THREAT MITIGATION FOR OPERATIONAL TECHNOLOGY AND CONTROL SYSTEMS

Jon Huddleston, Defense Critical Infrastructure and Operational Technology Program Manager
Headquarters U.S. Army Corps of Engineers (HQUSACE)

Federal Facilities Council
Standing Committee on Cyber and Physical Security and Hazard Mitigation

U.S. ARMY

US Army Corps of Engineers®

ADVERSARIAL TARGETING OF OT/CS SYSTEM

Adversaries demonstrate capabilities and intent of targeting Operational Technology (OT) and Control Systems (CS) through cyber means to impact physical processes

- This presents risk to mission readiness, production, and safety.

OT/CS Attacks

Volt Typhoon Threat Group

Joint CISA Alert-State Sponsored Compromise and Persistent across US. Critical Infrastructure

22 Danish Power Organizations (SektorCert) breached in 2023

Required shift to local control

6 Hours and 230k people

Time Ukraine lost power due to Cyberattack

$5M

Paid in ransom by Colonial Pipeline

JOINT CISA ALERT ON VOLT TYPHOON

Volt Typhoon actors tailor their TTPs to the victim environment; however, the U.S. authoring agencies have observed the actors typically following the same pattern of behavior across identified intrusions. Their choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable the disruption of OT functions across multiple critical infrastructure sectors (see Figure 1).

1. **Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization's network architecture and operational protocols.**

2. **Volt Typhoon typically gains initial access to the IT network by exploiting known or zero-day vulnerabilities in public-facing network appliances**

3. **Volt Typhoon aims to obtain administrator credentials within the network, often by exploiting privilege escalation vulnerabilities in the operating system or network services.**

