HC3: Threat Profile

August 16, 2023 TLP:CLEAR Report: 202308161700

China-Based Threat Actors

Executive Summary

This white paper outlines Chinese cyber threat actors who are known to target the U.S. public health and private health sector entities in cyberspace. The groups outlined within this document represent some of the most capable and deliberate threats to the U.S. healthcare sector, and should be treated with priority when designing and maintaining an appropriate risk posture for a health sector entity.

Overview

The U.S. Healthcare and Public Health (HPH) sector faces significant threats from both state and non-state threat actors in cyberspace. Cybercriminals have proven to be formidable adversries to the health sector in recent years, with digital extortion often in the form of ransomware, as well as data breaches being some of the most common criminal tactics being leveraged by these gangs. State-sponsored threat actors also pose a significant threat, with data exfiltration attacks for the purposes of intellectual property theft and espionage being the primary motivations behind foreign governments targeting the U.S. health sector in cyberspace.

The threat actors in this document consist of groups that have previously and are highly likely to continue to target U.S. healthcare organizations agressively. This very often involves stealing intellectual property related to medical technolgy and medicine, in order to operationalize it and bring it to market. It also involves national security and public health-related cyberattacks, such as the attempts to steal COVID-19 vaccine research in recent years. In the case of at least one threat actor, it can inolve attacks for financial gain.

A note about attribution in this report: For many of the cyber threat groups described within this document, we provide a number of aliases. It is common for cyber threat actors to have many labels, and this is due to the fact that these names are often applied to various intrusion sets as they are discovered, and subsequent to their being linked to other intrusion sets with varying levels of confidence. For this reason, attribution should not be considered 100% for these threat actors, and this includes any name given to them, as well as between the intrusion sets associted with different intrusion sets and labeled by different entities. Additionally, there is no official naming scheme, therefore the same group may be going by various names.

Threat Groups

APT41

Summary/Overview: APT41 has a history of targeting the health sector. They are known to conduct state-sponsored espionage activities as well as digital extortion through their cyber operations.

Affiliations/Aliases: APT41 is a hacking group believed to be based out of Chengdu, China, and has an alleged association with China's Ministry of State Security. APT41 is also known as BARIUM, Winnti, LEAD, WICKED SPIDER, WICKED PANDA, Blackfly, Suckfly, Winnti Umbrella, and Double Dragon, among other labels.

Targeting: APT41 has directly targeted organizations in over a dozen countries, dating back to its earlierst

known operations in 2007. Twelve of those countries can be seen in *Figure 1*. This includes both government and private organizations based in the U.S., the UK, China, Taiwan, Hong Kong, India, Thailand, Mongolia, Indonesia, Vietnam, Bangladesh, Ireland, and Brunei. The group's espionage campaigns have targeted healthcare (including pharamceuticals), telecommunications, software and the high-tech sector, media/news, retail, travel, hospitality, sports, education, logistics, finance, entertainment (especially video games) and digital currencies. They are also known to target state governments, which can include healthcare organizations. Much of their targeting has historically included theft of intellectual property, and generally has been observed to align with China's most recent 5-year plan. Their cybercriminal activities have primarily targeted the video game industry and virtual currency entities to date, and often involve the deployment of ransomware. There are also indications that the group tracks individuals and conducts surveillance, although HC3 is unaware of thiese types of activities specifically being leveraged against the U.S. health sector to date.

Figure 1: APT41 geographic targeting according to 2022 Mandiant data.

Analysis of Operations: APT41 is believed to have been in operations since at least 2007. They are a group whose goals include cyber espionage and financial gain. They distinguish themselves by primarily engaging in financially-motivated cybercriminal activities, possibly without the knowledge of the state and ostensibly for the benefit of the individual members of the group. This combination of operational goals is the reason they are referred to by some as Double Dragon.

APT41 will exploit known vulnerabilites. They demonstrated this when they targeted ProxyLogon vulnerabilities, as an example. They are known to be very aggressive when targeting such vulnerabilities. They reportedly began exploiting the Log4J vulnerabilities in December of 2021 within hours after they were disclosed to the public.

APT41 also uses well-known security tools, such as Acunetix, Nmap, JexBoss, Sqlmap, a customized version of Cobalt Strike, and fofa.su, which is roughly a Chinese equivalent of the popular website Shodan. To conduct reconnaissance, they are known to use the previously-mentioned Acunetix and Nmap, as well as Sqlmap, OneForAll, subdomain3, subDomainsBrute, and Sublist3r. They frequently use spearphishing as an infection vector, but are also heavily reliant on SQL injections to initially penetrate a target organization.

