APT41
10/24/2019
Agenda

• APT41
• Overview
• Industry targeting timeline and geographic targeting
• A very brief (recent) history of China
• China’s economic goals matter to APT41 because…
• Why does APT41 matter to healthcare?
• Attribution and linkages
• Weapons
• Indicators of Compromise (IOCs)
• References
• Questions

Slides Key:

- Non-Technical: managerial, strategic and high-level (general audience)
- Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
Overview

• APT41
  • Active since at least 2012
  • Assessed by FireEye to be:
    • Chinese state-sponsored espionage group
    • Cybercrime actors conducts financial theft for personal gain
  • Targeted industries:
    • Healthcare
    • High-tech
    • Telecommunications
    • Higher education
  • Goals:
    • Theft of intellectual property
    • Surveillance
    • Theft of money
  • Described by FireEye as…
    • “highly-sophisticated”
    • “innovative” and “creative”

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. - FireEye
Industry targeting timeline and geographic targeting

- Targeted industries:
  - Gaming
  - Healthcare
  - Pharmaceuticals
  - High tech
  - Software
  - Education
  - Telecommunications
  - Travel
  - Media
  - Automotive

- Geographic targeting:
  - France, India, Italy, Japan, Myanmar, the Netherlands, Singapore, South Korea, South Africa, Switzerland, Thailand, Turkey, the United Kingdom, the United States and Hong Kong
A very brief (recent) history of China

• First half of 20th century, Chinese Civil War
  • Between Kuomintang (Nationalists) and Communists
  • 1927 to 1949
    • Pause from 1937 to 1945 to fight Imperial Japan (WWII)
  • Ended with Communists victorious, taking mainland China and Nationalists retreating to Taiwan
  • No treaty signed, still questions about status and legitimacy today

• Communist China produces first “5-year Plan” in 1953
  • Current plan (13th):
    • Innovation and development are very big priorities
  • Made in China 2025 (released in 2015)
    • Shift China’s economy towards high-value products
    • Focuses on high-tech and pharmaceuticals, among other industries
China’s economic goals matter to APT41 because…

- APT41’s targeting aligns with China’s economic and political goals
  - Targets include:
    - Research and development of computer components (motherboards, processors, servers)
    - Cloud computing technologies (goal in 12th year economic plan)
    - Autonomous vehicle development
    - Medical imagery and research
    - Telecommunications
    - Historic surveillance operations against citizens in Taiwan and Hong Kong
Why does APT41 matter to healthcare?

• APT41 targets healthcare
  • Targets medical device companies and pharmaceuticals for intellectual property theft
  • Often looking for clinical trial data and research as well as corporate intelligence

“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)” – FireEye

• Examples:
  • July 2014 through May 2016 - APT41 targeted the medical device subsidiary of a large healthcare industry corporation
  • May 2015 - A biotech company being acquired was targeted by APT41
    • Sensitive corporate information about operations, human resources, tax information and other acquisition-related data was targeted
  • 2018, APT41 targeted a third healthcare company, with unknown intentions
  • 2018, a cancer research organization was spearphished by APT41; this was followed up by a malware attack against the same organization in 2019
Attribution and linkages

- FireEye’s analysis:
  - Assessed with “high confidence” that APT41 is attributable to Chinese individuals working on behalf of the Chinese government
    - These individuals are also conducting financially motivated cyber operations for themselves
  - Activities associated with:
    - BARIUM – Associated with Chinese government; supply-chain attacks against technology companies
    - Winnti – Associated with Chinese government; history of use of Winnti malware against gaming industry; Also shared with other Chinese espionage operators including APT17, APT20 and APT41
  - Previously known as GREF
  - Heavy code overlap and weapon-usage overlap with APT17
    - China-attributed APT targeting US defense, IT, mining, and legal targets
    - Appears to have shared access to source code/developers (likely a high-pri/sophisticated group)
Weapons

- HIGHNOON – backdoor which includes a loader, dynamic-link library (DLL), and a rootkit; one of APT41’s primary weapons, also used often by APT17 in 2015 to target semiconductor and chemical manufacturers

