx, 20h            |
| g000:0000F568 03 C1          | add   | eax, ecx            |
| g000:0000F56A 35 A3 D9 35 7C | xor   | eax, 7C35D9A3H      |
| g000:0000F56F 83 C6 02       | add   | esi, 2              |
| g000:0000F572 89 45 F4       | mov   | [ebp-0Ch], eax      |
| g000:0000F575 66 39 3E       | cmp   | [esi], di           |
| g000:0000F578 75 DD          | jnz   | short loc_F557      |
| g000:0000F57A 3D 61 12 5B FD | cmp   | eax, 0FD5B1261h     |

- FireEye malware analysis identified source code overlaps between malware used by APT41 in May 2016 targeting of a U.S.-based game development studio and the malware observed in supply chain compromises in 2017 and 2018.

- In May 2016, APT41 deployed a POISONPLUG sample at a U.S.-based game development studio. The stage-one loader for this sample (MD5: 830a09ff05eac9a5f42897ba5176a36a) shares code overlaps with the stage-one shellcode loader (MD5: a6c7db170bc7a4ee2cdb192247b59cd6) used in the Netsarang compromise, first reported by Kaspersky as ShadowPad. These connections, illustrated in Figure 10, led us to identify the malware used in the Netsarang incident as a variant of POISONPLUG (therefore: POISONPLUG.SHADOW).
- The POISONPLUG and POISONPLUG.SHADOW variants share the observed commonalities:
  - The entrypoint functions for both loaders use the same instructions, constants, and structures to pass control to loading routines.
  - The layout of functions and data within the loaders are the same; for example, following the entrypoint, both loaders contain an unusual region of structured data 0x60 bytes long.

- Both loaders use the same API hashing algorithm to resolve routines from system libraries (Figure 11 and Figure 12). The routine uses byte-wise operations to compute a hash, including byte-wise rotate-right by eight bytes, byte-wise binary, OR with 0x2, and byte-wise XOR using the four-byte key 0x7C35D9A3. Using this routine, the hash for kernel32.dll, a common DLL provided by Microsoft Windows, is 0xFD5B1261.

- FireEye analysis of a separate POISONPLUG payload (MD5: c8403fabda4d036a55d0353520e765c9) compiled in July 2017 and the POISONPLUG.SHADOW stage-two shellcode loader (MD5: 72584d6b7dd10c82d9118567b548b2b1) identified multiple additional plug-in similarities.
  - Core plug-in IDs between the samples are the same, including 100, 101, 102, 103, 104, and 201.
  - Core plug-in names are the same including Plugins, Online, Config, Install, and HTTP.
  - C&C plug-in IDs and names between both samples are the same, including 200/TCP, 201/HTTP, 202/UDP, 203/DNS, 204/HTTPS, and 205/SSL.
  - Both samples parse the C&C response by searching for "\$" characters and decoding the result.

# Attribution

We assess with high confidence that APT41 is attributable to Chinese individuals who are working on behalf of the Chinese state in conducting cyber espionage operations, and that these actors are also running financially motivated campaigns for personal gain.

Two identified personas using the monikers "Zhang Xuguang" and "Wolfzhi" linked to APT41's operations have also been identified in Chinese-language forums. Attribution to these individuals is backed by identified persona information, the previous work of these individuals, their apparent expertise in programming skills, and their targeting of Chinese market-specific games. It is uncertain how many other individuals may also be associated with APT41.

- Multiple domains leveraged by early APT41 activity were registered by emails and names associated with both Zhang Xuguang and Wolfzhi (or their alternative monikers). Registrant information also included references to Beijing and Chinese phone numbers (+86 country code).

Zhang Xuguang (张旭光) registered more than a dozen domains masquerading as video games or companies with trusted relationships with video game developers/distributors. Long-running activity provides a catalog of Zhang's efforts to improve his skills and expertise over time.

- Additional names include: kbkxlp, akbkxlp, injuriesa, ravinder10, Addison Lau, and addison jack
- Associated email addresses:
  - akbkxlp@126.com
  - akbkxlp@163.com
  - hackershby@126.com
  - injuriesa@126.com
  - injuriesa@163.com
  - injuriesa@gmail.com
  - injuriesa@hotmail.com

- injuriesa@qq.com
- kbkxlp@126.com
- ravinder10@126.com
- ravinder10@hotmail.com
- ravinder10@sohu.com

- Examples of domains registered to known aliases (some of these may have since been re-registered legitimately):
  - "Addison Lau"
    - agegamepay.com
    - ageofwuxia.com
    - ageofwuxia.info
    - ageofwuxia.net
    - ageofwuxia.org
    - gamewushu.com
    - microsOff.com
    - microsOtf.com
    - serverbye.com
  - "addison jack"
    - byeserver.com

In 2005, Zhang posted personal information on “**华夏黑客同盟**” (Chinese Hackers Alliance), a popular Chinese online forum, that listed his date of birth as 1989, that he previously lived in Inner Mongolia, and that he specialized in script hacking (Figure 13). Zhang's profile indicated he was 16, going on 17, and he was applying to be the administrator of a script hacking forum.

- Spoofed domains most likely targeted players of games such as "Age of Wuxia," a massively multiplayer online role-playing game (MMORPG) themed on cultural references to dynastic China. Zhang Xugang's interest in these games is also apparent in his registration and posting on a forum dedicated to the Age of Wuxia (Figure 14).

**Figure 13:**

Screenshot of Zhang's profile, with "Zhang Xuguang" highlighted in orange.

**四海边缘**

====【华夏黑客同盟】版主申请表=====

您在社区的注册名：四海边缘  
(为方便参与工作，请尽量用的注册名和QQ上的网名相同)

性别：男

申请的版面：脚本入侵

目前居住城市：内蒙古

职业及专长：脚本入侵

年龄（请填真实年龄）：16 过年 17 姓名：张旭光

上网类型：adsl

OICQ及OICQ网名：7891740

平均上网时间和时段（小时/天，请填具体点）：全天（差不多） 白天下午4点-第2天早上6点

您是否做过版主（副）或聊管？（如果是，请说明在那里）：NO 没做过

您平时常活动的版面有：脚本入侵

您申请当该版版主的详细理由：希望能为华夏出份力 也能自己学到一些知识和技巧，为了双方努力

**Figure 14:**

Zhang posting to Age of Wuxia forum, with his alias "injuriosa" highlighted in yellow.

《九阴真经》官方论坛

# 九陰真經

2010最值得期待的网络游戏大作

**标题：**(封贴已共享) 共享一区的号 有2区的来，，，，，留下QQ [\[打印本页\]](#)

**作者：**my113588      **时间：**2011-10-8 21:57      **标题：**(封贴已共享) 共享一区的号 有2区的来，，，，，留下QQ

这几忙 没时间玩 最多也就是晚上来看看 人物已建立 入武当 需要把二区的号给我共享 我晚上有时间玩 [ 本帖最后由 花儿相伴 于 2011-10-8 22:12 编辑 ]

**作者：**abc4525      **时间：**2011-10-8 21:58

2区的。。

**作者：**abc4525      **时间：**2011-10-8 21:59

怎么内线啊 不想把QQ留在帖子

**作者：**tianji007      **时间：**2011-10-8 21:59

397355685 2区

**作者：**beiai685      **时间：**2011-10-8 22:00

qq上谈吧，楼主 太急想进游戏里体验一番了 QQ: 546778473

**作者：**tianji007      **时间：**2011-10-8 22:00

**作者：**qq771232465      **时间：**2011-10-8 22:01

**作者：**injuriosa      **时间：**2011-10-8 22:01

**作者：**huangenhuan      **时间：**2011-10-8 22:01

五区的号和你共享 给我上10分钟就好了 Q1877259221

**作者：**tank1234ly      **时间：**2011-10-8 22:05

1132609844三区 只玩10分钟

Wolfzhi is linked to a 2017 profile on a data science community page, which indicated that he had 10 years working experience at the time of the posting, with significant experience in Oracle and Python. Other documents linked to his email accounts also highlight his programming skills and database experience.

- Additional aliases include: wolf\_zhi, wolfjiao, jiaozhiq, and jiaozhiqiang

- Examples of domains registered under the wolf\_zhi alias:
  - ibmupdate.com
  - linux-update.net
  - win7update.net
- Posts in a forum provide some indication he is from Beijing or Hebei, the surrounding Chinese province. This is also consistent with information found in early domain registrations created by Wolfzhi (Figure 15).

#### Domain: ibmupdate.com

**Figure 15:**

Domain registration by Wolfzhi.

|                         |   |
|-------------------------|---|
| <b>Registrant</b>       | wolfzhi<br>wolfzhi<br>beijingxxxadaxia<br>beijing<br>beijing, 100000<br>US<br>Tel. +86.2011111111 |
| <b>Creation Date:</b>   | 2011-08-23 15:23:29   |
| <b>Expiration Date:</b> | 2011-08-23 15:23:29   |

Additional indicators of Chinese attribution include: the reliance on malware used exclusively by Chinese espionage operators, the use of Chinese-language strings, time zone and operational time analysis, and targeting consistent with Beijing's interests.

- The use of tools leveraged only by several other Chinese operators such as HOMEUNIX and HIGHNOON provides some indication that APT41 relies on the similar resources and support as these other Chinese groups. APT41 also leverages PHOTO (aka "Derusbi") and SOGU (aka "Destroy RAT" and "PlugX"), tools shared much more widely among Chinese espionage groups. See the section "Links to Other Known Chinese Operators" for more details.
- An APT41 HIGHNOON sample (MD5: 36711896cfab67f599305b590f195aec) from 2012 contained a process debugging path (.pdb) with the Chinese-language directory "D:\桌面\木马," which translates to "D:\Desktop\trojan."

- Compiled HTML (.chm) files used in targeting contained a language code set to "Chinese (Simplified)" despite the lure content being in the target region's language (English or otherwise).
- Compile and operational times of APT41 activity suggest the bulk of the group's work hours, 10:00 and 23:00 (UTC +8), are consistent with the Chinese workday, especially for tech sector employees on a "996 schedule."
  - Figure 4 shows a breakdown of all of the operational activity within victim environments, separated between gaming and espionage (non-gaming) activity. Analysis of the times where APT41 modified or accessed a file within a victim environment, shows a concentration between 10:00 and 18:00 (UTC+8).
- Targeting of healthcare, semiconductors, and telecoms is consistent with Chinese state interests and parallels activity from other Chinese espionage groups.

# Status as Potential Contractors

We assess with moderate confidence that APT41 is constituted of contractors tasked by the Chinese state to conduct espionage operations. Individuals attributed to the group have previously indicated that they could be hired and advertised their skills and services. APT41's use of the same malware in both financial- and espionage-related operations could support their status as contractors; state employees are less likely to use such tools for personal financial gain over multiple years given the potential for greater scrutiny or punishment.

- APT41 cyber crime activity includes the use of espionage-only malware, indicating two possible conclusions: either APT41 is operating outside of state control but still working with other Chinese APT malware actors, tools, and infrastructure on a part-time or contractual basis, or APT41 is a full-time, state-sponsored APT actor but is also working outside of state control or direction for supplemental income.
  - Tools used by APT41 in financially motivated operations include the use of HOMEUNIX and PHOTO, which are non-public malware used only by other Chinese espionage actors.
  - A loose time separation between espionage and cyber crime activities provides some indication that the group divides its work hours between both types of operations. For additional details, see Figure 4 and the previous section "Financially Motivated Activity."

- **Public reports** on Chinese hackers highlight that skilled actors opt to work for private sector entities that have government contracts because of better pay.
- Underground activity dating back to 2009 indicated that Zhang Xuguang is a hacker for hire. Zhang advertised on forums that he was available for professional penetration and hacking services.
  - Zhang listed his online hours from 4:00 p.m. – 6:00 a.m., which are similar to the operational times observed at gaming targets displayed in Figure 4.
- He was also observed sharing an injection tool named Ocean hysi (海洋hysi注入工具) to demonstrate his skills, as displayed in Figure 16.

China has previously relied on contractors to bolster state resources dedicated to cyber espionage activity. Increased integration between government units and civilian entities, including contractors and freelancers, is believed to be a **key feature of Chinese cyber policy**.

- According to indictments unsealed by the U.S. Department of Justice (USDOJ) in December 2018, APT10 was operated by contractors working for the China's Ministry of State Security (MSS).
- In a USDOJ indictment unsealed in November 2017, individual contractors responsible for APT3 were found to be working for an MSS front company.

**Figure 16:**

Ocean injection tool posted by Zhang.



# Links to Other Known Chinese Espionage Operators

APT41 uses many of the same tools and compromised digital certificates that have been leveraged by other Chinese espionage operators. Initial reports about HIGHNOON and its variants (reported publicly as "Winnti") dating back to at least 2013 indicated the tool was exclusive to a single group, contributing to significant conflation across multiple distinct espionage operations.

