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 2025. 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: Continued Degrading of U.S. Cyber Security

This report contains selected cyber-security information from 4th to 17th April 2025.

Synopsis

1. Trump Administration fired head of NSA and U.S. Cyber Command, then investigates it's former CISA Director. Current CISA staff being 'Gutted'.The U.S. Government's Cybersecurity agency (CISA) 'played' with ending a critical cybersecurity program. Apparently the PRC admitted that 'Volt Typhoon' was their campaign. The PRC continues to launch agressive cyber espionage campaigns.

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 a primary source of cyber attacks. This includes government funded hackers (military, intelligence and civilian employees), affiliated hackers (criminals and mercenaries), and volunteer 'supporters'.

U.S. Government vs CyberSecurity

3. **Trump's 'Revenge Tour' Guts U.S. Cybersecurity**.

- **Head of NSA and U.S. Cyber Command Fired.** "*On April 3, President Trump fired Gen. Timothy Haugh, the head of the National Security Agency (NSA) and the U.S. Cyber Command, as well as Haugh's deputy, Wendy Noble."* Apparently the issue was 'Haugh's loyalty'.[2]
- **Former Trump Cyber Agency Director Under Investigation by Trump Administration.** The U.S. Attorney General has been directed "*to investigate Chris Krebs, calling him 'a significant bad-faith actor who weaponized and abused his government authority.' ... the inquiry will include 'a comprehensive evaluation of all of CISA's activities over the last 6 years and will identify any instances where Krebs' or CISA's conduct appears to be contrary to the administration's commitment to free speech and ending federal censorship, including whether Krebs' conduct was contrary to suitability standards for federal employees or involved the unauthorized*

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.

2 Source: Krebs on Security. Trump Revenge Tour Targets Cyber Leaders, Elections

dissemination of classified information'." Krebs 'sin' was "*declaring the 2020 election the most secure in U.S. history."*[3] In response Chris Krebs has left his position with SentinelOne, a major cybersecurity firm. "*He told company CEO Tomer Weingarten 'what I firmly believe: this is my fight, not the company's, and I offered my resignation. ... 'For those who know me, you know I don't shy away from tough fights."*[4] *... 'Illegitimi non carborundum'*[5]*."*

- **CISA Staff Gutted**. It is forecast that forty percent of the US govt's Cybersecurity and Infrastructure Security Agency (CISA) (1,300 employees) will be downsized as part of the effort to reduce federal staff. By 14th April, employees have to decide "*if they will take Secretary Kristi Noem's offer and choose deferred resignation, early retirement, or an immediate buyout."* No justification for the drastic reorganization has been offered. "*Retired US Navy Rear Admiral Mark Montgomery told The Register in an earlier interview the firings and funding cuts 'harm national security on a daily basis'."*[6]

4. **Brinkmanship with Global Cybersecurity Database.** On Tuesday, the 15th April, a letter was released saying "*the current contract ... for MITRE to develop, operate, and modernize CVE and several other related programs ... will expire."*[7] The Common Vulnerabilities and Exposures (CVE) program, operated by the non-profit research organization MITRE institute under contract to the U.S. Government, is one of the keystones of global cybersecurity. The 25-year-old CVE program is an invaluable tool for vulnerability management, offering a de facto standard to identify, define, and catalog publicly disclosed security flaws using CVE IDs. The program has listed over 274,000 CVE records to date. Late on the 15th, an options clause in the MITRE contract was executed, extending the contract for eleven months 'to ensure no continuity issues'. "*The CVE Program is invaluable to cyber community and a priority of CISA,*" the U.S. cybersecurity agency told BleepingComputer. "*Last night, CISA executed the option period on the contract to ensure there will be no lapse in critical CVE services."*[8]

5. MITRE Vice President Yosry Barsoum warned "*If a break in service were to occur, we anticipate multiple impacts to CVE, including deterioration of national vulnerability databases and advisories, tool vendors, incident response operations, and all manner of critical infrastructure,*"[9] John Hammond, a cybersecurity analyst with Huntress Labs, explained the risk of losing the CVE database in an explosive YouTube video. The title said it bluntly: "cybersecurity just got f***ed"[10]

6. Analysts Comments:

3 Source: Krebs on Security. Trump Revenge Tour Targets Cyber Leaders, Elections
4 Source: NextGov. Former cyber official Chris Krebs to leave SentinelOne in bid to fight Trump pressure
5 Loose translation from Latin: "Don't let the bastards grind you down."
6 Source: The Register. Cyber congressman demands answers before CISA gets cut down to size
7 Source: The Hacker News. U.S. Govt. Funding for MITRE's CVE Ends April 16, Cybersecurity Community on Alert
8 Source: Bleeping Computer. CISA extends funding to ensure 'no lapse in critical CVE services'
9 Source: Bleeping Computer. CISA extends funding to ensure 'no lapse in critical CVE services'
10 Source: YouTube / John Hammond. cybersecurity just got f***ed

A. Finding another leader as qualified as General Haugh is unlikely. Any change of command bring a certain amount of turmoil. This will almost certainly be reflected in the NSA and U.S. Cyber Command.