- HIGHNOON.BIN – modified version of Windows DLL apphelp.dll, used for persistence

- HIGHNOON.LITE – standalone, non-persistent version of HIGHNOON, can download and execute memory-resident modules after C2 authentication

- PHOTO – DLL backdoor that conducts system reconnaissance; 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
  - Rename, delete, copy, move, read, and write to files
Weapons (continued)

- COLDJAVA – backdoor that inserts shellcode and BLACKCOFFEE variant into the Windows registry

- BLACKCOFFEE – Has multiple capabilities
  - Reverse shell
  - File enumeration, and deletion
  - Identify processes
  - Communicate with C2 server through legitimate websites, obfuscating traffic

- CHINACHOP – code injection web shell that can execute Microsoft .NET code within HTTP POST commands which allows CHINACHOP to:
  - Upload and download files
  - Execute applications with web server account permissions
  - List directory contents
  - Access Active Directory
  - Access databases
Weapons (continued)

- SOGU – Backdoor capable of:
  - File upload/download
  - Arbitrary process execution
  - File system and registry access
  - Service configuration access
  - Remote shell access
  - Providing the C2 server with graphical access to the desktop.

- JUMPALL – malware dropper which is known to have dropped variants of HIGHNOON, ZXSHELL, and SOGU

- HOMEUNIX – Launcher for download plugins used by many other Chinese espionage groups such as APT1, APT10, APT17, APT18, and APT20

- LIFEBOAT – backdoor, communicates with C2 server via HTTP
Weapons (continued)

- ZXSHELL – Backdoor that can:
  - Launch port scans
  - Log keystrokes
  - Capture screenshots
  - Set up HTTP or SOCKS proxy
  - Reverse shell
  - Cause SYN floods
  - Transfer/delete/run files.

- POTROAST – Backdoor that can:
  - Connect to hard-coded C2 server
  - Download/upload/execute files
  - Reverse shell

- SWEETCANDLE – downloader that can download and execute payload from C2 server
Indicators of Compromise (IOCs)

HIGHNOON

MD5
- 46a557fbdc734a6794b228df0195474
- 77c60e5d2d99c3f63f2aea1773ed4653
- 849ab91e93116ae420d2fe2136d24a87
- ad77a34627192abdf32daa9208fbde8b4ebfb25c
- 7566558469ede04efc665212b45786a
- 730055770f6ea8f924d8c1e324cae8691
- 7cd17fc948eb5fa398b8554fea036bdb
- 3c0045880e03acbe532f4082c271e3c5

SHA1
- 41bac813ae07aef41436e8ad22d605f786f9e099
- ad77a34627192abdf32daa9208fbde8b4ebfb25c
- 3f1dee370a155dc2e8fb15e776821d7697583c75

SHA256
- 42d138d0938494fd64e1e919707e7201
- e6675b1122bf30ab51b1ae26adaec921
Indicators of Compromise (IOCs) (continued)

JUMPALL

MD5
ba08b593250c3ca5c13f56e2ca97d85e

SHA1
adde0644a572ed593e8b0566698d4e3de0fe8b8a

SHA256
c51c5bbc6f59407286276ce07f0f7ea9
94e76216e0abe34cbf20f1b1cbd9446d
Indicators of Compromise (IOCs) (continued)

GEARSHIFT

MD5:
5b26f5c7c367d5e976aaba320965cc7f
f8c89ccd8937f2b760e6706738210744

SHA1:
c2fb50c9ef7ae776a42409bce8ef1be464654a4e
f3c222606f890573e6128fbeb389f37bd6f6bda3

SHA256:
7e0c95fc64357f12e837112987333cda7f1e90c1db
8c1208ef8c100649eba7f1ea90c1db
4aa6970cac04ace4a930de67d4c18106c
f4004ba66670cfcdaa77a4c4821a213
Indicators of Compromise (IOCs) (continued)

