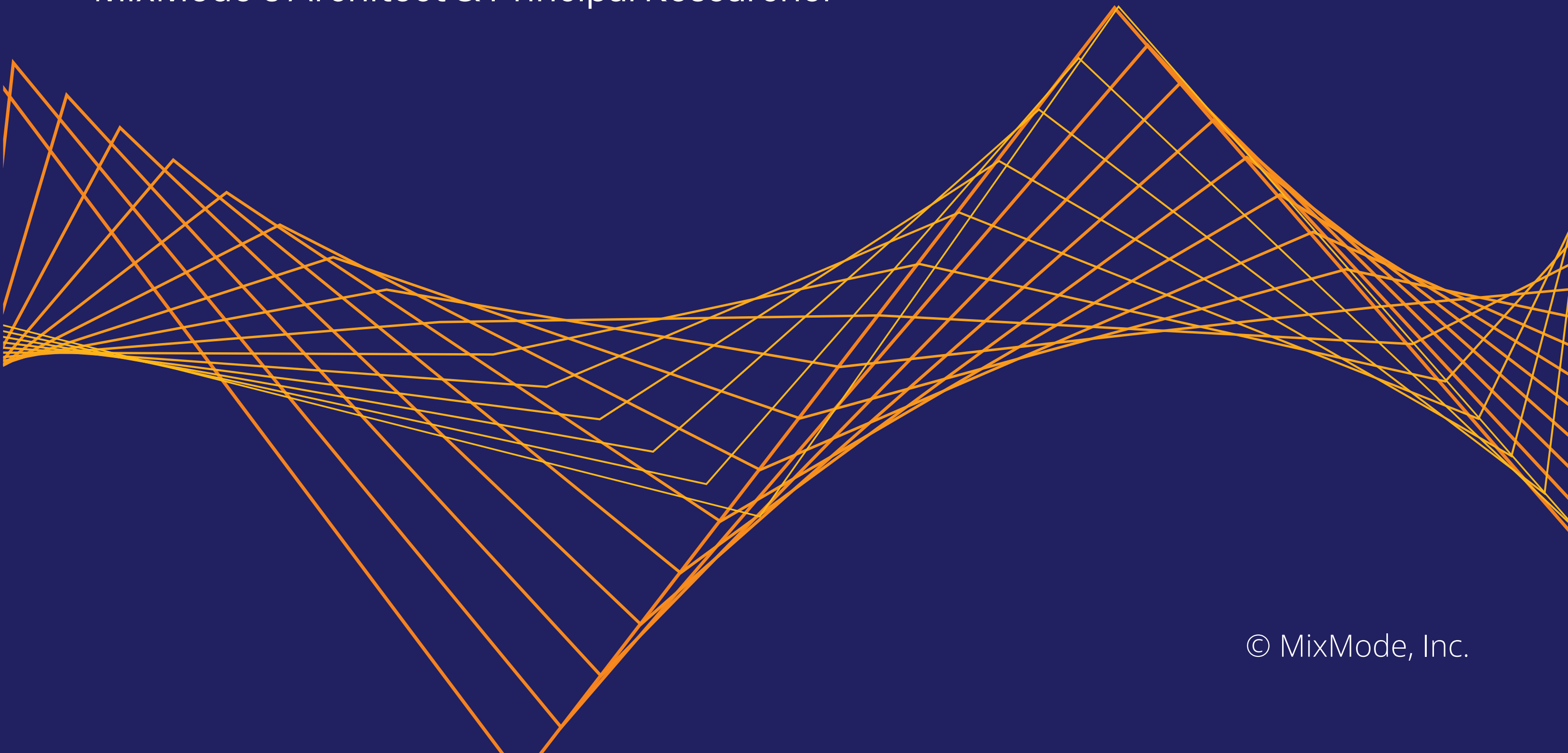
THREAT REPORT

# Volt Typhoon, Salt Typhoon & APT41: This is No Longer a Drill

**Michael Yelland**
MixMode's Architect & Principal Researcher



## China’s current cyber operations lead over the US represents an undeniable direct threat to the security of critical infrastructure and all US citizens.

PRC-sponsored cyber threat groups Volt Typhoon, Salt Typhoon, and APT41 have either already successfully penetrated, or with a nod from Beijing, can immediately penetrate a frightening number of US critical infrastructure defenses.

