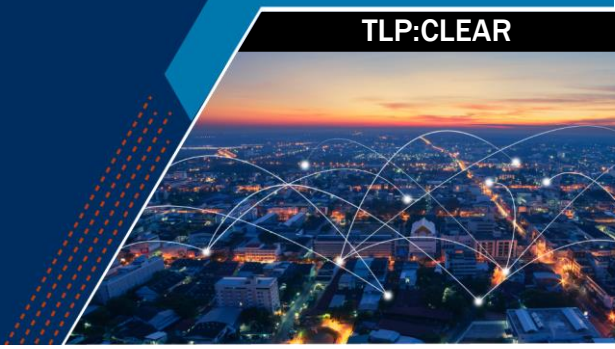
PRC STATE-SPONSORED CYBER ACTIVITY: ACTIONS FOR CRITICAL INFRASTRUCTURE LEADERS



SUMMARY

This fact sheet provides an overview for executive leaders on the urgent risk posed by People's Republic of China (PRC) state-sponsored cyber actors known as "Volt Typhoon." CISA—along with the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and other U.S. government and international partners[1]—released a major advisory on Feb. 7, 2024, in which the U.S. authoring agencies warned cybersecurity defenders that Volt Typhoon has been pre-positioning themselves on U.S. critical infrastructure organizations' networks to enable **disruption or destruction of critical services** in the event of increased geopolitical tensions and/or military conflict with the United States and its allies. This is a critical business risk for every organization in the United States and allied countries.[2]

The advisory provides detailed information related to the groups' activity and describes how the group has successfully compromised U.S. organizations, especially in the Communications, Energy, Transportation Systems, and Water and Wastewater Systems Sectors.[3] The authoring organizations urge critical infrastructure owners and operators to review the advisory for defensive actions against this threat and its potential impacts to national security.

CISA and partners[4] are releasing this fact sheet to provide leaders of critical infrastructure entities with guidance to help prioritize the protection of critical infrastructure and functions. The authoring agencies urge leaders to recognize cyber risk as a core business risk. This recognition is both necessary for good governance and fundamental to national security.

[1] U.S. Department of Energy (DOE), U.S. Environmental Protection Agency (EPA), U.S. Transportation Security Administration (TSA), Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Canadian Communications Security Establishment's (CSE's) Canadian Centre for Cyber Security (CCCS), United Kingdom National Cyber Security Centre (NCSC-UK), and New Zealand National Cyber Security Centre (NCSC-NZ)

[2] CCCS assesses that Canada would likely be affected as well, due to cross-border integration. ASD's ACSC and NCSC-NZ assess Australian and New Zealand critical infrastructure, respectively, could be vulnerable to similar activity from PRC state-sponsored actors.

[3] See Critical Infrastructure Sectors | CISA for descriptions of critical infrastructure sectors.

[4] NSA, FBI, DOE, EPA, TSA, U.S. Department of the Treasury, ASD's ACSC, CCCS, NCSC-UK, and NCSC-NZ

ACTIONS FOR LEADERS

Make Informed and Proactive Resourcing Decisions

Empower cybersecurity teams to make informed resourcing decisions to better detect and defend against Volt Typhoon and other malicious cyber activity. As a first step, organizations should use intelligence-informed prioritization tools, such as the Cybersecurity Performance Goals (CPGs) or derived guidance from an SRMA. The CPGs help leaders make strategic investments in a limited number of essential actions with high-impact security outcomes. Second, empower and resource cybersecurity teams so they can:

- **Effectively apply detection and hardening best practices** contained in Identifying and Mitigating Living off the Land Techniques and PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Volt Typhoon does not rely on malware to maintain access to networks and conduct their activity. Rather, they use built-in functions of a system. This technique, known as "living off the land," enables them to easily evade detection. To protect against living off the land, organizations need a comprehensive and multifaceted approach, as described in these joint products.

> Key best practices for your cybersecurity teams includes **ensuring logging, including for access and security, is turned on for applications and systems and logs are stored in a central system**. Robust logging is necessary for detecting and mitigating living off the land. Ask your IT teams which logs they maintain as certain logs reveal commands (referenced in the CSA) used by Volt Typhoon actors. If your IT teams do not have the relevant logs, ask which resources they may need to effectively detect compromise.

- **Receive continuous cybersecurity training and skill development** that is relevant to the threat environment. Continuous training ensures that staff have the capabilities needed to defend their unique environments and maintain good cyber hygiene.
- **Develop comprehensive information security plans and conduct regular tabletop exercises**.
    - Leaders should ensure personnel from all business sections, including executive leadership, are involved in development of the plan, sign off on it, and are aware of their roles and responsibilities. Ensuring comprehensive and tested plans are in place and approved enables cybersecurity teams to make appropriate risk-informed decisions.
    - Refresh and test plans on an appropriate basis, and test OT systems and manual mode.

For smaller organizations without their own in-house cybersecurity teams, leaders should obtain managed security services that can carry out this guidance to maintain sufficient cybersecurity posture.

Secure Your Supply Chain

Ensure effective risk management policies are in place to minimize the likelihood of damage resulting from a compromise.

- **Establish strong vendor risk management** processes to evaluate and monitor third-party risks, ensuring that suppliers and partners adhere to strict security standards and any foreign ownership, control, or influence (FOCI) are clearly identified and managed, including consideration of, for example, the U.S. Department of Commerce Entities List and Unverified List.
- **Ensure those responsible for procurement:**
    - **Exercise due diligence** when selecting software, devices, cloud service providers (CSPs), and managed service providers (MSPs).
        - **Use guidance including the secure by design principles to help inform vendor selection** to reduce the availability of attack pathways threat actors can leverage. Follow best practices for supply chain risk management and only source from reputable vendors.
        - **Ensure that the vendor has a patching plan** in place that supports your organization and that you can also support.

- **Identify and limit usage of any products** that break the principle of least privilege, do not clearly enumerate needed access, or require disabling antivirus tools.
- **Select vendors** that enable interoperability as a best practice for resilience and to avoid vendor lock-in.

As a leader, advocate for vendors to deliver secure and resilient systems and support staff efforts to integrate Secure by Design principles into procurement/vendor contracting processes, including mechanisms for ensuring compliance and patching. Additionally, direct software development teams to integrate the Secure Software Development Framework (SSDF) throughout your existing practices. Visit our webpage for more on Secure by Design.

Drive a Cybersecurity Culture

Ensure performance management outcomes are aligned to the cyber goals of the organization by:

- **Encouraging collaboration between IT, OT, cloud, cybersecurity, supply chain, and business units** to align security measures with business objectives and risk management strategies.
- **Championing organizational cybersecurity risk assessments and audits** to identify vulnerabilities and gaps in the security posture.
- **Engaging with external cybersecurity experts and advisors for independent assessments** and guidance tailored to your organization and performing GAP analysis on findings.
- **Increasing awareness of social engineering tactics** and facilitating a culture which encourages incident reporting.[5]

INCIDENT RESPONSE

If your organization is impacted by an incident or suspected incident:

- Implement your cyber incident response plan. See the joint cybersecurity advisory by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom on Technical Approaches to Uncovering and Remediating Malicious Activity for incident response best practices.
- Review and update your cyber incident response plans on a regular basis.
- Report incidents or anomalous activity immediately to an authoring agency (see the Contact Information section).
- Consider entering into a proactive retainer agreement with a reputable third-party cybersecurity organization to provide subject matter expertise and incident response services.

CONTACT INFORMATION

U.S. Organizations

- CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870 or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. CISA provides timely situational awareness and enables coordination with Sector Risk Management Agencies such as EPA, TSA, and Treasury.
- For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.
- Entities subject to regulatory requirements should follow established reporting requirements, as appropriate.

Australian Organizations

Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

[5] Avoiding Social Engineering and Phishing Attacks | CISA; Social engineering – ITSAP.00.166 - Canadian Centre for Cyber Security; https://www.cyber.gc.ca/en/guidance/how-protect-your-organization-insider-threats-itsap10003-0

Canadian Organizations

Report incidents by emailing CCCS at contact@cyber.gc.ca.

New Zealand Organizations

Report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

United Kingdom Organizations

Report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

RESOURCES

- Refer to CISA's Logging Made Easy page for free centralized log management solutions.
- Refer to CISA's Cyber Essentials for additional recommendations on managing cybersecurity risks.
- See CCCS's Cyber Hygiene publication for best practices for your organization.
- See Questions Every CEO Should Ask About Cyber Risks for additional best practices to help companies understand their risks and prepare for cyber threats.
- See CISA Director Jen Easterly's opening statement on Volt Typhoon before the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party.
- See CISA's Recommended Cybersecurity Best Practices for Industrial Control Systems for more guidance specific to organizations supporting U.S. critical infrastructure.
- See CISA's Cyber Resilience Review webpage for more information on CISA's no-cost, non-technical assessment to help organizations evaluate their operational resilience and cybersecurity practices.
- See CISA's Fact Sheet Rising Ransomware Threats to Operational Technology Assets for more information on reducing the vulnerability to severe business degradation if affected by malicious cyber activity. Although tailored to ransomware, the Fact Sheet has applicable guidance for other cyber threats.
- See EPA Cybersecurity for the Water Sector | US EPA for free cybersecurity assessments, training, funding and additional resources tailored to support drinking water and wastewater entities.

ACKNOWLEDGEMENTS

Cisco Talos, NTT Corporation, Google, Mandiant, and Sophos contributed to this fact sheet.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.