MITRE-ID: G0065

Name: Lviathan

Country: China

Description:

Leviathan is a Chinese state-sponsored cyber espionage group that has been attributed to the Ministry of State Security's (MSS) Hainan State Security Department and an affiliated front company. Active since at least 2009, Leviathan has targeted the following sectors: academia, aerospace/aviation, biomedical, defense industrial base, government, healthcare, manufacturing, maritime, and transportation across the US, Canada, Europe, the Middle East, and Southeast Asia.

TTPs:

1. Gathered victim identity information by collecting compromised credentials.
2. Acquire infrastructure to establish domains that impersonate legitimate entities, aka ‘typosquatting’, to use in watering hole attacks and as command and control (C2) infrastructure
3. Establish new and compromise existing email and social media accounts to conduct social engineering attacks
4. Initialize access through following channel:
   1. external remote services (e.g., virtual private network [VPN] services)
   2. Spearphishing emails with malicious attachments and links
   3. Drive-by compromises and exploitation of public-facing applications
   4. Access to valid, compromised administrative accounts
5. Command and scripting interpreters such as PowerShell
6. Exploitation of software vulnerabilities in client applications to execute code using lure documents that dropped malware exploiting various Common Vulnerabilities and Exposures (CVEs)
7. User execution of malicious files and links attached to spearphishing emails
8. APT40 has used a combination of tool frameworks and malware to establish persistence, escalate privileges, map, and move laterally on victim networks. Additionally, APT40 conducted internal spearphishing attacks

1. Use of steganography to hide stolen data inside other files stored on GitHub
2. Protocol impersonation by using Application Programming Interface (API) keys for Dropbox accounts in commands to upload stolen data to make it appear that the activity was a legitimate use of the Dropbox service
3. Protocol tunneling and multi-hop proxies, including the use of Tor
4. Use of domain typosquatting for C2 infrastructure
5. Archive, encrypt, and stage collected data locally and remotely for exfiltration