As outlined by the Cybersecurity and Infrastructure Security Agency (CISA), these critical infrastructure service providers include electricity, water, communications, law enforcement, emergency services, food processing, transportation and banking systems – services which support the safety, public health and security of every US citizen.

To borrow an oft used movie line, “this is no longer a drill.” Critical infrastructure leaders cannot wait for federal, state or local leaders to produce solutions to this ever-present national security danger.

Leadership, planning and execution must come from within to quickly patch and augment systems, drastically improve internal controls and cut red tape preventing the deployment of new technologies proven to detect advanced persistent threats.

## State of Current Critical Infrastructure Cyber Defenses

Technology innovation within the cyber defense industry has lagged behind the speed and scale of technology innovations being used by our cyber adversaries. This technology gap has been readily exploited by PRC-sponsored cyber threat actors, believed to number in the hundreds of thousands.

Observed examples of advanced technology utilization by PRC-sponsored cyber threat actors include the use of generative AI to generate scripts for automated reconnaissance and the use of generative AI to modify signatures to circumvent cyber defense tools built to detect known and previously observed signatures.

Recently, Chinese Active Persistent Threats (APTs) - a stealthy, continuous, and targeted cyberattack where an unauthorized user gains access to a network and remains undetected for an extended period, typically to steal data or surveil activity - connected with Volt Typhoon were discovered within a Massachusetts utility provider, where they operated undetected for nearly a year. Presumably due to a reliance on rules, signatures, and out of date systems.

While the cybersecurity industry is making rapid advances to close the technology gap for cyber defense, a majority of critical infrastructure organizations are moving too slow to upgrade, patch and deploy supplemental new cyber defense technologies. Existing tools are being improved to add new user behavior capabilities.

Recent breakthroughs have enabled new, purpose-built threat detection technologies designed to detect APTs with unknown signatures, to be introduced to the market. Despite these advances, slow budget approval, procurement and compliance processes within our critical infrastructure sector are proving to be a welcome gift to our Chinese adversaries, who by contrast, have few, if any, hoops to jump through prior to adding new technologies to their toolsets.

Critical infrastructure cyber defense leaders are haunted by "what if" scenarios.  They go to sleep each night knowing that beyond intelligence gathering, PRC-sponsored threat actors have present attacks capabilities unimaginable by US citizens.

Power grids can collapse, clean water can become inaccessible, planes can be made to fail, trains can derail, 911 systems can go down, traffic lights across entire cities can turn green. These nightmare scenarios are not theoretical. In each town across the US is a critical infrastructure cyber defense leader who understands the gravity of China's cyber threat.

## Volt Typhoon, Salt Typhoon and APT41

China's vast and advanced state-sponsored cyber operations include four highly effective groups focused on US critical infrastructure:  Volt Typhoon, Salt Typhoon and APT41. These sophisticated groups utilize advanced technologies to avoid detection.

To date their cyber operations have predominantly focused on reconnaissance, gathering information, mapping systems and understanding dependencies. Critical infrastructure leaders understand the imminent threat these PRC-sponsored cyber threat groups.

## Tactics, Techniques, and Procedures (TTPs)

Despite their different missions, these APT groups share several core tactics. All are known for using living-off-the-land (LotL) techniques, leveraging legitimate tools such as PowerShell, WMIC, and Certutil dynamically create malicious scripts locally with no known signature to avoid detection. Exploitation of edge devices—such as unpatched VPNs, Exchange servers, and Citrix gateways—is another common vector.

Once inside a network, they steal credentials by dumping Active Directory databases or using tools like Mimikatz. Lateral movement typically involves the use of RDP, PsExec, and SMB protocol abuse, while persistence is often achieved through subtle, long-term access that can go undetected for months or even years by rules and signature-based systems.

## Volt Typhoon

Volt Typhoon, active since at least mid-2021, has been silently embedding itself into critical infrastructure sectors, including water utilities, transportation systems, energy providers, and telecommunications. Typhoon utilizes "living off the land" techniques, utilizing legitimate administrative tools like PowerShell, WMI, and command-line utilities to avoid detection in addition to more traditional tactics like stolen certificates.

Volt Typhoon threat actors are able to masquerade their actions as seemingly normal network activity, maintain long-term access, and move laterally within systems. Using technology to avoid detection triggers associated with known signatures, Volt Typhoon threat actors are believed to have high success rates.

