CERTES

Unveiling AlphaV/BlackCat

The Emerging Threat in Ransomware Innovation and its Impact on Global Cybersecurity

BlackCat, also known as ALPHAV / ALPHV and Noberus is a ransomware family that made its first appearance in November 2021. It's also the name of the threat actor(s) that exploit it.

BlackCat operates on a ransomware as a service (RaaS) model, with developers offering the malware for use by affiliates and taking a percentage of ransom payments. For initial access, the ransomware relies essentially on stolen credentials obtained through initial access brokers. The group operates a public data leak site to pressure victims to pay ransom demands.

The group has targeted hundreds of organizations worldwide. Since its first appearance, it is one of the most active ransomware groups.

AlphaV/BlackCat utilizes mostly double or triple extortion tactics which involves exposing exfiltrated data and threatening to launch distributed denial-of-service (DDoS) attacks on victims’ infrastructure. Following on from the SEC requirements to report attacks within 4 business days, the threat actors are also now threatening to expose targets to the SEC if they do not do it themselves. Since mid-December 2023, of the nearly 70 leaked victims, the healthcare sector has been the most commonly victimized.

> **AlphaV/BlackCat's innovation was to post excerpts or samples of victims' data on a site accessible to anyone with a web browser, marking a new era in ransomware's public impact and pressure tactics.**
>
> *Simon Pamplin – CTO, Certes*

The organisation is known for being the first ransomware group to create a public data leaks website on the open internet. AlphaV/BlackCat's innovation was to post excerpts or samples of victims' data on a site accessible to anyone with a web browser. The group also mimics its victims' websites to post stolen data on typo squatted replicas on the web.

The adversaries leverage previously compromised user credentials to gain initial access to the victim system. Such use of legitimate credentials is of a growing concern given that traditional network security tools are unable to identify and prevent such threats. Once inside, the threat actors compromise Active Directory user and administrator accounts and use Windows Task Scheduler to configure malicious Group Policy Objects (GPOs) to deploy ransomware and switch off security controls.

The gang uses botnet malware as an entry point. It also uses Log4J to propagate the ransomware laterally within the network (TA0008). Malware tools like ExMatter are then used to steal sensitive data before deploying ransomware to encrypt files.

Threat actors associated with AlphaV/BlackCat have been observed, in many incidents, using hijacked webpages of legitimate organizations to redirect users to pages hosting malware. The rogue WinSCP installer distributed a backdoor containing a Cobalt Strike Beacon for follow-on intrusion activities. Cobalt Strike was used to conduct reconnaissance, post-compromise lateral movement, data exfiltration, and tampering with security software.

The ransomware incorporates techniques like junk code and encrypted strings to avoid detection. Once executed, BlackCat performs network discovery to find more systems to infect, deletes volume shadow copies, encrypts files, and drops a ransom note demanding cryptocurrency.

AlphaV/BlackCat have been actively targeting Healthcare (Change Healthcare, UnitedHealth Group, NextGen Healthcare, Lehigh Valley Health Network), Entertainment (MGM Resorts International, Caesars Entertainment) and online betting sites all demanding significant sums in cryptocurrency.