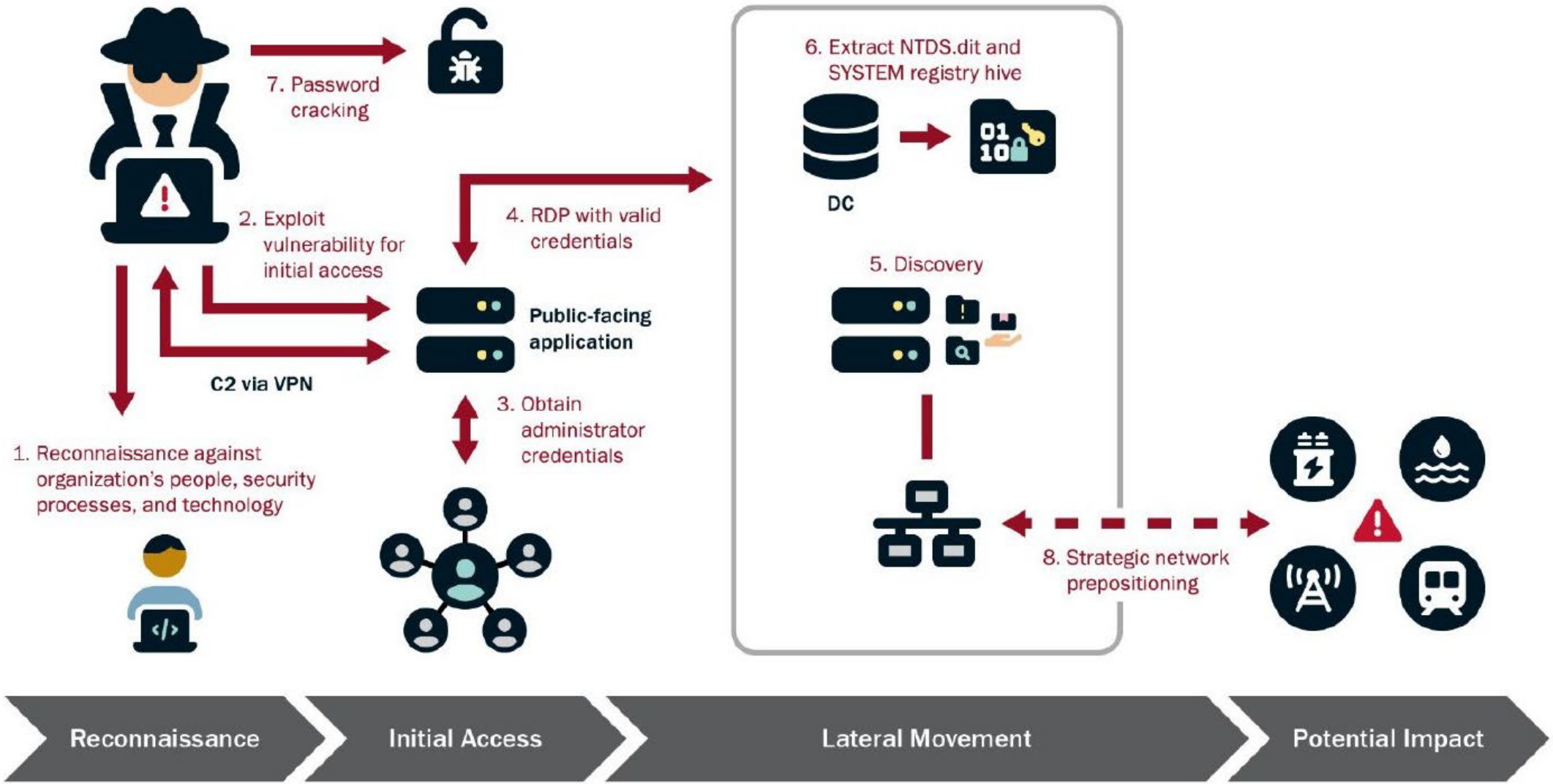


Figure 1: Typical Volt Typhoon Activity

TLP:CLEAR

4. **Volt Typhoon uses valid administrator credentials to move laterally to the domain controller (DC) and other devices via remote access services such as Remote Desktop Protocol (RDP).**

5. **Volt Typhoon conducts discovery in the victim's network, leveraging Living Off The Land (LOTL) binaries for stealth**.

6. **Volt Typhoon achieves full domain compromise by extracting the Active Directory database (`NTDS.dit`) from the DC.**

7. **Volt Typhoon likely uses offline password cracking techniques to decipher these hashes.**

8. **Volt Typhoon uses elevated credentials for strategic network infiltration and additional discovery, often focusing on gaining capabilities to access OT assets.**

