corelight

THE CASE FOR NETWORK DETECTION & RESPONSE

A SOC analyst's guide for combating Volt Typhoon attacks

UNDERSTANDING **VOLT TYPHOON**

Over the past year, several sophisticated cyber-espionage campaigns have grabbed the attention of our industry and challenged defenders and vendors alike with advanced tactics, techniques, and procedures (TTPs). One of the most visible campaigns is Volt Typhoon, named by the Microsoft threat intelligence team in May 2023 and attributed to Chinese state-sponsored threat actors.

Volt Typhoon primarily targets critical infrastructure organizations in the United States, focusing on sectors like telecommunications, manufacturing, and transportation. The campaign is notable for its stealthy approach, leveraging "living-off-the-land" (LOTL) techniques—using legitimate network administration tools to avoid detection—and it is believed to be part of a broader effort to to establish footholds into critical infrastructure for political-driven future disruptions.

Targets

Critical Infrastructure:

- Energy
- Communications
- Transportation
- Water
- Also manufacturing, utility, construction, maritime, government, and education sectors

Tactics

- Low and slow
- Persistence and stealth (log deletion)
- Living-off-the-land (LOTL) minimal use of malware, but not none
- Network equipment vulnerabilities in older systems

Strategy

- Initial access on VPNs and firewalls
- Target low maturity organizations
- Interested in OT networks

Goals

- Positioning for future access and disruption attacks
- Limited data exfil

Other Typhoon attacks

Salt Typhoon is another advanced persistent threat actor operated by China's Ministry of State Security (MSS), targeting telecommunications providers. The group's operations place an emphasis on counterintelligence targets in the United States and data theft of key corporate intellectual property. The group has infiltrated targets in dozens of other countries on nearly every continent. The TTPs for many of these campaigns overlap and include similar themes: initial compromise through internet-facing network devices, persistence and discovery utilizing LOTL tools and approaches, the use of VPN for covert tunneling and C2, and exfiltration over known web and cloud services.

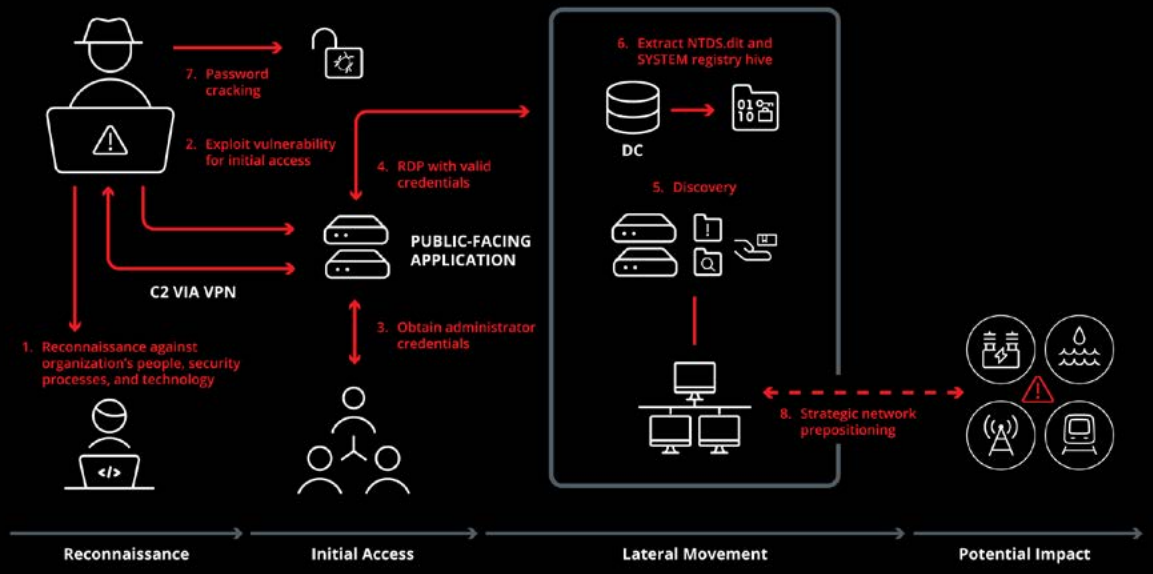
UNDERSTANDING **VOLT TYPHOON**

Volt Typhoon's TTPs begin with initial access through compromised internet-facing devices (as outlined in the **CISA Joint Cybersecurity Advisory**). The threat actors typically exploit vulnerabilities in routers, firewalls, and other network devices to gain an initial foothold. The specific devices targeted include a variety of Small Office/Home Office (SOHO) routers and devices from some of the most commonly used manufacturers like Asus, Netgear, and Zyxel. These devices provide excellent entry points for attackers because they are frequently outside of the scope of common security visibility and monitoring tools and are rarely updated.

Once inside, the attackers employ LOTL techniques, which involve using legitimate network tools and scripts to discover additional targets and to move laterally within the network while avoiding detection by conventional security systems. The group uses built-in Windows tools, such as PowerShell and Windows Management Instrumentation (WMI), to execute those commands and scripts, minimizing the use of malware that might be flagged by security solutions. They also leverage credential-dumping tools to harvest user credentials, enabling further access to sensitive systems.

1. Pre-compromise research on people, network architecture, or operations
2. Gain initial access from 0-day or known exploits
3. Obtain admin credentials
4. Use valid creds to RDP to AD to identify users and obtain credentials
5. Conduct discovery using LOTL techniques
6. Extract & exfil AD database from DC
7. Decipher AD database hashes
8. Use elevated credentials for strategic infiltration, focus on OT assets

Source: CISA Cybersecurity Advisory: AA24-038A



THE NETWORK IS **A CRUCIAL DEFENSE COMPONENT**

Many of the initial exploits targeted unmanaged or unmanageable devices where EDR cannot provide coverage. A critical component of a defense-in-depth approach against advanced adversaries is employing a **comprehensive network visibility and detection strategy.**

This involves monitoring network traffic patterns, employing network-based detections, and ensuring that security teams have the data to observe and track the behavior of their enterprise's myriad network-connected devices, particularly those that traditionally fall outside the purview of standard EDR solutions.

This recommendation is reinforced by **a recent CISA report** that evaluated a red team engagement against a critical infrastructure customer. The first "lesson learned" spells out that ***"The organization relied too heavily on host-based endpoint detection and response (EDR) solutions and did not implement sufficient network layer protections."***

In order to stop these advanced adversaries from compromising our most important networks, we must invest in the appropriate network monitoring tools to identify and contain these threats.

> ***The critical way to detect and disrupt Volt Typhoon is with the high visibility you only get from the network.***

ROB JOYCE, Corelight Advisor
Former NSA Cybersecurity Director

ENDPOINT DETECTION & RESPONSE **IS NOT ENOUGH**

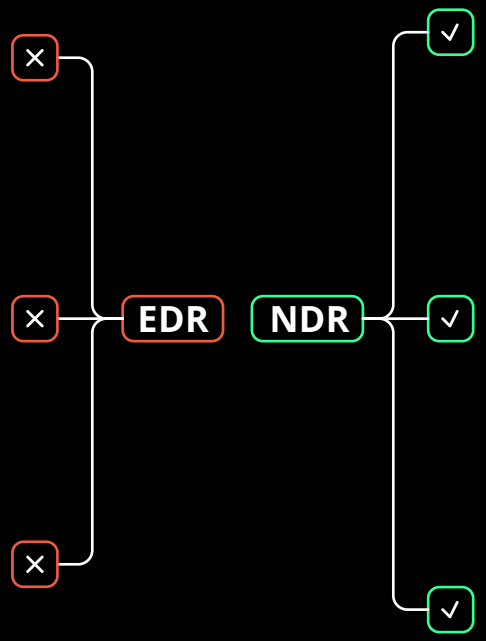
One of the biggest takeaways from initial Volt Typhoon reports and subsequent campaigns is that endpoint detection and response (EDR) is simply not sufficient for detecting and stopping attacks from advanced adversaries. The **Crowdstrike 2025 Global Threat Report** underscores this point: *"Unmanaged network appliances—particularly edge gateway devices—remained the most routinely observed initial access vector for exploitation."* Often, these devices are not covered by traditional EDR and in many cases are not even being tracked by the security team. Network visibility and detection are critical to closing security gaps being actively exploited by state-sponsored threat actors and effectively controlling the risks associated with these advanced attack campaigns.

EDR shortcoming

Endpoint agents can be misconfigured, go out of date, or not be installed.

EDR can be disabled or bypassed by attackers using legitimate processes or credentials, leaving it blind.

EDR struggles to see unmanaged assets.



Corelight solution

Corelight provides broad network visibility, complementing EDR by detecting threats that bypass endpoint defenses. This enables the detection of novel and previously unknown attacks through high-fidelity security data.

Corelight collects and analyzes rich contextual data and applies a multi-layered detection strategy to deliver prioritized, aggregated alerts. This strategy combines machine learning, behavioral analytics, curated signatures, and threat intelligence, reducing alert fatigue.

Corelight asset fingerprinting capability can analyze internal and external hosts, deriving context from Zeek® logs and delivering visibility into unmanaged assets.

