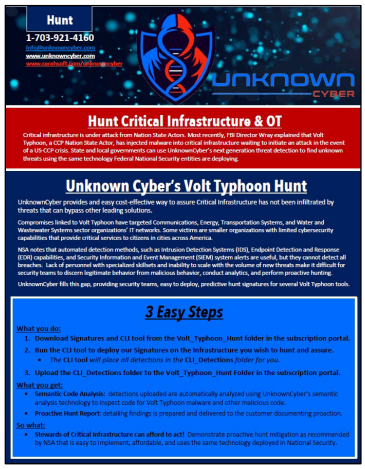

Hunt Critical Infrastructure and OT

Thank you for downloading this UnknownCyber product brief. Carahsoft is the distributor for UnknownCyber Cybersecurity solutions available via NASA SEWP V, NASPO, ITES, and other contract vehicles.

To learn how to take the next step toward acquiring UnknownCyber's solutions, please check out the following resources and information:

For additional resources:
carah.io/unknowncyber-resources

For upcoming events:
carah.io/unknowncyber-events

For additional UnknownCyber solutions:
carah.io/unknowncyber-solutions

For additional Cybersecurity solutions:
carah.io/cybersecuritysolutions

To set up a meeting:
unknowncyber@carahsoft.com
703-921-4160

To purchase, check out the contract vehicles available for procurement:
carah.io/unknowncyber-contracts

Hunt

1-703-921-4160
Info@unknowncyber.com
www.unknowncyber.com
www.carahsoft.com/unknowncyber

Hunt Critical Infrastructure & OT

Critical infrastructure is under attack from Nation State Actors. Most recently, FBI Director Wray explained that Volt Typhoon, a CCP Nation State Actor, has injected malware into critical infrastructure waiting to initiate an attack in the event of a US-CCP crisis. State and local governments can use UnknownCyber's next generation threat detection to find unknown threats using the same technology Federal National Security entities are deploying.

Unknown Cyber's Volt Typhoon Hunt

UnknownCyber provides and easy cost-effective way to assure Critical Infrastructure has not been infiltrated by threats that can bypass other leading solutions.

Compromises linked to Volt Typhoon have targeted Communications, Energy, Transportation Systems, and Water and Wastewater Systems sector organizations' IT networks. Some victims are smaller organizations with limited cybersecurity capabilities that provide critical services to citizens in cities across America.

NSA notes that automated detection methods, such as Intrusion Detection Systems (IDS), Endpoint Detection and Response (EDR) capabilities, and Security Information and Event Management (SIEM) system alerts are useful, but they cannot detect all breaches. Lack of personnel with specialized skillsets and inability to scale with the volume of new threats make it difficult for security teams to discern legitimate behavior from malicious behavior, conduct analytics, and perform proactive hunting.

UnknownCyber fills this gap, providing security teams, easy to deploy, predictive hunt signatures for several Volt Typhoon tools.

3 Easy Steps

What you do:

1. **Download Signatures and CLI tool from the Volt_Typhoon_Hunt folder in the subscription portal.**
2. **Run the CLI tool to deploy our Signatures on the Infrastructure you wish to hunt and assure.**
   - *The* **CLI tool** *will place all detections in the* **CLI_Detections** *folder for you.*
3. **Upload the CLI_Detections folder to the Volt_Typhoon_Hunt Folder in the subscription portal.**

What you get:

- **Semantic Code Analysis:** detections uploaded are automatically analyzed using UnknownCyber's semantic analysis technology to inspect code for Volt Typhoon malware and other malicious code.
- **Proactive Hunt Report**: detailing findings is prepared and delivered to the customer documenting proaction.

So what:

- **Stewards of Critical Infrastructure can afford to act!** Demonstrate proactive hunt mitigation as recommended by NSA that is easy to implement, affordable, and uses the same technology deployed in National Security.