- APT41 overlaps at least partially with public reporting on groups including BARIUM ([Microsoft](#)) and Winnti ([Kaspersky](#), [ESET](#), [Clearsky](#)). In some cases, the primary observed similarity in the publicly reported Winnti activity was the use of the same malware—including HIGHNOON—across otherwise separate clusters of activity.
- Previous FireEye Threat Intelligence reporting on the use of HIGHNOON and related activity was grouped together under both GREF and Mana, although we now understand this to be the work of several Chinese cyber espionage groups that share tools and digital certificates.
- APT41 reflects our current understanding of what was previously reported as GREF, as well as additional indicators and activity gathered during our extensive review of our intelligence holdings.

## Certificate Overlap

A digital certificate issued by YNK Japan that was publicly reported as being used by Winnti has been used by multiple Chinese espionage operators, including APT17, and APT20, and APT41.

A self-signed digital certificate purporting to be from the Microsoft Certificate Authority has been used by both APT41 and APT40 to sign samples of the PHOTO backdoor.

The overlaps in groups observed using these certificates is illustrated in Table 8.

**Issuer:** CN=VeriSign Class 3 Code Signing 2009-2 CA  
**Subject:** CN=YNK JAPAN Inc  
**Serial Number:** 67:24:34:0d:db:c7:25:2f:7f:b7:14:b8:12:a5:c0:4d  
**Issue-Date:** 11/27/09 , **Expiration-Date:** 11/27/11

**Issuer:** CN=Microsoft Certificate Authority  
**Subject:** CN=Microsoft Certificate Authority  
**Serial Number:** (Negative)77:62:e5:c6:c9:c2:75:59:b0:b8:f5:56:60:61:d8:78  
**Issue-Date:** 12/31/2009, **Expiration-Date:** 12/30/2035

**Table 8.** Example of shared certificates between APT groups.

| Serial Number   | Subject                         | APT17 | APT20 | APT40 | APT41 |
|---|---------------------------------|-------|-------|-------|-------|
| 67:24:34:0d:db:c7:25:2f:7f:b7:14:b8:12:a5:c0:4d           | YNK JAPAN Inc                   | X     | X     |       | X     |
| (Negative)77:62:e5:c6:c9:c2:75:59:b0:b8:f5:56:60:61:d8:78 | Microsoft Certificate Authority |       |       | X     | X     |

## Launcher Overlap

The use of DLL side-loading has been a source of continued confusion when used as an indicator for distinct operations. This **technique** uses a legitimate and often digitally signed executable to essentially trick a system into launching a malicious DLL because it has been given the same name as a legitimate DLL normally loaded by the executable. The use of a valid and digitally signed

executable allows actors to bypass host-based security measures. For this reason, it continues to be popular mechanism used by multiple groups. This also explains why the use of these DLL filenames is not a unique indicator for distinct APT operators. Table 9 contains legitimate executables used by APT41 and selected other Chinese cyber espionage groups for DLL side-loading:

**Table 9.** Legitimate files used by different APT groups for DLL side-loading.

| File MD5 Hash                    | Filename      | APT9 | APT10 | APT20 | APT41 |
|----------------------------------|---------------|------|-------|-------|-------|
| 09b8b54f78a10c435cd319070aa13c28 | nvSmartEx.exe | X    | X     | X     | X     |
| 26a196afc8e6aff6fc6c46734bf228cb | form.exe      | X    |       |       | X     |

## Code Family Overlap

A significant number of non-public tools used by APT41 are shared with other distinct Chinese espionage operators. Source code overlaps between observed code families indicate potential access to shared code repositories or common developers between groups.

- APT41 has used several malware families that have also been used by other Chinese espionage operators, including variants of HIGHNOON, HOMEUNIX, PHOTO, SOGU, and ZXHELL, among others. Table 10 illustrates some of overlap between malware families used by APT41 and other APT groups. Note that this is only for illustration purposes and is not indicative of all observed malware families used by these APT groups or all groups that have used those families.

- HIGHNOON, one of the main code families observed being used by APT41, was also used by APT17 in 2015 to target semiconductor and chemical manufacturers.
- HOMEUNIX, another popular backdoor used by APT41, has been used by at least 14 separate Chinese espionage groups, including APT1, APT10, APT17, APT18, and APT20.
- JUMPALL is a dropper that has been observed dropping variants of the HIGHNOON, ZXHELL, and SOGU code families attributed to APT17 and APT41.

**Table 10.** Code family overlap among different Chinese espionage groups.

| Malware       | APT1 | APT3 | APT10 | APT17 | APT18 | APT19 | APT40 | APT41 |
|---------------|------|------|-------|-------|-------|-------|-------|-------|
| BLACKCOFFEE   |      |      |       | X     |       |       | X     | X     |
| CHINACHOP     |      |      |       | X     |       |       | X     | X     |
| COLDJAVA      |      |      |       |       |       |       |       | X     |
| HIGHNOON      |      |      |       |       | X     |       |       | X     |
| HIGHNOON.BIN  |      |      |       |       | X     |       |       | X     |
| HIGHNOON.LITE |      |      |       |       |       |       |       | X     |
| HOMEUNIX      | X    |      | X     | X     | X     |       |       | X     |
| JUMPALL       |      |      |       |       | X     |       |       | X     |

**Table 11.** CLASSFON sample with internal name "DrvDll.dll" and contains reference to "PlusDll.dll".

| File MD5 Hash                    | Malware  | Internal Filename | Device Driver Name |
|----------------------------------|----------|-------------------|--------------------|
| 9e1a54d3dc889a7f0e56753c0486fd0f | CLASSFON | DrvDll.dll        | PlusDll.dll        |

**Table 12.** APT41 HIGHNOON.BIN samples that reference "PlusDll.Dll".

| File MD5 Hash                    | Malware      | Process Debugging Path                                      |
|----------------------------------|--------------|---|
| 36711896cfbe67f599305b590f195aec | HIGHNOON.BIN | D:\桌面\木马\Anti_winmm\ApplInit\ApplInit\Release\ApplInit.pdb  |
| a0a96138b57ee24eed31b652ddf60d4e | HIGHNOON.BIN | H:\RBDoor\Anti_winmm\ApplInit\ApplInit\Release\ApplInit.pdb |

- APT41 has not only shared the same tools with other Chinese espionage operators but also appears to have access to shared source code or developers as well.
- APT41 has used CROSSWALK.BIN, a kernel driver, to circumvent firewalls and covertly send data. Another Chinese espionage group used a similar tool, CLASSFON, to covertly proxy network communications in 2011.
- CLASSFON (MD5: 9e1a54d3dc889a7f0e56753c0486fd0f) has an internal name of DrvDll.dll and an embedded device driver that is internally named PlusDll.dll (Table 11). The PlusDll.dll filename has also been identified in APT41 HIGHNOON.BIN samples (Table 12).

- PDB paths identified in related APT41 HIGHNOON.BIN samples contain the name "RBDoor," which has also been identified in samples of HIGHNOON, HIGHNOON.LITE, HIGHNOON.CLI, and GEARSHIFT (Figure 17). APT41 files containing PDB paths referencing "RBDoor" are listed in Table 13. At least two of these malware families, HIGHNOON.CLI and GEARSHIFT, have been used by APT17 and another suspected Chinese espionage group.
- Further information regarding code family overlaps between variants can be found in "Technical Annex: Additional Malware Overlaps."

**Figure 17:**  
PDB paths  
containing  
"RBDoor".

H:\Double-V1\stone\_srv\Bin\RbDoor64.pdb  
H:\Double\Door\_wh\AppInit\x64\Release\AppInit.pdb  
H:\Double\Door\_wh\RbDoorX64\x64\Release\RbDoorX64.pdb  
H:\Double\door\_wh\_kav\Bin\RbDoor64.pdb  
H:\RBDoor\Anti\_winmm\AppInit\AppInit\Release\AppInit.pdb  
H:\RBDoor\Anti\_winmm\AppInit\AppInit\x64\Release\AppInit.pdb  
H:\RBDoor\Anti\_winmm\AppInit\ShutdownEvent\x64\Release\ShutdownEvent.pdb  
H:\RbDoor\Anti\_winmm\AppInit\AppInit\Release\AppInit.pdb  
H:\RbDoor\Anti\_winmm\AppInit\RbDoorX64\Release\RbDoor.pdb  
H:\RbDoor\Anti\_winmm\AppInit\ShutdownEvent\Release\ShutdownEvent.pdb  
H:\RbDoor\Lib\WMI\_SSL\RemoteLib\bin\TestRjLib.pdb  
H:\Svn\Double-V1\stone\_srv\Bin\RbDoor64.pdb

**Table 13.** APT41 samples with PDB paths containing "RBDoor".

| File MD5 Hash                     | Malware      |
|-----------------------------------|--------------|
| 46a557fbfce734a6794b228df0195474  | HIGHNOON     |
| 77c60e5d2d99c3f63f2aea1773ed4653  | HIGHNOON     |
| a0a96138b57ee24eed31b652ddf60d4e  | HIGHNOON.BIN |
| 7d51ea0230d4692eedc2d5a4cd66d2d   | HIGHNOON.BIN |
| 849ab91e93116ae420d2fe2136d24a87  | HIGHNOON.BIN |
| ba08b593250c3ca5c13f56e2ca97d85e  | JUMPALL      |
| f8c89cccd8937f2b760e6706738210744 | GEARSHIFT    |
| 5b26f5c7c367d5e976aaba320965cc7f  | GEARSHIFT    |

# Use of Code-Signing Certificates

**APT41 regularly leverages code-signing certificates to sign malware when targeting both gaming and non-gaming organizations. Notably, most of the digital certificates being used in this manner are valid unrevoked digital certificates stolen from East Asia-based game development studios. APT41 likely signs their malware to ensure compatibility with the targeted systems and to potentially avoid detection.**

- Microsoft **requires** all kernel-mode drivers to be signed in order to run on operating systems running Windows Vista or later.
- The use of code-signing certificates can also significantly decrease the likelihood that a malicious payload is detected.

Although we do not have direct evidence of APT41 specifically targeting and stealing code-signing certificates, we have some indication from targeting of affected organizations within the same time frame that digital certificates are first compromised and used to sign malware.

- Stealing private keys or compromising an organization's infrastructure to access and steal digital certificates abuses trust relationships between firms and certificate authorities. Malicious files signed with valid digital certificates can circumvent automated scanning/blocking solutions and bypass Windows group policies which restrict unsigned code from running.
- Even when detected, malicious files signed by a digital certificate from a trusted partner or associated business are less likely to draw suspicion. According to an advertisement in an underground marketplace, the success rate of installing a payload increases by as much as 50 percent when signing files with valid digital certificates.

- In most cases, multiple digital certificates are issued to an organization using the same public name, making it more difficult to identify a compromised certificate among others with identical names.
- Certificate authorities are responsible for revoking compromised digital certificates, although response times can vary greatly, and digital certificates can continue to be abused even long after they are first identified being misused.
- Several malware samples were signed very close to the certificate issue date, suggesting that APT41 or a related actor had access to the private key or build environment at that time. It is also possible the group acquired the private keys soon after they were issued.
- In some cases, digital certificates were used to sign malware samples just before they expired, most likely indicating the actors were actively managing a library of digital certificates for this purpose.
- Figure 18 depicts compile times of malware signed with compromised digital certificates within the time frame that the certificates were valid. All of the certificates listed in the graphic have either been revoked or are currently expired. Indicators associated with these certificates are listed in "Technical Annex: Code Signing Certificates Used by APT41."
- Alternatively, it is possible APT41 may have purchased the digital certificates used for signing malware within an underground market. FireEye researchers found that code signing certificates are currently available for sale in underground marketplaces for as little as \$399 USD, although ones that go through rigorous vetting can be sold for \$1,699 USD.

**Figure 18:** First observed malware samples signed with digital certificates (white) in relation to valid certificate dates (blue).



# Outlook and Implications

APT41 is a dual threat demonstrating creativity and aggressiveness in carrying out both espionage campaigns and financially motivated operations. The group's capabilities and targeting have both widened over time, signaling the potential for additional supply chain compromises affecting more victims in additional verticals.

APT41's links to both underground marketplaces and state-sponsored activity may indicate the group enjoys protections that enables it to conduct its own for-profit activities, or authorities are willing to overlook them. It is also possible that APT41 has simply evaded scrutiny from Chinese authorities. Regardless, these operations underscore a blurred line between state power and crime that lies at the heart of threat ecosystems and is exemplified by APT41.

