Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

2022-004: ACSC Ransomware Profile – ALPHV (aka BlackCat)

14 April 2022

Context: *ALPHV (aka BlackCat, Noberus) is a ransomware variant first observed in late 2021, used by cybercriminals to conduct ransomware attacks against multiple sectors and organisations worldwide, including Australia. ALPHV is offered as a Ransomware-as-a-Service (RaaS), in which affiliates pay a percentage of profits from using the ransomware to the ALPHV operators in return for use of the ransomware and other related services. This product provides information related to ALPHV's background, threat activity, tactics used and mitigation advice.*

The Australian Cyber Security Centre (ACSC) is providing this information to enable organisations to undertake their own risk assessments and take appropriate actions to secure their systems and networks. The ACSC will only revise and update this document in the event of further significant information becoming available.

Key Points

- ALPHV ransomware restricts access to corporate files and systems by encrypting them into a locked and unusable format. Victims receive instructions on how to engage with the offenders after encryption.
- ALPHV affiliates have successfully deployed ransomware on corporate systems in a variety of countries and sectors, including in Australia, where the ACSC is aware of multiple victims.
- ALPHV affiliates implement multiple extortion techniques in addition to encryption of files on the victim's network. These include uploading stolen victim data in part or full to a dedicated leak site (DLS), threatening to sell and/or release additional information, and threatening the victim with Distributed Denial of Service (DDoS) attacks if they do not comply with ransom demands.
- Threat actors involved in the deployment of the ALPHV ransomware use a range of vectors to gain initial access into victim networks, including but not limited to the use of phished and brute-forced access credentials.
- The ACSC advises against paying ransoms. Payment of the ransom may increase an organisation's vulnerability to future ransomware incidents. In addition, there is no guarantee that payment will undo the damage.

Background

First detected in late 2021, ALPHV (aka BlackCat, Noberus) is a ransomware-as-a-service (RaaS) affiliate program associated with Russian-speaking cybercrime actors. According to open source reporting, ALPHV is related to previous ransomware variants BlackMatter and DarkSide, which was used in the attack on Colonial Pipeline in May 2021. The operators of ALPHV have reportedly sought to recruit former members of the BlackMatter, DarkSide and REvil groups, and several similarities have been identified between the tactics, techniques and procedures (TTPs) of both ALPHV and BlackMatter ransomware actors.

The operators of ALPHV advertise the ransomware to potential affiliates in private forums, such as the darknet forum RAMP. ALPHV affiliates have successfully deployed ransomware to target networks worldwide, including in Australia, where the ACSC is aware of multiple Australian victims.

Threat activity

The ACSC is aware of an increase in ALPHV activity globally in 2022 relative to other competing ransomware variants, including against Australian organisations. The ACSC is aware of ALPHV targeting government and critical infrastructure organisations, as well as the energy, finance, construction and other sectors. In February 2022, ALPHV affiliates compromised a German oil storage operator and an energy distributor. The ALPHV operators claim to exclude the use of the ransomware in attacks on healthcare and charitable organisations.

In late March 2022, the ALPHV developers announced changes to the ransomware, reportedly including features to inhibit detection of ALPHV ransomware by antivirus and other signature-based detection systems using polymorphic features that change parts of ransomware code.

Tactics, Techniques and Procedures

ALPHV is written in the 'Rust' programming language. ALPHV ransomware has the capability to target both Windows, and Linux systems, as well as ESXi virtualisation infrastructure.

Threat actors deploying ALPHV ransomware use a range of initial access vectors to gain access to target networks, including:

- Exploiting known vulnerabilities or common security misconfigurations.
- Using legitimate credentials purchased, brute-forced or gained in phishing attacks, including credentials for Remote Desktop Protocol (RDP) connections and commercial Virtual Private Network (VPN) products.

Once initial access is obtained, ALPHV actors establish reverse SSH tunnels as a command-and-control (C2) channel between victims and ALPHV infrastructure. Actors have been observed propagating ALPHV throughout victim networks using PsExec. ALPHV ransomware can be configured to terminate VMware ESXi virtual machines (VMs), and to delete VM snapshots and backups to prevent recovery efforts.

Other observable Tactics, Techniques, and Procedures (TTPs) associated with ALPHV ransomware activity include but are not limited to:

- Utilising PowerShell to alter Windows Defender security settings
- Utilising PsExec for lateral movement, tool transfer and execution.
- Utilising the publicly available penetration testing tool CobaltStrike for network access and lateral movement.
- Exfiltrating data to publicly available cloud file-sharing services.

Post-Exploitation

Once encryption of victim data is complete, victims receive a ransom note directing them to either an email address or a URL, from which an affiliate will demand payment. ALPHV affiliates implement multiple extortion techniques in addition to encryption of the victim's network. These include:

- Uploading stolen victim data in part or full to a dedicated leak site (DLS) maintained on The Onion Router (TOR) network.
- Threatening to sell and/or release additional information.
- Threatening the victim with Distributed Denial of Service (DDoS) attacks if they do not comply with ransom demands.

ALPHV ransomware uses a unique access token feature to prevent third parties from monitoring and disrupting ransom negotiations. This access token is used to create an access key needed to enter a dedicated victim portal on a TOR site where ransom negotiations are conducted. In contrast to other ransomware variants, ALPHV is willing to engage with

firms hired to conduct ransom negotiations on behalf of victims, and features an 'Intermediary' login option on the victim portal.

Assistance

The ACSC monitors a variety of ransomware variant activity, including ALPHV. The ACSC is able to provide assistance and advice if required.