B. Given that the MITRE CVE contract extension was not announced by the White House nor any Cabinet level official, we are NOT confident the eleven month extension will be honoured. Even if the CVE database is preserved, I anticipate there will be a loss or at least a degradation of the CVE program.

C. CISA can not afford the loss of forty percent of its staff. This will produce another degradation in U.S. cyber defensive capabilities.

D. The lack of response from the U.S. cybersecurity industry to any of the Trump administrations cyber chaos suggests that companies are taking an 'every man for himself' approach. At best they are very quietly working with each other and industry partners, attempting to stay off Trump's radar.

E. Unfortunately the effects of the Trump administration actions are cumulative, meaning they will build on each other, further degrading U.S. defensive cybersecurity. There is no indication of anyone in the Trump sphere who would understand the implications of a major cyber attack. This implies it is a good season for cyber aggressors to get even busier.

PRC

7. **PRC Admits Responsibility For 'Volt Typhoon'**. At a December 2024 meeting between PRC officials and the Biden administration, Chinese officials admitted to directing cyberattacks on US infrastructure. The Chinese delegation reportedly implied their nation's cyberattacks on US infrastructure were linked to America's support for Taiwan. A former U.S. official familiar with the meeting described "*the Chinese official's remarks as 'indirect and somewhat ambiguous' but also "a tacit admission and a warning to the U.S. about Taiwan."*[11] "*The American delegation interpreted that the attacks tracked as Volt Typhoon were conducted in response to the US supporting Taiwan. ... the American delegation interpreted that the attacks tracked as Volt Typhoon were conducted in response to the US supporting Taiwan."*[12]

8. 'Volt Typhoon' was a campaign aimed at accessing critical infrastructure. "*The Volt Typhoon threat actors managed to gain access to systems in a wide range of sectors, including communications, manufacturing, utility, construction, government, IT, maritime, transportation, and energy. It came to light recently that the hackers managed to dwell in the US electric grid for 300 days in 2023."*[13]

9. Analysts Comment: The problem with this reporting is that it does not acknowledge that Volt Typhoon was (is?) a **global** campaign targeting communications, energy, transportation, water and wastewater systems. 'Volt Typhoon' detections were made in Europe, and Asia as well as the Americas. Starting in at least 2021 Volt Typhoon started with a botnet of Cisco and Netgear routers. It

11 Source: The Register. China reportedly admitted directing cyberattacks on US infrastructure
12 Source: Security Week. China Admitted to Volt Typhoon Cyberattacks on US Critical Infrastructure: Report
13 Source: Security Week. China Admitted to Volt Typhoon Cyberattacks on US Critical Infrastructure: Report

used used command-and-control (C2) infrastructure in the Netherlands, Latvia, and Germany. "*By October 2023, Volt Typhoon had taken up occupancy, rent-free, on a compromised VPN device in New Caledonia. This created 'a covert bridge between Asia-Pacific and the Americas' that kept 'their network alive, hidden from standard detection'.*"[14]

10. This raises the question of *WHY* the PRC delegation would admit a link to Volt Typhoon. The PRC has never admitted to any cyber espionage. We agree that the PRC wants no interference in its Taiwan takeover, however we believe this revelation should be taken as a threat. The threat might read: 'You should consider that the PRC has access to all your critical infrastructure so you should stay out of our way'. This threat aligns with increasing PRC frustration with nations supporting Taiwan.[15]

11. **PRC Continues to Expand Cyber Espionage Operations**. The PRC continues its cyber espionage activity, argueably at an accelerated rate. Here are a few headlines from the last two weeks.

- **PRC APT Group Targets Ivanti VPN Vulnerabilities to Breach Networks.** Cybersecurity firm TeamT5 reports "*Chinese Advanced Persistent Threat (APT) group leveraged critical vulnerabilities in Ivanti Connect Secure VPN appliances ... affecting nearly 20 industries across 12 countries*"[16]
- **'New' PRC State Security Hackers Create New 'RAT'**. "*The attacker, dubbed UNC5174 ... has infected global organizations with a remote access trojan (RAT) to enable its espionage and access resale campaigns.*"[17] UNC5174 is assessed as a 'State Security Hacking Group.'
- **Old Adversary Updates Its Attacks.** "*Mustang Panda ... is known for targeting government and military entities, as well as NGOs and minority groups, mainly in East Asia, but also in Europe. ... recently they"deployed an updated version of their ToneShell backdoor, along with a new tool dubbed StarProxy, the Paklog and Corklog keyloggers, and the SplatCloak EDR evasion driver.*"[18]

–

14 Source: The Register. China's Volt Typhoon crew and its botnet surge back with a vengeance
15 Source: Previous editions of our Cyber Intelligence Report with contributions from RUSI(NS) Security Advisory Committee (SAC).
16 Source: gbhackers. Chinese APT Group Targets Ivanti VPN Vulnerabilities to Breach Networks
17 Source: The Register. Chinese snoops use stealth RAT to backdoor US orgs – still active last week
18 Source: Security Week. Chinese APT Mustang Panda Updates, Expands Arsenal
19 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.

Cyber-Intelligence Report