

# Threat Hunting

---

## HW01 - Recognize the APT group

---

Name: 劉定睿 ID: M11409313

Date: 2025-10-02

# 目錄

---

- Task 1: Research an APT Group
  - APT41
- Task 2: Apply an OSINT Tool
  - Reference:

# Task 1: Research an APT Group

---

## APT41

---

- APT41 as known as AMOEBA, Winnti, APT41, BARIUM
- sponsor nation: China
- Common TTPs :
  - <https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0096%2FG0096-enterprise-layer.json> (<https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0096%2FG0096-enterprise-layer.json>)
  - Top 10 of TTPs (shout out to ChatGPT 5, prompt : <https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0096%2FG0096-enterprise-layer.json> 排名前十名的 TTPs 請用英文輸出 ) :
    1. **T1190 — Exploit Public-Facing Applications**
    2. **T1078 — Valid Accounts**
    3. **T1071.004 — Application Layer Protocol: DNS**
    4. **T1110 — Brute Force**
    5. **T1105 — Ingress Tool Transfer**
    6. **T1071.001 — Application Layer Protocol: Web Protocols**
    7. **T1574.001 — Hijack Execution Flow: DLL Search Order Hijacking**
    8. **T1036.004 — Masquerading: Masquerade Task or Service**
    9. **T1070.004 — Indicator Removal: File Deletion**
    10. **T1567.002 — Exfiltration Over Web Service: Exfiltration to Cloud Storage**
- Notable APT41 Campaigns / Incidents
  1. **Arisen from the DUST (2023-2024)**

Long-term access in logistics, media, tech, automotive across Europe & Asia. Used *DUSTPAN/DUSTTRAP* droppers, ANTSWORD/BLUEBEAM web shells, exfiltration via OneDrive. Ref: <https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen->

[from-dust](https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust) (<https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust>).

## 2. **US State Governments (2021)**

Exploited USAHERDS & ASP[.]NET apps; later Log4j. Compromised at least 6 U.S. state networks. Ref: <https://www.wired.com/story/china-apt41-hacking-usaherds-log4j> (<https://www.wired.com/story/china-apt41-hacking-usaherds-log4j>).

## 3. **World Tour 2021**

Four campaigns, 13 victims globally, heavy use of Cobalt Strike. Ref: <https://www.group-ib.com/blog/apt41-world-tour-2021/> (<https://www.group-ib.com/blog/apt41-world-tour-2021/>).

## 4. **Earth Longzhi subgroup (2020-2022)**

Sub-team targeting Taiwan, SE Asia, Ukraine. Used custom loaders, phishing, in-memory evasion. Ref: [https://www.trendmicro.com/en\\_in/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html](https://www.trendmicro.com/en_in/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html) ([https://www.trendmicro.com/en\\_in/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html](https://www.trendmicro.com/en_in/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html)).

## 5. **DOJ Indictment (2019-2020)**

Five members charged with hacking 100+ companies worldwide, stealing source code, certificates, customer data. Ref: <https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer> (<https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer>).

- Target sectors or regions : **UK, China, Taiwan, Hong Kong, India, Thailand, Mongolia, Indonesia, Vietnam, Bangladesh, Ireland, Brunei**

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,



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

Thailand, Mongolia, Indonesia, Vietnam, Bangladesh, Ireland, and Brunei. The group's espionage campaigns have targeted healthcare (including pharmaceuticals), 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 these types of activities specifically being leveraged against the U.S. health sector to date.

**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](#).

<https://www.hhs.gov/sites/default/files/china-based-threat-actor-profiles-tlpclear.pdf> (<https://www.hhs.gov/sites/default/files/china-based-threat-actor-profiles-tlpclear.pdf>).

## Task 2: Apply an OSINT Tool

- Look up domains or IPs historically linked to the group :
  - Domains (from <https://www.hhs.gov/sites/default/files/apt41.pdf> (<https://www.hhs.gov/sites/default/files/apt41.pdf>))
    - word[.]msapp[.]workers[.]dev
    - cloud[.]msapp[.]workers[.]dev
    - term-restore-satisfied-hence[.]trycloudflare[.]com
    - ways-sms-pmc-shareholders[.]trycloudflare[.]com
    - resource[.]infinityfreeapp[.]com
    - pubs[.]infinityfreeapp[.]com
  - IPs and relation domain (from <https://www.group-ib.com/blog/apt41-world-tour-2021/> (<https://www.group-ib.com/blog/apt41-world-tour-2021/>))

