EuRepoC

ADVANCED
PERSISTENT
THREAT profile

Volt Typhoon vs. Flax Typhoon

In the eye of the Chinese typhoons

Volt Typhoon APT designations

- **Volt Typhoon** (Microsoft)
- **DEV-0391** (Previous Microsoft designation)
- **Bronze Silhouette** (Secureworks)
- **Insidious Taurus** (Palo Alto Unit 42)
- **Vanguard Panda** (CrowdStrike)
- **UNC3263** (Mandiant)
- **VoltZite** (Dragos)

Flax Typhoon APT designations

- **Flax Typhoon** (Microsoft)
- **Storm-0919** (Previous Microsoft designation)
- **Ethereal Panda** (CrowdStrike)
- **Red Juliett** (RecordedFuture)

Sources: [1], [2], [3], [4], [5], [6], [7], [8], [9], [10]

Country of origin

Time period of activity

2021* - present

*While Volt Typhoon's operations began in 2021, we also acknowledge 2021 as the beginning of the operational period for Flax Typhoon, as it is the indicated start of operations by Ethereal Panda, according to CrowdStrike.

Sources: [1], [9]

Political affiliations

Volt Typhoon is a new but impactful APT (Advanced Persistent Threat). As such, there is currently a lack of extensive consolidated academic, industry-related, or official research on the group.

On the industry side, substantial primary reports on the group and its activities have been published by Microsoft's threat intelligence team, while the United States National Security Agency (NSA), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Communications Security Establishment's Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), and the United Kingdom National Cyber Security Centre (NCSC-UK) also issued a joint advisory on 24 May 2023. On 7 February 2024, US, Australian, British, and Canadian agencies followed up with another joint advisory. Microsoft's private reporting and the joint advisory from 2023 appear to have been a coordinated effort, describing Volt Typhoon as a state-sponsored group linked to China. The same attribution to China has been stated for Flax Typhoon; for Flax Typhoon, Microsoft released the most comprehensive threat intelligence report to date on 24 August 2023.

Sources: [1], [8], [11]

By Kerstin Zettl-Schabath

Agency type

State-sponsored hacker group(s): Beyond the attribution of being "state-sponsored" by the People's Republic of China, no further details have been disclosed thus far regarding the connection between Volt Typhoon or Flax Typhoon and any specific affiliated state entities.

However, based on the February 2024 joint advisory for Volt Typhoon by the NSA, CISA, FBI, and other US agencies, together with Australian, British, and Canadian agencies, together with Microsoft`s report for Flax Typhoon, which all suggest that the activities of both groups align with the Peole's Republic of China's (PRC) strategic objectives concerning the Taiwan conflict, it is plausible to infer a connection between both APTs and the Strategic Support Force (SSF) of the Chinese People's Liberation Army (PLA). The SSF was established in 2015 as part of a significant PLA reform initiated by Xi Jinping, aimed at achieving military dominance in space, cyberspace, and the electromagnetic domain — areas of critical strategic importance to the PLA. The SSF has consolidated control over a substantial portion of the PLA's space-based and space-related assets under its Space Systems Department (航天系统部). Reports indicate that the SSF provided strategic-level information support to the PLA, enhancing its capability to conduct integrated joint operations and remote missions.

Given Flax Typhoon's current focus on cyber espionage and intelligence gathering — contrasting with Volt Typhoon's operations, which have interpreted as "pre-positioning operations" (see sections "operation type(s)" and "basic attack pattern") — an alternative hypothesis may identify Flax Typhoon as a potential affiliate of the Ministry of State Security (MSS), given the Ministry's dominant role in espionage and information theft for CPC objectives. In any case, a PLA connection remains the most likely scenario within the context of the integrated military joint operations framework which the SSF has pursued for years, particularly concerning Taiwan and the South China Sea.

However, according to media reports, the PRC disbanded the SSF on 19 April 2024, replacing it with an Information Support Force directly subordinate to the Central Military Commission, the top political body overseeing China's armed forces. This recent restructuring of the PLA led to the creation of three new branches: the Information Support Force, the Cyberspace Force, and the Aerospace Force. It is likely that the latter two were previously SSF departments that have been renamed as part of this restructuring. Despite these internal changes, it is unlikely that they will result in prompt major shift in how the PLA conducts future cyber operations. Monitoring internal restructuring processes within autocratic security organisations may yet provide valuable insights for evaluating future cyber conflict strategies, particularly in understanding power dynamics among competing agencies.