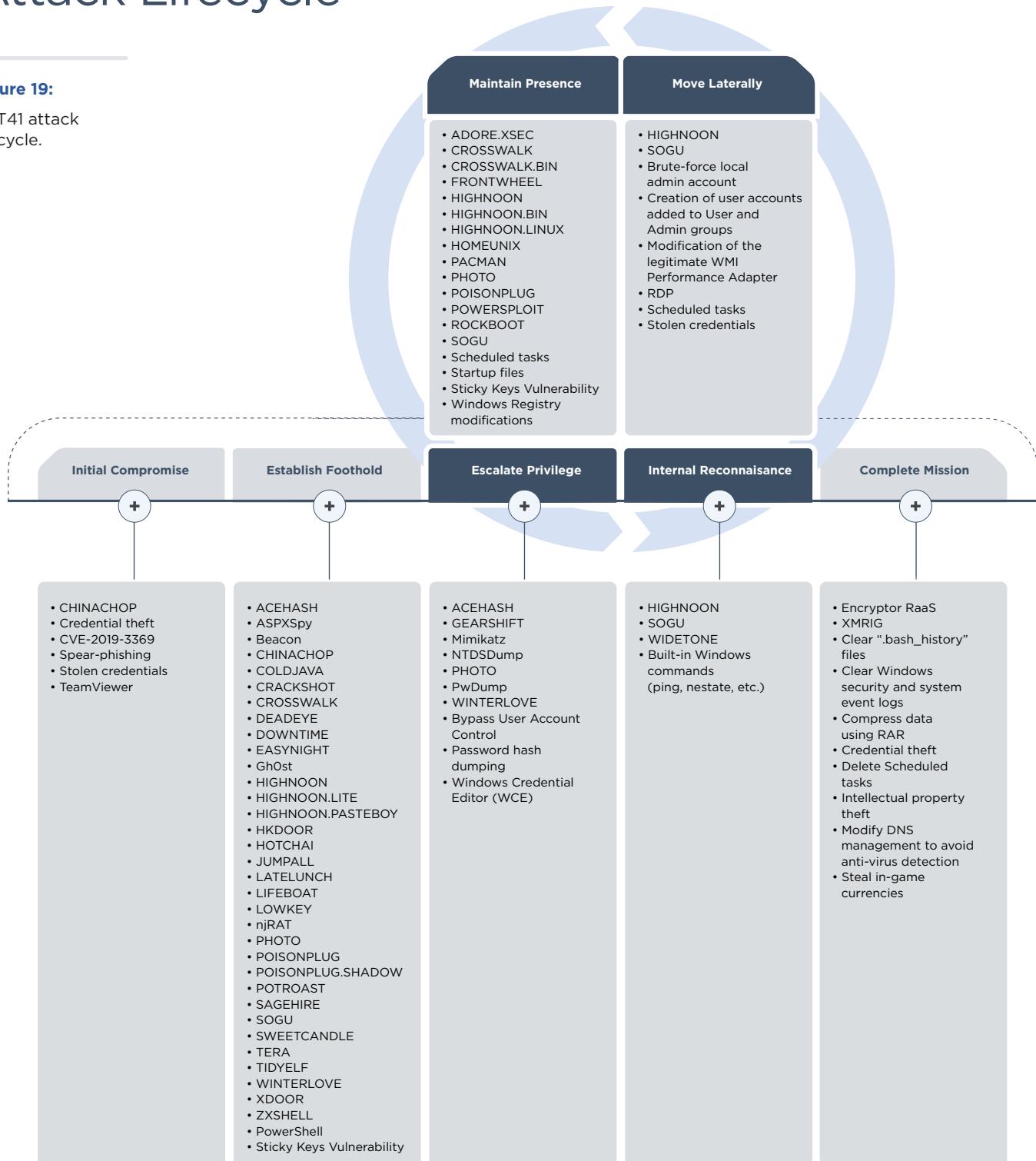


## TECHNICAL ANNEX

# Attack Lifecycle

**Figure 19:**

APT41 attack lifecycle.



## Initial Compromise

APT41 leverages a variety of techniques to perform an initial compromise, including spear-phishing, moving laterally from trusted third parties, leveraging stolen credentials, using the CHINACHOP web shell, and accessing victim organizations using remote desktop sharing software, such as TeamViewer. APT41 often relies on the use of simple spear-phishing email with attachments such as compiled HTML (.chm) files to initially compromise their victims. However, once in a victim organization, the operation can leverage more sophisticated TTPs and deploy additional malware tools.

- In a campaign running almost one year, APT41 compromised hundreds of systems and used close to 150 unique pieces of malware including backdoors, credential stealers, keyloggers, and rootkits.
- We have observed TeamViewer credentials used as an entry point in multiple intrusions across industries. In these instances, APT41 leveraged TeamViewer to transfer malware into the compromised environment, although we do not have direct evidence of APT41 compromising TeamViewer.
  - In July 2017, APT41 initiated a TeamViewer session and transferred files that were later deleted. Filenames and creation times indicate that these may have been the HIGHNOON backdoor.
  - In May 2018, APT41 used TeamViewer for initial entry in the compromise of a healthcare company. During this intrusion, APT41 started a TeamViewer session and shortly after transferred DLL files associated with the CROSSWALK backdoor to the victim environment before deploying CROSSWALK.

The group has leveraged several exploits in their operations. Notably, APT41 was observed using proof-of-concept exploit code for CVE-2019-3396 within 23 days after the Confluence vulnerability was announced.

### Observed Vulnerabilities

- CVE-2012-0158
- CVE-2015-1641
- CVE-2017-0199
- CVE-2017-11882
- CVE-2019-3396

APT41 compromised one organization and moved to a client environment.

## Establish Foothold

APT41 uses a variety of malware and tools, both public and unique to the group, to establish a foothold with a victim's environment, including:

- ASPXSpy
- ACEHASH
- Beacon
- CHINACHOP
- COLDJAVA
- CRACKSHOT
- CROSSWALK
- DEADEYE
- DOWNTIME
- EASYNIGHT
- Gh0st
- HIGHNOON.LITE
- HIGHNOON.PASTEBOY
- HOTCHAI
- HKDOOR
- JUMPALL
- LATELUNCH
- LIFEBOAT
- LOWKEY
- njRAT
- POISONPLUG
- POISONPLUG.SHADOW
- POTROAST
- SAGEHIRE
- SOGU
- SWEETCANDLE
- TERA
- TIDYELF
- XDOOR
- WINTERLOVE
- ZXHELL

APT41 has been observed using Linux and Windows variants of the same malware families, such as PHOTO and HIGHNOON. The group often initially installs its backdoors to c:\windows\temp.

We have observed APT41 attempting to masquerade their files and domains as popular anti-virus software:

- kaspersky.net
- macfee.ga
- symanteclabs.com

APT41 appears to use the commercially available Beacon backdoor that is part of the Cobalt Strike pen-testing software platform. In at least one instance, a server used for Beacon C&C was also leveraged for CROSSWALK C&C.

On multiple occasions, APT41 leveraged the Sticky Keys vulnerability and PowerShell to deploy malware families in victims' environments.

## Escalate Privileges

APT41 escalates its privileges in systems by leveraging custom-made and publicly available tools to gather credentials and dump password hashes. The tools include:

- ACEHASH
- GEARSHIFT
- GOODLUCK
- Mimikatz
- NTDSDump
- PHOTO
- PwDump
- WINTERLOVE

### Windows Credential Editor (WCE)

APT41 frequently uses the Windows Credential Editor to dump password hashes from memory and authenticate other user accounts.

## Internal Reconnaissance

APT41 conducts network reconnaissance after using compromised credentials to log on to other systems. The group leverages built-in Windows commands, such as "netstat" and "net share," in addition to the custom and non-public malware families SOGU, HIGHNOON, and WIDGETONE.

- HIGHNOON includes the ability to collect host information by enumerating active Remote Desktop Protocol (RDP) sessions.
- SOGU is capable of listing TCP and UDP network connections, respectively.
- WIDGETONE is capable of conducting port scans and password brute-force attacks and collecting network information. It contains an embedded variant of a publicly available enumeration tool and can be run with the following options:
  - "-hbs" option runs a port scan on the specified subnet.
  - "-hscan" scans the specified IP range for IPC and SQL services.
  - "-enum" queries a Windows host for requested information, such as users, groups/members, policies, and more.

## Lateral Movement

APT41 assesses the network architecture of an organization and identifies pivotal systems for enabling further access. The group has repeatedly identified intermediary systems that provide access to otherwise segmented parts of an organization's network (as outlined in Case Study: Video Game Industry Targeting). Once APT41 has identified intermediary systems, it moves quickly to compromise systems. In one case, hundreds of systems across several geographic regions were compromised in as little as two weeks.

APT41 uses multiple methods to perform lateral movement in an environment, including RDP sessions, using stolen credentials, adding accounts to User and Admin groups, and password brute-forcing utilities. The group will also use a compromised account to create scheduled tasks on systems or modify legitimate Windows services to install the HIGHNOON and SOGU backdoors.

- We observed APT41 using a compromised account to create a scheduled task on a system, write a binary component of HIGHNOON containing the payload and C&C information to disk, and then modify the legitimate Windows WMI Performance Adaptor (wmiApSrv) to execute the HIGHNOON payload.

APT41 frequently uses the publicly available utility WMIEEXEC to move laterally across an environment. WMIEEXEC is a tool that allows for the execution of WMI commands on remote machines. Examples of commands executed by the utility include:

```
cmd.exe /c whoami > C:\wmi.dll 2>&1  
cmd.exe /c del C:\wmi.dll /F > nul 2>&1  
cmd.exe /c a.bat > C:\wmi.dll 2>&1
```

## Maintain Presence

To maintain presence, APT41 relies on backdoors, a Sticky Keys vulnerability, scheduled tasks, bootkits, rootkits, registry modifications, and creating or modifying startup files. APT41 has also been observed modifying firewall rules to enable file and printer sharing to allow for inbound Server Message Block (SMB) traffic.

- APT41 leveraged ROCKBOOT as a persistence mechanism for PHOTO and TERA backdoors. The bootkit performs raw disk operations to bypass the typical MBR boot sequence and execute the backdoors prior to the host operating system. This technique was implemented to ensure the malware would execute at system runtime and was designed to be difficult to detect and prevent. APT41 ROCKBOOT samples have been signed with legitimate code-signing certificates from MGame and Neowiz, two South Korean video game companies.
- APT41 leveraged ADORE.XSEC, a Linux backdoor launched by the Adore-NG rootkit, throughout an organization's Linux environment. The group installed the backdoor and the Adore-NG rootkit persistently by creating a hidden shell script in "/etc/rc.d/init.d," a directory that contains the startup scripts for many system services. The Adore-NG rootkit is used to hide the backdoor and authenticate any incoming connections using a provided password.
- The group also uses CROSSWALK.BIN, FRONTWHEEL, HIGHNOON.BIN, HIGHNOON.LINUX, HOMEUNIX, and PACMAN to maintain presence.

In some instances, APT41 leveraged POISONPLUG as a first-stage backdoor to deploy the HIGHNOON backdoor in the targeted environment. We observed APT41 use PowerSploit with the capability to use WMI as a persistence mechanism. The group also deploys the SOGU and CROSSWALK malware families as means to maintain presence.

APT41 has demonstrated it is highly agile, responding quickly to changes in victim environments and incident responder activity.

- Hours after a victimized organization made changes to thwart APT41, the group registered a new C&C domain, compiled a new SOGU backdoor variant, and deployed the new backdoor to several systems across multiple geographic regions.
- APT41 sent spear-phishing emails to multiple HR employees three days after the compromise had been remediated and systems were brought back online. Within hours of a user opening the malicious attachment dropping a HOMEUNIX backdoor, APT41 regained a foothold within the environment by installing PHOTO on the organization's servers across multiple geographic regions.

### Avoiding C&C Detection

At times APT41 uses legitimate websites, such as GitHub, Pastebin, and Microsoft TechNet, to avoid detection. Interestingly, some of the group's POISONPLUG malware samples leverage the Steam Community website associated with Valve, a video game developer and publisher. This technique of storing encoded or encrypted strings, known as dead drop resolvers (DDR), on legitimate websites that can subvert network defenders as traffic to and from the sites is typically benign.

The group has also configured Linux backdoors to run on ports used by legitimate applications within victim environments, enabling malicious traffic to bypass network security measures and hide malicious activity within the organization's regular application traffic.

### Preventing Anti-Virus Updates

Before attempting to deploy the publicly available Ransomware-as-a-Service (RaaS) Encryptor RaaS through group policy, APT41 blocked victim systems from retrieving anti-virus updates by accessing the DNS management console and implementing a forward lookup on the domain used for anti-virus updates to the park IP address "1.1.1.1."

## Complete Mission

APT41 has been observed creating a RAR archive of targeted files for exfiltration. The group has also manipulated in-game currencies using the targets' databases after compromising production environments. During multiple engagements, APT41 attempted to remove evidence of some of its activity by deleting Bash histories, clearing Windows security and system events, and modifying DNS management to avoid anti-virus detections.

In at least one instance, the group attempted to deploy Encryptor RaaS. However, an operator's typo prevented the ransomware from executing in the victim's environment.

