Going on the Offensive - Tackling Volt Typhoon attacks on Active Directory

CISA, the FBI and NSA have identified that the People's Republic of China (PRC) state sponsored cyber attackers are seeking to pre-position themselves on IT networks for disruptive cyber- attacks against U.S. critical infrastructure. Numerous critical infrastructure operators have had their IT systems compromised by Volt Typhoon (aka Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, and Insidious Taurus).

Volt Typhoons activities are challenging to identify and respond to due to the actor's primary method of attack, "Living off the Land", which leverages legitimate tools and functionalities already present within a compromised system or network to carry out malicious activities. Rather than relying on conspicuous malware or custom tools that may trigger security alerts, attackers use built-in utilities, scripts, or administrative functionalities to blend in with normal network activity and evade detection.

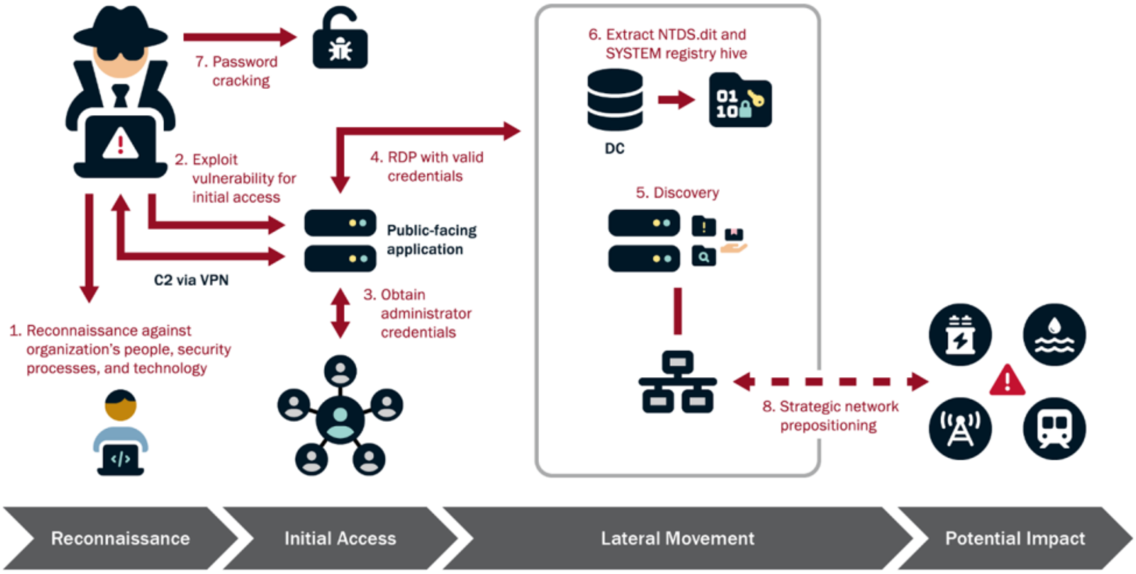
Active Directory (AD), a cornerstone of enterprise network infrastructure, manages user identities and facilitates access control. Given its pivotal role, AD becomes a prime target for cyber attackers like Volt Typhoon. The compromise of AD can lead to catastrophic outcomes, including the unauthorised access to sensitive information and disruption of critical operations.

> **"Certes DPRM's innovative approach ensures data protection even in the face of sophisticated threats like Volt Typhoon."**
>
> *Simon Pamplin – CTO, Certes*

The challenge of safeguarding AD against such adversaries is daunting. Traditional security measures often fall short, unable to contend with the cunning and persistence of state-sponsored hackers. This white-paper delves into the complexities of protecting AD from Volt Typhoon, advocating for a revolutionary approach: data-centric segmentation. By rethinking security from the ground up, organizations can fortify their defences against the sophisticated tactics employed by such actors.

Initial Access: The Volt Typhoon Threat

Volt Typhoon exploits known, or zero-day vulnerabilities found in public-facing network appliances such as VPNs, firewalls, and routers to initially breach the IT network. Once inside, it leverages legitimate administrator credentials to move laterally towards domain controllers. These credentials are often obtained through exploiting privilege escalation vulnerabilities in network services.



