



## **Brief**

# **Primer on China's APT41**

**B-2023-11-17b**

**Classification: TLP:CLEAR**

**Criticality: Medium**

**Intelligence Requirements: Military, Government, Geopolitical, Threat Actor Targeting**

**November 17, 2023**

## Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 6:00 PM (EST) on November 16, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# **Brief | Primer on China's APT41**

## **Executive Summary**

APT41 is among the first advanced persistent threat (APT) groups the Chinese government utilized to conduct malicious cyber activities, targeting nations and sectors of strategic relevance to China; however, the group is one of the very few APTs that also conduct cybercrime. China leverages a number of highly competent APT groups in pursuit of its strategic objectives, such as regional and global leadership in economic and security issues, control over claimed territory, and domestic regime stability. APT41, like other Chinese APT groups, continues to evolve its tactics, techniques, and procedures (TTPs) in an attempt to maintain proficiency while obfuscating its involvement in attacks. The group tends to focus on specific sectors and nations in accordance with China's strategic requirements and likely at the direction of the Chinese intelligence service, the Ministry of State Security (MSS).

## **Background**

APT41 (aka Double Dragon, BARIUM, LEAD, Winnti, Winnti Umbrella, WICKED SPIDER, WICKED PANDA, Blackfly, Grayfly, Suckfly, BRONZE ATLAS, BRONZE EXPORT, Brass Typhoon, Red Kelpie, Amoeba, and HOODOO) is a China-based threat group targeting a wide range of government and private sector entities across the globe. While APT41 likely originated in 2006, differing sources attribute the group's illicit activities in espionage and commercial cybercrime as beginning anywhere from 2006 to 2014.<sup>1</sup> APT41 is widely assessed to have

---

<sup>1</sup> [hXXps://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)

deep ties to the MSS.<sup>2</sup> The group was identifiable due to its proprietary, modular malware kit ShadowPad,<sup>3</sup> which has been in use in some form for much of APT41's operational lifespan.

APT41's modus operandi is two-pronged: 1) to conduct state-sponsored cyber espionage campaigns against foreign government and business entities, as well as internal Chinese political dissidents (i.e., pro-democracy, Hong Kong activists), on behalf of the People's Republic of China (PRC)<sup>4</sup> and 2) to compromise various private sector entities for its own personal financial gain, possibly outside of PRC authority.<sup>5</sup> In blurring the lines between state-sponsored cyber espionage and commercial cybercrime operations, the group has earned the moniker "Double Dragon."<sup>6</sup>

Congruent with other PRC-sponsored espionage groups, APT41 targets verticals that could help the PRC accomplish its current Five-Year economic plan, which potentially includes intellectual property theft from the global healthcare, pharmaceutical, high-tech, software, and telecommunications sectors. This is in addition to its targeting of the media, retail, finance, hospitality, academic, and entertainment spaces.<sup>7</sup> From 2019 to 2020, APT41 allegedly compromised over 100 public and private organizations and individuals in these sectors in the United States, Taiwan, Singapore, Japan, South Korea, India, and Australia.<sup>8</sup> Additionally, from May 2021 to February 2022, APT41 successfully compromised the networks of at least six U.S. state governments via the exploitation of vulnerable internet-facing web applications—most notably the livestock app USAHERDS.<sup>9</sup> APT41 has historically also targeted such entities in the United Kingdom, Mongolia, Indonesia, Vietnam, Bangladesh, Brunei, Ireland, France, Myanmar, the Netherlands, Switzerland, Italy, South Africa, and Turkey.<sup>10</sup>

---

<sup>2</sup>

<sup>2</sup> [hXXps://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)

<sup>3</sup> [hXXps://www.cyfirma\[.\]com/outofband/the-origins-of-apt-41-and-shadowpad-lineage/](https://www.cyfirma[.]com/outofband/the-origins-of-apt-41-and-shadowpad-lineage/)

<sup>4</sup> [hXXps://www.cfr\[.\]org/cyber-operations/apt-41](https://www.cfr[.]org/cyber-operations/apt-41)

<sup>5</sup> [hXXps://socradar\[.\]io/5-facts-you-should-know-about-apt41-double-dragon/](https://socradar[.]io/5-facts-you-should-know-about-apt41-double-dragon/)

<sup>6</sup> *Ibid.*

<sup>7</sup> [hXXps://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)

<sup>8</sup> [hXXps://www.lookout\[.\]com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41](https://www.lookout[.]com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41)

<sup>9</sup> [hXXps://vulners\[.\]com/thn/THN:C73B84809CDC20C90C26FF1B7F56F5D4](https://vulners[.]com/thn/THN:C73B84809CDC20C90C26FF1B7F56F5D4)

<sup>10</sup> [hXXps://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)

Unlike most other PRC-sponsored threat actors, APT41 also pursues personal financial gain for its members through commercial cybercriminal activities. To this end, APT41 has largely targeted the video game industry and focuses on manipulating digital currency. The TTPs APT41 built to target the video game industry were supposedly used in later supply chain attacks in the software development sector.<sup>11</sup>

Five members of APT41—several with leadership positions with Chinese company Chengdu 404 Network Technology—were indicted by the U.S. Department of Justice in 2020. Charges against the members included money laundering, wire fraud, aggravated identity theft, racketeering, and unauthorized access to protected computers.<sup>12</sup> In spite of the highly publicized charges, the APT41 members are believed to continue operating in China with impunity.



