LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

APT41

10/24/2019

Report #: 201910241000

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

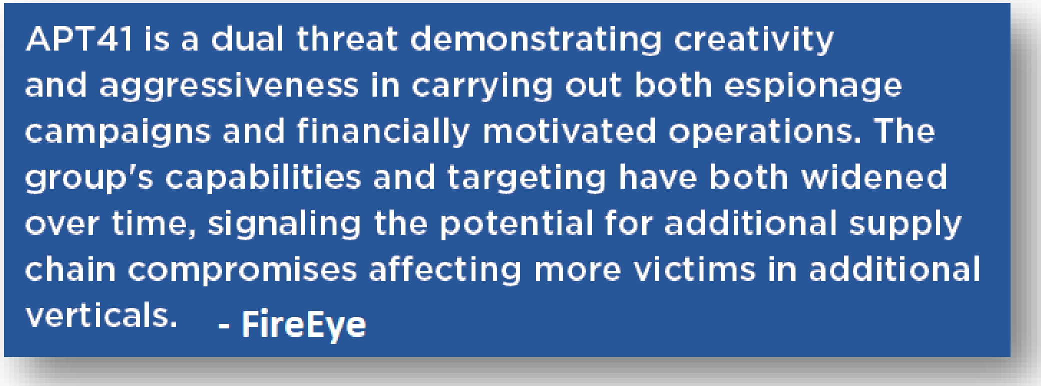
Image courtesy of PCMag.com

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”



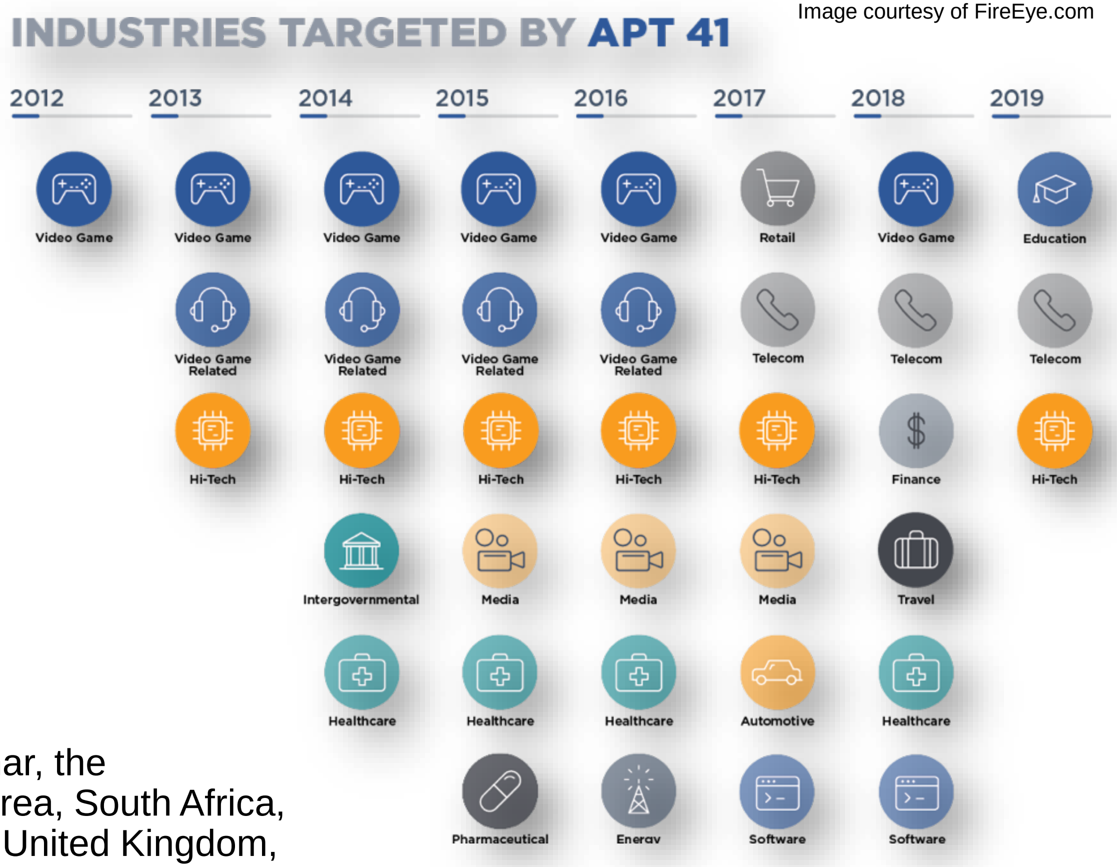
APT41 is a dual threat demonstrating creativity and aggressiveness in carrying out both espionage campaigns and financially motivated operations. The group's capabilities and targeting have both widened over time, signaling the potential for additional supply chain compromises affecting more victims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