7. Password cracking
6. Extract NTDS.dit and SYSTEM registry hive
DC
2. Exploit vulnerability for initial access
4. RDP with valid credentials
Public-facing application
5. Discovery
C2 via VPN
3. Obtain administrator credentials
1. Reconnaissance against organization's people, security processes, and technology
8. Strategic network prepositioning
Reconnaissance
Initial Access
Lateral Movement
Potential Impact

*https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf

Active Directory: A Prime Target

The centrality of Active Directory in network infrastructure makes it a prime target for Volt Typhoon. AD's role in managing user identities and access controls means that compromising it can provide attackers with the keys to the kingdom. The sensitive nature of the data stored in the NTDS.dit file, including hashed password values, makes it particularly attractive to attackers. The NTDS.dit file is in constant use which makes it difficult to extract. However attackers can use existing tools such as Volume Shadow Copy, NTDSUtil or snapshots in a virtual environment, to extract NTDS.dit from critical systems. Once extracted use of tools like Mimikatz or Hashcat on this file can enable adversaries to manipulate and elevate privileges, further entrenching their presence within the network with post-compromise lateral movement, maintaining persistence detection evasion.

Ultimately, the end goal often involves gaining access to Operational Technology (OT) assets. Regulatory fines for breaches of Personally Identifiable Information (PII) become secondary concerns as the threat of critical infrastructure shutdown becomes a stark reality.

The Challenge of Defense

Protecting critical infrastructure from sophisticated threats is increasingly challenging. Traditional perimeter defenses are no longer sufficient when an adversary is using legitimate user credentials and native tools, enabling Volt Typhoon to bypass these barriers with relative ease. Once inside the network, the actor's ability to move laterally and escalate privileges makes it difficult to detect and contain the threat.

Further, adopting reactive mitigations to known TTPs may lack practicality in the context of specific environments. For example, there are 17 Techniques reference in the MITRE Attack Framework under Credential Access, with numerous sub-techniques. Deploying controls to mitigate each of these is not foreseeable. In any event, even if an organization managed to implement a full suite of specific controls, new techniques will have evolved in the interim that are not protected against.

As Microsoft says in a recent threat blog:

> **“Mitigating risk from adversaries like Volt Typhoon that rely on valid accounts and living-off-the-land binaries (LOLBins) is particularly challenging”.**

This is because it is assumed that approved credentials = approved access to data. Network access and Data access should be treated separately, the right credentials from the wrong location should be treated as suspicious.

Traditional methods

Traditional methods of defense attempt to fix defects in perimeter hardware devices such as routers and firewalls as well as remote access software such as VPN’s. Recently identified vulnerabilities in vendors such as Fortinet, NETGEAR, Citrix, Cisco and Ivanti Connect Secure VPN demonstrate that this reactive approach to security is not keeping pace with the threat attackers.

A new approach is required

A new approach is required, security needs to go on the offensive and focus on protecting the target of the attacks and not relying on perimeter and credentials security both of which are regularly compromised leading to access to IT and OT systems. Critical assets such as the Active Directory Domain Controller database should be independently protected in a way that ensures critical infrastructure operators retain total control of the integrity of their sensitive data.

This can be achieved by data-centric security approaches such as cryptographical anonymization and individual data flow segmentation (defined though consistent customer owned policies). The data flows need to be protected in such a way that only the intended recipient and location can access the data irrespective of where the data flows or is taken.

Certes DPRM (Data Protection Risk Mitigation) is the Answer

In the evolving landscape of cyber threats, particularly from sophisticated actors like Volt Typhoon, identity and credentials are the new perimeter - traditional security measures are increasingly inadequate.