HC3: Threat Profile

August 16, 2023 TLP:CLEAR Report: 202308161700

APT41 is known to maintain a significant dwell time, and once they have established persistent access to a target, they often leverage more sophisticated TTPs and deploy additional malware as part of multi-staged attacks. As one example, in a campaign that lasted roughly a year, they leveraged almost 150 unique malware variants to compromise hundreds of target systems. These variants included backdoors, credential stealers, keyloggers, and rootkits. Some of the malware they have been known to use includes CROSSWALK, HIGHNOON, xDoor, Xmrig, ASPXSpy, China Chopper, BEACON, MESSAGETAP, Gh0st, njRAT, PlugX, ZxShell, Mimikatz, BLACKCOFFEE, and POISONPLUG.

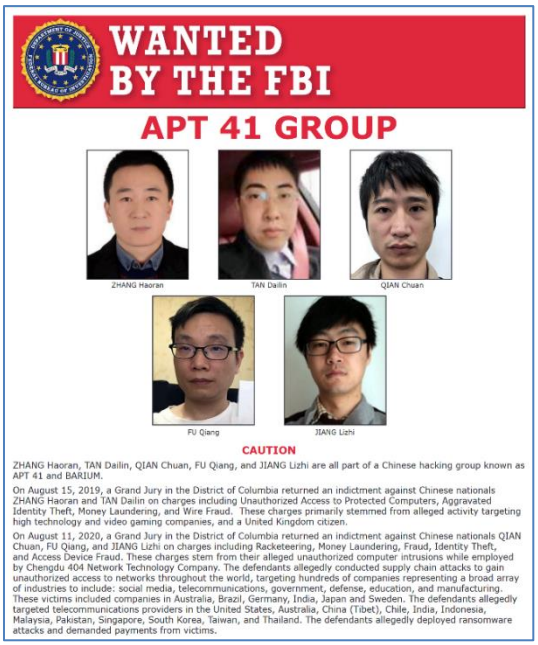

Figure 2: APT41 Wanted Poster.

Some members of APT41 were indicted by the U.S. Department of Justice in 2020; charges against them included unauthorized access to protected computers, aggravated identity theft, money laundering, and wire fraud.

MITRE has mapped APT41 in accordance with their ATT&CK framework, which can be found here.

One of the subgroups that is believed to operate as part of APT41 is called Earth Longzhi. They were first identified as being active in 2020, and were observed as using both public as well as custom malware.

APT10

Summary/Overview: APT10 is known to conduct cyberespionage and cyberwarfare activities, and have leveraged zero day vulnerabilities as well as an array of public and custom tools. Much of their activities are believed to involve the collection of military and intelligence data in support of China's national security goals, but also other operations in support of Chinese business operations.

Affiliations/Aliases: APT10 is also known as Menupass Team, Stone Panda, Red Apollo, Cicada, CVNX, HOGFISH and Cloud Hopper. According to the U.S. Department of Justice, APT10 is a capability of the Tianjin State Security Bureau of China's Ministry of State Security.

Targeting: APT10's geographic targeting has been reported to cover six continents (particularly the United States, Japan, and various European countries) and includes industries such as healthcare, construction, telecommunicationns, government, engineering, and aerospace.

Analysis of Operations: APT10 relies heavily on traditional spearphishing and access to victim's networks through managed service providers (MSPs). They are known to be able and willing to establish and maintain a long dwell time. They also frequently leverage "living off the land" techniques, exploiting and utilizing capabilities already existing in a victim's environment, as well as DLL-side-loading and custom DLL loaders. Legitimate tools and malware known to be used by APT10 includes certutil, adfind, csvde, ntdsutil, WMIExec, PowerShell, HAYMAKER AKA ChChes AKA Scorpion, SNUGRIDE, BUGJUICE AKA RedLeaves (overlap with PlugX), and QUASARRAT, also known as xRAT.

Members of APT10 were indicted by the U.S. District Court of New York in 2018.

APT18

Summary/Overview: Very little is known about APT18. They are believed to be affiliated with China's military and, despite limited public knowledge, appear to be as capable as any of China's other cyberwarfare capabilities. They target a number of industries, including healthcare, and are capable of leveraging complex vulnerabilities and utilizing a wide array of malware.

Affiliations/Aliases: APT18, also known as Wekby, TA-428, TG-0416, Scandium, and Dynamite Panda, is believed to be affiliated with the Chinese People's Liberation Navy.