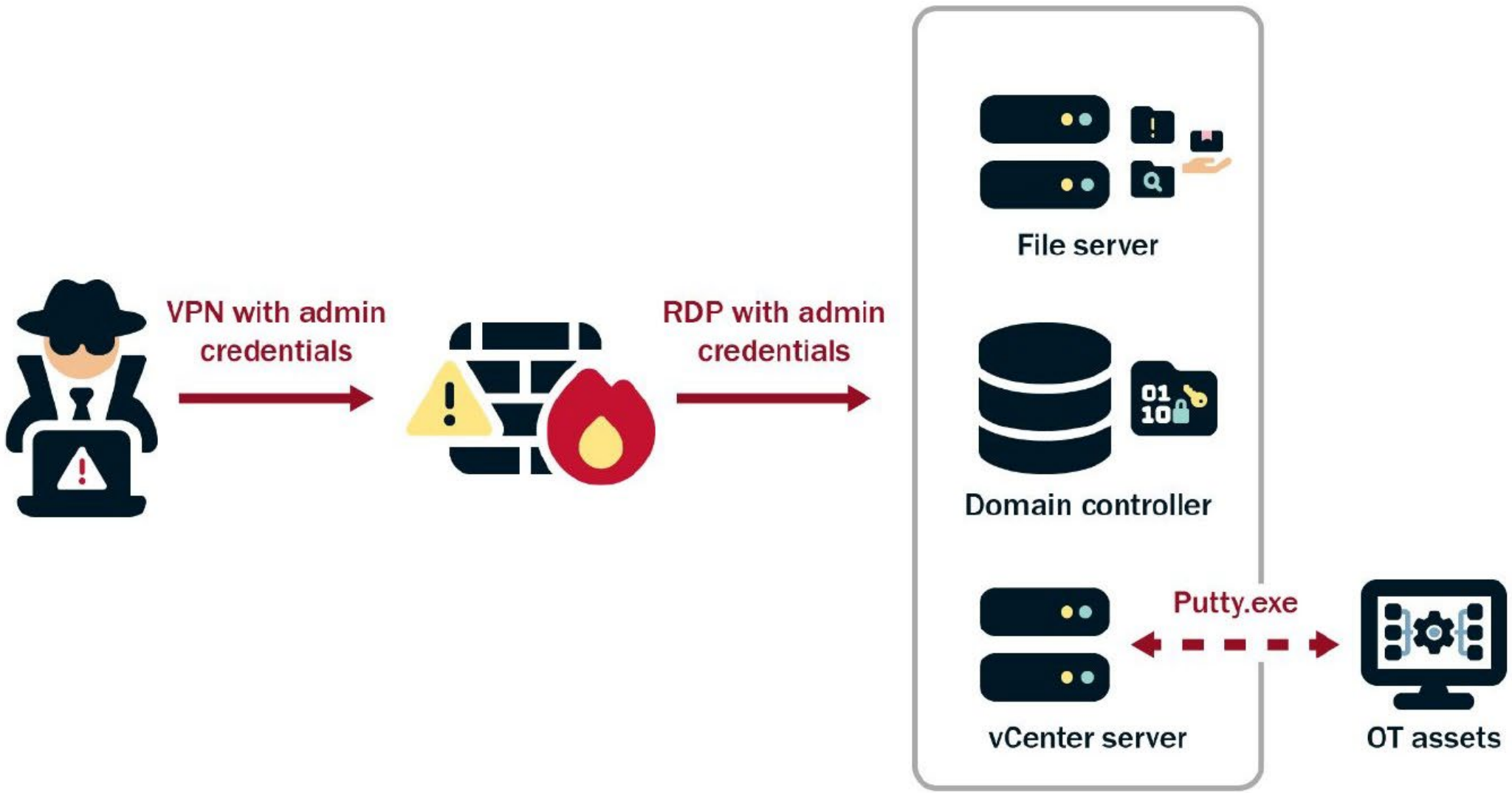


Figure 2: Volt Typhoon Lateral Movement Path File Server, DC, and OT-Adjacent Assets

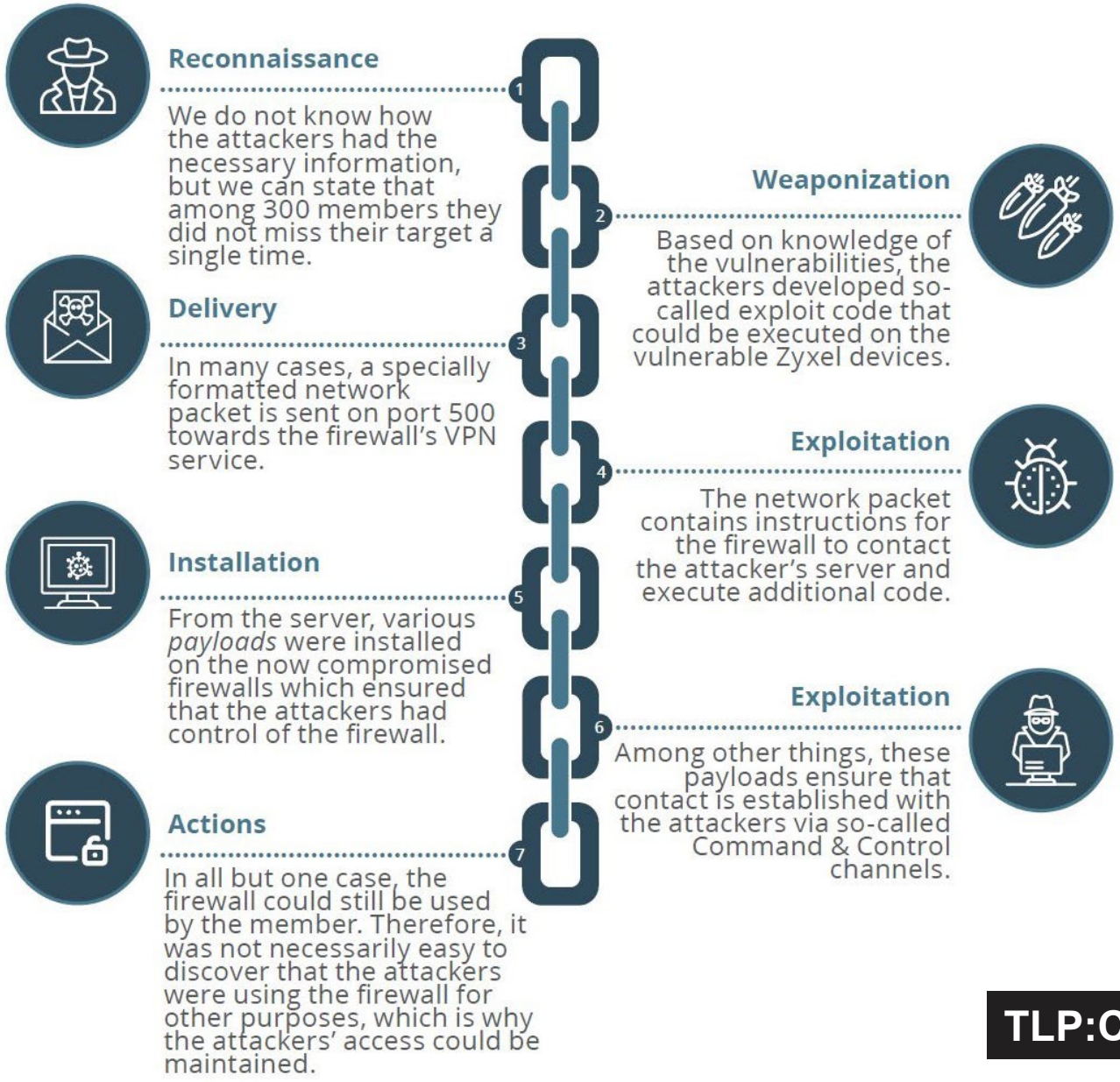
JOINT CISA ALERT MITIGATIONS

- Harden the Attack Surface
- Secure Credentials
- Secure Accounts
- Secure Remote Access Services
- Secure Sensitive Data
- Implement Network Segmentation
- Secure Cloud Assets
- Be Prepared

2023 DANISH POWER SEKTORCert ANALYSIS

Largest cyber attack against Danish Critical Infrastructure. Power sector targeted. Initial access predominantly gained through exploitation of Firewall Vulnerability (Zyxel). Two zero days used and one recently released vulnerability.

Timeline
11MAY2023 11 companies were compromised using recently released vulnerabilities.
22MAY2023 Second wave of attacks (12-13)
23MAY2023 Continued attacks
24MAY2023 Continued attacks (15-20)
25MAY2023 Continued attacks (21,22)
30MAY2023 Attacks Suppressed. 200K attack attempts were detected.



TLP:CLEAR

SEKTORCert Recommendation Highlights

1. **Firewall**
   Firewall is implemented and kept up to date - preferably with geo-blocking of countries not needed to receive traffic from.
2. **Exposure of services**
   Only absolutely necessary services are exposed to the Internet.
3. **Endpoint protection**
   Endpoint protection and firewall enabled and updated on all systems.
4. **Backup**
   Backup is present (including off-site backup) and restore is tested regularly.
5. **Password length**
   Passwords are designed according to current standards - i.e. rather very long passwords that are changed rarely than shorter passwords that are changed frequently.
6. **No password reuse**
   No password reuse across IT and OT.
7. **No shared logins and default passwords**
   No common login and no default passwords.

8 **Remove inactive users**
User accounts that are not used are removed or disabled.

9 **Multifactor validation**
All services with login exposed to the Internet are secured with multifactor validation and remote access is limited as much as possible.

10 **Update**
The systems are kept up to date / patched - including third-party software.

11 **Identify outdated systems**
Vulnerable systems that cannot be patched (end-of-life e.g.) are identified and appropriate countermeasures are implemented to protect them.

12 **Contingency plan**
A contingency plan is drawn up and maintained.

13 **Log collection**
Monitoring / logging implemented so that attacks can be detected and responded to in a timely manner - e.g. via EnergiCERT sensors, honeypots on the OT network and extended, internal monitoring.

ENERGI CERT

14 Awareness
Awareness training of employees is conducted on an ongoing basis to ensure focus on OT and IT security.

15 Map network entries
All network entries to the production network are mapped.

16 Segmentation
The network is segmented into several layers - at least so that OT is separated from IT. Consider further isolation or segmentation to contain or limit the potential of an incident.

17 Identify devices
All units in the production environment are identified and documented.

18 Documentation
Both logical and physical documentation of the architecture is produced.

19 Limit rights
Limiting rights on user accounts - special focus on limiting administrative rights for users when not necessary.

20 Access policy
Policy on access to the production network is established.

21 **Policy for changes**
Policy for changes to the digital part of the production network is established.

22 **Vendor management**
Vendor management policy, including how to verify that vendors meet your security requirements, is established.

23 **Alternative communication channels**
Alternative communication methods, e.g. satellite phone or SINE radio to complement e-mail and telephone, are established.

24 **Emergency procedures**
Emergency procedures for all business-critical processes are drawn up so that the function can be performed in the event of prolonged IT outages, including a plan for operation in island mode.

25 **Vulnerability Scans**
Ongoing vulnerability scans and possibly penetration tests are conducted to provide an overview of the attack surface towards the Internet.