In addition to the previously mentioned Massachusetts utility compromise where they avoided detection for nearly a year, Volt Typhoon was discovered in Guam's electricity provider. This discovery raised alarms in Washington as a result of Guam's essential role to US Navy operations in the Pacific.

### Tactics:

- 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.

- Seek to obtain administrator credentials, 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.

- Use valid administrator credentials to move laterally to the domain controller (DC) and other devices via remote access services such as Remote Desktop Protocol (RDP).

- Conduct 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.

- Achieve 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.

- Use 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.

- Use 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.

## Salt Typhoon

Highly effective PRC-sponsored threat group, also known as GhostEmperor and FamousSparrow. Known to have infiltrated critical infrastructure targets throughout the west.  In 2024, officials announced Salt Typhoon hackers had infiltrated the systems of nine major US telecommunications companies.

Not only did they infiltrate standard corporate systems, but they gained entry into lawful intercept platforms—those systems telecom providers use to comply with law enforcement surveillance requests. In doing so, Salt Typhoon effectively hijacked America's surveillance capabilities and used them against U.S. citizens and political leaders, including President-elect Donald Trump and Vice President-elect J.D. Vance.

The FBI and NSA later confirmed that these intrusions may have resulted in the exposure of metadata, SMS content, call records, and even live audio in some instances.

### Tools

BITS Admin
CertUtil
Cheat Engine driver
Demodex
Get-PassHashes.ps1
Ladon
Malleable C2
mimkat_ssp
NBTscan
Powercat
PowerShell
ProcDump
PsExec
PsList
SMB
SparrowDoor
Token.exe
WinRAR
WMIExec

## APT 41

PRC-sponsored cyber threat group also known as Wicked Panda, Brass Typhoon and Barium.  APT41, distinct in its hybrid approach, combines state espionage with financially motivated attacks on software supply chains and healthcare institutions.  APT41 distinguishes itself by its dual-purpose approach, conducting espionage while simultaneously engaging in profit-driven activities, such as compromising software development environments for supply chain attacks.

### Tactics:

- Access Token Manipulation
- Local Account Discovery:  use built-in net commands to enumerate local admin groups
- Domain Account:  use built-in net commands to enumerate domain admin users
- Account Manipulation:  added user accounts to User and Amin groups
- Acquire Infrastructure Serverless:  use infrastructure hosted behind Cloudfare or utilized Cloudflare workers for command and control.
- Wordlist Scanning:  use various tools to brute-force directories on web servers
- App Layer Protocols:  use HTTP to download payloads for CVE-2019-19781 and CVE-2020-10189 exploits.
- App Layer Protocols:  used exploit payloads that initiate download via ftp.

## APT 41 Tactics cont:

- App Layer Protocol: used DNS for C2 communications.
- Archive via Utility: created a RAR archive of targeted files for exfiltration.
- Additionally, APT41 used the makecab.exe utility to both download tools, such as NATBypass, to the victim network and to archive a file for exfiltration.
- PowerShell: leveraged PowerShell to deploy malware families in victims' environments.
- Windows Command Shell: used cmd.exe /c to execute commands on remote machines. APT41 used a batch file to install persistence for the Cobalt Strike BEACON loader.
- Cloud Accounts: used compromised Google Workspace accounts for command and control.
- Data Obfuscation: frequently configured the URL endpoints of their stealthy passive backdoor LOWKEY.PASSIVE to masquerade as normal web application traffic on an infected server.
- Lateral Tool Transfer: uses remote shares to move and remotely execute payloads during lateral movement.
- Proxy: used a tool called CLASSFON to covertly proxy network communications.
- 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.

## Recommendations

Defending against these APT groups, especially in OT environments where legacy systems, limited patching capabilities, and operational uptime requirements reduce traditional security effectiveness, requires a layered security approach grounded in network design and implementation of new advanced threat detection technologies.

### Network Design Recommendations

- Ensure IT and OT systems are isolated via data diodes or air gaps.

- Multifactor authentication (MFA) should be enforced, particularly for vendor accounts.

- Privileged credentials should never be stored on endpoints or appliances.

- Access Audit & Improvement:
    - Encrypt Remote Access Vectors—including VPNs, RDP sessions, dial-back modems —Access audit logging review
    - Access policies review
    - Ensure strict time-based access policies
    - Read-only access granted whenever possible
    - Sessions should be continuously monitored for behavioral anomalies.