In another instance, APT41 deployed XMRig, a Monero cryptocurrency mining tool in a victim's environment.

## TECHNICAL ANNEX

# MITRE ATT&CK Mapping

| <b>Initial Access</b> |                                    | <b>Persistence</b>          |                                  |
|-----------------------|------------------------------------|-----------------------------|----------------------------------|
| <b>t1190</b>          | Exploit Public-Facing Application  | <b>t1015</b>                | Accessibility Features           |
| <b>t1133</b>          | External Remote Services           | <b>t1098</b>                | Account Manipulation             |
| <b>t1193</b>          | Spear-phishing Attachment          | <b>t1067</b>                | Bootkit                          |
| <b>t1195</b>          | Supply Chain Compromise            | <b>t1136</b>                | Create Account                   |
| <b>t1199</b>          | Trusted Relationship               | <b>t1038</b>                | DLL Search Order Hijacking       |
| <b>t1078</b>          | Valid Accounts                     | <b>t1133</b>                | External Remote Services         |
| <b>Execution</b>      |                                    | <b>t1179</b>                | Hooking                          |
| <b>t1059</b>          | Command-Line Interface             | <b>t1031</b>                | Modify Existing Service          |
| <b>t1223</b>          | Compiled HTML File                 | <b>t1050</b>                | New Service                      |
| <b>t1106</b>          | Execution through API              | <b>t1034</b>                | Path Interception                |
| <b>t1129</b>          | Execution through Module Load      | <b>t1108</b>                | Redundant Access                 |
| <b>t1203</b>          | Exploitation for Client Execution  | <b>t1060</b>                | Registry Run Keys / Start Folder |
| <b>t1061</b>          | Graphical User Interface           | <b>t1165</b>                | Startup Items                    |
| <b>t1170</b>          | Mshta                              | <b>t1078</b>                | Valid Accounts                   |
| <b>t1086</b>          | PowerShell                         | <b>t1100</b>                | Web Shell                        |
| <b>t1053</b>          | Scheduled Task                     | <b>Privilege Escalation</b> |                                  |
| <b>t1085</b>          | Rundll32                           | <b>t1134</b>                | Access Token Manipulation        |
| <b>t1064</b>          | Scripting                          | <b>t1015</b>                | Accessibility Features           |
| <b>t1035</b>          | Service Execution                  | <b>t1038</b>                | DLL Search Order Hijacking       |
| <b>t1204</b>          | User Execution                     | <b>t1034</b>                | Path Interception                |
| <b>t1047</b>          | Windows Management Instrumentation | <b>t1055</b>                | Process Injection                |
|                       |                                    | <b>t1078</b>                | Valid Accounts                   |
|                       |                                    | <b>t1100</b>                | Web Shell                        |

| <b>Defense Evasion</b>   |   | <b>Discovery</b>           |   |
|--------------------------|---|----------------------------|---|
| t1134                    | Access Token Manipulation                 | t1087                      | Account Discovery                             |
| t1009                    | Binary Padding                            | t1482                      | Domain Trust Discovery                        |
| t1146                    | Clear Command History                     | t1083                      | File and Directory Discovery                  |
| t1116                    | Code Signing                              | t1169                      | Permission Groups Discovery                   |
| t1140                    | Deobfuscate / Decode Files or Information | t1057                      | Process Discovery                             |
| t1089                    | Disabling Security Tools                  | t1063                      | Security Software Discovery                   |
| t1038                    | DLL Search Order Hijacking                | t1082                      | System Information Discovery                  |
| t1073                    | DLL Side-Loading                          | t1016                      | System Network Configuration Discovery        |
| t1107                    | File Deletion                             | t0149                      | System Network Connections Discovery          |
| t1054                    | Indicator Blocking                        | t1033                      | System Owner/User Discovery                   |
| t1070                    | Indicator Removal on Host                 | t1124                      | System Time Discovery                         |
| t1036                    | Masquerading                              | t1497                      | Virtualization and Sandbox Evasion            |
| t1112                    | Modify Registry                           |                            |   |
| t1170                    | Mshta                                     |                            |   |
| t1027                    | Obfuscated Files or Information           |                            |   |
| t1055                    | Process Injection                         |                            |   |
| t1014                    | Rootkit                                   |                            |   |
| t1085                    | Rundll32                                  |                            |   |
| t1064                    | Scripting                                 |                            |   |
| t1045                    | Software Packing                          |                            |   |
| t1099                    | Timestamp                                 |                            |   |
| t1078                    | Valid Accounts                            |                            |   |
| t1497                    | Virtualization and Sandbox Evasion        |                            |   |
| t1102                    | Web Service                               |                            |   |
| <b>Credential Access</b> |   | <b>Lateral Movement</b>    |   |
| t1098                    | Account Manipulation                      | t1075                      | Pass the Hash                                 |
| t1110                    | Brute Force                               | t1076                      | Remote Desktop Protocol                       |
| t1003                    | Credential Dumping                        | t1105                      | Remote File Copy                              |
| t1081                    | Credentials in Files                      |                            |   |
| t1056                    | Input Capture                             |                            |   |
| t1145                    | Private Keys                              |                            |   |
| <b>Collection</b>        |   | <b>Command and Control</b> |   |
| t1119                    | Automated Collection                      | t1043                      | Commonly Used Port                            |
| t1213                    | Data from Information Repositories        | t1090                      | Connection Proxy                              |
| t1005                    | Data from Local System                    | t1094                      | Custom Command and Control Protocol           |
| t1056                    | Input Capture                             | t1132                      | Data Encoding                                 |
| t1113                    | Screen Capture                            | t1001                      | Data Obfuscation                              |
|                          |   | t1483                      | Domain Generation Algorithms                  |
|                          |   | t1219                      | Remote Access Tools                           |
|                          |   | t1105                      | Remote File Copy                              |
|                          |   | t1071                      | Standard Application Layer Protocol           |
|                          |   | t1032                      | Standard Cryptographic Protocol               |
|                          |   | t1095                      | Standard Non-Application Layer Protocol       |
|                          |   | t1065                      | Uncommonly Used Port                          |
| <b>Exfiltration</b>      |   | <b>Impact</b>              |   |
|                          |   | t1002                      | Data Compressed                               |
|                          |   | t1022                      | Data Encrypted                                |
|                          |   | t1041                      | Exfiltration Over Command and Control Channel |
|                          |   |                            |   |
|                          |   | t1487                      | Data Encrypted for Impact                     |

## TECHNICAL ANNEX

# Code-Signing Certificates Used by APT41

**Table 14.** Code-signing certificates used by APT41.

| Serial  | Common Name                      | Issue Date | Expiry Date | Status  |
|---|----------------------------------|------------|-------------|---------|
| 0b:72:79:06:8b:eb:15:ff:e8:06:0d:2c:56:15:3c:35 | Guangzhou YuanLuo Technology Co. | 6/12/12    | 6/12/13     | Revoked |
| 18:63:79:57:5a:31:46:e2:6b:ef:c9:0a:58:0d:1b:d2 | Webzen Inc.                      | 8/2/11     | 9/30/13     | Revoked |
| 63:66:a9:ac:97:df:4d:e1:73:66:94:3c:9b:29:1a:aa | xlgames                          | 7/5/11     | 7/4/12      | Revoked |
| 5c:2f:97:a3:1a:bc:32:b0:8c:ac:01:00:59:8f:32:f6 | Neowiz CORPORATION               | 11/16/11   | 12/15/12    | Expired |
| 01:00:00:00:00:01:30:73:85:f7:02                | Mgame Corp                       | 6/9/11     | 6/9/12      | Expired |
| 4c:0b:2e:9d:2e:f9:09:d1:52:70:d4:dd:7f:a5:a4:a5 | Fuqing Dawu Technology Co.       | 1/31/13    | 1/31/14     | Revoked |
| 14:0d:2c:51:5e:8e:e9:73:9b:b5:f1:b2:63:7d:c4:78 | Guangzhou YuanLuo Technology Co. | 10/22/13   | 10/22/14    | Revoked |
| 58:01:5a:cd:50:1f:c9:c3:44:26:4e:ac:e2:ce:57:30 | Nanjing Ranyi Technology Co.     | 8/8/12     | 8/8/13      | Revoked |
| 7b:d5:58:18:c5:97:1b:63:dc:45:cf:57:cb:eb:95:0b | XL Games Co.                     | 6/21/12    | 6/21/13     | Revoked |
| 47:6b:f2:4a:4b:1e:9f:4b:c2:a6:1b:15:21:15:e1:fe | Wemade Entertainment co.         | 3/2/14     | 1/9/16      | Revoked |
| 53:0c:e1:4c:81:f3:62:10:a1:68:2a:ff:17:9e:25:80 | NetSarang Computer               | 10/13/16   | 11/12/18    | Revoked |
| 30:d3:c1:67:26:5b:52:0c:b8:7f:25:84:4f:95:cb:04 | Shanda Games                     | 10/29/13   | 12/27/16    | Revoked |
| 54:c6:c1:40:6f:b4:ac:b5:d2:06:74:e9:93:92:c6:3e | GameUS Inc                       | 5/15/14    | 7/13/16     | Expired |
| 1e:52:bb:f5:c9:0e:c1:64:d0:5b:e0:e4:16:61:52:5f | En Masse Entertainment           | 2/3/15     | 4/5/17      | Expired |
| fd:f2:83:7d:ac:12:b7:bb:30:ad:05:8f:99:9e:cf:00 | Zepetto Co.                      | 5/10/18    | 7/1/19      | Expired |
| 25:f8:78:22:de:56:d3:98:21:59:28:73:ea:09:ca:37 | Electronics Extreme Limited      | 1/20/17    | 1/20/19     | Expired |
| 67:24:34:0d:db:c7:25:2f:7f:b7:14:b8:12:a5:c0:4d | YNK JAPAN Inc                    | 11/27/09   | 11/27/11    | Revoked |

## TECHNICAL ANNEX

# Additional Malware Overlaps

### Background

Throughout the course of our analysis, we consolidated multiple malware families into a single family with variants based on identified overlaps. Some of the malware families, such as HIGHNOON, are shared with other suspected Chinese espionage groups. The malware families contain similar functionalities, code overlaps, and encoding routines. Detailed descriptions on specific malware families are listed as follows.

**Figure 20:** HIGHNOON.BIN and HIGHNOON.LITE in memory DLL loading function.

```

char *v8; // ecx
int v9; // eax
char *v10; // eax
char *v11; // [esp+10h] [ebp-4h]

v1 = (char *)a1 + a1[15];
v2 = (char *)VirtualAlloc(*((LPVOID *)v1 + 13), *((_DWORD *)v1 + 20), 0x2000u, 0x40u);
v11 = v2;
if ( !v2 )
{
    result = (char *)VirtualAlloc(0, *((_DWORD *)v1 + 20), 0x2000u, 0x40u);
    v11 = result;
    if ( !result )
        return result;
    v2 = result;
}
v4 = GetProcessHeap();
v5 = (int *)HeapAlloc(v4, 0, 0x14u);
v5[1] = (int)v2;
v5[3] = 0;
v5[2] = 0;
v5[4] = 0;
VirtualAlloc(v2, *((_DWORD *)v1 + 20), 0x1000u, 0x40u);
v6 = (char *)VirtualAlloc(v2, *((_DWORD *)v1 + 21), 0x1000u, 0x40u);
qmemcpy(v6, a1, a1[15] + *((_DWORD *)v1 + 21));
v7 = (int)&v6[a1[15]];
*v5 = v7;
*(DWORD*)(v7 + 52) = v11;
sub_10002150((int)a1, (int)v1, v5);
v8 = (char *)*((_DWORD *)v1 + 13);
if ( v11 != v8 )
    sub_10002370(v5, v11 - v8);
if ( !sub_100023F0(v5) )
    goto LABEL_10;
sub_100022B0(v5);
v9 = *(DWORD*)(v5 + 40);
if ( v9 )
{
    v10 = &v11[v9];
    if ( !v10 || !(int (_stdcall *))((char *, int, _DWORD))v10(v11, 1, 0) )
    {
        ABEL _10
        sub_100025B0(v5);
        return 0;
    }
    v5[4] = 1;
}
return (char *)v5;
000021BF sub_1000020B0;52 (100021BF)

```

### HIGHNOON

HIGHNOON variants include HIGHNOON.LITE, HIGHNOON.BIN, HIGHNOON.PASTEBOY, HIGHNOON.CLI, and HIGHNOON.LINUX. Some of the variants, such as HIGHNOON.BIN, were used by multiple suspected Chinese groups, including APT41 and APT17.

