Cyber-Intelligence Report

This cyber-intelligence product is a snapshot of selected cyber events. Collection of information is in accordance with clients' guidelines. It contains 'observations', meaning headlines and links to online information. It *MAY* contain comments and analysis. It is copyright ©David Swan 2024. This report is **TLP:CLEAR**[1] and MAY be shared freely.

If this report does not meet your requirements, is in error or if you need additional information, contact David Swan at DSC.Ops.Vulcan@gmail.com

Cyber Intelligence: Special Edition: People's Republic of China

This report contains selected cyber-security information from 15th to 27th November 2024.

Synopsis

1. It's time to focus on the PRC's hacking efforts. We start with two ongoing, major PRC hacking campaigns, 'Volt Typhoon' and 'Salt Typhoon', both telecommunications hacks. This is followed by four newly discovered cyber campaigns: exploiting a Fortinet VPN vulnerability, another telecommunications hack, an attack on Linux servers, and the shut-down of 1,000 fake news sites.

2. It is our *assessment* that the three major cyber conflicts, (Russia vs Ukraine, Iran vs Israel, and the People's Republic of China) are the most likely sources for the creation of next generation malware and/or the source of cyber attacks. This includes government funded hackers (military, intelligence and civilian employees), affiliated hackers (criminals and mercenaries), and volunteer 'supporters'.

Analyst's Comments

3. The most common theme in my email preamble to these reports is: 'The People's Republic of China hackers have been busy too, but I have run out of time and space to report them.' Most aggressor nations (IE. Russia and Iran) and criminal hackers launch Distributed Denial of Service and ransomware attacks. Since the PRC rarely poses the same type of immediate threat, we make editorial decisions to prioritize direct attacks. It is time to address the ongoing cyber threat posed by the People's Republic of China, excluding her criminal and volunteer hackers.

4. Everything in this report was either reported in the previous two weeks or is being tracked as a major ongoing cyber campaign.

'Volt Typhoon'

5. In May 2023 "*Microsoft and intelligence agencies from the Five Eyes nations disclosed that Volt Typhoon had accessed networks belonging to US critical infrastructure organizations as far back as 2021.*" First detected in a U.S. base on

1 Definition **TLP:CLEAR.** From U.S. Govt Cyber Defense Agency. Traffic Light Protocol (TLP) Definitions and Usage, Recipients may share this information without restriction. Information is subject to standard copyright rules.

© David Swan Consulting 2024

Cyber-Intelligence Report

Guam, security researchers used the 'indications of compromise' discovered in Guam to check connected networks. U.S. bases globally were discovered to be compromised. Security researchers followed clues for months, discovering a vast network of compromised devices, not just on U.S. military bases, but globally. Volt Typhoon "*burrowed deep into thousands of organizations spanning communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and the education sectors.*" One component of Volt Typhoon is "*The botnet, which is packed with outdated Cisco, Netgear and Fortinet devices ... and set up a Tor-like covert data transfer network to perform malicious operations. ... the collection of hijacked routers (called KV-botnet based on artifacts in the malware), features a complex infection process and a well concealed command-and-control network*"[2]

6. **The Threat.** "*[We] have confirmed that Volt Typhoon has compromised the IT environments of multiple critical infrastructure organizations in the continental and non-continental United States and its territories, including Guam," CISA said in an advisory, warning that* ***the hacking team's choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations.*** *... the US government believes the Chinese hackers are "pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions," also noting that U.S. agencies have recently observed "indications of Volt Typhoon actors maintaining access and footholds within some victim IT environments for at least five years. ... [We] are concerned about the potential for these actors to use their network access for disruptive effects in the event of potential geopolitical tensions and/or military conflicts."*[3]

7. **The Take-Down.** In January 2024, the White House authorized the FBI to take down the 'Volt Typhoon' botnet. "*An FBI team infiltrated the operation and harvested crucial data before remotely wiping the KV Botnet, according to four warrants ... filed by the FBI in a southern Texas court. ... Volt Typhoon malware enabled China to hide as they targeted our communications, energy, transportation, and water sectors. The Feds claim the Middle Kingdom's cyber-spies downloaded a virtual private network module to the vulnerable routers and set up an encrypted communication channel to remotely control the botnet, and potentially order the devices to carry out attacks as well as hide their activities. Specifically: Volt Typhoon used the US-based routers and IP addresses to target US critical infrastructure. ... The warrants allowed law enforcement to remotely install software on the routers to search for, and then seize or copy, information about the illicit activity before wiping the malware from the compromised devices.*"[4]