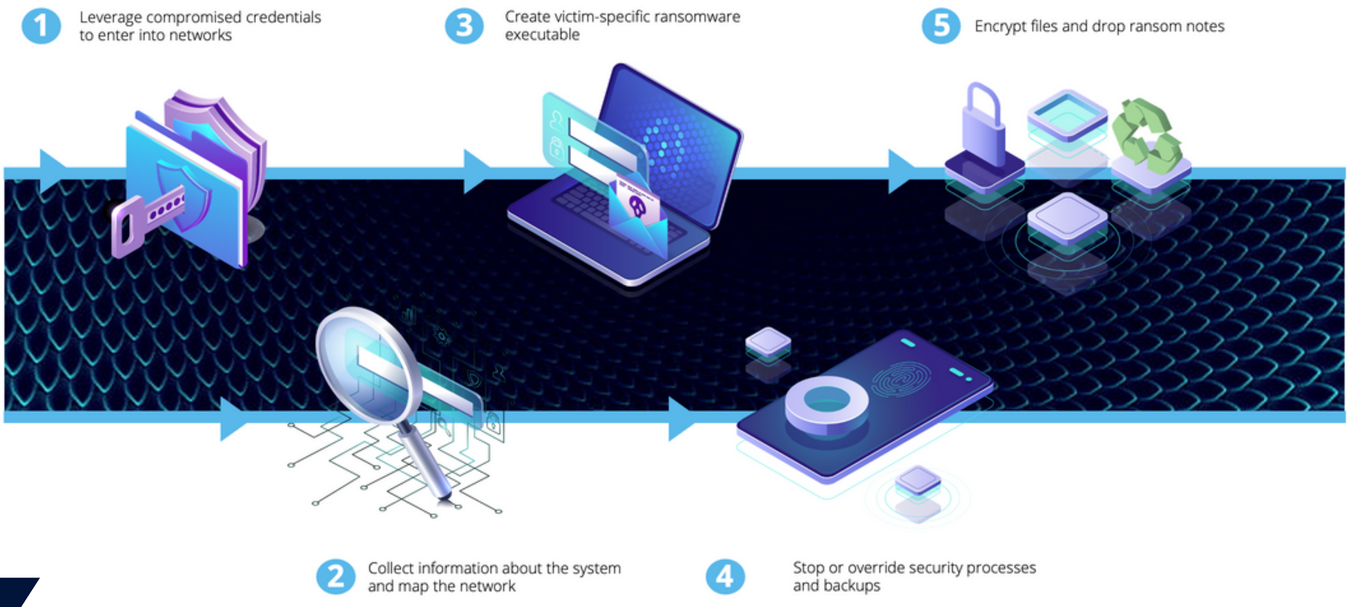
> **The daunting challenge of safeguarding Active Directory against cunning and persistent adversaries necessitates a revolutionary approach. This white paper advocates for data-centric segmentation, a fundamental rethinking of security that empowers organizations to bolster their defenses against the sophisticated tactics of threat actors like AlphaV/BlackCat.**
>
> *Simon Pamplin – CTO, Certes*

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 AlphV/Blackcat. The compromise of AD can lead to catastrophic outcomes, including the unauthorised access to sensitive information and disruption of critical operations.

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 threat actors such as AlphaV / Blackcat, 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

AlphaV/BlackCat exploit five vulnerabilities – CVE-2016-0099, CVE-2019-7481, CVE-2021-31207, CVE-2021-34473, and CVE-2021-34523 as well as fake websites and malware based on the RUST framework to initially breach the IT network. Once inside, it leverages compromised legitimate administrator credentials to move laterally towards domain controllers, mapping the entire network and manipulating accounts for deeper access. These credentials are often obtained through exploiting privilege escalation vulnerabilities in network services.


1 Leverage compromised credentials to enter into networks
3 Create victim-specific ransomware executable
5 Encrypt files and drop ransom notes
2 Collect information about the system and map the network
4 Stop or override security processes and backups

> Given the pivotal role of Active Directory in network infrastructure, its compromise can lead to catastrophic outcomes, offering attackers the keys to the kingdom and underscoring the need for advanced security measures.

Active Directory: A Prime Target

The centrality of Active Directory in network infrastructure makes it a prime target for AlphaV/BlackCat. 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 (TA0010).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 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 AlphaV/BlackCat 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 AlphaV/Blackcat 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 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.

> **Mitigating risk from adversaries like AlphaV/Blackcat that rely on valid accounts and living-off-the-land binaries (LOLBins) is particularly challenging...**

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.

Certes DPRM (Data Protection Risk Mitigation) is the Answer

In the evolving landscape of cyber threats, particularly from sophisticated actors like AlphaV/BlackCat, 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 AlphaV/BlackCat.