### **U.S. Department of Justice Announcing Indictments of Five APT41 Members in 2020**

*Source: DOJ*

A recently identified subgroup of APT41, Earth Longzhi, reportedly emerged in 2020 and has since launched two major campaigns targeting multiple sectors across several Asian countries. The first campaign, from May 2020 to February 2021, targeted the banking industry in China as well as the government, infrastructure, academic, and

<sup>11</sup> <https://socradar.io/5-facts-you-should-know-about-apt41-double-dragon/>

<sup>12</sup> <https://www.fbi.gov/wanted/cyber/apt-41-group>

healthcare sectors in Taiwan. The second, from August 2021 to June 2022, targeted prominent assets in the defense, aviation, insurance, and urban development sectors in China, Taiwan, Thailand, Malaysia, Indonesia, Pakistan, and Ukraine. Both campaigns' primary attack vector was malware distribution via spear phishing or exploiting exposed public applications. The group also utilized custom hacking tools and Cobalt Strike loaders throughout both campaigns, in addition to publicly-available malware. Additional suspected subgroups of APT41 with similar TTPs and regional interests include Earth Baku and GroupCC.<sup>13</sup>

## **| Recent Activities and TTPs**

APT41 has a long history of conducting cyber espionage against targets pertinent to the Chinese MSS. The group has demonstrated proficiency with the general TTPs of Initial Access, Establish Foothold, Escalate Privileges, Internal Reconnaissance, Lateral Movement, Maintain Presence, and Mission Completion. The following are key APT41 activities along with noteworthy TTPs used in its attacks that occurred within the past year:

- In October 2022, Google identified a campaign whereby APT41 weaponized the open-source red teaming tool Google Command and Control (GC2) to target victims, including an Italian and a Taiwanese organization.<sup>14</sup> APT41 first used the "Living off the Island Tactic,"<sup>15</sup> which leverages legitimate tools such as Cobalt Strike and penetration testing software that can be obtained from public sources such as GitHub. The group conducted a spear-phishing campaign to trick targets into downloading a maliciously-coded file. For example, a Taiwanese media organization was targeted with phishing emails containing links to a password-protected file hosted on Google Drive. The payload then utilized GC2 to run commands to exfiltrate sensitive data discreetly. GC2 allows the attacker to

---

<sup>13</sup>

[hXXps://www.trendmicro\[.\]com/en\\_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html](https://www.trendmicro.com/en_us/research/22/k/hack-the-real-box-apt41-new-subgroup-earth-longzhi.html)

<sup>14</sup>

[hXXps://www.bleepingcomputer\[.\]com/news/security/hackers-abuse-google-command-and-control-red-team-tool-in-attacks/](https://www.bleepingcomputer.com/news/security/hackers-abuse-google-command-and-control-red-team-tool-in-attacks/)

<sup>15</sup> [hXXps://www.linkedin\[.\]com/pulse/from-friend-foe-how-apt41-weaponized-googles-red-teaming-tool/](https://www.linkedin.com/pulse/from-friend-foe-how-apt41-weaponized-googles-red-teaming-tool/)

download more files from Google Drive onto the victim's machine in addition to exfiltration via Google Drive.

- In April 2023, two advanced Android spyware tools called Wyrmspy and DragonEgg were linked back to APT41.<sup>16</sup> Upon investigation of each spyware, it was determined the two are related via hard-coded certificates and common infrastructure. Both tools appear to have sophisticated data collection and exfiltration capabilities, but these functions are hidden in additional modules that must be downloaded after installation. Wyrmspy primarily disguises itself as a default operating system app, whereas DragonEgg masquerades as a third-party keyboard or messaging app. The spyware enables collection of log files, photos, SMS traffic, device location, audio recording, contacts, and external storage files on an infected device.
- In July 2023, another advanced mobile spyware was linked to APT41.<sup>17</sup> Unlike DragonEgg and Wyrmspy, this spyware implant—dubbed LightSpy—was targeted against iOS users. LightSpy mirrored DragonEgg in many ways; however, LightSpy was discovered to have 14 different plugins that were not identified in the Android spyware. This included a plugin that enables private data exfiltration in addition to a number of other plugins that mirror the collection capabilities of the Android spyware.