Industry targeting timeline and geographic targeting

Image courtesy of FireEye.com

- 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



INDUSTRIES TARGETED BY APT 41

2012	2013	2014	2015	2016	2017	2018	2019
Video Game	Video Game	Video Game	Video Game	Video Game	Retail	Video Game	Education
	Video Game Related	Video Game Related	Video Game Related	Video Game Related	Telecom	Telecom	Telecom
	Hi-Tech	Hi-Tech	Hi-Tech	Hi-Tech	Hi-Tech	Finance	Hi-Tech
		Intergovernmental	Media	Media	Media	Travel	
		Healthcare	Healthcare	Healthcare	Automotive	Healthcare	
			Pharmaceutical	Energy	Software	Software	

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

Image courtesy of thecoldwarexperience.weebly.com

Image courtesy of South China Morning Post

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

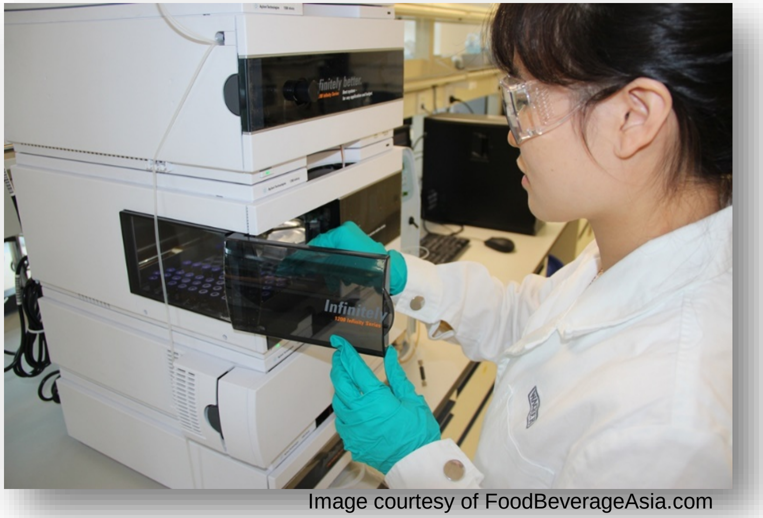


Image courtesy of FoodBeverageAsia.com

Image courtesy of WallStreetJournal.com

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

<u>MD5</u>

- 46a557fbdce734a6794b228df0195474
- 77c60e5d2d99c3f63f2aea1773ed4653
- 849ab91e93116ae420d2fe2136d24a87

<u>SHA1</u>

- 41bac813ae07aef41436e8ad22d605f786f9e099
- ad77a34627192abdf32daa9208fbde8b4ebfb25c
- 3f1dee370a155dc2e8fb15e776821d7697583c75

<u>SHA256</u>

- 42d138d0938494fd64e1e919707e7201
- e6675b1122bf30ab51b1ae26adaec921
- ad77a34627192abdf32daa9208fbde8b4ebfb25c
- 7566558469ede04efc665212b45786a
- 730055770f6ea8f924d8c1e324cae8691
- 7cd17fc948eb5fa398b8554fea036bdb
- 3c0045880e03acbe532f4082c271e3c5

Indicators of Compromise (IOCs) (continued)

JUMPALL

MD5

ba08b593250c3ca5c13f56e2ca97d85e

SHA1

adde0644a572ed593e8b0566698d4e3de0fefb8a

SHA256

c51c5bbc6f59407286276ce07f0f7ea9

94e76216e0abe34cbf20f1b1cbd9446d

Indicators of Compromise (IOCs) (continued)

GEARSHIFT

MD5:

5b26f5c7c367d5e976aaba320965cc7f

f8c89ccd8937f2b760e6706738210744

SHA1:

c2fb50c9ef7ae776a42409bce8ef1be464654a4e

f3c222606f890573e6128fbeb389f37bd6f6bda3

SHA256:

7e0c95fc64357f12e837112987333cdaf

8c1208ef8c100649eba71f1ea90c1db

4aa6970cac04ace4a930de67d4c18106c

f4004ba66670cfcdaa77a4c4821a213

Indicators of Compromise (IOCs) (continued)