- Legacy systems should be upgraded or segmented if updates are no longer available.

- Hardware-based interlocks and fail-safes should be implemented to prevent malicious PLC commands from causing physical damage.

- Continuous behavioral monitoring tools with proven APT detections capabilities should be deployed across IT and OT networks to provide early warning of precursor attacks and support rapid root cause analysis.

## Advanced Threat Detection Technology Implementation

To effectively counter today's advanced persistent threats, critical infrastructure organizations must adopt purpose-built detection technologies capable of identifying novel attack patterns and tactics in real time. Traditional tools, reliant on signatures or known indicators, are increasingly outpaced by modern threat actors using stealthy, adaptive techniques. New advancements in threat detection now offer a transformative leap forward—enabling proactive identification of threats that would otherwise bypass legacy systems and remain undetected until after damage is done.

One new advanced threat detection technology proving particularly effective in SCADA environments comes from MixMode. MixMode's 3rd Wave AI platform delivers out-of-band, passive, real-time behavioral analysis without relying on signatures or CVEs. MixMode is able to detect both precursor activity and exploitation attempts by establishing dynamic, constantly evolving and predictive behavior baselines across IT and OT environments. By operating invisibly to attackers and correlating subtle anomalies to root causes, MixMode closes visibility gaps left by traditional SIEM, IDS/IPS, and endpoint tools.

## MixMode's Role Across APT Profiles

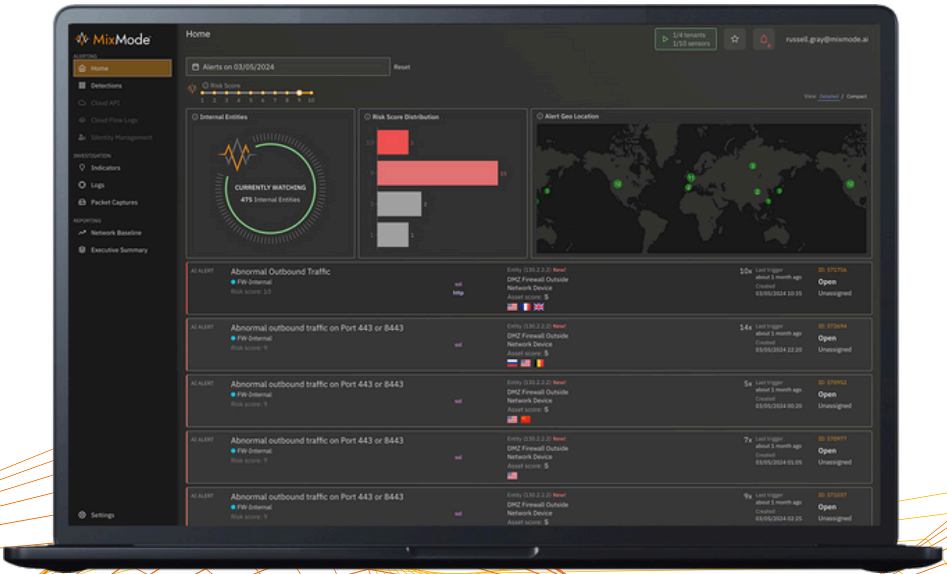
In the face of such multifaceted threats, traditional detection tools—those reliant on known signatures or vulnerability profiles—fall short. MixMode's 3rd Wave AI operates without dependence on pre-existing threat intelligence and is proven to detect anomalies preceding exploitations.  This capability is critical given the low-and-slow techniques being deployed by China's cyber operations.

MixMode functionally operates entirely out-of-band, passively observing an environment without participating in the traffic it monitors. This differential architectural approach significantly reduces its exposure to the attack surface.

Many APT campaigns, including Volt Typhoon, begin with exploiting vulnerabilities in perimeter devices like firewalls, VPNs, or endpoint detection and response (EDR) tools. By staying outside the direct communication path and avoiding active querying or intrusive scanning, MixMode remains invisible to attackers during the reconnaissance and initial exploitation phases.

For example, in the context of improving cyber defenses against Volt Typhoon, MixMode identifies vendor login anomalies and detect reconnaissance activity using tools like FOFA or Censys. To defend against Salt Typhoon, MixMode's recognizes abnormal encrypted sessions or anomalies in certificate validation that might suggest misuse of digital certificates.

