APT17

Overview

APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same.

Tactics

APT19's tactics focus on attacking law and investment firms around the world through phishing. Their tactics include gaining initial access through phishing emails with malicious attachments, exploiting vulnerabilities to execute code, and using sophisticated obfuscation techniques to circumvent detection. They maintain persistence and launch further attacks by exploiting known vulnerabilities and bypassing whitelisting mechanisms.

Techniques

APT19 uses phishing emails (T1566.001) with attached RTF files that utilize CVE-2017-0199 and macro-enabled Excel files (T1203) to deliver malicious payloads such as Cobalt Strike.They also use PowerShell (T1059.001) to execute coded commands that utilize application whitelisting bypassing technique (T1211). The malicious load establishes communication with the Command and Control (C2) server via HTTP requests (T1071.001).

1. **Techniques Used:** Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter, PowerShell, Create or Modify System Process: Windows Service, Data Encoding: Standard Encoding, Deobfuscate/Decode Files or Information, Drive-by Compromise, Hide Artifacts: Hidden Window, Hijack Execution Flow: DLL Side-Loading, Modify Registry, Obfuscated Files or Information: Command Obfuscation, Obfuscated Files or Information: Encrypted/Encoded File, Obtain Capabilities: Tool, Phishing: Spearphishing Attachment, System Binary Proxy Execution: Regsvr32, System Binary Proxy Execution: Rundll32, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, User Execution: Malicious File
2. **Software used:** Cobalt Strike, Empire

Procedures

APT19 first sends phishing emails from the cloudsend[.] net domains with phishing emails that contain RTF documents that exploit the CVE-2017-0199 vulnerability or

XLSM files that ask users to enable macros. Once macros are enabled, the document executes PowerShell commands to decode and download the Cobalt Strike BEACON load. The load communicates with the C2 server via a GET request with minimal HTTP headers. The commands use ZLIB and Base64 encoding to obfuscate network traffic.APT19 also utilizes Casey Smith's “Squiblydoo” technique to bypass application whitelisting, execute additional commands, and launch the SCT file to load additional malicious code for long-term access control.