DOMAINS

agegamepay[.]com

ageofwuxia[.]com

ageofwuxia[.]info

ageofwuxia[.]net

ageofwuxia[.]org

bugcheck.xigncodeservice[.]com

byeserver[.]com

dnsgogle[.]com

gamewushu[.]com

gxxservice[.]com

ibmupdate[.]com

Infestexe[.]com

kasparsky[.]net

exe[.]com

kasparsky[.]net

linux-update[.]net

macfee[.]ga

micros0ff[.]com

micros0tf[.]com

notped[.]com

operatingbox[.]com

paniesx[.]com

serverbye[.]com

sexyjapan.ddns[.]info

symanteclabs[.]com

techniciantext[.]com

win7update[.]net

xigncodeservice[.]com

Indicators of Compromise (IOCs) (continued)

E-mail addresses:

akbklxp@126[.]com

akbklxp@163[.]com

hackershby@126[.]com

hrsimon59@gmail[.]com

injuriesa@126[.]com

injuriesa@163[.]com

injuriesa@gmail[.]com

injuriesa@hotmail[.]com

injuriesa@qq[.]com

kbklxp@126[.]com

petervc1983@gmail[.]com

ravinder10@126[.]com

ravinder10@hotmail[.]com

ravinder10@sohu[.]com

wolf_zhi@yahoo[.]com

Reference Materials

References

- Greenberg, Andy, A Mysterious Hacker Group Is On a Supply Chain Hijacking Spree, May 3, 2019, Wired, https://www.wired.com/story/barium-supply-chain-hackers/
- M.Léveillé , Marc-Etienne and Tartare, Mathieu, Gaming industry still in the scope of attackers in Asia, welivesecurity.com, March 11, 2019, https://www.welivesecurity.com/2019/10/14/connecting-dots-exposing-arsenal-methods-winnti/
- Winnti. More than just a game, April 11, 2013, Kaspersky, https://securelist.com/winnti-more-than-just-a-game/37029/
- Detecting threat actors in recent German industrial attacks with Windows Defender ATP, January 25, 2017, Mirosoft Security blog, https://www.microsoft.com/security/blog/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/
- Eddy, Max, APT41 Is Not Your Usual Chinese Hacker Group, August 7, 2019, Pcmag.com, https://www.pcmag.com/news/370008/apt41-is-not-your-usual-chinese-hacker-group
- Palmer, Danny, Chinese cyber spies are stealing money from video game firms on the side, August 7, 2019, ZDNet.com, https://www.zdnet.com/article/chinese-cyber-spies-are-stealing-money-from-video-game-firms-on-the-side/
- Goud, Naveen, FireEye identifies APT41 as the latest Chinese Cyber Threat, Cybersecurity Insiders, https://www.cybersecurity-insiders.com/fireeye-identifies-apt41-as-the-latest-chinese-cyber-threat/
- 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

- Menn, Joseph; Stubbs, Jack and Bing, Christopher, Chinese government hackers suspected of moonlighting for profit, August 7, 2019, https://www.reuters.com/article/us-china-cyber-moonlighters/chinese-government-hackers-suspected-of-moonlighting-for-profit-idUSKCN1UX1JE
- FireEye, State of the Hack: APT41 - Double Dragon: The Spy Who Fragged Me, Youtube.com, https://www.youtube.com/watch?v=Gls7S_6iaRE
- M.Léveillé , Marc-Etienne and Tartare, Mathieu, Connecting the dots: Exposing the arsenal and methods of the Winnti Group, welivesecurity.com, https://www.welivesecurity.com/2019/10/14/connecting-dots-exposing-arsenal-methods-winnti/
- ClearSky Research Team, Recent Winnti Infrastructure and Samples, July 18,2017, Clearskysec.com, https://www.clearskysec.com/winnti/
- Lyngaas, Sean, Meet APT41, the Chinese hackers moonlighting for personal gain, Aug. 7, 2019, CyberScoop, https://www.cyberscoop.com/apt41-fireeye-china/
- FireEye Confirms that APT41 Group Hacked TeamViewer; Attackers Might have Accessed Billions of Devices, Information Security Newspaper, https://www.securitynewspaper.com/2019/10/14/fireeye-confirms-that-apt14-group-hacked-teamviewer-attackers-would-have-accessed-billions-of-devices/
- The Fuzzy Boundaries of APT41 - CyberWire podcast, Episode 105, October 5, 2019, The Cyberwire, https://thecyberwire.com/podcasts/cw-podcasts-rs-2019-10-05.html
- Hiding in Plain Sight: FireEye and Microsoft Expose Chinese APT Group's Obfuscation Tactic, May 14, 2015, FireEye, https://www.fireeye.com/blog/threat-research/2015/05/hiding_in_plain_sigh.html

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.**

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

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