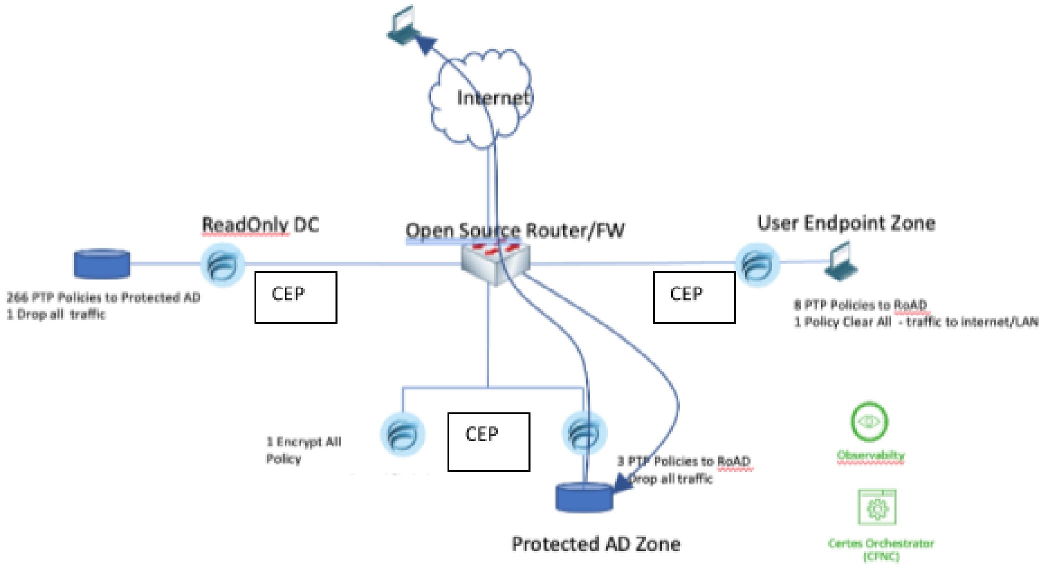
The need for innovative solutions that not only prevent unauthorised access but also protect data from being useful even after a breach is paramount. Certes Data Protection and Risk Mitigation (DPRM) ensures that data in transit is protected at all times, even when traversing network segments managed by both known or unknown third parties. By applying policies to the data itself, the impacts of a data breach are mitigated (even in a worst-case scenario where data is lost or stolen). **Here's why Certes DPRM is the answer to mitigating threats posed by entities like Volt Typhoon.**

Certes DPRM Unique features:

Certes DPRM distinguishes itself with several key features that specifically address the challenges posed by advanced cyber threats:

Crypto-Segmentation: At the heart of Certes DPRM's approach is crypto-segmentation. This technology allows for the individual securing of application data flows with unique policies and encryption keys (each key changed or rotated every 60 minutes), effectively creating discrete crypto segments that safeguard sensitive data from unauthorised access and post compromise lateral movement due to credential dumping. This protects against Volt Typhoon’s preferred method of moving through a network.

Customer-Controlled Key Management: Another critical feature is the Certes Customer Controlled Key Management. This ensures that encryption keys and policies are solely under the control of the customer's security team. A combination of quantum safe techniques combined with key seed material partially provided by the customer and only known to the customer mean that even if data flow is exfiltrated successfully, the encrypted payload remains inaccessible to unauthorised users, appearing as indecipherable gibberish (resulting ciphertext). This protects against Volt Typhoon dumping credential databases to remote locations for decryption.



Here we can see an example where users are directed only to the RODC – they are not allowed direct access to the AD DC, their traffic passing through a Certes DPRM enforcement point (CEP) into a crypto-segmented flow LAN side, another CEP fronts all traffic to the RODC ensuring that only traffic from legitimate end users within a crypto-segmented flow can access the RODC. Another CEP fronts the writeable AD Domain Controller with policies that define not only who but where admins can access it from. Anyone trying to access the RODC or AD DC with legitimate credentials but from a location not within a crypto-segmented flow (via a VPN for example) will be either dropped or sent fully protected traffic.

Securing Active Directory Against Volt Typhoon

Given Volt Typhoon's proclivity for targeting Active Directory (AD) to enable espionage and information gathering, Certes DPRM's capabilities are particularly relevant. The solution offers:

Enhanced Protection for AD: By applying policy based crypto-segmentation, Certes DPRM can protect AD from the kinds of sophisticated attacks carried out by Volt Typhoon. This includes preventing unauthorised access and manipulation of sensitive data within the NTDS.dit file.

Policies can be created to define not only how to protect certain data flows but also where legitimates access to this data flow should be coming from or going to – outside of these approved directions would be considered suspicious. By defining end user access to only the Read Only Domain Controllers (RODC) and defining the direction and location that updates to the RODC can flow, DPRM can control and prevent any changes to privilege levels. For example, persistent threats to Active Directory such as DCSync Attacks and Golden Ticket Attacks would be prevented and adversaries would be compelled to communicate solely with RODCs, which lack replication permissions, essentially bringing a halt to malevolent activities.

Any suspicious data flow such as exfiltration of databases files via a VPN connection will either be dropped by policy or sent out as fully encrypted and unusable depending on the policy set.

Mitigation of Post-Compromise Lateral Movement and Privilege Escalation: The unique segmentation and encryption approach of DPRM significantly hampers Volt Typhoon's capability to carry out surveillance of critical communications flows or post-compromise credential dumping, crucial steps in the attack chain. By individually anonymising data flows it renders it impossible to identify what flows are of interest to what are not. Before the attacker can target the AD they need to identify the data flows to attack.