### HIGHNOON.BIN and HIGHNOON.LITE

HIGHNOON.BIN (MD5: 2862c9bff365dc8d51ba0c4953869d5d) and HIGHNOON.LITE (MD5: b5120174d92f30d3162ceda23e201cea) contain an identical in memory DLL loading function, which can be seen in Figure 20.

```

char *v7; // [esp+60h] [ebp-ch]
	DWORD v8; // [esp+68h] [ebp-4h]

8    if ( !a1 )
9        return;
10   v7 = (char *)a1 + a1[15];
11   ipAddress = (char *)VirtualAlloc(*((LPVOID *)v7 + 13), *((_DWORD *)v7 + 20), 0x2000u, 0x40u);
12   if ( !IpAddress )
13       ipAddress = (char *)VirtualAlloc(0, *((_DWORD *)v7 + 20), 0x2000u, 0x40u);
14   if ( !IpAddress )
15       return 0;
16   v2 = GetProcessHeap();
17   v8 = HeapAlloc(v2, 0, 0x14u);
18   v8[1] = ipAddress;
19   v8[3] = 0;
20   v8[2] = 0;
21   v8[4] = 0;
22   VirtualAlloc(ipAddress, *((_DWORD *)v7 + 20), 0x1000u, 0x40u);
23   dst = (char *)VirtualAlloc(ipAddress, *((_DWORD *)v7 + 21), 0x1000u, 0x40u);
24   memcpy(dst, a1, *((_DWORD *)v7 + 21) + a1[15]);
25   v8 = &dst[a1[15]];
26   *(DWORD *)(*v8 + 52) = ipAddress;
27   sub_4020A0(a1, v7, v8);
28   v4 = (int)&ipAddress[-*((_DWORD *)v7 + 13)];
29   if ( v4 )
30       sub_402320(v8, v4);
31   if ( sub_402320(v8) )
32   {
33       sub_4021C0(v8);
34       if ( !(*(_DWORD *)(*v8 + 40) ) )
35           return v8;
36       v3 = &IpAddress[((_DWORD *)(*v8 + 40));
37       if ( v3 && ((int (_stdcall *))((char *, int, _DWORD))v3)(IpAddress, 1, 0) )
38       {
39           v8[4] = 1;
40           return v8;
41       }
42   }
43   sub_402740(v8);
44   return 0;
45 } [REDACTED]
46
47
48
00002084 t_in_memory_DLL_loader;46 (402084)

```

HIGHNOON (MD5: df143c22465b88c4bdb042956fef8121) uses an API hashing algorithm to resolve its imports at runtime, but the layout of the in-memory DLL loading functionality is identical between HIGHNOON, HIGHNOON.BIN, and HIGHNOON.LITE samples (Figure 21). The specific samples of HIGHNOON, HIGHNOON.BIN, and HIGHNOON.LITE referenced previously are not attributed to APT41 but are instead used by other suspected Chinese groups.

- HIGHNOON and HIGHNOON.LITE also share the same configuration encoding routine.
- HIGHNOON, HIGHNOON.LITE, and HIGHNOON.BIN store a unique host identifier under the registry key HKLM\SOFTWARE\Microsoft\HTMLHelp

**Figure 21:**  
HIGHNOON DLL  
loading function.

```
resolve_APIS():
v3 = (_DWORD *)((char *)a1 + a1[15]);
v4 = (_DWORD *)VirtualAlloc(v3[13], v3[20]. 0x2000, 0x40);
if ( !v4 )
{
    result = (_DWORD *)VirtualAlloc(0, v3[20], 0x2000, 0x40);
    if ( !result )
        return result;
    v4 = result;
}
v6 = (void *)GetProcessHeap(0, 0x14);
v7 = HeapAlloc(v6, v13, v14);
v7[1] = v4;
v7[3] = 0;
v7[2] = 0;
v7[4] = 0;
VirtualAlloc(v4, v3[20], 0x1000, 0x40);
v8 = (char *)VirtualAlloc(v4, v3[21], 0x1000, 0x40);
qmemcpy(v8, a1, a1[15] + v3[21]);
v9 = (int)&v8[*(_DWORD *)(&a3 + 60)];
*v7 = v9;
*( _DWORD *) (v9 + 52) = a1;
sub_100016A0(a3, v3, v7);
v10 = (char *)v3[13];
if ( a1 != (_DWORD *)v10 )
    sub_10001830(v7, (char *)a1 - v10);
if ( !sub_10001770(v7) )
    return 0;
sub_10001770(v7);
v11 = *(_DWORD *)(*v7 + 40);
if ( v11 )
{
    v12 = (char *)a1 + v11;
    if ( !v12 || !((int (cdecl * )(_DWORD *, int, _DWORD))v12)(a1, 1, 0) )
        return 0;
    v7[4] = 1;
}
return v7;
}
```

## HIGHNOON.LINUX and HIGHNOON

HIGHNOON.LINUX is a Linux variant of HIGHNOON that shares multiple component overlaps with HIGHNOON.

- HIGHNOON.LINUX and HIGHNOON share a message component that use the same headers and XOR encoding.
- The two share a transport component that provides HTTP, Fake TLS, and raw protocol options.
- HIGHNOON.LINUX and HIGHNOON share a similar commands component. The code for processing the commands "Tunnel" and "Plus" (to add plugins) are nearly identical.

## CROSSWALK and CROSSWALK.BIN

CROSSWALK and CROSSWALK.BIN share several notable overlaps. Significantly, the two code families share a large amount of code in their respective shellcode components (Figure 22).

## Shellcode Component Overlaps

- The shellcode that handles C&C messages uses the same function in both families.
  - Interestingly, additional functions used for C&C in CROSSWALK.BIN are present within CROSSWALK but unused.
  - This suggests the families are slightly different builds originating from the same codebase.
- CROSSWALK.BIN's user-mode shellcode and the shellcode appended at the end of CROSSWALK contain approximately three-fourths of the same code.
- Both CROSSWALK and CROSSWALK.BIN's backdoors are implemented through user-mode shellcode.

**Figure 22:** CROSSWALK (left) and CROSSWALK.BIN (right) shellcode.

```

37  __int64 v37; // [rsp+58h] [rbp+10h]
38
● 39  v37 = a2;
● 40  v2 = 0;
● 41  v3 = a1[47] == 1;
● 42  v4 = a1;
● 43  strcpy(&v36, "ok1234\n");
● 44  if ( v3 )
● 45  {
● 46 LABEL_14:
● 47  if ( cgp_dyn_resolve_maybe_03(v4) <= 0 )
● 48  return v2;
● 49  v24 = v4[24];
● 50  v25 = *(v4 + 13);
● 51  v26 = v4[48];
● 52  *(v4 + 11) = v4;
● 53  *(v4 + 10) = v4 - v24;
● 54  v27 = v4 + v25 - v24;
● 55  v28 = (*(v4 + 31))(0i64, v26, 4096i64, 4i64);
● 56  *(v4 + 25) = v28;
● 57  if ( !v28 )
● 58  return v2;
● 59  v29 = v4[25];
● 60  v30 = *(v4 + 28);
● 61  if ( v29 > 0 )
● 62  {
● 63    v31 = v27;
● 64    do
● 65    {
● 66      *v31++ ^= v30;
● 67      --v29;
● 68    }
● 69    while ( v29 );
● 70  }
● 71  if ( sub_BBA0(v4, v27) <= 0 )
● 72  return v2;
● 73  v32 = v4[25];
● 74  v33 = *(v4 + 28);
● 75  if ( v32 > 0 )
● 76  {
● 77    do
● 78    {
● 79      *v27++ ^= v33;
● 80      --v32;
● 81    }
● 82    while ( v32 );
● 83  }
● 84  (*(v4 + 25) + 2032i64) = *(v4 + 17) + *v4 + 10;
● 85  *(v4 + 35) = *(v4 + 17) + *(v4 + 10);
● 86  (*(v4 + 25) + 752i644)(32775i64);
● 87  v34 = (*(v4 + 25) + 32i644)(0i64, 0i64, *(v4 + 10) + *(v4 + 95), v4, 0, 0i64);
● 88  (*(v4 + 35))&v36;
● 89  (*(v4 + 25) + 272i644)(v34, 0xFFFFFFFFFi64);
● 90  (*(v4 + 25) + 48i644)(v24);
● 91  v2 = 1;
● 92  return v2;
● 93 }
● 94  v5 = a1[12];
● 95  v6 = a1[13];
● 96  v7 = a1[11];
● 97  v8 = v4[24];
● 98  v9 = v4[19];
● 99  v10 = v4[25];
● 100 v4[12] = v7;
● 101 v11 = v10 + v9 + v8;
● 102 v4[13] = v7;
● 103 v12 = 0;
● 104 v13 = v10 + v9 + v8;
● 105 v14 = v4 - v8;
● 106 do
● 107 {
● 108   v15 = *v14++;
● 109   v12 = v15 + __ROR4__(v12, v7);
● 110   --v13;
● 111 }
● 112 while ( v13 );
● 113 if ( v6 != v12 )
● 114  return v2;
● 115 v16 = v4 + 48;
● 116 v17 = v9 + v10 - 192;
● 117 v18 = v17;
● 118 if ( v17 > 0 )
● 119 {
● 120   v19 = v4[14];
● 121 }

39  __int64 v39; // [rsp+58h] [rbp+10h]
40
● 41  v39 = a2;
● 42  v2 = 0;
● 43  v3 = a1[47] == 1;
● 44  v4 = a1;
● 45  strcpy(&v38, "ok1234\n");
● 46  if ( v3 )
● 47  {
● 48 LABEL_14:
● 49  if ( cgp_dyn_resolve_maybe_03(v4) <= 0 )
● 50  return v2;
● 51  v24 = v4[24];
● 52  v25 = *(v4 + 13);
● 53  v26 = v4[48];
● 54  *(v4 + 11) = v4;
● 55  *(v4 + 10) = v4 - v24;
● 56  v27 = v4 + v25 - v24;
● 57  v28 = (*(v4 + 31))(0i64, v26, 4096i64, 4i64);
● 58  *(v4 + 25) = v28;
● 59  if ( !v28 )
● 60  return v2;
● 61  v29 = v4[25];
● 62  v30 = *(v4 + 28);
● 63  if ( v29 > 0 )
● 64  {
● 65    v31 = v27;
● 66    do
● 67    {
● 68      *v31++ ^= v30;
● 69      --v29;
● 70    }
● 71    while ( v29 );
● 72  }
● 73  if ( sub_8C58(v4, v27) <= 0 )
● 74  return v2;
● 75  v32 = v4[25];
● 76  v33 = *(v4 + 28);
● 77  if ( v32 > 0 )
● 78  {
● 79    do
● 80    {
● 81      *v27++ ^= v33;
● 82      --v32;
● 83    }
● 84    while ( v32 );
● 85  }
● 86  (*(v4 + 25) + 2032i64) = *(v4 + 17) + *v4 + 10;
● 87  *(v4 + 35) = *(v4 + 17) + *(v4 + 10);
● 88  (*(v4 + 25) + 752i644)(32775i64);
● 89  v34 = (*(v4 + 25) + 32i644)(0i64, 0i64, *(v4 + 10) + *(v4 + 95), v4, 0, 0i64);
● 90  (*(v4 + 35))&v38;
● 91  (*(v4 + 25) + 272i644)(v36, 0xFFFFFFFFFi64);
● 92  (*(v4 + 25) + 48i644)(v36);
● 93  v2 = 1;
● 94  return v2;
● 95 }
● 96  v5 = a1[12];
● 97  v6 = a1[13];
● 98  v7 = a1[11];
● 99  v8 = v4[24];
● 100 v9 = v4[19];
● 101 v10 = v4[25];
● 102 v4[12] = v7;
● 103 v11 = v10 + v9 + v8;
● 104 v4[13] = v7;
● 105 v12 = 0;
● 106 v13 = v10 + v9 + v8;
● 107 v14 = v4 - v8;
● 108 do
● 109 {
● 110   v15 = *v14++;
● 111   v12 = v15 + __ROR4__(v12, v7);
● 112   --v13;
● 113 }
● 114 while ( v13 );
● 115 if ( v6 != v12 )
● 116  return v2;
● 117 v16 = v4 + 48;
● 118 v17 = v9 + v10 - 192;
● 119 v18 = v17;
● 120 if ( v17 > 0 )
● 121 {
● 122   v19 = v4[14];
● 123 }
```

## Obfuscation and Anti-Analysis Overlaps

- Both code families share the same function at the start of their shellcode to de-obfuscate subsequent shellcode.
- A key function within the shellcode component that generates a semi-random XOR key and is used in multiple code locations for decoding is identical in CROSSWALK and CROSSWALK.BIN.
- Both use the same function for import resolution via an ASCII hash.