8. **But Wait ... There's More.** Cynthia Kaiser, deputy assistant director for the FBI's cybersecurity division said to journalists: "*even more concerning is that Volt Typhoon is certainly not the only Chinese group conducting this type of activity," Kaiser noted. She declined to identify the other Beijing-backed gangs that have been found*

2 Source: Security Week. Chinese APT Volt Typhoon Linked to Unkillable SOHO Router Botnet
3 Source: Security Week. US Says China's Volt Typhoon Hackers 'Pre-Positioning' for Cyberattacks Against Critical Infrastructure
4 Source: The Register. FBI confirms it issued remote kill command to blow out Volt Typhoon's botnet

© David Swan Consulting 2024

burrowing into US critical infrastructure. ... The US Department of Energy's Mara Winn echoed this assessment, and noted that DoE has been working with energy system owners and operators "over the last several months" to detect compromised systems and stamp out the intruders. "Our assessment is that the threat is actively positioning itself on critical infrastructure IT networks with the explicit goal of being able to disrupt the functioning of operational technology," said Winn, the deputy director for preparedness, policy, and risk assessment in the DOE's Office of Cybersecurity, Energy Security, and Emergency Response."[5]

9. **Volt Typhoon Returns.** In June 2024, 'Volt Typhoon' was observed as active, growing and "*sporting plenty of previously undisclosed stealth mechanisms.*" The hackers were "*using a two-year old critical vulnerability in Zoho's ManageEngine ADSelfService Plus, a single sign-on and password management solution.*" The investigators discovered "*the attacker — Volt Typhoon — had deployed a Web shell to the network a whole six months prior.*" Those web shells were used as the foundation to rebuild the 'Volt Typhoon' network. The rebuilding process was described as a "*cruder, manual approach ... going to "extensive lengths to clear out multiple log files and remove excess files from disk.*"[6] The attackers forgot to erase some java files which lead to their discovery.

10. Earlier this month (November 2024) cyber security companies began reporting that they observed that 'Volt Typhoon' was being rebuilt. 'SecurityScorecard' researchers observed "*several Cisco RV320s, DrayTek Vigor routers, and NETGEAR ProSAFEs*" were part of a rebuilt 'Volt Typhoon' network.[7] This is described as a 'sophisticated escalation' as the attackers "*leverage end-of-life routers that no longer receive security updates. ... This renewed activity comes nearly ten months after US authorities dismantled parts of the group's botnet, which had initially targeted US energy, water, and telecommunications networks. ... The DOJ then claimed that the authorities had "removed the malware from US-based victim routers and taken steps to prevent reinfection". ... Volt Typhoon's botnet spans global networks, using the JDYFJ SSL certificate cluster for encrypted, untraceable communication. Every layer of Volt Typhoon's infrastructure is designed to blend malicious activities into everyday operations, making them difficult to detect and even harder to remove*"[8]

'Salt Typhoon' Campaign and Hacking Collective

11. Starting in 2023, a new PRC Campaign and hacking crew named 'Salt Typhoon' emerged. The hacker may also be known as Earth Estries, FamousSparrow, GhostEmperor and UNC2286, although those groups are *more probably* a collective rather than one organization. According to 'Trend Micro', the group's primary targets are critical sectors such as telecommunications (including Internet service providers), consulting, chemical, transportation, government entities and NGO's. Targeting also includes vendors, companies that supply network and telecommunications products to

5 Source: The Register. Volt Typhoon not the only Chinese crew lurking in US energy, critical networks
6 Source: Dark Reading. China's 'Volt Typhoon' APT Turns to Zoho ManageEngine for Fresh Cyberattacks
7 Source: Security Affairs. China's Volt Typhoon botnet has re-emerged
8 Source: CSO Online. Volt Typhoon returns with fresh botnet attacks on critical US infrastructure