Beyond Data Protection: Certes DPRM does not stop at merely protecting data from unauthorised access. Its innovative approach ensures that, even in the event of a data breach, the stolen information remains protected and unusable to the attacker. This directly counters Volt Typhoon's information gathering and espionage objectives, rendering their efforts futile.

Future-proofing Against Quantum Threats: Looking ahead, Certes DPRM is designed to be quantum-safe and Crypto-agile, offering protection against the quantum computing threats of tomorrow with an architecture that can easily take advantage of new algorithms as they become available. This positions Certes DPRM not just as a solution for today's challenges but as a forward-looking tool that anticipates and neutralises future cybersecurity threats.

Crypto-Segmentation

Customer-Controlled Key Management

Enhanced Protection for AD

Futureproofing Against Quantum Threats

Case Studies: Demonstrating DPRM's Effectiveness

While specific case studies involving Certes Data Protection and Risk Mitigation (DPRM) are proprietary and confidential, hypothetical scenarios can illustrate the solution's effectiveness against threats like Volt Typhoon. These scenarios demonstrate how just a few of DPRM's advanced features—crypto-segmentation, customer-controlled key management, and quantum agility—provide robust protection for Active Directory and sensitive data, mitigating the risks associated with state-sponsored cyber espionage.

Scenario 1: Preventing Unauthorized Active Directory Access

Situation:

An organization faces a sophisticated spear-phishing attack aimed at compromising Active Directory credentials. Volt Typhoon seeks to exploit these credentials for lateral movement and access to sensitive data.

Action:

Certes DPRM is implemented, crypto-segmentation policy is applied to segment each data flow between the read and write AD Domain Controllers. Each policy or flow is protected with unique encryption keys controlled solely by the organization's security team and rotated / changed every 60 minutes. The policy describes what can and cannot perform updates to the writable domain controller, it also describes what direction these access attempts are legitimate and by association anything else is classed as suspicious.

Outcome:

Even after the phishing attack compromises some user credentials, the attacker cannot escalate privileges because through policy they can only access a read-only DC, cannot move laterally within the network or access data flows because each flow is anonymised, so they have no idea what flow to focus their attacks on. Attempts to access sensitive data result in failure, as the attacker lacks the necessary encryption keys, rendering the compromised credentials useless.

Scenario 2: Thwarting Post-Compromise Lateral Movement and Data Exfiltration

Situation:

Volt Typhoon successfully infiltrates a network segment through a compromised device. The goal is to move laterally to access high-value targets and exfiltrate sensitive data.

Action:

With Certes DPRM, the network's sensitive data flows are individually secured, and access between segments is prohibited through encryption. Abnormal data flows, indicative of exfiltration attempts are seen as policy breaches and either dropped, or alerts are triggered and sent to SIEM (Security Information and Event Management).

Outcome:

The attacker's movement is confined to the initially compromised, user, device or segment. Any attempt to access or exfiltrate data is blocked by crypto segmentation, preventing the attacker from reaching sensitive information or exfiltrating outside the network.

Scenario 3: Future-proofing Against Quantum Computing Threats

Situation:
An organization anticipates the future threat posed by quantum computing, capable of breaking traditional encryption methods, and seeks to safeguard its Active Directory and sensitive data against this emerging threat.

Action:
Implementing Certes DPRM, the organization benefits from patented Quantum-Safe, Crypto-Agile technologies that ensure data remains protected even against adversaries equipped with quantum computing capabilities.

Even if they possessed sufficient compute power to crack a quantum safe form of encryption their work would have to complete within 60 minutes, or their results would be worthless as all existing keys would rotate by policy.

Outcome:
As quantum computing becomes viable, the organization’s data security remains uncompromised. The advanced protection provided by Certes DPRM, designed to withstand quantum attacks, ensures that sensitive data and Active Directory remain secure, thwarting any quantum-enabled attempts by Volt Typhoon or similar actors.

Summary

In summary, Certes DPRM represents a change in thinking in security. Moving beyond traditional perimeter / credential-based defences to a more dynamic, data centric approach that focuses on protecting the target of the attack and not the infrastructure hurdles put in the way. DPRM’s unique features and capabilities make it an essential tool in the fight against sophisticated cyber adversaries like Volt Typhoon, providing unparalleled protection for Active Directory and beyond.

Contact Certes

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

1 (888) 833-1142
sales@certes.ai