**Figure 23:**

CROSSWALK (left) and CROSSWALK.BIN (right) code for answering different C&C message types.

```

strcpy(&v22, "r c:%d,l:%d\n");
v11 = 0i64;
v12 = 0;
(*(v3 + 2032))(&v22, v8, v5);
switch (*msg_type)
{
    case 0x64u:
        if ( msg_type[1] != 216 )
        {
            v16 = 100;
            goto LABEL_37;
        }
        v21 = (*(v9 + 248))(0i64, 216i64, 4096i64, 4i64);
        if ( !v21 )
            return 0;
        (*(v9 + 200) + 1856i64))(&v21, v7, msg_type[1]);
        if ( (*(v9 + 200) + 928i64))(*(v9 + 832), 100i64, v21, msg_type[1]) >
0 )
            return 1;
        v10 = 0;
        v14 = (*(v9 + 200) + 320i64))();
        v15 = 7021i64;
        goto LABEL_42;
    case 0x6Eu:
        return 1;
    case 0x78u:
        if ( msg_type[1] != 16 )
        {
            v16 = 120;
            goto LABEL_37;
        }
        v20 = (*(v9 + 248))(0i64, 16i64, 4096i64, 4i64);
        if ( !v20 )
            return 0;
        (*(v9 + 200) + 1856i64))(&v21, v7, msg_type[1]);
        if ( (*(v9 + 200) + 928i64))(*(v9 + 832), 100i64, v21, msg_type[1]) >
0 )
            return 1;
        v10 = 0;
        v14 = (*(v9 + 200) + 320i64))();
        v15 = 7021i64;
        goto LABEL_42;
    case 0x7Au:
        v19 = msg_type[1];
        if ( v19 <= 0x1000 )
        {
            if ( v19 )
            {
                v11 = (*(v9 + 248))(0i64, 16i64, 4096i64, 4i64);
                if ( !v11 )
                    return 10;
                (*(v9 + 200) + 1856i64))(&v11, v7, msg_type[1]);
                v12 = msg_type[1];
            }
            if ( (*(v9 + 200) + 928i64))(*(v9 + 832), 122i64, v11, v12) > 0 )
                return 1;
            v14 = (*(v9 + 200) + 320i64))();
            v15 = 7023i64
            goto LABEL_42
        }
        v16 = 122;
        goto LABEL_37;
    case 0x82u:

```

```

strcpy(&fmt_msg, "r c%d,l:%d\n");
if ( !v3 )
    goto LABEL_48;
v6 = sub_3398();
v2 = v6;
if ( v6 == 2 )
    return 1;
if ( v6 <= 0 )
    return v2;
LABEL_48:
v7 = (msg_type + 11);
(*(v5 + 200) + 1872i64))(&fmt_msg, *msg_type, msg_type[1]);
switch (*msg_type)
{
    case 0x64u:
        (*(v5 + 200) + 1872i64))(&v5 + 1320, 22i64);
        v13 = cgp_cb_msctype_0x64_wrapper(v5, (msg_type + 11));
        v9 = v5;
        if ( v13 > 0 )
        {
            *(v5 + 760) = 1;
            if ( sub_5F44(v5) > 0 )
                return 1;
            v9 = v5;
        }
        v11 = 100;
        goto LABEL_43;
    case 0x6Eu:
        return 1;
    case 0x78u:
        v10 = cgp_cb_msctype_0x78(v5, v8, msg_type + 11);
        goto LABEL_38;
    case 0x7Au:
        v10 = cgp_cb_msctype_07A(v5, v8, (msg_type + 11));
        goto LABEL_38;
}

```

However, there are differences between the two malware families, including how they communicate to C&C servers.

- CROSSWALK beacons with HTTP GET and POST requests, while CROSSWALK.BIN uses a custom binary protocol.
- CROSSWALK.BIN contains a driver component for covert C&C, which CROSSWALK lacks.
- Both families contain similar code to process identical message types, but their answers differ.
  - CROSSWALK.BIN answers to 0x78 and 0x7A message types by calling large functions wrapping the business logic.
  - CROSSWALK has different, much shorter code embedded directly in the "case" statement.

## TECHNICAL ANNEX

# Malware Used by APT41

**Table 15.** Malware used by APT41.

| Malware       | Description   | Detected as   |
|---------------|---|---|
| ACEHASH       | ACEHASH is a credential theft/password hash dumping utility. The code may be based in Mimikatz and appears to be publicly available.  | FE_Trojan_AceHash   |
| ADORE.XSEC    | ADORE.XSEC is a Linux backdoor that may be used with the ADORE rootkit.   | FE_APT_Backdoor_Linux64_ADORE_1<br>FE_APT_Rootkit_Linux64_ADORE_1<br>FE_APT_Rootkit_ADORE   |
| ASPXSPY       | ASPXSPY is a publicly available web shell that may contain the text "ASPxSpy Ver: 2009."  | FE_Webshell_ASPX_ASPXSPY_1<br>FE_Webshell_ASPX_ASPXSPY_2<br>FE_Webshell_ASPX_ASPXSPY_3<br>FE_Webshell_ASPX_ASPXSPY_4                                    |
| BEACON        | BEACON malware is a backdoor that is commercially available as part of the Cobalt Strike software platform, commonly used for pen-testing network environments. The malware supports several capabilities, such as injecting and executing arbitrary code, uploading and downloading files, and executing shell commands.   | FE_Backdoor_Win_BEACON_1<br>FE_Trojan_PS1_BEACON_1  |
| CHINACHOP     | CHINACHOP is a simple code injection web shell that can execute Microsoft .NET code within HTTP POST commands. This allows CHINACHOP to upload and download files, execute applications with web server account permissions, list directory contents, access Active Directory, access databases, and perform any other action allowed by the .NET runtime. CHINACHOP is composed of at least two parts: a small bit of code on a server and a client that provides C&C. | FE_Webshell_JSP_CHOPPER_1<br>FE_Webshell_Java_CHOPPER_1<br>FE_Webshell_MSIL_CHOPPER_1   |
| COLDJAVA      | COLDJAVA is a backdoor that drops shellcode and a BLACKCOFFEE variant payload into the Windows registry.  | FE_APT_Trojan_COLDJAVA_Dropper<br>FE_APT_Trojan_COLDJAVA_64<br>FE_APT_Trojan_COLDJAVA_32<br>FE_APT_Backdoor_COLDJAVA<br>FE_APT_Trojan_COLDJAVA_Launcher |
| CRACKSHOT     | CRACKSHOT is a downloader that can download files, including binaries, and run them from the hard disk or execute them directly in memory. It is also capable of placing itself into a dormant state.   | FE_Backdoor_Win32_CRACKSHOT_1<br>Backdoor.Win.CRACKSHOT   |
| CROSSWALK     | CROSSWALK is a skeletal, modular backdoor capable of system survey and adding modules in response to C&C replies.   | FE_APT_Backdoor_Win_CROSSWALK_1<br>FE_APT_Loader_Win_CROSSWALK_1<br>APT.Backdoor.Win.CROSSWALK  |
| CROSSWALK.BIN | CROSSWALK.BIN is a kernel driver that can implement firewall-level filters to detect tasking packets and covertly send data.  | FE_APT_Dropper_Win64_CROSSWALK_1<br>FE_APT_Dropper_Win64_CROSSWALK_2<br>FE_APT_Trojan_Win64_CROSSWALK_1   |

**Table 15.** Malware used by APT41.

| Malware       | Description  | Detected as  |
|---------------|--|--|
| DEADEYE       | DEADEYE is a downloader that is installed as a Service DLL. It can use RC5 encryption to decrypt and install payloads obtained from its C&C server.  | FE_APT_Loader_Win64_DEADEYE_1<br>FE_APT_Loader_Win64_DEADEYE_2   |
| DOWNTIME      | DOWNTIME is a backdoor dropped as an embedded PE file to a variety of locations on disk or loaded and executed in memory. The final payload is a DLL used to install, manage, and execute plugin DLLs.   | FE_Dropper_Win32_DOWNTIME_1<br>FE_Loader_Win32_DOWNTIME_1  |
| EASYNIGHT     | EASYNIGHT is a loader observed used with several malware families, including HIGHNOON and HIGHNOON LITE. The loader often acts as a persistence mechanism via search order hijacking.  | FE_APT_Loader_Win_EASYNIGHT_1  |
| ENCRYPTORRAAS | ENCRYPTORRAAS (Encryptor RaaS) is a ransomware that encrypts all files on the system that match an included file extensions list. As is typical of most ransomware, a combination of both public-key and symmetric-key cryptography is used to encrypt the data. File data is encrypted using RC6, with the RC6 key for each file being encrypted with RSA. A ransom note in the form of a text file, typically named "readme_liesmich_encryptor_raas.txt," is dropped in every directory in which a file was encrypted. Encryptor RaaS was sold via a RaaS operation that was available around the 2015–2016 time frame via a Tor (.onion) website. | FE_Ransomware_Win32_ENCRYPTORRAAS_1<br>FE_Ransomware_Win32_ENCRYPTORRAAS_2   |
| FRONTWHEEL    | FRONTWHEEL is a driver for the HIGHNOON.BIN backdoor.  | FE_APT_Rootkit_Win64_FRONTWHEEL_1  |
| GEARSHIFT     | GEARSHIFT is a memory-only dropper for two keylogger DLLs. It is designed to replace a legitimate Fax Service DLL.   | FE_APT_Keylogger_GEARSHIFT   |
| GHOST         | Gh0st is a remote access tool (RAT) derived from publicly available source code. It provides threat actors with the ability to perform screen and audio captures, enable a webcam, list and kill processes, open a command shell, wipe event logs, and create, manipulate, delete, launch, and transfer files.   | Backdoor.APT.Gh0stRat<br>Backdoor.APT.Gh0st.Trojan.Ghost   |
| GOODLUCK      | GOODLUCK is a credential-stealing DLL that modifies the registry, so it loads when a user logs on to the system. It steals credentials from the logon screen and saves the information to a local file.  | Hacktool.APT.GOODLUCK  |
| HIGHNOON      | HIGHNOON is a backdoor that may consist of multiple components. The components may include a loader, a DLL, and a rootkit. Both the loader and the DLL may be dropped together, but the rootkit may be embedded in the DLL. The HIGHNOON loader may be designed to run as a Windows service.   | FE_APT_Backdoor_Win64_HIGHNOON_1<br>FE_APT_Dropper_HIGHNOON_B<br>FE_APT_Loader_Win64_HIGHNOON_2<br>FE_APT_Loader_Win64_HIGHNOON_3<br>FE_APT_Rootkit_Win64_HIGHNOON_1<br>FE_APT_Rootkit_Win64_HIGHNOON_2<br>FE_APT_Rootkit_Win64_HIGHNOON_3 |

**Table 15.** Malware used by APT41.

| Malware               | Description   | Detected as   |
|-----------------------|---|---|
| HIGHNOON.BIN          | HIGHNOON.BIN is a modified version of the Windows DLL apphelp.dll, which is loaded via search order hijacking. HIGHNOON.BIN contains a malicious shellcode backdoor that is loaded into memory at runtime.  | FE_APT_Trojan_Win32_HIGHNOON_1<br>FE_APT_Loader_Win32_HIGHNOON_1<br>FE_APT_Loader_Win64_HIGHNOON_1<br>FE_APT_Trojan_Win32_HIGHNOON_2<br>APT.Backdoor.Win.HIGHNOON<br>APT.BackdoorWin.HIGHNOON   |
| HIGHNOON.LITE         | HIGHNOON.LITE is a standalone, non-persistent variant of the HIGHNOON backdoor. This version accepts a hostname and port on the command line. If no port is specified, the malware will use port 80 by default. HIGHNOON.LITE can download and execute additional memory-resident modules after it authenticates with the C&C server.   | FE_APT_Trojan_Win32_HIGHNOON_7  |
| HIGHNOON.LINUX        | HIGHNOON.LINUX is a Linux backdoor designed to operate with a rootkit and can launch and establish persistence for an sshd client whose presence and activity is hidden by the rootkit.   | FE_APT_Trojan_Linux64_HIGHNOON_1<br>FE_APT_Rootkit_Linux64_HIG<br>HNOON_1   |
| HIGHNOON.<br>PASTEBOY | HIGHNOON.PASTEBOY is a variant of HIGHNOON that utilizes legitimate websites hosting encoded base64 strings that decode to the actual C2 address.   | TROJAN.APT.PASTEBOY   |
| HKDOOR                | HKDOOR (aka Hacker's Door) is a remote administration tool designed as a DLL that can either run as a service or with rundll32.exe. HKDOOR drops and installs a kernel rootkit and has a variety of capabilities, including manipulating files and processes, connecting to URLs, and shutting down the compromised system. All HKDOOR's string resources are encoded with a transposition algorithm. | Backdoor.APT.HKDOOR   |
| HOMEUNIX              | HOMEUNIX is primarily a generic launcher for downloaded plugins. The plugins are stored in a memory buffer and then loaded and linked manually by the malware, meaning the plugins never have to touch disk. However, HOMEUNIX may also store and save plugins. The plugins will run after the system is rebooted without the actor having to send them again to the victim system.                   | FE_APT_HOMEUNIX_1<br>FE_APT_HOMEUNIX_2<br>FE_APT_HOMEUNIX_3<br>FE_APT_HOMEUNIX_4<br>FE_APT_HOMEUNIX_5<br>FE_APT_HOMEUNIX_6<br>FE_APT_HOMEUNIX_7<br>FE_APT_HOMEUNIX_8<br>FE_APT_HOMEUNIX_9<br>FE_APT_HOMEUNIX_10<br>FE_APT_HOMEUNIX_11<br>FE_APT_HOMEUNIX_12<br>FE_APT_HOMEUNIX_13<br>FE_APT_HOMEUNIX_14<br>FE_APT_HOMEUNIX_15<br>FE_APT_HOMEUNIX_16<br>APT.Backdoor.Win.HOMEUNIX<br>Backdoor.HOMEUNIX.SNK.DNS<br>Trojan.APT.9002, Backdoor.APT.9002 |