## **| Analyst Commentary**

Chinese APT groups appear to maintain a steady operational pace. However, like other adversarial nation-state APT groups, Chinese APT groups do operate in concert with their sponsor's national priorities and requirements. As such, Chinese APT groups can be expected to mirror China's national priorities in operational tempo and targeting guidance. For example, in the event of hostilities in Taiwan, APT41 could be expected to conduct attacks against infrastructure in line with preparations and reconnaissance the group has already conducted against Taiwanese infrastructure.

---

<sup>16</sup> <https://www.lookout.com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41>

<sup>17</sup> <https://www.threatfabric.com/blogs/lightspy-mapt-mobile-payment-system-attack>

Chinese APT groups, including APT41, have recently adapted to TTPs that are more likely to obscure their role in any attack they have carried out. This includes adopting some of the aforementioned TTPs, such as leveraging open-source/widely-available tools to gain network access, maintain persistent access, and exfiltrate targeted data without needing to use tools that are identifiable with Chinese cyber activity.

## **Recommendations**

Chinese APT groups, including APT41, leverage many of the same open-source tools and techniques as do other APT groups. Phishing and other attacks against internet-facing devices are the group's preferred methods for gaining initial access and exploiting a target network for long-term, low-visibility collection and malicious activity.

- Implement next-generation email security and filtering.
- Patch vulnerabilities on public, internet-facing assets.
- Conduct social engineering awareness and training for relevant stakeholders.
- Assess software supply chain risks, especially with the use of third-party and open-source software.
- Implement next-generation firewalls and configure strong policies to block known malicious or suspicious domains.

Along with the threat posed by APT41 and its cohorts in the Chinese cyber domain, there are opportunities to gain insight into China's national requirements. Monitoring Chinese APT activity and conducting analysis in concert with key events will provide insight into the status of China's strategic efforts. In turn, this data can be extrapolated out to identify sectors that China might be targeting more aggressively or adversary military organizations that might be at higher risk of near-term action by the Chinese state and its assets—via cyber activities or other instruments of national power.

## | Appendix A: Indicators of Compromise (IOCs)

### IOCs: Wyrmspy

#### SHA1

- 92ddbe438c8c8c1ef82fa5bb02e526db10829736
- 0b4a9a3f167178054ef9f9a97463cbe31f078c2f
- d713b8b0f3764157cc18d5dc1cb0f9c558067728
- 589d88093dad377d46f34415a7f9df11d65b81ed
- ab560af6baff8f58ea5bc53c0391501415aed14
- 5891fa6a3a8232192ebd57a171bad29f53c7598c
- 4405af38c4a6b6130fcf242a11b0ce7963albe28
- 5c16637848d6f1eb4aa6c5b2a4928a1144cd2113
- 2fbd56b1f3859c6d03dec47f8fcee7e37dc303a1
- 085191fb59d3933f8447610126600754b35697d4

#### Infrastructure

- 116.205.4[.]18
- dns.win10micros0ft[.]com
- www.andropwn[.]xyz
- 121.42.149[.]52
- Update.umisen[.]com

### IOCs: DragonEgg

#### SHA1

- b456a61a3e0ac6073a716b06293a3295a261de56
- 209567f4f28c5c8abcbe56d789e558aa64239534
- b456a61a3e0ac6073a716b06293a3295a261de56
- cab70e99516a36ab0f0d3851375adf0740f4bd5e
- 81762cfae0bd5585e8c0c86e4fdbbe47d2dd614a
- fbda76a2c2834f89d642a72c24b1988a1f56e4b8

**Infrastructure**

- 118.193.39[.]165
- 121.201.109[.]98
- alxc.tbtiyan[.]com
- yxwasec[.]com
- smiss.imwork[.]net
- huaxin-bantian.duckdns[.]org
- 103.43.17[.]99

**IOCs: LightSpy****Infrastructure**

- spaceskd[.]com
- 103.27.108[.]207
- 46.17.43[.]74

**SHA256**

- 407abddf78d0b802dd0b8e733aee3eb2a51f7ae116ae9428d554313f12108a4c
- Bd6ec04d41a5da66d23533e586c939eece483e9b105bd378053e6073df50ba99

## | Appendix B: Traffic Light Protocol for Information Dissemination

|                                |                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | <b>Red</b>                                                                                                                                                                                             | <b>Amber</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:RED</b> when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                                | <b>Green</b>                                                                                                                                                                                           | <b>Clear</b>                                                                                                                                                                                                                                                                                                                 |
| <b>WHEN SHOULD IT BE USED?</b> | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| <b>HOW MAY IT BE SHARED?</b>   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> information without restriction, subject to copyright controls.                                                                                                                                                                                                              |

## | Appendix C: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

| Almost No Chance | Very Unlikely | Unlikely | Roughly Even Chance | Likely | Very Likely | Almost Certain |
|------------------|---------------|----------|---------------------|--------|-------------|----------------|
| 1-5%             | 5-20%         | 20-45%   | 45-55%              | 55-80% | 80-95%      | 95-99%         |