APT41 and Recent Activity

September 22, 2022

TLP: WHITE, ID# *202209221300*

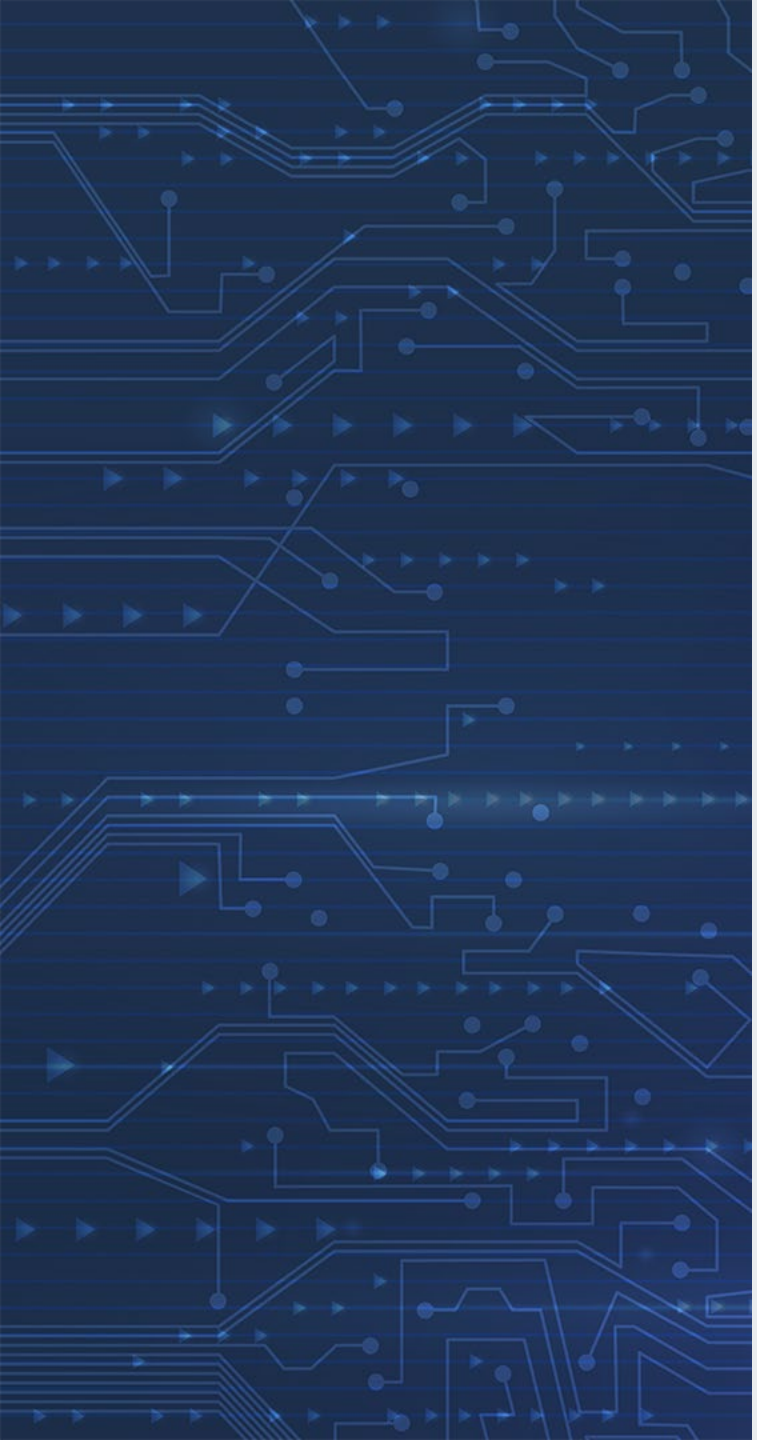
Agenda

- 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

Indictment

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

Source: FBI

2021 Operations

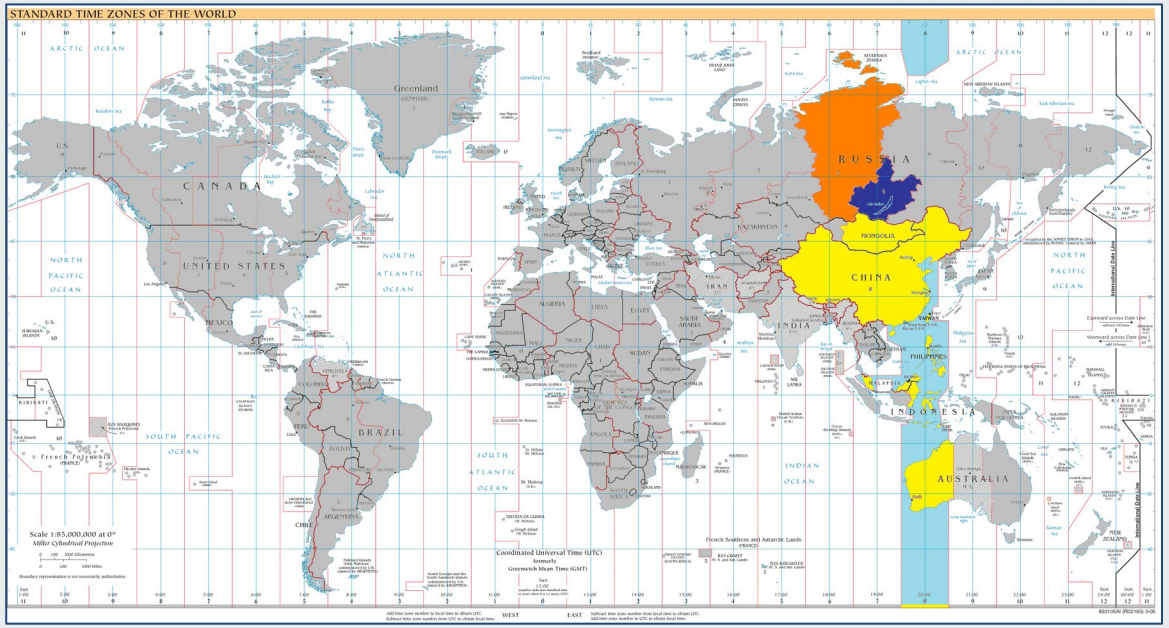
The indictment did not hinder APT41's operations as they progressed into 2021. By the end of the year, 13 victims were impacted globally.

- 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