**Table 15.** Malware used by APT41.

| Malware   | Description  | Detected as   |
|-----------|--|---|
| HOTCHAI   | HOTCHAI is a backdoor that receives and XOR-decodes a DNS response message to retrieve the true C&C IP address.  | FE_APT_Backdoor_HOTCHAI   |
| JUMPALL   | JUMPALL is a malware dropper that has been observed dropping HIGHNOON/ZXSHELL/SOGU.  | FE_Dropper_Win_JUMPALL_1<br>FE_Dropper_Win_JUMPALL_2  |
| LATELUNCH | LATELUNCH is a loader that decodes a file specified on the command line and loads and executes it in memory.   | FE_Loader_Win64_LATELUNCH_1   |
| LIFEBOAT  | LIFEBOAT is a backdoor that has the capability to communicate with its C&C over HTTP.  | FE_APT_Dropper_Win32_LIFE<br>BOAT_1 FE_APT_Downloader_Win32_LIFEBOAT_1 APT.Downloader.Win.LIFEBOAT  |
| LOWKEY    | LOWKEY is a passive backdoor that utilizes a user mode rootkit to provide covert communications with the backdoor component by forwarding packets in between a TCP Socket and a named pipe.  | FE_APT_ROOTKIT_WIN64_LOWKEY_1<br>FE_APT_LOADER_WIN64_LOWKEY_1<br>FE_APT_BACKDOOR_WIN64_LOWKEY_1<br>APT.BACKDOOR.Win.LOWKEY  |
| NJRAT     | njRAT is a RAT project that was in development possibly as early as 2010, and it has seen a number of incremental updates since that time. The author of njRAT is widely believed to be a Kuwaiti actor using the handle "njq8." njq8, whose real name is believed to be Naser Al Mutairi, and who has previously used the handles "NJN" and "XNJQ8x," has been involved in the development of multiple hacking tools, including RATs, worms, crypters, and binders. He is, however, primarily known as the developer of njRAT, which he has distributed on private hacking forums and more visibly via Twitter. | Trojan.Njrat<br>Backdoor.Bladabindi<br>Trojan.Bladabindi<br>Backdoor.MSIL.Bladabindi<br>Trojan.Bladabindi.F<br>Trojan.Bladabindi.njRat<br>Trojan.Bladabindi.DNS<br>Backdoor.Bladabindi.DNS<br>Backdoor.Ratenjay<br>Backdoor.LV<br>Backdooor.njRat.MVX<br>Backdoor.njRat.MVX<br>Win.Worm.Njrat-2<br>Trojan.NjRAT, Win.Worm.Njrat<br>Malware.DTI.Bladabindi,<br>Trojan.MSIL.Bladabindi<br>Hacktool.Bladabindi |
| PACMAN    | PACMAN is a backdoor designed to run as a service. Once active, PACMAN calls out to a hard-coded C&C domain. PACMAN has the following capabilities: retrieve drive types, terminate processes, create directories, obtain a directory listing, move files, return file attributes, remove directories, create files, read files, and copy files. PACMAN can also extract credentials from Internet Explorer.   | FE_Backdoor_Win32_PACMAN_1<br>Backdoor.Win.PACMAN   |
| PHOTO     | PHOTO is a DLL backdoor that can obtain directory, file, and drive listings, create a reverse shell, perform screen captures, record video and audio, list, terminate, and create processes, enumerate, start, and delete registry keys and values, log keystrokes, return user names and passwords from protected storage, and rename, delete, copy, move, read, and write to files.  | Backdoor.APT.PHOTO<br>FE_APT_Photos_Metadata  |

**Table 15.** Malware used by APT41.

| Malware           | Description  | Detected as   |
|-------------------|--|---|
| POISONPLUG        | POISONPLUG is a highly obfuscated modular backdoor with plug-in capabilities. The malware is capable of registry or service persistence, self-removal, plug-in execution, and network connection forwarding. POISONPLUG has been observed using social platforms to host encoded C&C commands.   | Backdoor.Win.POISONPLUG<br>APT.Backdoor.Win.POISONPLUG  |
| POISONPLUG.SHADOW | POISONPLUG.SHADOW is a modular backdoor with plugin capabilities. The first stage is shellcode, observed within compromised legitimate software. It connects to a C&C server for validation and configuration information to download the second stage. The second stage is a modular backdoor that can download plugins for additional functionality. POISONPLUG.SHADOW is assessed as an evolution of the POISONPLUG family. | FE_Backdoor_Win_POISONPLUG_1<br>FE_Backdoor_Win32_POISONPLUG_1<br>FE_Backdoor_Win_POISONPLUG_2  |
| POTROAST          | POTROAST is a backdoor that connects to a hard-coded C&C server. Its capabilities include downloading, uploading, and executing files and creating a reverse shell.  | FE_APT_Backdoor_Win_POTROAST_1<br>APT.Backdoor.Win.POTROAST   |
| ROCKBOOT          | ROCKBOOT can access and write to the compromised system's hard disk drive beneath the operating system and file system to bypass the normal MBR boot sequence and execute malware prior to the host operating system being initialized. ROCKBOOT does not contain a malicious payload but relies on a secondary payload for malicious activities, which is specified at install time.  | FE_APT_Backdoor_ROCKBOOT<br>FE_Loader_Win_ROCKBOOT_1  |
| SAGEHIRE          | SAGEHIRE is a multistage implant that decodes each stage using shellcode and includes keylogging capabilities.   | FE_APT_Sunshop_Dialog   |
| SWEETCANDLE       | SWEETCANDLE is a downloader that can download and execute a payload received from the C&C server.  | FE_APT_Downloader_Win32_SWEETCANDLE_1<br>FE_APT_Downloader_Win32_SWEETCANDLE_2<br>APT.Downloader.Win.SWEETCANDLE  |
| SOGU              | SOGU is a backdoor that is capable of file upload and download, arbitrary process execution, filesystem and registry access, service configuration access, remote shell access, and implementing a custom VNC/RDP-like protocol to provide the C&C server with graphical access to the desktop.  | Backdoor.APT.SOGU<br>Backdoor.APT.Kaba<br>Trojan.Plugx  |
| TERA              | TERA is a backdoor that uses legitimate services, such as Google Translate and Yahoo! Babel Fish, as proxies to download C&C configurations. It also uses a rootkit to mask network activity. After resolving the IP address of its C&C server, TERA will provide an input output control (IOCTL) code to its driver (rootkit component).  | FE_APT_Backdoor_Win32_TERA_1<br>FE_APT_Backdoor_Win32_TERA_2<br>FE_APT_Backdoor_Win32_TERA_3<br>FE_APT_Backdoor_Win64_TERA_1<br>FE_APT_Rootkit_Win64_TERA_1 |
| TIDYELF           | TIDYELF is a dropper for the WINTERLOVE backdoor. WINTERLOVE has been observed embedded within a resource within TIDYELF. TIDYELF will load the main WINTERLOVE component by injecting it into the iexplore.exe process. It will then create a registry key named HKLM\SOFTWARE\RAT to store configuration data for WINTERLOVE components to use.  | FE_APT_Dropper_Win32_TIDYELF_1  |

**Table 15.** Malware used by APT41.

| Malware    | Description  | Detected as   |
|------------|--|---|
| WIDGETONE  | WIDGETONE is a command-line tool that can perform network-based reconnaissance tasks, including port scans, service banner scans, and pingscans. WIDGETONE can brute-force credentials for SQL servers and Inter-Process Communication (IPC) shares. WIDGETONE can also query Windows host information and perform dictionary and brute-force attacks.   | FE_Trojan_Win_WIDGETONE_1<br>FE_Trojan_Win32_WIDGETONE_1  |
| WINTERLOVE | WINTERLOVE is a backdoor used by suspected Chinese cyber espionage actors. WINTERLOVE attempts to load and execute remote code in a running process and can enumerate system files and directories.  | FE_APT_Loader_Win32_WINTERLOVE_1<br>FE_APT_Keylogger_Win32_WINTERLOVE_1<br>FE_APT_Loader_Win32_WINTERLOVE_2<br>FE_APT_Trojan_Win32_WINTERLOVE_1<br>FE_APT_Backdoor_Win32_WINTERLOVE_1   |
| XDOOR      | X-Door is a full-featured remote administration tool (RAT) with a configurable deployment and plug-in architecture. It is freely downloadable through a Chinese website, and the deployment interface and server use the Chinese language. X-Door contains functionality for keylogging, audio and video capture, file transfers, acting as a proxy, retrieving system information, providing a reverse command shell, injecting DLLs, and downloading and launching commands.   | FE_APT_Backdoor_XDOOR<br>Backdoor.APT.XDOOR   |
| XMRIG      | XMRIG is an open-source Monero cryptocurrency miner. It has variants for CPU, NVIDIA GPU, and AMD GPU mining.  | FE_Trojan_Win_XMRMiner_1<br>FE_PUP_Win_XMRig_1  |
| ZXSHELL    | ZXSHELL is a backdoor that can be downloaded from the internet, particularly Chinese hacker websites. The backdoor can launch port scans, run a keylogger, capture screenshots, set up an HTTP or SOCKS proxy, launch a reverse command shell, cause SYN floods, and transfer/delete/run files. The publicly available version of the tool provides a graphical user interface that malicious actors can use to interact with victim backdoors. Simplified Chinese is the language used for the bundled ZXSHELL documentation. | Backdoor.APT.ZXShell<br>FE_APT_Backdoor_ZXShell<br>FE_APT_ZXSHELL_1<br>FE_APT_ZXSHELL_2<br>FE_APT_ZXSHELL_3<br>FE_APT_ZXSHELL_4<br>FE_APT_ZXSHELL_5<br>FE_APT_ZXSHELL_6<br>Backdoor.APT.ZXShell.SYSINFO_Command<br>Backdoor.APT.ZXShell.GETCMD_Command<br>Backdoor.APT.ZXShell.FILEMG_Command<br>Backdoor.APT.ZXShell.TRANSFILE_Command,<br>ZXSHELL RAT, Trojan.ZxShell<br>Backdoor.APT.Viper<br>FE_APT_VIPER |

## TECHNICAL ANNEX

# APT41 IOCs

**Table 16.** CRACKSHOT

| File MD5                         | File SHA1                                | File SHA256  |
|----------------------------------|--|--|
| 04fb0ccf3ef309b1cd587f609ab0e81e | 44260a1dfd92922a621124640015160e621f32d5 | 993d14d00b1463519fea78ca65d852966<br>3f487cd76b67b3fd35440bcdf7a8e31 |
| 0b2e07205245697a749e422238f9f785 | dde82093decde6371eb852a5e9a1aa4acf3b56ba | 049a2d4d54c511b16f8bc33dae670736bf<br>938c3542f2342192ad877ab38a7b5d |
| 272537bbd2a8e2a2c3938dc31f0d2461 | a045939f53c5ad2c0f7368b082aa7b0bd7b116da | d00b3edc3fe688fa035f1b919ef6e8f4<br>51a9c2197ef83d9bac3fa3af5e752243 |
| dd792f9185860e1464b4346254b2101b | a260dcf193e747cee49ae83568eea6c04bf93cb3 | 7096f1fdefa15065283a0b7928d1ab9792<br>3688c7974f98a33c94de214c675567 |
| fcfab508663d9ce519b51f767e902806 | 8272c1f41f7c223316c0d78bd3bd5744e25c2e9f | c667c9b2b9741247a56fcf0deebb4dc52<br>b9ab4c0da6d9cdaba5461a5e2c86e0c |

**Table 17.** GEARSHIFT

| File MD5                          | File SHA1                                | File SHA256   |
|-----------------------------------|--|---|
| 5b26f5c7c367d5e976aab320965cc7f   | c2fb50c9ef7ae776a42409bce8ef1be464654a4e | 7e0c95fc64357f12e837112987333cdf<br>8c1208ef8c100649eba71f1ea90c1db   |
| f8c89cccd8937f2b760e6706738210744 | f3c222606f890573e6128fbe389f37bd6f6bda3  | 4aa6970cac04ace4a930de67d4c18106c<br>f4004ba66670cfcdada77a4c4821a213 |