Brass Typhoon's preparation and lateral movement within Exchange environments are detectable by MixMode through deviations in administrative session timing and access patterns. Lastly, with APT41, MixMode can be used to track changes in development environments, identifying the use of previously unseen signed binaries or unusual traffic originating from developer workstations.



AI ALERT Abnormal Outbound Traffic
FW-Internal
Risk score: 10
ssl http
Entity (130.2.2.2) New!
DMZ Firewall Outside
Network Device
Asset score: 5
10x Last trigger about 1 month ago
Created 03/05/2024 10:35
ID: 571756
Open
Unassigned

AI ALERT Abnormal outbound traffic on Port 443 or 8443
FW-Internal
Risk score: 9
ssl
Entity (130.2.2.2) New!
DMZ Firewall Outside
Network Device
Asset score: 5
14x Last trigger about 1 month ago
Created 03/05/2024 22:20
ID: 572694
Open
Unassigned

AI ALERT Abnormal outbound traffic on Port 443 or 8443
FW-Internal
Risk score: 9
ssl
Entity (130.2.2.2) New!
DMZ Firewall Outside
Network Device
Asset score: 5
5x Last trigger about 1 month ago
Created 03/05/2024 00:20
ID: 570952
Open
Unassigned

AI ALERT Abnormal outbound traffic on Port 443 or 8443
FW-Internal
Risk score: 9
ssl
Entity (130.2.2.2) New!
DMZ Firewall Outside
Network Device
Asset score: 5
7x Last trigger about 1 month ago
Created 03/05/2024 01:05
ID: 570977
Open
Unassigned

AI ALERT Abnormal outbound traffic on Port 443 or 8443
FW-Internal
Risk score: 9
ssl
Entity (130.2.2.2) New!
DMZ Firewall Outside
Network Device
Asset score: 5
9x Last trigger about 1 month ago
Created 03/05/2024 02:25
ID: 571037
Open
Unassigned

## MixMode's Role Across APT Profiles (cont.)

Beyond pre-attack APT detection, MixMode also excels in correlating post-exploitation activity. It detects OT protocol misuse, such as unauthorized Modbus or DNP3 commands, and identifies abnormal data flows indicative of configuration exfiltration. MixMode's ability to correlate activities across IT and OT environments proves critical in identifying root causes, whether those are misconfigured firewalls, compromised vendor accounts, or failed segmentation policies.

MixMode's independence from signature libraries or CVE repositories represents a departure from traditional cyber threat detection technologies. This independence uniquely allows MixMode to detect zero-day attacks, misconfigurations, and novel TTPs without prior exposure. Also, because MixMode's 3rd Wave AI continuously learns and adapts to normal network behavior, detection accuracy is increased while reducing false positives.

MixMode was purpose-built to detect the most sophisticated cyber threats, including China-sponsored cyber threats. With the only 3rd Wave AI technology in the cyber defense market, including real-time behavioral analysis, eliminated reliance on known signatures and out-of-band monitoring which bridges the IT/OT divide, MixMode is helping critical infrastructure leaders regain the technology advantage over adversaries.

| Threat Group | Operational Focus | Signature Behaviors and Tactics | High-Level Mitigation and Prevention Guidance |
|---|---|---|---|
| Volt Typhoon | U.S. Critical Infrastructure, OT Systems | LotL techniques, SOHO device exploits, proxy botnets (KV Botnet), SCADA infiltration | Enforce network segmentation, patch edge devices, monitor vendor access, deploy OT-aware anomaly detection tools |
| Salt Typhoon | Telecommunications, Satellite, Aerospace | Use of stolen certs, long-term telecom compromise, Middle East & APAC focus | Audit certificate chains, restrict external SSH/VPN access, monitor encrypted session behavior |
| Brass Typhoon | Defense Contractors, Maritime Logistics, Politics | Exchange server exploits, post-exploit persistence, long lateral movement | Harden Exchange infrastructure, monitor PowerShell usage, employ time-based access controls |
| APT41 | Pharma, Gaming, Supply Chain (Espionage + Crime) | Dual-use attacks, supply chain compromise, financial theft via dev systems | Secure software pipelines, restrict signing cert access, monitor dev workstation behavior |

MixMode®

mixmode.ai