Sources: [12], [13]

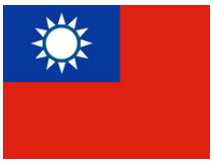
Most frequent target: Volt Typhoon

USA*

**USA (incl. Guam; critical infrastructure targets in the following sectors: communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors)*

Sources: [1], [8]

Most frequent target: Flax Typhoon



Taiwan**

***Taiwan, alongside other victims also located in Southeast Asia, North America, and Africa (government agencies and education, critical manufacturing, and information technology organisations)*

Group composition/organisational structure

No information is currently available regarding the composition or organisational structure of either the Volt Typhoon or Flax Typhoon group.

Impact type(s): Volt Typhoon

Indirect

- *Intelligence Impact (Potential future physical effects in the case of sabotage operations; psychological impact in the case of intended signalling efforts towards the US)*

Indirect

- *Reputational Impact (Potential future physical effects in the case of sabotage operations; psychological impact in the case of intended signalling efforts towards the US)*

Sources: [1], [8]

Impact type(s): Flax Typhoon

Direct

- Intelligence impact

Operation type(s): Volt Typhoon

- *Hijacking with misuse + data theft (potential "pre-positioning" operations in order to establish beachheads in future target networks for sabotage operations)*

Source: [1], [8], [14], [15]

Operation type(s): Flax Typhoon

- *Hijacking with misuse + data theft (cyber espionage/reconaissance)*

Operation type(s)

Both groups have engaged in hijacking activities with potential data theft against their respective victim organisations; however, the interpretation of their intentions regarding potential future actions varies significantly between Volt Typhoon and Flax Typhoon. Microsoft, which has been instrumental in shaping the industry-driven discourse on these groups, states in its May 2023 report, with medium confidence, that Volt Typhoon "is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises." In contrast, its assessment of Flax Typhoon's infiltration of Taiwanese organisations was more subdued: it states that the group "gains and maintains long-term access to Taiwanese organizations' networks with minimal use of malware, relying on tools built into the operating system, along with some normally benign software to quietly remain in these networks. Microsoft has not observed Flax Typhoon using this access to conduct additional actions."

These differing views on the two groups and their future intentions may plausibly be traced back to the criticality of the reported victims, but also their perceived intelligence value, as highlighted by the US Deputy National Security Advisor for Cyber and Emerging Technologies, Anne Neuberger, at the Munich Security Conference 2024. Volt Typhoon targeted US critical infrastructures in the Pacific region, which hold significant strategic importance in the event of an armed conflict between China and the United States, e.g., over Taiwan or North Korea; however, the infrastructure targets hold little value for genuine espionage purposes. In contrast, Microsoft initially described the Taiwanese entities targeted by Flax Typhoon as simply "organisations," while acknowledging in a subsequent section that the group's general targeting also includes entities involved in critical manufacturing and information technology.

The broader geopolitical tensions between the US and China at the time may have had a role in amplifying the diverging assessments; for example, Microsoft's report for Volt Typhoon from 2023 was released on the same day as the CISA advisory. The latter acknowledged the extensive industry-collaboration with a list of companies assisting in tracking the group, also stating that "private sector partners have identified that this activity affects networks across US critical infrastructure sectors." It therefore can be assumed that Microsoft's report and the advisory were coordinated content-wise *and* regarding the date of publication, presumably as a joint effort to signal to China the "whole-of-society" awareness among US actors who are closely monitoring and analyzing PRC cyber activities within US networks.

From a legal perspective, the US may also have tried to signal red lines to its Chinese counterparts, drawing on the UN's norms of responsible state behaviour in cyberspace. These norms state that a "State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." By framing Volt Typhoon's activities as "pre-positioning operations," the US identifies them as potentially non-compliant behaviour, in contrast to handling them as mere data theft, which would lack indications of preparation for later sabotage.

Sources: [1], [8], [14], [15]

Basic attack patterns

Volt Typhoon

Volt Typhoon's attack pattern begins with extensive reconnaissance to understand the target's network architecture, security measures, and key personnel. They gain initial access by exploiting vulnerabilities in public-facing network appliances and then secure this access through VPN connections. Once inside, they aim to obtain administrator credentials by exploiting privilege escalation vulnerabilities or extracting them from insecurely stored locations. Using these credentials, they move laterally within the network via Remote Desktop Protocol (RDP) and other remote access services, often achieving full domain compromise by extracting and decrypting the NTDS.dit file from domain controllers. Throughout their operations, Volt Typhoon employs living-off-the-land (LOTL) techniques, using native tools and commands to avoid detection, maintain persistence, and gather intelligence while evading traditional security measures.

Flax Typhoon

Flax Typhoon employs a distinct attack pattern primarily targeting organisations in Taiwan using living-off-the-land techniques (LOTL) and compromised valid accounts. They achieve initial access by exploiting vulnerabilities in public-facing servers and deploying web shells like China Chopper. Following initial access, they use command-line tools to establish persistent access via remote desktop protocol (RDP) and deploy a VPN connection to their infrastructure. The group leverages tools such as Mimikatz for credential access and relies on techniques like disabling Network Level Authentication (NLA) and modifying Sticky Keys behavior for persistence.

Sources: [8], [16]

Zero-day exploits

Volt Typhoon*

- Fortinet FortiOS SSL-VPN Vulnerabilities (CVE-2023-27997, CVE-2024-21762, CVE-2024-23113)
- Ivanti Connect Secure Vulnerabilities (CVE-2024-22024, CVE-2023-46805, CVE-2024-21887)
- ADSelfService Plus (CVE-2021-40539)

Flax Typhoon

No exploitation known.

*Most of the zero-days reported could not be directly linked to incidents that would have met the EuRepoC inclusion criteria; in other cases, it was not clear in which of the mentioned compromises which zero-day was exploited.

Sources: [17]

Utilised Malware (tools):

Volt Typhoon

Volt Typhoon (thus far) rarely uses traditional malware in their post-compromise activities. Instead, the group relies heavily on built-in Windows utilities and custom versions of open-source tools.

Living-off-the-land commands:

- Local Security Authority Subsystem Service (LSASS) memory dumping: This involves dumping credentials from the LSASS process memory space.
- Ntdsutil.exe: This command-line tool is used to create installation media from domain controllers, containing usernames and password hashes.
- PowerShell: Used for discovering system information and additional devices on a network.
- Windows Management Instrumentation Command-line (WMIC): Used for network discovery and system information.
- Ping command: Used to discover other systems on the compromised network.

Command and Control (C2):

- netsh portproxy command: Used to create proxies on compromised systems.
- Custom versions of open-source tools:
  - Impacket: A collection of Python classes for working with network protocols.
  - Fast Reverse Proxy (FRP): A tool to establish a C2 channel over proxy.

Sources: [8], [16]

Flax Typhoon

Similar to Volt Typhoon, Microsoft observes a minimal use of traditional malware by Flax Typhoon. Instead, the group relies on tools built into an operating system, along with some normally benign software, to stay undetected these networks:

- China Chopper web shell
- Metasploit
- Juicy Potato privilege escalation tool
- Mimikatz
- SoftEther virtual private network (VPN) client

Select tactics and techniques leveraged by the group based on the MITRE ATT&CK Framework:

	Volt Typhoon	Flax Typhoon
MITRE Initial Access	Exploit Public-Facing Application	Exploit Public-Facing Application
MITRE Execution	Command and Scripting Interpreter	Command and Scripting Interpreter
MITRE Defense Evasion	Living off the land techniques Command and Scripting Interpreter	Living off the land techniques Command and Scripting Interpreter

Sources: [8], [16]

Major attribution milestones

Volt Typhoon

- 24 May 2023: First public reporting by Microsoft and the United States National Security Agency (NSA), the US Cybersecurity and Infrastructure Security Agency (CISA), the US Federal Bureau of Investigation (FBI), the Australian Signals Directorate's Australian Cyber Security Centre (ACSC), the Communications Security Establishment's Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), and the United Kingdom National Cyber Security Centre (NCSC-UK) (public).

Sources: [1], [8]

Flax Typhoon

- 24 August 2023: First public reporting by Microsoft on the group.

Attribution Ambiguities

Threat intelligence companies frequently discuss "overlaps" between the APTs (Advanced Persistent Threats) they track under certain names and similarly named groups identified by other companies. At times, they even suggest a complete match between these groups. However, due to variations in terminology across different sources, it is often unclear whether these groups are collaborating, or if they are simply the same entities operating under different names.

This ambiguity is evident in the case of Flax Typhoon; Microsoft notes that the group "overlaps" with Ethereal Panda. Similarly, Dragos' report on the VOLTZITE group mentions that it "shares overlaps with the adversary described by the US Cybersecurity and Infrastructure Security Agency (CISA) in May 2023, and the Microsoft threat group Volt Typhoon." However, some reports suggest that these different designations refer to the same actor, such as the joint CISA advisory on Volt Typhoon from 7 February 2024, or Microsoft's general naming conventions for Flax Typhoon and Ethereal Panda.

Given the commonality of shared Tactics, Techniques, and Procedures (TTPs) and malware types among Chinese APTs, the use of the term "overlap" may simply serve as a cautious approach to an unknown situation. This allows the attributing entity to present its findings without fully committing to a single APT designation.

Interestingly, the Chinese National Computer Virus Emergency Response Centre, the National Engineering Laboratory for Computer Virus Prevention Technology, and the 360 Digital Security Group released two consecutive joint reports in July and August 2024. In these reports, they first attempted to portray Volt Typhoon as a ransomware group, then sought to "debunk" US claims about Volt Typhoon, alleging that these statements were fabricated to secure more funding from Congress for the extensive US surveillance program under FISA Section 702. The revelations of these cyber operations clearly struck a nerve and were not meant to be uncovered, which would explain the considerable effort put into the reports and serves as a fitting transition to the next section.

Sources: [2], [7], [8], [16], [19]

Attribution and detection sensitivity

The use of (relatively costly and sophisticated) "living off the land" techniques by Volt Typhoon and Flax Typhoon demonstrates a strong desire to remain undetected within target networks for as long as possible. Additionally, both groups appear to seamlessly blend into normal network activity by routing traffic through compromised SOHO (small office/home office) network equipment, such as routers, firewalls, and VPN hardware. They also utilise custom versions of open-source tools to establish a command and control (C2) channel over proxies, further evading detection.

If the US' interpretation of these infiltration TTPs is accurate, and Volt Typhoon did indeed intend to establish a foothold within US critical infrastructure systems for potential future sabotage, then "flying under the radar" for a long time becomes even more crucial from the attackers' perspective. However, it is always worth considering the possibility that certain operations are designed to be detected eventually, as a means of signaling to an adversary that their critical assets are (and will stay) vulnerable in cyberspace.

Still, in the case of Volt Typhoon and its alleged sponsor, China, there is no indication that operational security failures were intentional, nor have any such failures been reported. This suggests that the primary goal was stealth, rather than a calculated revelation of capabilities.

Sources: [8], [16]

POLITICAL/LEGAL/LAW ENFORCEMENT ACTIONS

In December 2023, a court-authorised operation by the US Department of Justice successfully disrupted a botnet consisting of hundreds of US-based small office/home office (SOHO) routers that had been hijacked by Volt Typhoon. According to court documents, the US government entities thoroughly tested the operation on relevant Cisco and NetGear routers, ensuring it did not interfere with legitimate functions or collect any content information. The court-approved measures temporarily disconnected the routers from the KV Botnet and prevented reinfection; however, this protection would be undone by a simple restart initiated by the router's owner. Without applying similar mitigation steps after a restart, however, the router would remain vulnerable to reinfection.

Sources: [18]

Indicted Individuals

No indicted individuals so far (August 2024).

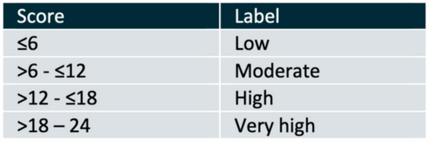
Incident type(s)

- **Data Theft** (intelligence gathering/cyber espionage)
- **Hijacking with misuse** (financial theft against banks or cryptocurrencies)
- **Disruption** (wiper attacks/DDoS operations)

Threat Level Index

The Threat Level Index is derived from the EuRepoC dataset 1.0. It is a composite indicator covering five dimensions: the sectorial and geographical scope of the APT's attacks, the intensity of the attacks, the frequency of attacks and the use of zero-days. Please note that only attacks that have been publicly attributed to the APT group during its period of activity and which meet the specific EuRepoC criteria for inclusion are considered. The scores account for the practice of other APT groups analysed by EuRepoC, as thresholds used for determining low/high scores are based on the range of scores obtained across multiple APT groups. For more detailed information on the methodology underpinning the Threat Level Index see here and here.

Index scoring scale



Score	Label
≤6	Low
>6 - ≤12	Moderate
>12 - ≤18	High
>18 – 24	Very high

Volt Typhoon

12/24 moderate

Flax Typhoon

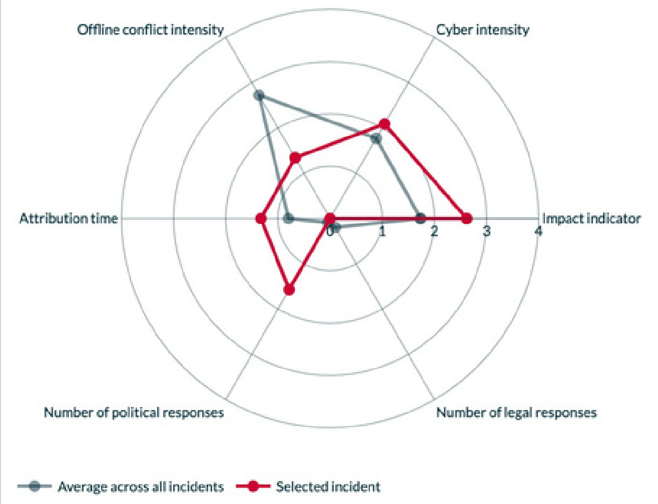
10/24 moderate

Threat level sub-indicator	Volt Typhoon	Flax Typhoon	Explanation
Intensity of attacks	1/5	1/5	This sub-indicator represents the average "Weighted Cyber Intensity" score from the EuRepoC codebook for all attacks attributed to the APT for its period of activity. It assesses the type of attacks, their potential physical effects, and their socio-political severity – see here for more information.
Sectorial scope of attacks	2/8	2/8	This sub-indicator calculates average number of targeted sectors per attack attributed to the APT groups over its period of activity. If the majority of the targeted sectors are critical to the functioning of the targeted societies (i.e. political systems and critical infrastructure) a multiplier is applied. Incidents attributed to the Lazarus Group in the EuRepoC database, targeted, on average, 1.5 sectors per attack and 66% were against state institutions/political systems or critical infrastructure.
Geographical scope of attacks	2/4	3/4	This sub-indicator considers the average number of targeted countries per attack attributed to the APT group. Whole regions or continents affected during one attack are weighted higher. In the case of the Lazarus Group, on average three countries were targeted per incident attributed to the group in the EuRepoC database.
Frequency of attacks	4/4	4/4	This sub-indicator is calculated by dividing the total number of attacks attributed to the APT group within the EuRepoC database by the number of years of activity of the APT group. The obtained scores are then converted to a four-level scale. The Lazarus Group was responsible for more than 3 incidents per year of activity.
Exploitation of Zero days	3/3	0/3	This indicator calculates the percentage of attacks attributed to the APT that use one or multiple zero days. The score obtained is then converted to a three-level scale. 2 incidents (4%) in the EuRepoC database attributed to the Lazarus Group used zero-days.

Landmark operation: Volt Typhoon

The Chinese state-sponsored hacking group Volt Typhoon gained access to a variety of critical infrastructure organisations on Guam and the US mainland beginning in mid-2021, as disclosed by Microsoft and a Joint Cybersecurity Advisory by the National Security Agency (NSA) as well as other US and other Five Eye cybersecurity agencies on 24 May 2023. Microsoft's technical report concluded with medium confidence that the Chinese hacking group intended to build capabilities that could disrupt critical communications infrastructure between the United States and Asia in future crises. The affected organisations are active in the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors. On 18 March 2024, the Biden administration sent a letter to the US governors, raising awareness for cyber operations against water and wastewater systems in the US, citing the Volt Typhoon operations as an example.

Incident Radar Chart

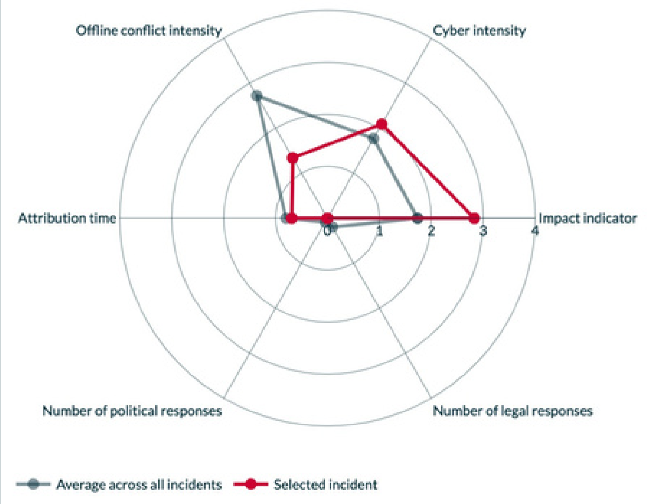


Sources: [20]

Landmark operation: Flax Typhoon

From November 2023 to April 2024, the Chinese state-sponsored cyber espionage group tracked by Microsoft as Flax Typhoon conducted an espionage campaign predominantly targeting Taiwan, but also affecting entities in Laos, Kenya, and Rwanda. This operation compromised a total of 24 organisations across sectors such as government, technology, academia, and diplomatic relations. Flax Typhoon employed the SoftEther VPN client to exploit vulnerabilities in network edge devices like firewalls, VPNs, and load balancers, allowing the group to gain initial access. This access enabled them to launch advanced SQL injection and directory traversal attacks on web and SQL applications, employing tools like devilzShell and AntSword, and exploiting the Linux vulnerability CVE-2016-5195 to escalate privileges. Additionally, they utilised Acunetix Web Application Security Scanners to identify and exploit deeper vulnerabilities. While the focus was on Taiwanese entities, Flax Typhoon's activities extended globally, including targeted operations in Hong Kong, Malaysia, Laos, South Korea, the United States, Djibouti, Kenya, and Rwanda.

Incident Radar Chart



Sources: [21]

- Offline conflict intensity: This indicator applies to cyber incidents which are related to an offline conflict. The offline intensity scores are based on the HIIK conflict database.
- Cyber intensity: This indicator assesses each cyber incident, based on its physical effects and socio-political severity. Scores range from 1-15, however, for this specific radar chart, they are scaled down to a range of 0-4. This is designed to offer a more nuanced comparison of the selected incident against the backdrop of other incidents. For more information on the cyber intensity indicator, see our methodology page.
- Impact indicator: This indicator measures the overall economic, political, intelligence and functional impact of a cyber incident.
- Number of political/legal responses: Note that the radar chart does not indicate the absolute number of responses, but uses a score to reflect how the incident fares in comparison to other incidents in terms of the number of responses.
- Attribution time: This indicator measures the number of days between the start of an incident and its first public attribution. As above, the score in the chart does not indicate the absolute number of days but reflects how the incident fares in comparison to other incidents.

SOURCES

[1] Microsoft Threat Intelligence (2023). *Volt Typhoon targets US critical infrastructure with living-off-the-land techniques*. Microsoft. Available at https://web.archive.org/web/20240819122512/https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/ [Archived on: 19.08.2024].

[2] Microsoft (2024). *How Microsoft Names Threat Actors*. Available at https://web.archive.org/web/20240819122753/https://learn.microsoft.com/de-de/defender-xdr/microsoft-threat-actor-naming%20 [Archived on: 19.08.2024].

[3] Secureworks Counter Threat Unit Research Team (2023). *Chinese Cyberespionage Group BRONZE SILHOUETTE Targets U.S. Government and Defense Organizations*. Secureworks. Available at https://web.archive.org/web/20240808102104/https://www.secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations [Archived on: 08.08.2024].

[4] Unit 42 Threat Research Center (2024). *Threat Brief: Attacks on Critical Infrastructure Attributed to Insidious Taurus (Volt Typhoon).* Unit 42. Available at https://web.archive.org/web/20240813172813/https://unit42.paloaltonetworks.com/volt-typhoon-threat-brief/ [Archived on: 13.08.2024].

[5] CrowdStrike (n.d.). *Adversaries: Vanguard Panda*. Available at https://web.archive.org/web/20240514164715/https://www.crowdstrike.com/adversaries/vanguard-panda/ [Archived on: 14.05.2024].

[6] Microsoft Threat Intelligence (2023). *Sophistication, scope, and scale: Digital threats from East Asia increase in breadth and effectiveness*. Microsoft. Available at https://web.archive.org/web/20240814083913/https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW [Archived on: 14.08.2024].

[7] Josh Hanrahan (2024). *VOLTZITE Espionage Operations Targeting U.S. Critical Systems*. Dragos. Available at https://web.archive.org/web/20240718190106/http://hub.dragos.com/hubfs/116-Datasheets/Dragos_IntelBrief_VOLTZITE_FINAL.pdf [Archived on: 18.07.2024].

[8] Microsoft Threat Intelligence (2023). *Flax Typhoon using legitimate software to quietly access Taiwanese organizations*. Microsoft. Available at https://web.archive.org/web/20240816013144/https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/ [Archived on: 16.08.2024].

[9] CrowdStrike (n.d.). *Adversaries: Ethereal Panda*. Available at https://web.archive.org/web/20240624044749/https://www.crowdstrike.com/adversaries/ethereal-panda/ [Archived on: 24.06.2024].

[10] Insikt Group (2024). *Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation*. Recorded Future. Available at https://web.archive.org/web/20240816025902/https://www.recordedfuture.com/research/redjuliett-intensifies-taiwanese-cyber-espionage-via-network-perimeter [Archived on: 16.08.2024].

[11] Cybersecurity and Infrastructure Security Agency (2023). *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection*. Available at https://web.archive.org/web/20240813164113/https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a [Archived on: 13.08.2024].

[12] Elsa B. Kania and John K. Costello (2018). *The Strategic Support Force and the Future of Chinese Information Operations.* In *Cyber Defense Review 2018*. Available at https://web.archive.org/web/20240420015814/https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_Costello.pdf [Archived on: 20 April 2024].

[13] Gordon Arthur (2024). *China dissolves Strategic Support Force, focused on cyber and space*. DefenseNews. Available at https://www.defensenews.com/global/asia-pacific/2024/04/23/china-dissolves-strategic-support-force-focused-on-cyber-and-space/.

[14] Bart Hogeveen (2022). *The UN norms of responsible state behaviour in cyberspace Guidance on implementation for Member States of ASEAN*. ASPI International Cyber Policy Centre. Available at https://web.archive.org/web/20240418095724/https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf [Archived on: 18.04.2024].

[15] Dina Temple-Raston (2024). *Neuberger: Defining espionage vs. pre-positioning for attacks is key to battling state actors*. The Record. Available at https://web.archive.org/web/20240226084158/https://therecord.media/volt-typhoon-china-defining-espionage-pre-positioning-neuberger-munich [Archived on: 26.02.2024].

[16] Cybersecurity and Infrastructure Security Agency (2024). *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. Available at https://web.archive.org/web/20240419163621/https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a [Archived on: 19.04.2024].

[17] Versa Security Research Team (2024). *Versa Security Bulletin: Volt Typhoon Exploitation of N-Day and Zero-Day Vulnerabilities*. Versa Blog. Available at https://web.archive.org/web/20240819151143/https://versa-networks.com/blog/versa-security-bulletin-volt-typhoon-exploitation-of-n-day-and-zero-day-vulnerabilities/ [Archived on: 19.08.2024].

[18] US Department of Justice Office for Public Affairs (2024). *U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure*. US Department of Justice. Available at https://web.archive.org/web/20240816222406/https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical [Archived on: 16.08.2024].

[19] National Computer Virus Emergency Response Center, National Engineering Laboratory for Computer Virus Prevention Technology, and 360 Digital Security Group (2024). *Volt Typhoon II: A secret Disinformation Campaign targeting U.S.Congress and Taxpayers conducted by U.S. Government agencies*. Available at https://web.archive.org/web/20240721070839/https://regmedia.co.uk/2024/07/19/china_volt_typhoon_inside_job_allegations.pdf [Archived on: 21.07.2024].

[20] European Repository of Cyber Incidents (2024). *Chinese state-sponsored hacking group Volt Typhoon gained access to critical infrastructure organisations on Guam and US mainland beginning in mid-2021.* Available at https://eurepoc.eu/table-view/?cyber_incident=2276.

[21] European Repository of Cyber Incidents (2024). *Chinese State Sponsored Group RedJuliett aka Flax Typhoon Group Compromised 24 organisations in Taiwan, Laos, Kenya, and Rwanda between November 2023 to April 2024*. Available at https://eurepoc.eu/table-view/?cyber_incident=3579.

About the authors

- **Kerstin Zettl-Schabath** is a post-doc researcher at the Institute of Political Science (IPW) at Heidelberg University.
- **Jonas Hemmelskamp** is a PhD-candidate at the Institute of Political Science (IPW) at Heidelberg University and provided data analysis support.

Last updated 19.08.2024