<table>
<thead>
<tr>
<th>DOMAINS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>agegamepay[.]com</td>
<td>kaspersky[.]net</td>
</tr>
<tr>
<td>ageofwuxia[.]com</td>
<td>linux-update[.]net</td>
</tr>
<tr>
<td>ageofwuxia[.]info</td>
<td>macfee[.]ga</td>
</tr>
<tr>
<td>ageofwuxia[.]net</td>
<td>micros0ff[.]com</td>
</tr>
<tr>
<td>ageofwuxia[.]org</td>
<td>micros0tf[.]com</td>
</tr>
<tr>
<td>bugcheck.xigncodeservice[.]com</td>
<td>notped[.]com</td>
</tr>
<tr>
<td>byeserver[.]com</td>
<td>operatingbox[.]com</td>
</tr>
<tr>
<td>dnsgogle[.]com</td>
<td>paniesx[.]com</td>
</tr>
<tr>
<td>gamewushu[.]com</td>
<td>serverbye[.]com</td>
</tr>
<tr>
<td>gxxservice[.]com</td>
<td>sexyjapan.ddns[.]info</td>
</tr>
<tr>
<td>ibmupdate[.]com</td>
<td>symanteclabs[.]com</td>
</tr>
<tr>
<td>Infestexe[.]com</td>
<td>techniciantext[.]com</td>
</tr>
<tr>
<td>kaspersky[.]net</td>
<td>win7update[.]net</td>
</tr>
<tr>
<td>exe[.]com</td>
<td>xigncodeservice[.]com</td>
</tr>
</tbody>
</table>
**Indicators of Compromise (IOCs) (continued)**

**E-mail addresses:**

<table>
<thead>
<tr>
<th>E-mail Address 1</th>
<th>E-mail Address 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>akbklxp@126[.]com</td>
<td>petervc1983@gmail[.]com</td>
</tr>
<tr>
<td>akbklxp@163[.]com</td>
<td>ravinder10@126[.]com</td>
</tr>
<tr>
<td>hackershby@126[.]com</td>
<td>ravinder10@hotmail[.]com</td>
</tr>
<tr>
<td>hrsimon59@gmail[.]com</td>
<td>ravinder10@sohu[.]com</td>
</tr>
<tr>
<td>injuriesa@126[.]com</td>
<td>wolf_zhi@yahoo[.]com</td>
</tr>
<tr>
<td>injuriesa@163[.]com</td>
<td></td>
</tr>
<tr>
<td>injuriesa@gmail[.]com</td>
<td></td>
</tr>
<tr>
<td>injuriesa@hotmail[.]com</td>
<td></td>
</tr>
<tr>
<td>injuriesa@qq[.]com</td>
<td></td>
</tr>
<tr>
<td>injuriesa@qq[.]com</td>
<td></td>
</tr>
<tr>
<td>kbklxp@126[.]com</td>
<td></td>
</tr>
</tbody>
</table>
Reference Materials
References

- Paganini, Pierluigi, China-linked APT41 group targets US-Based Research University, August 21, 2019, Security Affairs, https://securityaffairs.co/wordpress/90179/apt/apt41-targets-research-university.html  
- Fraser, Nalani; Plan, Fred; O’Leary, Jacqueline; Cannon, Vincent; Leong, Raymond; Perez, Dan and Shen, Chi-en, APT41: A Dual Espionage and Cyber Crime Operation, August 7, 2019, FireEye, https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html
References


• Lyngaas, Sean, Meet APT41, the Chinese hackers moonlighting for personal gain, Aug. 7, 2019, CyberScoop, https://www.cyberscoop.com/apt41-fireeye-china/


References

• Pennino, Alex and Bromiley, Matt, GAME OVER: Detecting and Stopping an APT41 Operation, August 19, 2019, FireEye, https://www.fireeye.com/blog/threat-research/2019/08/game-over-detecting-and-stopping-an-apt41-operation.html

• Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation, FireEye, https://content.fireeye.com/apt-41/rpt-apt41/
Questions
Questions

Upcoming Briefs

• Social Engineering and You
• Supply Chain Risk Management

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

About Us

Sector & Victim Notifications
Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers
Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar
Briefing document and presentation that provides 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.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
Contact

Health Sector Cybersecurity Coordination Center (HC3)
(202) 691-2110
HC3@HHS.GOV