Targeting: APT18 is known to target human rights groups, governments, and various sectors, including medical (especially pharmaceutical and biotechnology), aerospace, defense, construction, engineering, education, industrial, transportation, and information technology.

Analysis of Operations: Very little has been released publicly about APT18, but they are believed to be responsible for the 2014 attack on a healthcare provider, which resulted in theft of SSNs and PII for 4.5 million patients. They are also known to use sophisticated malware, including Gh0st RAT, HTTPBrowser, pisloader, and PoisonIvy. They frequently develop and adapt zero-day exploits for operations, and are believed to have exploited the OpenSSL heartbleed vulnerability in the the previously-mentioned 2014 compromise of a healthcare provider.

APT22

Summary/Overview: APT22 has likely been operational since at least 2014. They often target political entities (especially dissidents against the Chinese government) and the health sector.

Affiliations/Aliases: APT22 is also known as Barista, Group 46 and Suckfly. It is unknown which area of the Chinese government they are affiliated with.

Targeting: APT22 is known to target information technology companies, healthcare companies (especially biomedical and pharmaceutical), and political, military, and economic targets in the United States, in Europe and across East Asia.

Analysis of Operations: APT22 is known to leverage complex malware such as PISCES, SOGU (AKA PlugX), FLATNOTE, ANGRYBELL, BASELESS, SEAWOLF and LOGJAM. They are known to use strategic web compromises in order to passively exploit targets of interest, and identify vulnerable public-facing web servers on victim networks and uploaded web shells in order to gain access to the victim network.

Countermeasures, Mitigations and Defensive Actions

Due to the nature of advanced persistent threats, including their high level of sophistication as well as their constant evolution of capabilities, it is challenging to attempt to compile a list of specific technical steps to defend agaisnt a single threat, much less a list of them such as is in this white paper. However, we recommend healthcare organizations begin by implementing the following:

HC3: Threat Profile

August 16, 2023 TLP:CLEAR Report: 202308161700

The table below lists some of the top infection vectors used to generally compromise U.S. healthcare organizations with the threat actors in this document:

	Phishing	Vulnerabilities	RDP/VPN	Supply Chain	Watering Holes
APT41	✓	✓	✓	✓	✓
APT22	✓	✓	✓		
APT10	✓	✓	✓	✓	✓
APT18	✓	✓			✓
APT27	✓	✓	✓		

Be sure to understand the above infection vectors and ensure they are part of the focus of the enterprise risk management plan.

1. The National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) released a resource on Chinese state-sponsored cyber operations. It includes valuable technical data that should be understood when defending against Chinese threat actors. It can be found here.
2. The Department of Homeland Security (DHS) maintains a page on the cyber threat posed by China, including resources for defense. It can be found here.
3. There are a number of resources available to understand China's strategic approach towards cyberwarfare. Several valuable documents are as follows:
    a. Atlantic Council: The 5×5—China's cyber operations
    b. Booz Allen: China's Cyberattack Strategy Explained
    c. U.S.-China Economic AND Security Review Commission: Hearing on "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States"
    d. Ball, D., China's Cyber Warfare Capabilities, Security Challenges , Winter 2011, Vol. 7, No. 2 (Winter 2011), pp. 81-103, Institute for Regional Security

Appendix A: Threat Actor Targeting Matrix

The table below is a summary of the threat actors covered in the body of this paper. The first four are covered in depth due to the fact that based on known activities, they present the greatest threat the the U.S. HPH in cyberspace. The remaining actors also serve as threats to the U.S. HPH.

HC3: Threat Profile

August 16, 2023 TLP:CLEAR Report: 202308161700

Threat Actor	Aliases	Notable Attacks on the Health Sector
APT41	Barium, Winnti, Brass Typhoon, Wicked Panda, Wicked Spider	• Between July 2014 and May 2016, targeted a medical devices subsidiary of a large corporation • Targeted a biotech company being acquired in 2015 • Targeted of US health center focused on cancer research in 2018 • Campaign in 2021 targeting Citrix, Zoho and Cisco technologies in the health sector • Stealing at least $20M in US Covid relief funds in 2022
APT22	Barista, G0039, Suckfly, BRONZE OLIVE, Group 46	• Has a documented focus on biomedical, pharmaceutical, and healthcare organizations • Conducted a multi-year campaign against cancer researchers.
APT10	STONE PANDA, Menupass Team, happyyongzi, POTASSIUM, Red Apollo, CVNX, HOGFISH, Cloud Hopper, BRONZE RIVERSIDE, ATK41, G0045, Granite Taurus	• Leveraged healthcare-themed documents in phishing attacks targeting entities in Japan
APT18	Wekby, DYNAMITE PANDA, TA-428, TG-0416, SCANDIUM, PLA Navy, G0026	• Targeting biotech, pharmaceutical, cancer-specialty research organizations and healthcare manufacturing companies since 2013 • Targeting a healthcare company in for medical espionage purposes; collecting data on medical device development
APT27	Earth Smilodon, TG-3390, Emissary Panda, BRONZE UNION, APT27, Iron Tiger, LuckyMouse	• https://www.hipaajournal.com/chinese-apt-group-compromised-healthcare-organizations-by-exploiting-zoho-password-management-platform-flaw/ • https://www.hivepro.com/apt27-group-uses-the-hyperbro-remote-access-trojan-to-inject-backdoors-into-victims-network/