ENERGI CERT

SOURCES AND REFERENCES

- *Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems (ICS)*, US Cyber Command, https://apps.dtic.mil/sti/citations/AD1056116

- *Guide to Industrial Control Systems (ICS) Security*. SP 800-82, rev. 3., NIST (National Institute of Standards and Technology), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

- *Identifying and Mitigating Living Off the Land Techniques*, Joint Publication led by DHS CISA multiple co-authors, https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques

- *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Joint Publication led by DHS CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

- *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*, Joint Publication led by DHS CISA multiple co-authors, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

- The attack against Danish, critical infrastructure, SEKTORCert, https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf
  - SEKTORCert Handbook on Threat Assessments, https://sektorcert.dk/wp-content/uploads/2022/10/EnergiCERT-Handbook-on-Threat-Assessments-v1-.pdf

- *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure,* Joint Publication led by DHS CISA multiple co-authors, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a

Questions?

Backup Slides

JOINT CISA ALERT ON VOLT TYPHOON

Volt Typhoon actors tailor their TTPs to the victim environment; however, the U.S. authoring agencies have observed the actors typically following the same pattern of behavior across identified intrusions. Their choice of targets and pattern of behavior is not consistent with traditional cyber espionage or intelligence gathering operations, and the U.S. authoring agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves on IT networks to enable the disruption of OT functions across multiple critical infrastructure sectors (see Figure 1).

1. **Volt Typhoon conducts extensive pre-compromise reconnaissance to learn about the target organization's network architecture and operational protocols.** This reconnaissance includes identifying network topologies, security measures, typical user behaviors, and key network and IT staff. The intelligence gathered by Volt Typhoon actors is likely leveraged to enhance their operational security. For example, in some instances, Volt Typhoon actors may have abstained from using compromised credentials outside of normal working hours to avoid triggering security alerts on abnormal account activities.
2. **Volt Typhoon typically gains initial access to the IT network by exploiting known or zero-day vulnerabilities in public-facing network** appliances (e.g., routers, virtual private networks [VPNs], and firewalls) and then connects to the victim's network via VPN for follow-on activities.
3. **Volt Typhoon aims to obtain administrator credentials within the network, often by exploiting privilege escalation vulnerabilities in the operating system or network services.** In some cases, Volt Typhoon has obtained credentials insecurely stored on a public-facing network appliance.

4. **Volt Typhoon uses valid administrator credentials to move laterally to the domain controller (DC) and other devices** via remote access services such as Remote Desktop Protocol (RDP).
5. **Volt Typhoon conducts discovery in the victim's network, leveraging LOTL binaries for stealth**. A key tactic includes using PowerShell to perform targeted queries on Windows event logs, focusing on specific users and periods. These queries facilitate the discreet extraction of security event logs into `.dat` files, allowing Volt Typhoon actors to gather critical information while minimizing detection. This strategy, blending in-depth pre-compromise reconnaissance with meticulous post-exploitation intelligence collection, underscores their sophisticated and strategic approach to cyber operations.
6. **Volt Typhoon achieves full domain compromise by extracting the Active Directory database (`NTDS.dit`) from the DC.** Volt Typhoon frequently employs the Volume Shadow Copy Service (VSS) using command-line utilities such as `vssadmin` to access `NTDS.dit`. The `NTDS.dit` file is a centralized repository that contains critical Active Directory data, including user accounts, passwords (in hashed form), and other sensitive data, which can be leveraged for further exploitation. This method entails the creation of a shadow copy—a point-in-time snapshot—of the volume hosting the `NTDS.dit` file. By leveraging this snapshot, Volt Typhoon actors effectively bypass the file locking mechanisms inherent in a live Windows environment, which typically prevent direct access to the `NTDS.dit` file while the domain controller is operational.
7. **Volt Typhoon likely uses offline password cracking techniques to decipher these hashes.** This process involves extracting the hashes from the `NTDS.dit` file and then applying various password cracking methods, such as brute force attacks, dictionary attacks, or more sophisticated techniques like rainbow tables to uncover the plaintext passwords. The successful decryption of these passwords allows Volt Typhoon actors to obtain elevated access and further infiltrate and manipulate the network.

8. **Volt Typhoon uses elevated credentials for strategic network infiltration and additional discovery, often focusing on gaining capabilities to access OT assets.** Volt Typhoon actors have been observed testing access to domain-joint OT assets using default OT vendor credentials, and in certain instances, they have possessed the capability to access OT systems whose credentials were compromised via `NTDS.dit` theft. This access enables potential disruptions, such as manipulating heating, ventilation, and air conditioning (HVAC) systems in server rooms or disrupting critical energy and water controls, leading to significant infrastructure failures (in some cases, Volt Typhoon actors had the capability to access camera surveillance systems at critical infrastructure facilities). In one confirmed compromise, Volt Typhoon actors moved laterally to a control system and were positioned to move to a second control system.