APT40 | Examining a China-Nexus Espionage Actor | Mandiant

By Mandiant

Published: 2019-03-04 · Archived: 2026-04-05 15:12:36 UTC

Written by: Fred Plan, Nalani Fraser, Jacqueline O'Leary, Vincent Cannon, Ben Read

---

FireEye is highlighting a cyber espionage operation targeting crucial technologies and traditional intelligence targets from a China-nexus state sponsored actor we call APT40. The actor has conducted operations since at least 2013 in support of China's naval modernization effort. The group has specifically targeted engineering, transportation, and the defense industry, especially where these sectors overlap with maritime technologies. More recently, we have also observed specific targeting of countries strategically important to the Belt and Road Initiative including Cambodia, Belgium, Germany, Hong Kong, Philippines, Malaysia, Norway, Saudi Arabia, Switzerland, the United States, and the United Kingdom. This China-nexus cyber espionage group was previously reported as TEMP.Periscope and TEMP.Jumper.

Mission

In December 2016, China's People Liberation Army Navy (PLAN) seized a U.S. Navy unmanned underwater vehicle (UUV) operating in the South China Sea. The incident paralleled China's actions in cyberspace; within a year APT40 was observed masquerading as a UUV manufacturer, and targeting universities engaged in naval research. That incident was one of many carried out to acquire advanced technology to support the development of Chinese naval capabilities. We believe APT40's emphasis on maritime issues and naval technology ultimately support China's ambition to establish a blue-water navy.

In addition to its maritime focus, APT40 engages in broader regional targeting against traditional intelligence targets, especially organizations with operations in Southeast Asia or involved in South China Sea disputes. Most recently, this has included victims with connections to elections in Southeast Asia, which is likely driven by events affecting China's Belt and Road Initiative. China's "One Belt, One Road" (一带一路) or "Belt and Road Initiative" (BRI) is a $1 trillion USD endeavor to build land and maritime trade routes across Asia, Europe, the Middle East, and Africa to develop a trade network that will project China's influence across the greater region.

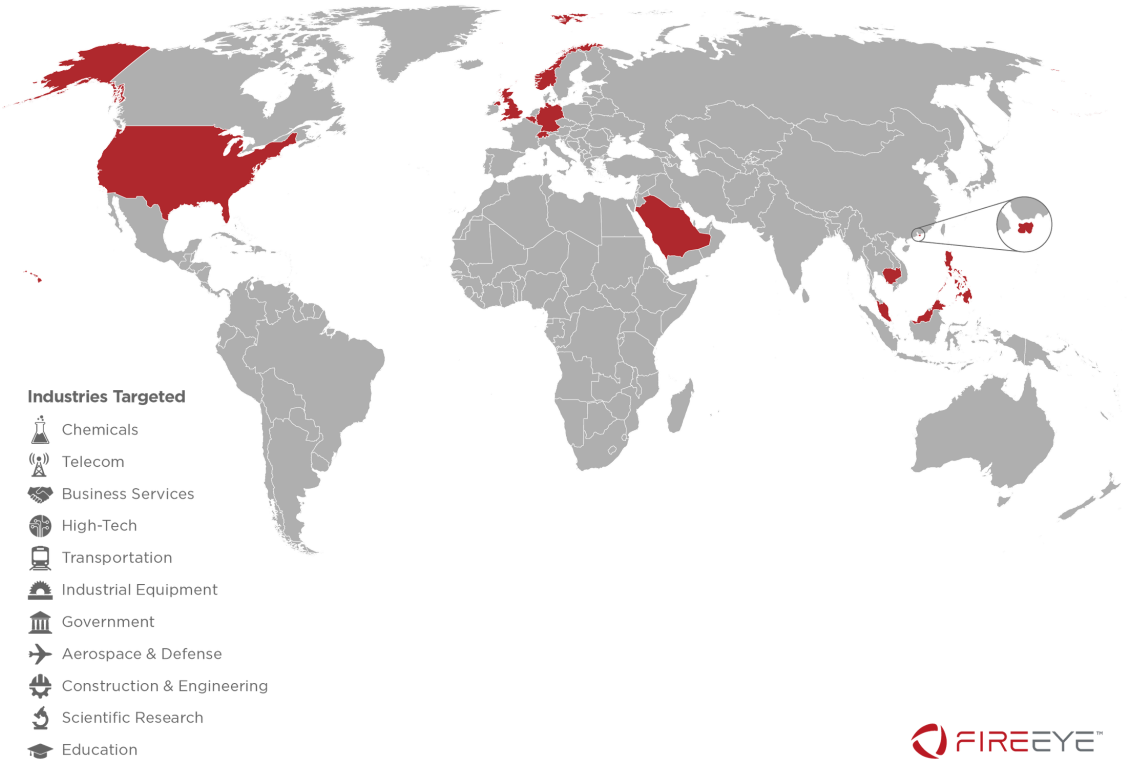

Figure 1: Countries and industries targeted. Countries include the United States, United Kingdom, Norway, Germany, Saudi Arabia, Cambodia and Indonesia

Attribution

We assess with moderate confidence that APT40 is a state-sponsored Chinese cyber espionage operation. The actor's targeting is consistent with Chinese state interests and there are multiple technical artifacts indicating the actor is based in China. Analysis of the operational times of the group's activities indicates that it is probably centered around China Standard Time (UTC +8). In addition, multiple APT40 command and control (C2) domains were initially registered by China based domain resellers and had Whois records with Chinese location information, suggesting a China based infrastructure procurement process.

APT40 has also used multiple Internet Protocol (IP) addresses located in China to conduct its operations. In one instance, a log file recovered from an open indexed server revealed that an IP address (112.66.188.28) located in Hainan, China had been used to administer the command and control node that was communicating with malware on victim machines. All of the logins to this C2 were from computers configured with Chinese language settings.

Attack Lifecycle

Initial Compromise

APT40 has been observed leveraging a variety of techniques for initial compromise, including web server exploitation, phishing campaigns delivering publicly available and custom backdoors, and strategic web compromises.

- APT40 relies heavily on web shells for an initial foothold into an organization. Depending on placement, a web shell can provide continued access to victims' environments, re-infect victim systems, and facilitate lateral movement.
- The operation's spear-phishing emails typically leverage malicious attachments, although Google Drive links have also been observed.
- APT40 leverages exploits in their phishing operations, often weaponizing vulnerabilities within days of their disclosure. Observed vulnerabilities include:
    - CVE-2012-0158
    - CVE-2017-0199
    - CVE-2017-8759
    - CVE-2017-11882

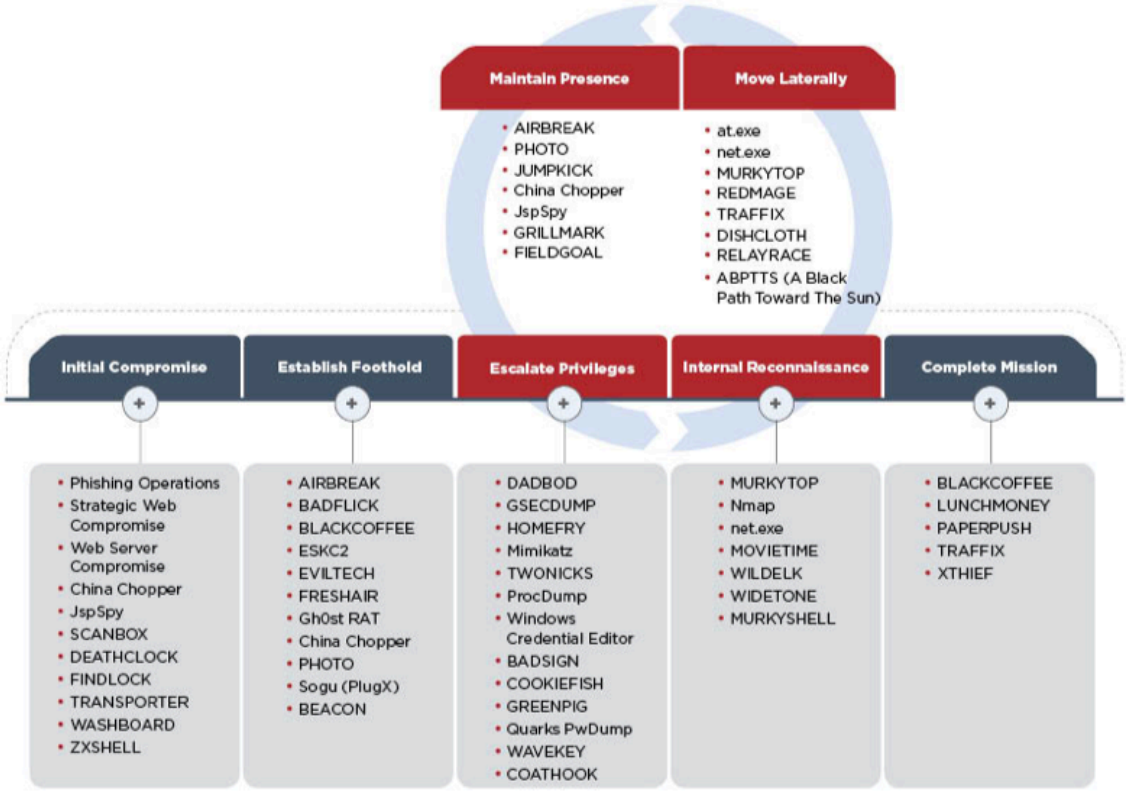

Figure 2: APT40 attack lifecycle

Establish Foothold

APT40 uses a variety of malware and tools to establish a foothold, many of which are either publicly available or used by other threat groups. In some cases, the group has used executables with code signing certificates to avoid detection.

- First-stage backdoors such as AIRBREAK, FRESHAIR, and BEACON are used before downloading other payloads.
- PHOTO, BADFLICK, and CHINA CHOPPER are among the most frequently observed backdoors used by APT40.

- APT40 will often target VPN and remote desktop credentials to establish a foothold in a targeted environment. This methodology proves to be ideal as once these credentials are obtained, they may not need to rely as heavily on malware to continue the mission.

Escalate Privileges

APT40 uses a mix of custom and publicly available credential harvesting tools to escalate privileges and dump password hashes.

- APT40 leverages custom credential theft utilities such as HOMEFRY, a password dumper/cracker used alongside the AIRBREAK and BADFLICK backdoors.
- Additionally, the Windows Sysinternals ProcDump utility and Windows Credential Editor (WCE) are believed to be used during intrusions as well.

Internal Reconnaissance

APT40 uses compromised credentials to log on to other connected systems and conduct reconnaissance. The group also leverages RDP, SSH, legitimate software within the victim environment, an array of native Windows capabilities, publicly available tools, as well as custom scripts to facilitate internal reconnaissance.

- APT40 used MURKYSHELL at a compromised victim organization to port scan IP addresses and conduct network enumeration.
- APT40 frequently uses native Windows commands, such as net.exe, to conduct internal reconnaissance of a victim's environment.
- Web shells are heavily relied on for nearly all stages of the attack lifecycle. Internal web servers are often not configured with the same security controls as public-facing counterparts, making them more vulnerable to exploitation by APT40 and similarly sophisticated groups.

Lateral Movement

APT40 uses many methods for lateral movement throughout an environment, including custom scripts, web shells, a variety of tunnelers, as well as Remote Desktop Protocol (RDP). For each new system compromised, the group usually executes malware, performs additional reconnaissance, and steals data.

- APT40 also uses native Windows utilities such as at.exe (a task scheduler) and net.exe (a network resources management tool) for lateral movement.
- Publicly available tunneling tools are leveraged alongside distinct malware unique to the operation.
- Although MURKYTOP is primarily a command-line reconnaissance tool, it can also be used for lateral movement.
- APT40 also uses publicly available brute-forcing tools and a custom utility called DISHCLOTH to attack different protocols and services.

Maintain Presence

APT40 primarily uses backdoors, including web shells, to maintain presence within a victim environment. These tools enable continued control of key systems in the targeted network.

- APT40 strongly favors web shells for maintaining presence, especially publicly available tools.
- Tools used during the Establish Foothold phase also continue to be used in the Maintain Presence phase; this includes AIRBREAK and PHOTO.
- Some APT40 malware tools can evade typical network detectiona by leveraging legitimate websites, such as GitHub, Google, and Pastebin for initial C2 communications.
- Common TCP ports 80 and 443 are used to blend in with routine network traffic.

Complete Mission

Completing missions typically involves gathering and transferring information out of the target network, which may involve moving files through multiple systems before reaching the destination. APT40 has been observed consolidating files acquired from victim networks and using the archival tool rar.exe to compress and encrypt the data before exfiltration. We have also observed APT40 develop tools such as PAPERPUSH to aid in the effectiveness of their data targeting and theft.

Outlook and Implications

Despite increased public attention, APT40 continues to conduct cyber espionage operations following a regular tempo, and we anticipate their operations will continue through at least the near and medium term. Based on APT40's broadening into election-related targets in 2017, we assess with moderate confidence that the group's future targeting will affect additional sectors beyond maritime, driven by events such as China's Belt and Road Initiative. In particular, as individual Belt and Road projects unfold, we are likely to see continued activity by APT40 which extends against the project's regional opponents.

Posted in

- Threat Intelligence
- Security & Identity