References

APT41 — The spy who failed to encrypt me
https://medium.com/@DCSO_CyTec/apt41-the-spy-who-failed-to-encrypt-me-24fc0f49cad1

Hackers linked to Chinese government stole millions in Covid benefits, Secret Service says
https://www.nbcnews.com/tech/security/chinese-hackers-covid-fraud-millions-rcna59636

APT41 Taps Google Red-Teaming Tool in Targeted Info-Stealing Attacks
https://www.darkreading.com/vulnerabilities-threats/apt41-taps-google-red-teaming-tool-targeted-info-

stealing-attacks

Lookout Attributes Advanced Android Surveillanceware to Chinese Espionage Group APT41
https://www.lookout.com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41

APT41 hackers target Android users with WyrmSpy, DragonEgg spywar
https://www.bleepingcomputer.com/news/security/apt41-hackers-target-android-users-with-wyrmspy-dragonegg-spyware/

APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat
https://www.mandiant.com/resources/blog/apt10-menupass-group

Two Birds, One STONE PANDA
https://www.crowdstrike.com/blog/two-birds-one-stone-panda/

Chinese hackers allegedly stole data of more than 100,000 US Navy personnel
https://www.technologyreview.com/2018/12/20/239760/chinese-hackers-allegedly-stole-data-of-more-than-100000-us-navy-personnel/

Beyond Compliance: Cyber Threats and Healthcare
https://www.bankinfosecurity.com/whitepapers/beyond-compliance-cyber-threats-healthcare-w-5570

NSA/CISA: Chinese State-Sponsored Cyber Operations: Observed TTPs
https://media.defense.gov/2021/Jul/19/2002805003/-1/-1/0/CSA_CHINESE_STATE-SPONSORED_CYBER_TTPS.PDF

CISA: China Cyber Threat Overview and Advisories
https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china

Mandiant: Beyond Compliance: Cyber Threats and Healthcare
https://experience.trellix.com/noelhollistx/home/beyond-compliance-cyber-threats-and-healthcare

Chinese APT Groups Target Cancer Research Facilities: Report
https://www.bankinfosecurity.com/chinese-apt-groups-target-cancer-research-facilities-report-a-12952

SecureWorks: BRONZE OLIVE
https://www.secureworks.com/research/threat-profiles/bronze-olive

China's Cyber Warfare Capabilities
https://www.jstor.org/stable/pdf/26461991.pdf

China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States
https://www.uscc.gov/hearings/chinas-cyber-capabilities-warfare-espionage-and-implications-united-states

The 5×5—China's cyber operations

https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/

China's Cyberattack Strategy Explained
https://www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html

CHINA'S CYBER CAPABILITIES: WARFARE, ESPIONAGE, AND IMPLICATIONS FOR THE UNITED STATES
https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf

What Are China's Cyber Capabilities and Intentions?
https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

APT Gang Branches Out to Medical Espionage in Community Health Breach
https://threatpost.com/apt-gang-branches-out-to-medical-espionage-in-community-health-breach/107828/

New Wekby Attacks Use DNS Requests As Command and Control Mechanism
https://unit42.paloaltonetworks.com/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/

Bugcrowd: 18
https://www.bugcrowd.com/glossary/apt18/

APT41 World Tour 2021 on a tight schedule
https://www.group-ib.com/blog/apt41-world-tour-2021/

Researchers uncover years-long espionage campaign targeting dozens of global companies
https://therecord.media/operation-cuckoobees-apt41-cybereason-winnti-group

APT41: A Dual Espionage and Cyber Crime Operation
https://www.mandiant.com/resources/blog/apt41-dual-espionage-and-cyber-crime-operation

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback