Know Your Enemy: Volt Typhoon

CISA Issues New Advisory on Volt Typhoon

In February 2024, CISA issued a second advisory on the PRC-state-backed Volt-Typhoon (the first was in May 2023). At H2OSeccon, BlastWave led a paneldiscussion with our partner Gray Matter Systems, discussing cyberattacks, witha particular focus on the threats to water systems posed by Volt Typhoon. Thisissue is so pressing that our customers often ask, 'Are they a significant risk toour water system?'

The advisory made one thing very clear: Volt Typhoon has been pre-positioningtheir stolen access and living off the land (LOTL) on IT networks with the goal oflateral movement to OT assets to disrupt functions. Many of the public hacksthat have occurred are believed to be test runs for future coordinated actions.The US agencies are deeply concerned about the potential for Volt Typhoon tobecome active on the networks they are hiding on to support other geopoliticalactivities worldwide, a threat that could have severe implications for watersystem operators and organizations vulnerable to cyber threats.

Tactics, Techniques, and Procedures of Volt Typhoon

Volt Typhoon is known for conducting extensive reconnaissance on the organization and compromising valid accounts by stealing credentials (phishing is a common technique). Once they gain initial access, they conduct in-depth reconnaissance on the target. Through their reconnaissance, they identify the known vulnerabilities on the network (in network elements, OT devices, etc.). They can then optimize their tactics, techniques, and procedures (TTPs) to ensure they can hide (LOTL) and become active when they pounce through lateral movement. The diagram below (Credit CISA) demonstrates typical Volt Typhoon Activity.

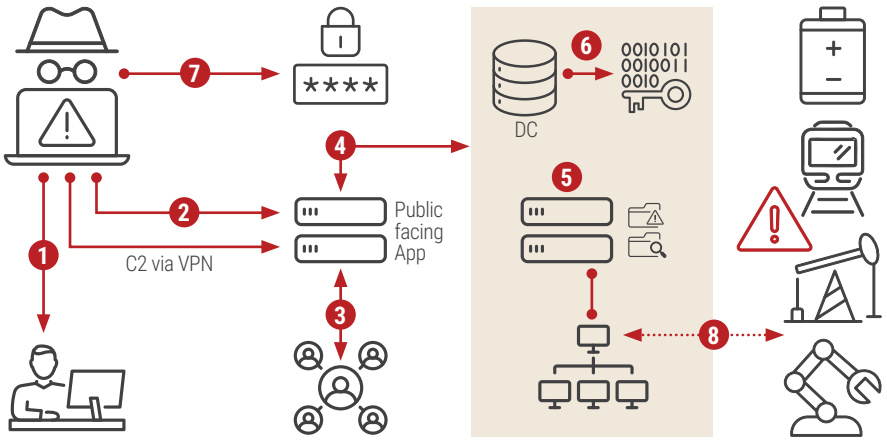
Volt Typhoon's common TTP

Reconnaissance: They can't perform reconnaissance if they can't see your network. You can effectively deter Volt Typhoon's reconnaissance attempts by implementing robust security techniques like Network Cloaking. Volt Typhoon looks for information on the organization, staff, and network (to target phishing or to identify key accounts to attempt to compromise) and its network (to look for known vulnerabilities).

Initial Access: Volt Typhoon is known to exploit publicly available vulnerabilities in network appliances from Fortinet, Ivanti, Netgear, Citrix, and Cisco. Besides the obvious (Don't use these systems for OT Security!), network cloaking and patching these systems is key to preventing these exploits. Protecting your OT network with a different system than your IT network is also advisable in these scenarios, as using the same security system throughout your network creates a fast lane for vulnerability exploitation.

Credential Access: Volt Typhoon is known to obtain credentials from compromised appliances, either stealing credentials insecurely stored on the appliance or extracting the Active Directory Database file and cracking the hashing used to protect passwords offline. Again, the obvious solution is not to use passwords so no credentials can be stolen.

Figure 1 Typical Volt Typhoon Activity



1. **Reconnaissance against organization's people, security processes, and technology**
2. **Exploit vulnerability for initial access**
3. **Obtain Administrator credentials**
4. **RDP with valid credentials**
5. **Discovery**
6. **Extract NTDS.dit and SYSTEM registry hive**
7. **Password cracking**
8. **Strategic network prepositioning**

Let's pause there for a minute. If these three vectors are blocked, then there is NO HACK. The attackers are blocked and can't get into your network. So to recap, stopping Volt Typhoon is as easy as:

1. **Cloak your network**
2. **Separate IT from OT**
3. **Eliminate passwords**

Let's return to the TTPs and take a final look at their techniques.

Lateral Movement: The predominant technique used for lateral movement is compromising administrator credentials to RDP servers. To quote the CISA advisory on a specific attack on the Water and Wastewater sector:

"In one confirmed compromise of a Water and Wastewater Systems Sector entity, after obtaining initial access, Volt Typhoon actors connected to the network via a VPN with administrator credentials they obtained and opened an RDP session with the same credentials to move laterally. Over a nine-month period, they moved laterally to a file server, a domain controller, an Oracle Management Server (OMS), and a VMware vCenter server. The actors obtained domain credentials from the domain controller and performed discovery, collection, and exfiltration on the file server (see the Discovery and Collection and Exfiltration sections). Volt Typhoon's movement to the vCenter server was likely strategic for pre-positioning to OT assets. The vCenter server was adjacent to OT assets, and Volt Typhoon actors were observed interacting with the PuTTY application on the server by enumerating existing stored sessions. With this information, Volt Typhoon potentially had access to a range of critical PuTTY profiles, including those for water treatment plants, water wells, an electrical substation, OT systems, and network security devices. This would enable them to access these critical systems [T1563]."

Credential theft and poor network segmentation enabled the lateral movement. In the worst-case scenario, better Microsegmentation would have helped stop the hackers in their tracks.

From this analysis, you can see that bad actors like Volt Typhoon can be frustrated, and their common techniques are simply blocked from working on your network with the right OT Cybersecurity solution. BlastWave's OT Cybersecurity solutions aim to frustrate and block attackers by protecting your network with a solution optimized for OT.

v20250630

About BlastWave

BlastWave securely connects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks with Zero Trust Protection and delivers industrial-grade cybersecurity with consumer-grade ease-of-use. Visit **www.blastwave.com** to learn more.

1045 Hutchinson Ave.
Palo Alto, CA 94301 USA
T: +1 650 206 8499