**Table 18.** HIGHNOON

| File MD5                         | File SHA1                                | File SHA256  |
|----------------------------------|--|--|
| 46a557fbdc734a6794b228df0195474  | 41bac813ae07aef41436e8ad22d605f786f9e099 | 42d138d0938494fd64e1e919707e7201<br>e6675b1122bf30ab51b1ae26adaec921 |
| 77c60e5d2d99c3f63f2aea1773ed4653 | ad77a34627192abdf32daa9208fbde8b4ebfb25c | 7566558469ede04efc665212b45786a<br>730055770f6ea8f924d8c1e324cae8691 |
| 849ab91e93116ae420d2fe2136d24a87 | 3f1dee370a155dc2e8fb15e776821d7697583c75 | 7cd17fc948eb5fa398b8554fea036bdb<br>3c0045880e03acbe532f4082c271e3c5 |

**Table 19.** HIGHNOON.BIN

| File MD5                         | File SHA1                                | File SHA256  |
|----------------------------------|--|--|
| 36711896cfcb67f599305b590f195aec | 1036a7088b060250bb66b6de91f0c6ac462dc24c | 490c3e4af829e85751a44d21b25de1781cfe4961afdef6bb5759d9451f530994 |
| 7d51ea0230d4692eedc2d5a4cd66d2d  | 5ee7c57dc84391f63eaa3824c53cc10eafc9e388 | 63e8ed9692810d562adb80f27bb1aeaf48849e468bf5fd157bc83ca83139b6d7 |
| a0a96138b57ee24eed31b652ddf60d4e | 03de2118aac6f20786043c7ef0324ef01dcf4265 | 79190925bd1c3fae65b0d11db40ac8e61fb9326ccfed9b7e09084b891089602d |

**Table 20.** JUMPALL

| File MD5                         | File SHA1                               | File SHA256  |
|----------------------------------|---|--|
| ba08b593250c3ca5c13f56e2ca97d85e | adde0644a572ed593e8b0566698d4e3de0feb8a | c51c5bbc6f59407286276ce07f0f7ea994e76216e0abe34cbf20f1b1cbd9446d |

**Table 21.** POISONPLUG

| File MD5                          | File SHA1                                | File SHA256   |
|-----------------------------------|--|---|
| 223e4cc4cf5ce049f300671697a17a01  | 1835c7751436cc199c55b42f34566d25fe6104ca | e65d39fa659f64a57ee13e8a638abd9031fa1486311d2782f32e979d5dee1ca5  |
| 37e100dd8b2ad8b301b130c2bca3f1ea  | 32466d8d232d7b1801f456fe336615e6fa5e6ffb | 2eea29d83f485897e2bac9501ef000cc266ffe10019d8c529555a3435ac4aab   |
| 557ff68798c71652db8a85596a4bab72  | 971bb08196bba400b07cf213345f55ce0a6eedc8 | 5d971ed3947597fbb7e51d806647b37d64d9fe915b35c7c9eaf79a37b82dab90  |
| 830a09ff05eac9a5f42897ba5176a36a  | 2366d181a1697bcb4f368df397dd0533ab8b5d27 | 70c03ce5c80aca2d35a5555b0532eedede24d4cc6bdb32a2c8f7e630bba5f26e  |
| b0877494d36fab1f9f4219c3deffbfb19 | 4dc5fadece500ccd8cc49cf8a1b59baee3382a   | 3e6c4e97cc09d0432fbbbfb3f3e424d4aa967d3073b6002305cd6573c47f0341f |
| c8403fabda4d036a55d0353520e765c9  | d0429abec299ddfee7e1d9ccff1766af4c0992b  | 9283703dfbc642dd70c8c7667528552690e998bcb3f3374273c0b5c90c0d1366  |
| ff8d92dfbcda572ef97c142017eec658  | 6f065eea36e28403d4d518b8e24bb7a915b612c3 | f4d57acde4bc546a10cd199c70cdad09f576fdf66a36b08a00c19ff6ae19661   |
| ffd0f34739c1568797891b9961111464  | 82072cb53416c89bfee95b239f9a90677a0848df | 0055dfacc952c99b1171ce431a02abfce5c6f8fb5dc39e4019b624a7d03bfc    |

**Table 22.** POISONPLUG.SHADOW

| File MD5                         | File SHA1                                | File SHA256  |
|----------------------------------|--|--|
| 72584d6b7dd10c82d9118567b548b2b1 | f067443c2c4d99dc6577006a2f105e51af731659 | faedf9fef6edac2f0565882112b2eae14e<br>dda024239d3218a9fe9ac7e0b12db6 |
| 97363d50a279492fda14cbab53429e75 | f1a181d29b38dfe60d8ea487e8ed0ef30f064763 | 462a02a8094e833fd456baf0a6d4e18<br>bb7dab1a9f74d5f163a8334921a4ffde8 |
| a6c7db170bc7a4ee2cdb192247b59cd6 | 5a85d1e19e0414fc59e454ccbaef0a3c6bb41268 | 92cb362ae8d24c05f368d13036534fe01<br>4344994d46031a0a8636a7ca0b792c6 |

**Phishing Payloads****Table 23.** 中東呼吸器症候群(MERS)の予防.7z

| File MD5                         | File SHA1                                | File SHA256  |
|----------------------------------|--|--|
| 5e87b09f9a3f1b728c9797560a38764b | 67c957c268c1e56cc8eb34b02e5c09eae62680f5 | 354c174e583e968f0ecf86cc20d59ecd<br>6e0f9d21800428453b8db63f344f0f22 |

**Table 24.** Documents.7z

| File MD5                         | File SHA1                                | File SHA256  |
|----------------------------------|--|--|
| 8c6cceae2eea92deb6f7632f949293f0 | b193ff40a98cd086f92893784d8896065faa3ee3 | bae8f4f5fc959bff980d6a6d12797b0d<br>647e97cc811c5b9e827d0b985d87f68f |

## Domains

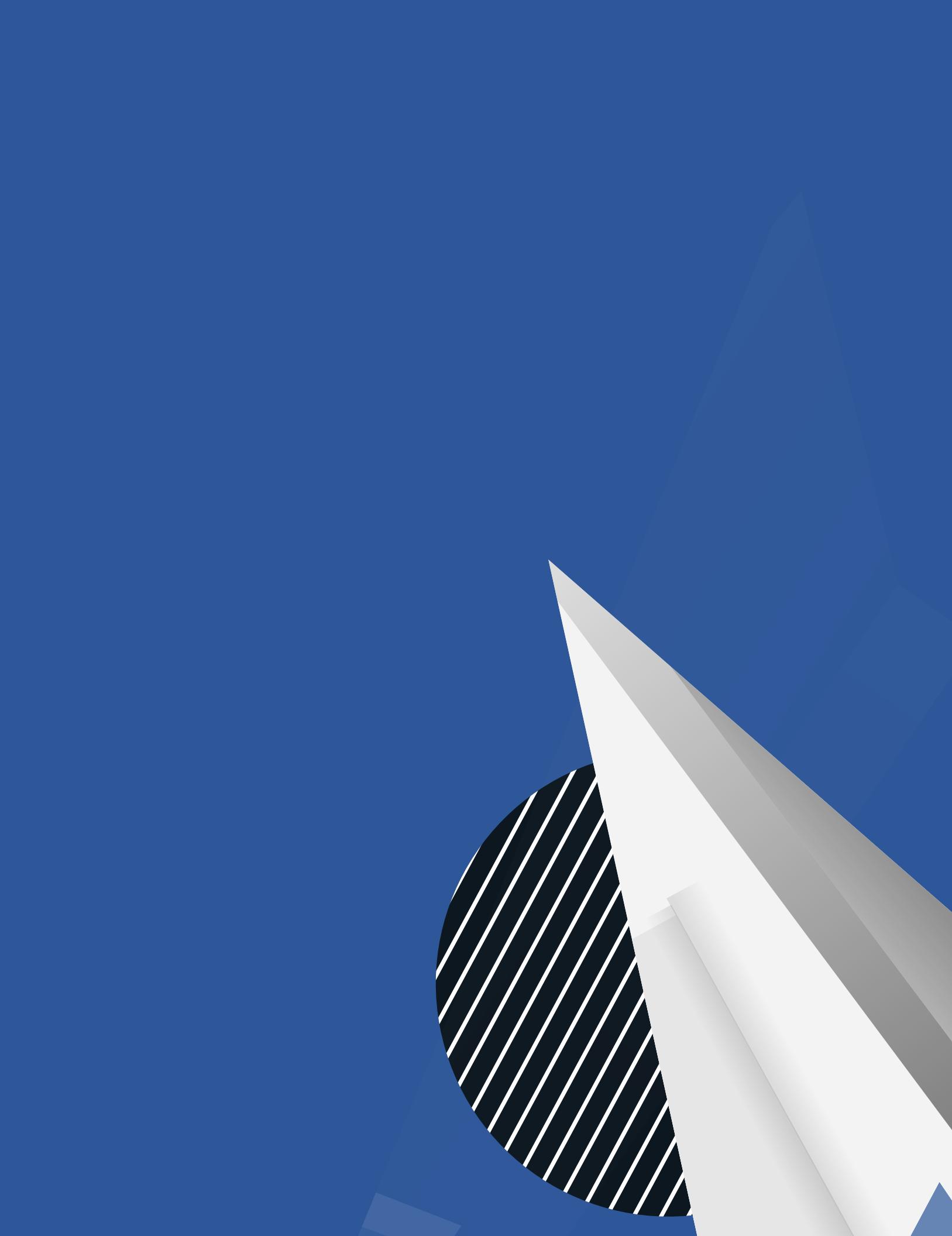
- agegamepay[.]com
- ageofwuxia[.]com
- ageofwuxia[.]info
- ageofwuxia[.]net
- ageofwuxia[.]org
- bugcheck.xigncodeservice[.]com
- byeserver[.]com
- dnsgoogle[.]com
- gamewushu[.]com
- gxxservice[.]com
- ibmupdate[.]com
- infestexe[.]com
- kaspersky[.]net
- linux-update[.]net
- macfee[.]ga
- microsOff[.]com
- microsOtf[.]com
- notped[.]com
- operatingbox[.]com
- paniesx[.]com
- serverbye[.]com
- sexyjapan.ddns[.]info
- symanteclabs[.]com
- techniciantext[.]com
- win7update[.]net
- xigncodeservice[.]com

## Email Addresses

- akbkxp@126[.]com
- akbkxp@163[.]com
- hackershby@126[.]com
- hrsimon59@gmail[.]com
- injuriesa@126[.]com
- injuriesa@163[.]com
- injuriesa@gmail[.]com
- injuriesa@hotmail[.]com
- injuriesa@qq[.]com
- kbkxp@126[.]com
- petervc1983@gmail[.]com
- ravinder10@126[.]com
- ravinder10@hotmail[.]com
- ravinder10@sohu[.]com
- wolf\_zhi@yahoo[.]com

## URLs

- [https://docs.google\[.\]com/document/d/1ICySd5ZNGj9Jz8pigZsuv8IciusYKqOq0Rpe2E0zgMU](https://docs.google[.]com/document/d/1ICySd5ZNGj9Jz8pigZsuv8IciusYKqOq0Rpe2E0zgMU)
- [https://docs.google\[.\]com/document/d/1KJ\\_RJRtkKhcuJjXOCKtEOLuwH3sRi72PUhtfuknCyRc](https://docs.google[.]com/document/d/1KJ_RJRtkKhcuJjXOCKtEOLuwH3sRi72PUhtfuknCyRc)
- [https://docs.google\[.\]com/document/d/1TkTC3fHUvEBsBurZIGw7Kf5YsPjblpahl1FksRDCuTo](https://docs.google[.]com/document/d/1TkTC3fHUvEBsBurZIGw7Kf5YsPjblpahl1FksRDCuTo)
- [https://docs.google\[.\]com/document/d/1iQwnF3ibWPZ6-95VHrRAPrL6u\\_UT\\_K7X-rQrB7xt95k](https://docs.google[.]com/document/d/1iQwnF3ibWPZ6-95VHrRAPrL6u_UT_K7X-rQrB7xt95k)
- [https://steamcommunity\[.\]com/id/119887132](https://steamcommunity[.]com/id/119887132)
- [https://steamcommunity\[.\]com/id/869406565](https://steamcommunity[.]com/id/869406565)
- [https://steamcommunity\[.\]com/id/oswal053](https://steamcommunity[.]com/id/oswal053)



To learn more about FireEye, visit: [www.FireEye.com](http://www.FireEye.com)

---

**FireEye, Inc.**

601 McCarthy Blvd. Milpitas, CA 95035  
408.321.6300/877.FIREEYE (347.3393)  
[info@FireEye.com](mailto:info@FireEye.com)

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. SP.APT41.2019.US-EN-000209-01

**About FireEye, Inc.**

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks.