© David Swan Consulting 2024

their primary targets. Countries targeted include: the US, Asia-Pacific, Middle East, and South Africa. The group has compromised over twenty organizations using "*advanced attack techniques and multiple backdoors, such as GHOSTSPIDER, SNAPPYBEE, and MASOL RAT*". 'Trend Micro' analysts have identified this group as "*one of the most aggressive Chinese advanced persistent threat (APT) groups*".[9]

12. 'Salt Typhoon' hacks victim's public-facing servers utilizing known vulnerabilities. Once the server is accessed, backdoors such as 'GhostSpider' and 'Masol RAT' are planted. This provides: increased access between the target servers and their command and control networks, detection avoidance and enables prolonged espionage operations. Analysts noted that the command and control networks appear to be *shared between multiple different PRC hacker groups.* The Demodex rootkit is used to mask the presence of malware within the victims network.[10]

13. The obvious question is how effective has this group been - how bad is the threat? "*Representatives from the U.S. intelligence community briefed congressional committees about a recent sweeping Chinese infiltration into a slew of telecommunications firms and infrastructure tied to court-authorized wiretap requests.*" The briefing included information on the compromise of "*several telecom companies including AT&T, Lumen, Verizon and others.*" The hackers were described as "*exceptionally talented, with members who are very skilled and patient.*"[11] *"A joint alert from the US cybersecurity agency CISA and the FBI"* described the hack as "*a broad and significant cyber espionage campaign ... to steal call records and data and to spy on individuals.*" This includes "*the copying of certain information that was subject to U.S. law enforcement requests pursuant to court orders* (wiretap information)."[12]

14. Senator Mark R Warner, Chair of the Senate Intelligence Committee said his '*hair is on fire*' as the 'Middle Kingdom' has established "*a persistent presence ... and may require the replacement of "literally thousands and thousands and thousands" of switches and routers. The senator added that China's activities make Russia-linked incidents like the SolarWinds supply chain incident and the ransomware attack on Colonial Pipeline look like "child's play. ... Warner told 'The Times' the extent of China's activity remains unknown, and that "**The barn door is still wide open, or mostly open.**"*[13] *"The US government's Consumer Financial Protection Bureau (CFPB) sent an email to all its employees with a simple directive: 'Do NOT conduct CFPB work using mobile voice calls or text messages'."*[14]

15. 'Trend Micro' conclusions are: The hackers "*conduct stealthy attacks that start from edge devices and extend to cloud environments, making detection challenging. Their notable TTPs include exploiting known vulnerabilities and using widely available*

9 Source: Trend Micro. Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions
10 Source: Info Security. Aggressive Chinese APT Group Targets Governments with New Backdoors
11 Source: Next Gov. Intelligence community briefed Congress on Chinese telecom intrusions
12 Source: Security Week. CISA, FBI Confirm China Hacked Telecoms Providers for Spying
13 Source: The Register. China has utterly pwned 'thousands and thousands' of devices at US telcos
14 Source: Security Week. US Gov Agency Urges Employees to Limit Phone Use After China 'Salt Typhoon' Hack

© David Swan Consulting 2024

shared tools." This includes using tools that exist of the victims network. "*They employ various methods to establish operational networks that effectively conceal their cyber espionage activities, demonstrating a high level of sophistication in their approach to infiltrating and monitoring sensitive targets. ... Our analysis suggests that Earth Estries is a well-organized group with a clear division of labor. Based on observations from multiple campaigns, we speculate that attacks targeting different regions and industries are launched by different actors. Additionally, the C&C infrastructure used by various backdoors seems to be managed by different infrastructure teams, further highlighting the complexity of the group's operations."*[15]

16. **Other PRC Campaigns.**

- **BrazenBamboo Exploited an Unpatched, Undisclosed Fortinet Vulnerability.** Threat intelligence vendor Volexity discovered an archive file tied to BrazenBamboo, in an archive connected to Windows malware families dubbed 'Deepdata' and 'Deeppost', in a clients system. The attackers used a "*zero-day credential disclosure vulnerability in Fortinet's Windows VPN client that allowed credentials to be stolen from the memory of the client's process.*"[16]
- This campaign has been noted because it targets user communication applications:
  - Scoops up data from WhatsApp, and Signal;
  - Records audio; collect contacts and emails from local Microsoft Outlook instances
  - Steals messages and data from WeChat, Line, QQ, DingDing, Skype, Telegram, and Feishu applications;
  - Collects history, cookies, and passwords from Firefox, Chrome, Opera, and Edge web browsers.[17]