Certes DPRM Unique features:

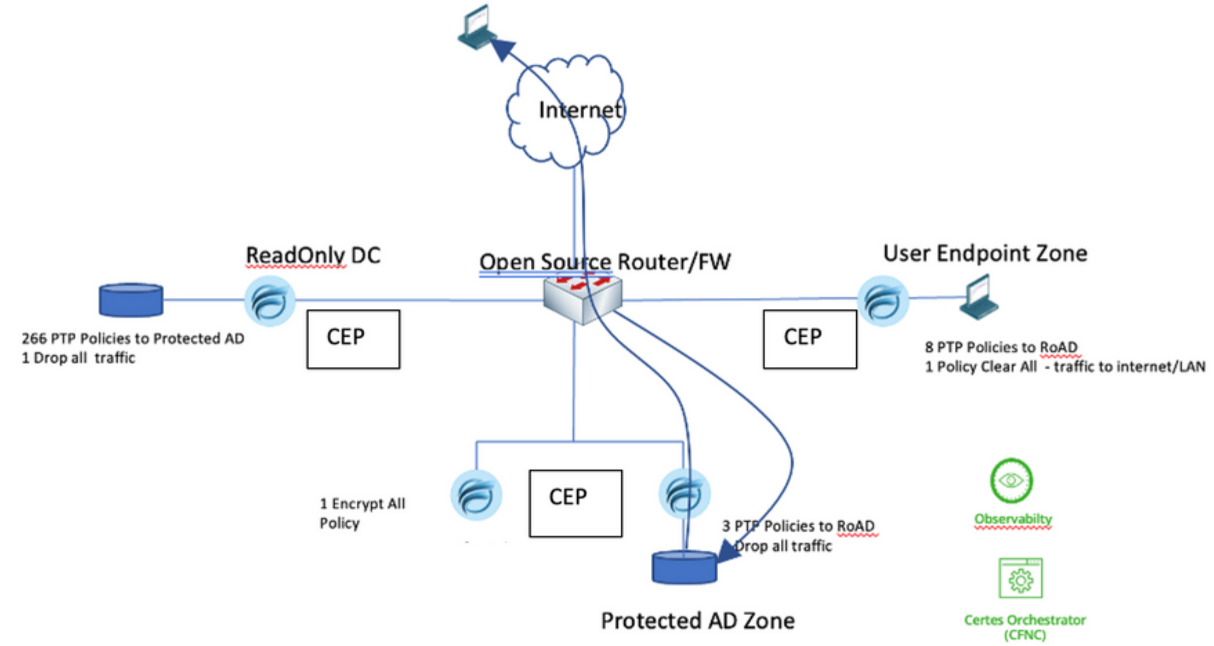
Certes DPRM distinguishes itself with several key features that specifically address the challenges posed by advanced cyber threats:

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 AlphaV/BlackCat preferred method of moving through a network and identifying valuable data flows.

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 AlphaV/BlackCat 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 AlphaV/BlackCat

Given the 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 AlphaV/BlackCat. 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.

> “**By applying policy based crypto-segmentation, Certes DPRM can protect AD from the kinds of sophisticated attacks carried out by AlphaV/BlackCat.**
>
> *Simon Pamplin – CTO, Certes*”

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 AlphaV/BlackCat 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. his directly counters AlphaV/BlackCat information gathering and espionage objectives, rendering their efforts futile.

Futureproofing 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 not just as a solution for today's challenges but as a forward-looking tool that anticipates and neutralises future cybersecurity 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 AlphaV/BlackCat. 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. AlphaV/BlackCat 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:
AlphaV/BlackCat 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 organisation 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 organisation 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 organisation'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 AlphaV/BlackCat or similar actors.

> **Certes DPRM represents a change in thinking in security. Moving beyond traditional perimeter / credential-based defences to a more dynamic, data centric approach...**
>
> *Simon Pamplin – CTO, Certes*

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 AlphaV/BlackCat, 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

CERTES