- 45.142.212[.]47 | socialpt2021[.]club, mute-pond-371d.zalocdn[.]workers.dev
- 185.250.150[.]22 | mute-pond-371d.zalocdn[.]workers.dev
- 45.133.216[.]21
- 45.153.231[.]32
- 185.118.166[.]66 | olunm[.]tk

- virustotal :

resource.infinityfreeapp.com

15 / 95  
Community Score

15/95 security vendors flagged this domain as malicious

resource.infinityfreeapp.com  
infinityfreeapp.com

DETECTION    DETAILS    **RELATIONS**    COMMUNITY 5

[Join our Community](#), and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Passive DNS Replication (7) ⓘ

Date resolved	Detections	Resolver	IP
2025-08-19	0 / 95	VirusTotal	185.27.134.164
2025-08-15	0 / 95	VirusTotal	51.77.231.201
2025-06-06	1 / 95	VirusTotal	185.27.134.19
2025-03-05	1 / 95	VirusTotal	199.59.243.228
2024-10-15	0 / 95	VirusTotal	199.59.243.227
2024-10-06	1 / 95	VirusTotal	199.59.243.226
2024-08-20	1 / 95	VirusTotal	185.27.134.60

- Explore malware samples or indicators of compromise (IOCs) :

**APT41** [\(Back to overview\)](#)

aka: Amoeba, BARIUM, BRONZE ATLAS, BRONZE EXPORT, Blackfly, Brass Typhoon, Double Dragon, Earth Baku, G0044, G0096, Grayfly, HOODOO, LEAD, Leopard Typhoon, Red Kelpie, TA415, TG-2633, WICKED PANDA, WICKED SPIDER, Winnti

APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control.

Associated Families

apk.dragonegg   apk.wyrmspy   elf.messagetap   win.biopass   win.crackshot   win.dboxagent   win.easynight   win.highnoon   win.highnoon\_bin  
 win.jumpall   win.serialvlogger   win.pinegrove   win.acehash   win.crosswalk   win.dusttrap   win.gearshift   win.lowkey   win.moonbounce   win.moonwalk  
 win.skip20   elf.keyplug   win.poisonplug   win.chinachopper   win.blackcoffee   win.derusbi   win.zxshell   win.toughprogress   win.shadowpad  
 win.coldlock   php.aspxspy   win.sharpyshell   win.plugx   win.cobalt\_strike

<https://malpedia.caad.fkie.fraunhofer.de/actor/apt41>

(<https://malpedia.caad.fkie.fraunhofer.de/actor/apt41>)

- Review public datasets or repositories of threat reports :

- <https://services.google.com/fh/files/misc/m-trends-2025-en.pdf>  
(<https://services.google.com/fh/files/misc/m-trends-2025-en.pdf>)

- <https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/>  
(<https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/>).
- Why you selected this tool : I use virustotal to find "relation" information and try to link them together.
- How you applied it :
  1. search the IoC(IP, Domain, hash...) which I found on the public report
  2. use `details` to find the malware hash
  3. use `relation` function to find relation IP / Domain name
  4. use `community` to find the report that upload by others researcher.
- What results (if any) you obtained :
  1. Relation IPs / Domain name (suspective C2 or families)
  2. Relation malware filename or software or Application
  3. Relation malware hash
- Reflections on the usefulness and limitations of OSINT in this context :
  1. The information can be wrong(because everyone can upload their research on it.). Need more intelligence to cross-validation their authenticity.
  2. The information is not attribute only one hacker group. Maybe can be more relation to others hacker group or cyber criminal
  3. Must be suspect to everthings that didn't been validation. The intelligence can be polluted.

## Reference:

---

- ChatGPT : help me to summarize information of APT41's TTPs and campaigns / incidents
- <https://www.hhs.gov/sites/default/files/apt41.pdf>  
(<https://www.hhs.gov/sites/default/files/apt41.pdf>).
- <https://cloud.google.com/security/resources/insights/apt-groups>  
(<https://cloud.google.com/security/resources/insights/apt-groups>).
- <https://malpedia.caad.fkie.fraunhofer.de/actor/apt41>  
(<https://malpedia.caad.fkie.fraunhofer.de/actor/apt41>).

- <https://www.hhs.gov/sites/default/files/china-based-threat-actor-profiles-tlpclear.pdf> (<https://www.hhs.gov/sites/default/files/china-based-threat-actor-profiles-tlpclear.pdf>).
- <https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/> (<https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/>).