Chinese APT: A Master of Exploiting Edge Devices

Published: 2024-08-28 · Archived: 2026-04-05 16:30:41 UTC

China-nexus actors have compromised edge devices such as firewall, VPN, IoT devices, etc. against Taiwan Government since 2020 during COVID19, and have compromised those devices to build Botnet, spread disinformation, and exfiltrate sensitive data. However, edge devices belong to closed embedded platforms, and installing antivirus/EDR on those platforms and extracting malware are difficult. Moreover, some models have already reached end-of-life, so no patches are available. Worst of all, Chinese APT has owned the capabilities to find and exploit 0-day on edge devices such as Sophos Firewall, Array SSL VPN, and Barracuda Email Security Gatwall, etc. Consequently, the presentation will reveal a 0-day surveillance router exploited in the wild by Chinese APT groups and will share multiple case studies of edge devices abused by Chinese threat actors such as spread disinformation, Botnet implanted, data exfiltration, and compromised C2. In addition, we also disclose the special and new malware family implanted in edge devices, such as port-knocking backdoors and living-of-the-land binary(LoLbin) attacks in edge devices. Lastly, this presentation also provides related approaches to mitigate attacks of edge devices. By: Greg Chen | CTI Researcher, TeamT5 Charles Li | Chief Analyst, TeamT5 Che Chang | Senior Cyber Threat Analyst, TeamT5 Full Abstract & Presentation Materials: https://www.blackhat.com/asia-24/brie...
