APT41 and Recent Activity

September 22, 2022
Agenda

- Overview of APT41
- Targeting Operations
- Indictment
- Historical Targeting
- Threats to Healthcare
- Why Healthcare
- Recent Activity
- Popular Tools and Techniques

Slides Key:

**Non-Technical:** Managerial, strategic and high-level (general audience)

**Technical:** Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
Overview
Overview

- Chinese State-Sponsored Threat Actor
- Members of APT41 have been actively tracked since 2012
- **Also Known As:** Double Dragon, Barium, Winnti, Wicked Panda, Wicked Spider, TG-2633, Bronze Atlas, Red Kelpie
- Has been tracked as two separate groups; dependent on operation
- History of targeting healthcare, high-tech, telecommunications, higher education, video games, travel, and news organizations
- Frequently likes to use the following:
  - Spear phishing
  - Water holes
  - Supply chain attacks
  - Backdoors

Source: Mandiant
APT41 Targeting Operations
Targeting Operations: Industries

APT41 frequently targets one of the sectors below for industry-specific information, and to collect information that would be beneficial in future attacks:

• Healthcare
• High-tech
• Media
• Pharmaceuticals
• Retail
• Software companies

• Telecoms
• Travel services
• Education
• Video games
• Virtual currencies
Targeting Operations: Countries

APT41 typically operates their campaigns on one or more of the 14 countries below:

- United States
- Myanmar
- United Kingdom
- Netherlands
- Singapore
- South Korea
- South Africa
- France
- Switzerland
- India
- Thailand
- Italy
- Turkey
- Japan
Indictment and 2021 Operations
The Chinese Threat Group was issued two separate indictments in 2019 and 2020 for malicious activity. Despite these efforts, the group was still very active in 2021.

- August 15, 2019
- August 11, 2020
- Federal grand jury in Washington, D.C.
- Computer intrusions affecting 100 companies globally
- Indictment did not appear to slow down any operations
2021 Operations

The indictment did not hinder APT41’s operations as they progressed into 2021. By the end of the year, 13 victims were impacted globally.

• Conducted four different malicious campaigns
• Group-IB, generated 80 notifications for organizations
  ▪ Private and government
  ▪ In progress, and completed attacks
• Were only able to breach half of the targeted websites
• New techniques were observed
  ▪ SQL Injections were performed for initial attack
  ▪ Cobalt strike beacons were uploaded in smaller chunks
  ▪ Typically employs spear phishing emails, watering holes, or supply chain attacks
2021 Operations, part 2

The actor was able to impact victims all over the globe, and targeted political and military groups during one of their campaigns.

• 13 confirmed victims globally:
  ▪ The US, Taiwan, India, Thailand, China, Hong Kong, Mongolia, Indonesia, Vietnam, Bangladesh, Ireland, Brunei, and the UK

• Targets also included:
  ▪ Political groups, military organizations, and airlines

• Working hours were identified:
  ▪ Monday – Friday
  ▪ UTC +8 time zone

2021 Countries and Sectors Impacted

Map with a breakdown of organizations compromised by APT41 by industry and country:

- **USA**
  - Healthcare
  - Software development

- **China**
  - Financial services
  - Software development

- **Taiwan**
  - Government
  - Manufacturing
  - Media
  - Healthcare
  - Hospitality

- **Vietnam**
  - Aviation
  - Financial Education

Source: Group-IB
APT41 and Healthcare
Targeting Healthcare

- Years healthcare was targeted:
  - 2014, 2015, 2016, 2018, 2019
- 2014 and 2016: Interested in IT and medical device software
  - Supply chain attack
  - Medical device information was targeted
- 2016: Targeted biotech company
  - HR data, tax information, acquisition, and clinical trial data
- 2018: Goals of the campaign were unknown
- 2019: Targeted US cancer research facility
  - Malware EVILNUGGET
  - CVE-2019-3396 exploited
Targeting Healthcare, continued

- Attacks on healthcare
  - January – March 2020
- APT41 was identified as attempting to exploit Citrix, Cisco, and Zoho endpoints as a part of their campaign
- Attempted to exploit over 75 customers
- Several sectors in the United States were targets
- Attempted exploitation of:
  - CVE-2019-19781: Citrix vulnerability which allows directory transversal. Gives the attacker access to areas of a system they would not normally have.
  - CVE-2020-10189: Zoho vulnerability which allows for remote code execution that can allow an attacker to deliver malware and advance malicious efforts.
Why Healthcare, and the Five-Year Plan
The 14th Five-Year Plan

Chapter 5 describes seven core industries and ten areas where technology should be cultivated and applied:

- Cloud computing
- Big data
- Internet of things (IoT)
- Industrial internet
- Blockchain
- Artificial intelligence
- Virtual and augmented reality
- Smart transportation
- Smart energy
- Smart manufacturing
- Smart medicine
- Smart government
Chapter 2 of the Fiver-Year Plan lists several areas where China should advance themselves through major science and technological advancements:

1. New Generation Artificial Intelligence
2. Quantum Information
3. Integrated Circuits (or Semiconductors)
4. Neuroscience and Brain-Inspired Research
5. Genetics and Biotechnology
6. Clinical Medicine and Health
Recent Activity
Recent Activity – MoonBounce

• Late 2021
• Unified Extensible Firmware Interface (UEFI) Firmware Implant
  ▪ Most advanced implant found “in the wild”
• Implanted on the SPI flash memory of the motherboard
• Used to deploy additional malware
• High level of sophistication
• Mitigations:
  ▪ Updating firmware
  ▪ Verifying BootGuard
  ▪ Enable trusted Platform Modules
Recent Activity – USAHERDS

Two zero-day attacks were used to exploit the web-based Animal Health Reporting Diagnostic System (USAHERDS) application.

- May 2021 – February 2022
- Compromised at least six U.S. state governments
- Potentially more unknown victims
- APT41 was quickly detected and removed
- System was compromised via zero-day CVE-2021-44207 and Log4j attacks
- Investigation is still ongoing
Two zero-day attacks were used to compromise the USAHERDS application. One CVE was accessed by using a MachineKey and the other was from Log4Shell.

- **CVE-2021-44207**: Zero-day; used hard-coded credentials, allowing the attacker to bypass the authentication process in the software
  - Use of a MachineKey for access
  - Unknown how APT41 was able to obtain the key
- **CVE-2021-44228**: Zero-day in Log4j that causes remote code execution
  - Generated payloads to perform reconnaissance
  - Deployed variants of the KEYPLUG backdoor
Recent Activity – Government Espionage

• Cyber-espionage activity
  ▪ Focused on governments in Asia

• Additional targeting of:
  ▪ Aerospace, defense firms, telecom, and IT organizations

• Attacks have been ongoing since 2021

• Previously unseen info stealer
  ▪ Keylogging
  ▪ Screenshots
  ▪ Connecting to and querying SQL databases
  ▪ Code injection
  ▪ Downloading files
  ▪ Stealing clipboard data

• Evidence suggests ties with APT41
Popular Tactics, Techniques, and Procedures (TTPs) and Tools
Popular TTPs and Tools

- **Initial Access**: Frequent use of spear phishing with malicious attachments, watering holes, and supply chain attacks
- **Establish Foothold**: The group utilizes a variety of public and private malware
- **Escalate Privileges**: Usually leverages custom tools to obtain credentials
- **Internal Reconnaissance**: Performs internal reconnaissance using compromised credentials
- **Lateral Movement**: Remote Desktop Protocol (RDP), stolen credentials, adding admin groups, and brute forcing utilities
- **Maintain Presence**: APT41 relies on the use of backdoors
- **Mission Complete**: Creation of a RAR archive for exfiltration and removal of evidence

**Recommended Reading:**

**APT41**

Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center
## Popular TTPs and Tools

<table>
<thead>
<tr>
<th>Software</th>
<th>MITRE ID</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLACK COFFEE</td>
<td>S0069</td>
<td>Multiuse; reverse shell, enumeration, deletion to C2 communications, and obfuscation</td>
</tr>
<tr>
<td>China Chopper</td>
<td>S0020</td>
<td>Web shell that can provide access back to an enterprise network</td>
</tr>
<tr>
<td>Cobalt Strike</td>
<td>S0154</td>
<td>Commercial tool; allows attacker to drop payloads</td>
</tr>
<tr>
<td>Gh0st Rat</td>
<td>S0032</td>
<td>Remote Access Tool (RAT)</td>
</tr>
<tr>
<td>Mimikatz</td>
<td>S0002</td>
<td>Credential dumper for obtaining plaintext Windows account information</td>
</tr>
<tr>
<td>PlugX</td>
<td>S0013</td>
<td>Remote Access Tool (RAT) with modular plugins</td>
</tr>
<tr>
<td>ShadowPad</td>
<td>S0596</td>
<td>Modular backdoor; frequently used in C2 communications</td>
</tr>
</tbody>
</table>
Reference Materials
References


References


References

- “APT41”. Attack.MITRE. [https://attack.mitre.org/groups/G0096/](https://attack.mitre.org/groups/G0096/)
References


References


• MITRE ATT&CK. https://attack.mitre.org/mitigations/enterprise/
Questions
FAQ

Upcoming Briefing
• 10/6 – The Use of Legitimate Tools in Cyberattacks Against the Health Sector

Product Evaluations
Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information
Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer
These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.
About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

<table>
<thead>
<tr>
<th>Sector and Victim Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alerts and Analyst Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat Briefings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.</td>
</tr>
</tbody>
</table>
Contacts

HHS.GOV/HC3

HC3@HHS.GOV