Source: Wikipedia

2021 Countries and Sectors Impacted

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

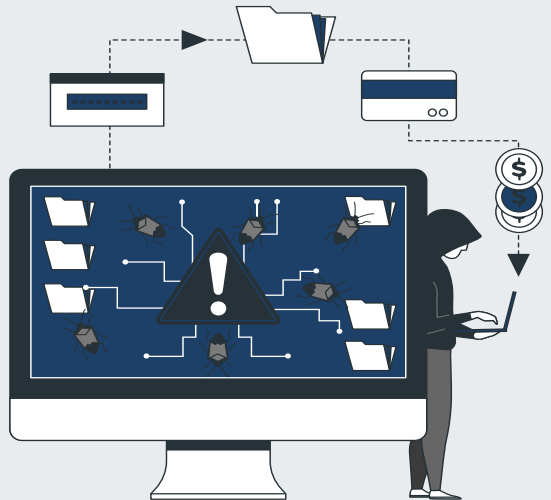
- Attacks on healthcare
  - January -- March 2020
- APT41 was identified as attempting to exploit Citrix, Cisco, and Zoho endpoints as a part of their campaign
- Attempted to exploit over 75 customers
- Several sectors in the United States were targets
- Attempted exploitation of:
  - CVE-2019-19781: 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:

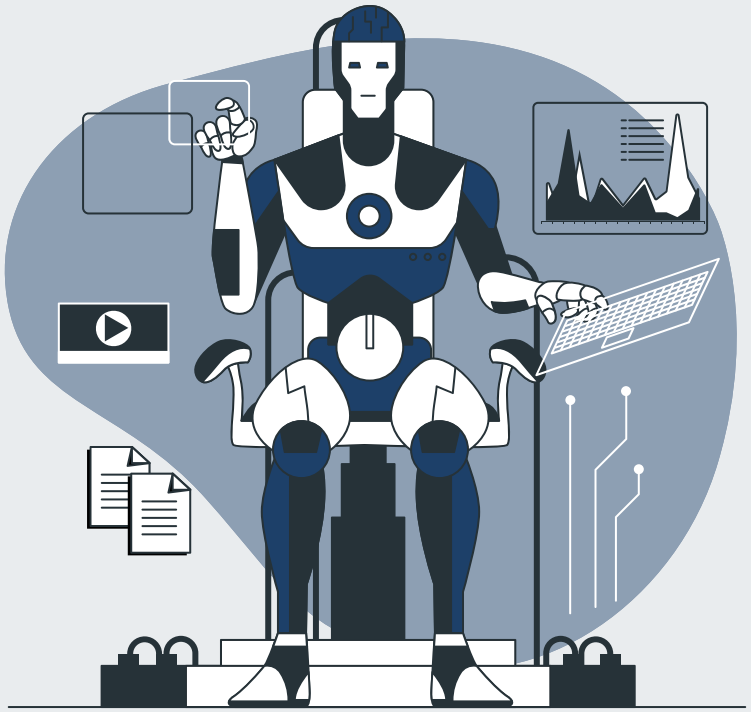
- Cloud computing
- Big data
- Internet of things (IoT)
- Industrial internet
- Blockchain
- Artificial intelligence
- Virtual and augmented reality
- Smart transportation
- Smart energy
- Smart manufacturing
- Smart medicine
- Smart government



The 14th Five-Year Plan

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
7. Deep Sea, Deep Space, and Polar Exploration



Recent Activity

Recent Activity – MoonBounce

- Late 2021
- Unified Extensible Firmware Interface (UEFI) Firmware Implant
  - Most advance 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

Recent Activity – USAHERDS CVEs

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

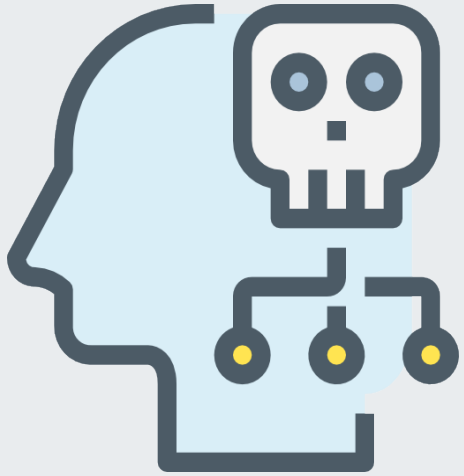
Recent Activity – Government Espionage

- 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

Popular TTPs and Tools

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

Reference Materials

References

- “Seven International Cyber Defendants, Including “Apt41” Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally”. Justice. Sep 16, 2020. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer
- Lakshmanan, Ravie. “China-backed APT41 Hackers Target 13 Organizations Worldwide Last Year”. Thehackernews. Aug 18, 2020. https://thehackernews.com/2022/08/china-backed-apt41-hackers-targeted-13.html
- Kovacs, Eduard. “Chinese Cyberspies Continue Targeting Medical Research Organizations”. Securityweek. Aug 21, 2019. https://www.securityweek.com/chinese-cyberspies-continue-targeting-medical-research-organizations
- Kovacs, Eduard. “U.S. State Governments Targeted by Chinese Hackers via Zero-Day in Agriculture Tool. Securityweek”. Mar 8, 2022. https://www.securityweek.com/us-state-governments-targeted-chinese-hackers-zero-day-agriculture-tool