3 TACTICS **TO SHIELD YOUR ORGANIZATION**

1

Build cyber resilience

- Patch and address known vulnerabilities before they become targets
- Monitor the use of outdated or obsolete cipher suites
- Monitor and disable any unnecessary, unused, exploitable, or plaintext services

2

Implement network monitoring & threat detection

- Implement strong network monitoring and visibility
- Monitor all devices that accept external connections and validate security posture using network data
- Establish a baseline of normal network behavior and alert on abnormal behavior

3

Enact people & process guidelines

- Maintain a variety of technical controls (EDR is not sufficient)
- Implement continuous training, support, and resources to maintain secure configurations and detect malicious activity
- Don't minimize the business risk of a cybersecurity attack

The Volt Typhoon campaign is a stark reminder of the evolving landscape of cyber threats, in which advanced, often state-sponsored adversaries continuously refine their tactics to evade detection and achieve their objectives. Guidance from CISA and others highlights the importance of a comprehensive cybersecurity strategy that extends **beyond traditional EDR.**

Corelight develops powerful network data and detections, focused around our **Open NDR Platform** with Zeek at its core. We believe that a vital aspect of defending against attacks is to have the most comprehensive and industry-leading data in your SOC team's hands. Combining metadata and a full detection suite with behavioral, signature, and machine learning capabilities, as well as packet capture (PCAP) and file analysis (YARA), the Corelight Platform enables you to address the gaps between your existing tools, and ultimately reduce the risk to your organization.

While we can't know exactly what the next campaign will look like, we do know that the power of Corelight's data and our Open NDR approach—which builds on the "strength in numbers" community of defenders—will be instrumental in identifying the IOCs and detecting the components, regardless of the origin and motivations of the attack.

CORELIGHT'S **MULTI-LAYERED DETECTION STRATEGY**

Corelight's high-fidelity security data fuels proactive threat hunting, enabling the detection of novel and previously unknown attacks that can bypass endpoint defenses.

Corelight collects and analyzes rich contextual data and applies a multi-layered detection strategy that fuses machine learning, behavioral analytics, curated signatures, and threat intelligence to deliver prioritized aggregated alerts based on risk and expert-tuned detections without relying on any single method resulting in reduced alert fatigue. Using machine learning, heuristics, and anomaly detection, Corelight uncovers unknown attacks, lateral movement, and stealthy adversary techniques without relying on pre-defined indicators.

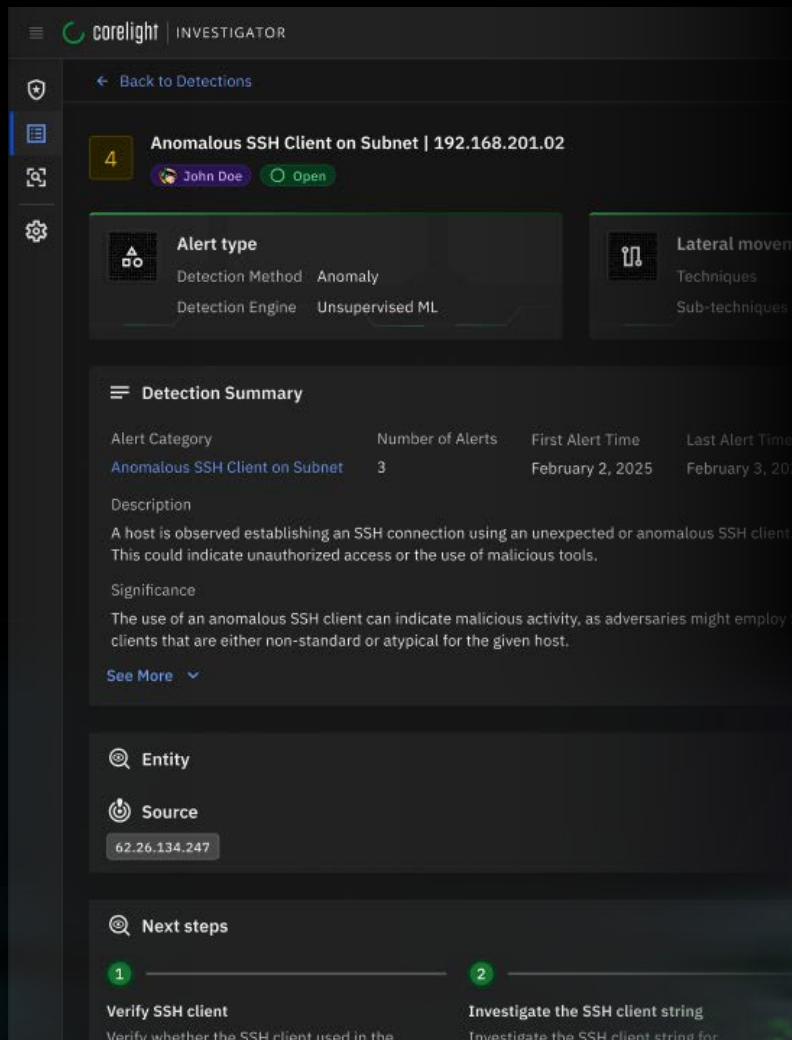
Some of the most interesting non-signature models include:

Supervised ML:

- C2 HTTP Frameworks
- Exfiltration via DNS
- DGA Malware
- Malicious File Download
- Tor Connections
- Discovery via Network Service Scanning
- Malicious SSL Certificate
- ASCII Homograph
- Social Engineering Domain
- Attempted Connection to a DGA Domain
- Domain Combosquatting
- IDN Homograph
- Domain Typosquatting
- NXDomain Beaconing
- DNS Reconnaissance

Unsupervised ML:

- Anomalous Service on Internet Facing Server
- Anomalous SSH Client
- Anomalous Service for Internal Communication
- Anomalous SSH Connection Pair
- Anomalous HTTP User Agent Family



Security teams also benefit from interactive visual timelines, instant raw log access, and native asset context derived from live network traffic—delivering a level of transparency and investigative power that sets Corelight apart in the industry. Moreover, our single-sensor (e.g., Zeek, Suricata, etc.) architecture enhances efficiency, reduces cost, and delivers comprehensive threat protection without the overhead of managing multiple sensors.

CORELIGHT **DETECTION & REMEDIATION**

Corelight's capabilities in detecting unusual network patterns and encryption misuse are highlighted as **essential components in identifying and neutralizing threats** posed by malicious tools. These network tools used by attackers, as highlighted by CISA in the Volt Typhoon campaign, include:

Fast Reverse Proxy (FRP)

- Corelight provides detections for identifying tunnels and unusual encryption that may be used by such proxy tools, including our **Encryption Detection** package (part of our Encrypted Traffic Collection), used to identify proprietary encryption and anomalous use of encryption, and our DNS and ICMP tunnel detection packages in our **Command and Control (C2) Collection**. (These detections are available only for Corelight customers.)
- Attackers have used hard-coded C2 callbacks with the proxy software to ports 8080, 8443, 8043, 8000, and 10443. Use Corelight's connection data to identify unusual patterns related to the use of these ports.
- A specific mention of Zeek® and the GAIT package (developed by Sandia National Labs) appears in this **CISA advisory** as a possible way to identify proxy traffic. The GAIT package can be loaded onto Corelight sensors; however, we have observed that the package's performance requirements are usually a barrier to deployment in enterprise environments.

Impacket & CovalentStealer

- Use Corelight's Windows logs (SMB, DCE/RPC, NTLM, and Kerberos) to monitor suspicious activity that could indicate inappropriate or unauthorized use of administrator accounts, service accounts, or third-party accounts.
- The Corelight Platform integrates YARA for file matching and analysis. A set of YARA rules for Impacket and CovalentStealer appear in **the CISA report**, and can be loaded onto Corelight sensors for alerting when licensed for the YARA feature.
- Corelight's Application Identification package can identify many common types of services and applications destined to major cloud service providers. Exfiltration can also be discovered by examining unexpected **cloud services and related cloud detections.**

Remote administration tools & VPNs

- As part of its **Entity Collection**, Corelight associates known applications, including many remote access and administration tools, with network connections. Corelight customers can quickly identify the use of these tools and hunt for unexpected or anomalous use on their networks.
- Corelight's SSH and RDP inferences packages (part of the **Encrypted Traffic Collection**) provide detailed information about the use of these common management tools, including authentication details, attempts at brute force attacks, identification of file transfers, human interactivity (a human typing), and more. This powerful data (produced through encrypted signal analysis, with no decryption required) allows for quick threat hunting and response.
- Part of CISA's guidance includes monitoring logs for connections from unexpected virtual private servers (VPSs) and VPNs. Corelight provides comprehensive monitoring of VPN usage, identifying over 350+ types of common VPN types and providers as part of the VPN Insights package (built into our **Encrypted Traffic Collection**). By examining the VPN logs as well as the originating location (optionally logged for all network connections), Corelight customers can quickly identify unusual access patterns and providers which could indicate adversary activity.
- Corelight's intel matching can identify M247-associated IP addresses (a questionable service provider) used along with VPN providers (e.g., SurfShark). Customers can look for successful remote logins (e.g., VPN, OWA) for IPs coming from M247- or using SurfShark-registered IP addresses as mentioned in the **CISA advisory**.

info@corelight.com | 888-547-9497

TRUSTED BY