- **Liminal Panda: Another Telecommunications Hack.** This PRC hacking group focuses on targets in Africa and Asia, notably countries and organizations "*associated with China's Belt and Road Initiative (BRI), a national-level strategy seeking to establish economic opportunities aligned with Beijing's prioritized interests outlined in China's 13th and 14th Five-Year Plans.*" Liminal Panda targets telecommunications providers "*using protocols that support mobile telecommunications, such as emulating global system for mobile communications (GSM) protocols to enable C2, and developing tooling to retrieve mobile subscriber information, call metadata and text messages (SMS).*" Their objective is *assessed* as "*enable covert access, command and control (C2) and data exfiltration."*[18]

- **PRC's APT Gelsemium Targets East and Southeast Asia.** This hacker group, detected since March 2023, was identified targeting organizations in

15 Source: Trend Micro. Game of Emperor: Unveiling Long Term Earth Estries Cyber Intrusions
16 Source: TechTarget. Chinese APT exploited unpatched Fortinet zero-day flaw
17 Source: The Register. China-linked group abuses Fortinet 0-day with post-exploit VPN-credential stealer
18 Source: CrowdStrike. Unveiling LIMINAL PANDA: A Closer Look at China's Cyber Threats to the Telecom Sector

© David Swan Consulting 2024

Cyber-Intelligence Report

Taiwan, the Philippines, and Singapore. The group is known for "*cyberespionage, targeting sensitive data while evading detection.*"[19] They are in the news because of a shift in their tactics, shifting from attacking Windows servers to deploying two previously unknown Linux backdoors, 'WolfsBane' and 'Firewood'.

- **Fake News Websites.** Google has identified a network of 'fake news websites' being used to "*publish thematically similar, inauthentic content that emphasizes narratives aligned to the political interests of the People's Republic of China (PRC). ... Google's Threat Intelligence Group has blocked a network China-related firms from its search results for operating fake news services and websites. ... these firms bulk-create and operate hundreds of domains that pose as independent news websites from dozens of countries*". Google named the network 'Glassbridge'. "*Overall, Google revealed it has blocked over 1,000 sites from Google News and Google Discover since 2022.*"[20]
- Google identified four firms, Shanghai Haixun Technology, Times Newswire, Durinbridge, and Shenzhen Bowen Media as taking direction in outsourcing pro-PRC content. Mixed with public relations material and digital content was 'regurgitated state sponsored media'. The attacks are attributed to a PRC 'state threat actor (hacker group) known as 'Storm-2077'. Also known as 'TAG-100', the group "*conducted cyber attacks against the Defense Industrial Base (DIB), aviation, telecommunications, and financial and legal services across the world*". In addition to propagation of fake news the group is "*said to orchestrate intelligence-gathering missions*".[21]

17. **Analysts Comments:** The amount of cyber capability demonstrated by the 'Typhoon' campaigns dwarfs the output of all other aggressor nations combined. When considered as a whole, the political vision and determination to leverage cyber is unique. Further, the personnel, technology and sustained effort requires an extraordinary financial investment (even for a country as large as the PRC) over a long time period in order to produce results. Lastly, the command and control and integration required to drive these campaigns, infer a highly dangerous threat.

This cyber-intelligence product is produced by David Swan. It is copyright ©David Swan 2024. This report is **TLP:CLEAR**[22] and MAY be shared freely.

To unsubscribe from this service send an email to DSC.Ops.Vulcan@gmail.com

19 Source: Security Affairs. China-linked APT Gelsemium uses a new Linux backdoor dubbed WolfsBane

20 Source: The Register. Google blocked 1,000-plus pro-China fake news websites from its search results

21 Source: The Hacker News. Google Exposes GLASSBRIDGE: A Pro-China Influence Network of Fake News Sites

22 Definition **TLP: CLEAR.** From U.S. Govt Cyber Defense Agency. Traffic Light Protocol (TLP) Definitions and Usage, Recipients may share this information without restriction. Information is subject to standard copyright rules.

© David Swan Consulting 2024