References

- Kaja, Ashwin. Stein, Sean. Xiang, Ting. “China’s 14th Fiver-Year Plan (2021-2025): Signpost for Doing Business in China”. Covington. Apr 6, 2021. https://www.globalpolicywatch.com/2021/04/chinas-14th-five-year-plan-2021-2025-signposts-for-doing-business-in-china/
- Gyler, Christopher. Perez, Dan. Jones, Sarah. Miller, Steve. “This is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits”. Mandiant. Mar 25, 2020. https://www.mandiant.com/resources/blog/apt41-initiates-global-intrusion-campaign-using-multiple-exploits
- Mascellino, Alessandro, “China-backed APT41 Group Hacked at Least 13 Victimes in 2021”. Infosecurity-magazine. Aug 19, 2022. https://www.infosecurity-magazine.com/news/china-apt41-campaign-13-victims/
- “APT41 Perfects Code Signing Abuse to Escalate Supply Chain Attacks”. Venafi. https://www.venafi.com/sites/default/files/2021-11/Venafi_WhitePaper_CodeSigningAPT41_2021_f_0.pdf

References

- “APT41”. Attack.MITRE. https://attack.mitre.org/groups/G0096/
- HC3. “APT41 Citrix and Zoho Attacks on Healthcare”. HHS. Mar 26, 2020. https://www.hhs.gov/sites/default/files/apt41-citrix-and-zoho-attacks-on-healthcare.pdf
- Kaspersky. “Technical details of MoonBounce Implementation”. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2022/01/19115831/MoonBounce_technical-details_eng.pdf
- Brown, Rufus. Ta, Van. Bienstock, Douglas. Ackerman, Geoff. Wolfram, John. “Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments”. Mandiant. Mar 8, 2022. https://www.mandiant.com/resources/blog/apt41-us-state-governments
- “MoonBounce: the dark side of UEFI firmware”. Kaspersky. Jan 20, 2022. https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/
- Naraine, Ryan. “Prolific Chinese APT Caught Using ‘MoonBounce’ UEFI Firmware Implant”. Securityweek. Jan 20, 2022. https://www.securityweek.com/prolific-chinese-apt-caught-using-moonbounce-uefi-firmware-implant

References

- Vaas, Lisa. “APT41 Spies Broke Into 6 US State Networks via a livestock App”. Threatpost. Mar 9, 2022. https://threatpost.com/apt41-spies-broke-into-6-us-state-networks-via-livestock-app/178838/
- Henriquez, Maria. “A deep dive into China APT41’s breach of six U.S. state governments”. Securitymagazine. Mar 10, 2022. https://www.securitymagazine.com/articles/97236-a-deep-dive-into-china-apt41s-breach-of-six-us-state-governments
- Choudhury, Surendra. “Log4j Vulnerability Explanations in Details”. Infosecwriteup. Dec 21, 2021. https://infosecwriteups.com/log4j-vulnerability-explanation-in-details-73f7556c5ff1
- Photon Research Team. “Q1 2022 Vulnerability Roundup”. Digitalshadows. Apr 14, 2022. https://www.digitalshadows.com/blog-and-research/q1-2022-vulnerability-roundup/
- Greig, Jonathan. “Researchers uncover years-long espionage campaign targeting dozens of global companies”. Therecord. May 5, 2022. https://therecord.media/operation-cuckoobees-apt41-cybereason-winnti-group/
- Arghire, Ionut. “Chinese Cyber-Spies Target US-Based Research University”. Securityweek. Aug 20, 2019. https://www.securityweek.com/chinese-cyber-spies-target-us-based-research-university

References

- Threat Hunter Team. “New Wave of Espionage Activity Targets Asian Governments”. Symantec. Sep 13, 2022. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-asia-governments
- Toulas, Bill. “Winnti hackers split Cobalt Strike into 154 pieces to evade detection”. Bleepingcomputer. Aug 18, 2022. https://www.bleepingcomputer.com/news/security/winnti-hackers-split-cobalt-strike-into-154-pieces-to-evade-detection/
- “APT41, A Dual Espionage And Cyber Crime Operation”. Mandiant. https://www.mandiant.com/resources/report-apt41-double-dragon-a-dual-espionage-and-cyber-crime-operation
- Faife, Corin. “China-backed hackers breached government networks in at least six US States, per new report”. Theverge. Mar 8, 2022. https://www.theverge.com/2022/3/8/22966517/china-hack-government-networks-apt41-usaherd
- 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

Sector and Victim Notifications

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.

Alerts and Analyst Notes

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

Threat Briefings

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.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

HHS.GOV/HC3

HC3@HHS.GOV