All victims are strongly encouraged to report ransomware-related cybercrime and cyber security incidents to the ACSC. Organisations that have been impacted or require assistance in regards to an ALPHV ransomware incident can contact the ACSC via 1300 CYBER1 (1300 292 371), or by submitting a report to cyber.gov.au.

MITRE ATT&CK Techniques and Suggested Mitigations

The ACSC recommends to implement the following mitigations:

- Implement multifactor authentication to prevent actors from accessing valid accounts with stolen credentials.
- Implement network segmentation and network traffic filtering to prevent actors from directly connecting to remote access services they have established for persistence.
- Configure the Windows Registry to require User Account (UAC) approval for any PsExec operations requiring administrator privileges to reduce the risk of lateral movement by PsExec.
- Implement hypervisor log monitoring and ensure that logs are processed on a separate system.
- Implement application whitelisting (at least in monitor mode to capture unusual activity).
- Perform daily backups and keep them offline and encrypted.

The below table maps the mitigations to the techniques leveraged by the actor and to the resources to implement these mitigations to protect your infrastructure.

Technique	Procedure	Mitigations
Initial Access [TA0001]		
Valid Accounts [T1078]	Actors have obtained credentials for valid accounts and used these to gain access to victim networks. Actors have used phishing and password brute forcing techniques to obtain credentials. They have also purchased credentials or collected them from publicly available breaches.	Multi-factor authentication [M1032] Require multifactor authentication for all user accounts, particularly privileged accounts. This prevents actors from accessing valid accounts with stolen credentials. See also: • Multi-factor Authentication - Technique D3-MFA • Implementing Multi-Factor Authentication • Strategies to Mitigate Cyber Security Incidents – Mitigation Details User training [M1017]

		Educate users to avoid password reuse. This prevents actors from obtaining credentials through public breaches or by compromising non-corporate systems. See also: • Creating Strong Passphrases
Persistence [TA0003]		
External Remote Services [T1133]	Actors have used remote access services, such as valid Remote Desktop Protocol and SSH credentials, to persist on victim's systems.	Filter Network Traffic [M1037] Prevent network traffic from unknown or untrusted origins from accessing remote services on internal systems. This prevents actors from directly connecting to remote access services they have established for persistence. See also: • Inbound Traffic Filtering - Technique D3-ITF Network Segmentation [M1030] Segment networks and restrict traffic for remote access services where possible. This limits the ability of threat actors moving laterally within compromised networks. Utilising network segmentation as a form of defence in depth also prevents actors from connecting to external remote access services that they have established for persistence via compromised systems within victim networks. See also: • Broadcast Domain Isolation - Technique D3-BDI • Implementing Network Segmentation and Segregation
Execution [TA0002]		
System Services: Service Execution [T1569.002]	Actors have used the legitimate Windows Sysinternals tool PsExec [S0029] to execute malicious content.	Enable Attack Surface Reduction (ASR) on Microsoft Windows 10, and configure ASR to block process creations originating from PsExec commands. Note: PsExec is commonly used for legitimate system administration tasks. Organisations should consider how this mitigation could impact business practices before implementing. See also:

		• Hardening Microsoft Windows 10 version 21H1 Workstations
Exfiltration [TA0010]		
Exfiltration Over Web Service [T1567]	Actors have exfiltrated data to legitimate and publicly available web services, including legitimate cloud storage services.	Encrypt Sensitive Information [M1041] Encrypt sensitive data at rest. This prevents actors from accessing sensitive data even if they can access the systems storing the data. Network Segmentation [M1030] Segment networks to separate sensitive data, and services that provide access to sensitive data, from corporate environments. This prevents adversaries from compromising vulnerable systems, such as desktop environments, and immediately accessing and exfiltrating sensitive data. See also: • Broadcast Domain Isolation - Technique D3-BDI • Implementing Network Segmentation and Segregation Restrict Web-Based Content [M1021] Restrict access to web-based storage services from corporate networks, except where required for legitimate business activity. This prevents actors from directly uploading sensitive data to blocked web-based storage services.
Lateral Movement [TA0008], Privilege Escalation [TA0004], Discovery [TA0007]		
Various	Actors have deployed the widely-used post-exploitation framework Cobalt Strike on victim networks [S0154]. Actors have also used the legitimate SysInternals tool PsExec [S0029].	Network Segmentation [D3-BDI] Segment networks and restricting or monitor certain types of traffic that are commonly used for lateral movement or reconnaissance. This prevents actors from moving laterally in networks and accessing sensitive systems or data. See also: • Implementing Network Segmentation and Segregation Privileged Account Management [M1026] Restrict administrative privileges to operating systems and applications based on user duties. This reduces actors' ability to elevate privilege,

		move laterally in networks, bypass security controls and access sensitive data. See also: • Restricting Administrative Privileges Update Software [M1051] Patch applications and operating systems and keep them up to date. This prevents actors from exploiting known vulnerabilities in applications and operating systems to elevate privilege, bypass security controls and move laterally in networks. See also: System Patching
Impact [TA0040]		
Data Encrypted for Impact [T1486]	Actors have used ALPHV ransomware to encrypt valuable data, disrupt operations, and extort payment from victims.	Backup Data [M1053] Perform daily backups and keep them offline and encrypted. Test recovery and integrity procedures to make sure data and operations can be quickly and reliably restored. This will allow business operations to be recovered if data is encrypted, reducing the impact of a ransomware attack. Note that backups will not mitigate risks where sensitive data is exfiltrated and released. See also: • Data backup and restoration
Network Denial of Service [T1498]	Actors have threatened victims with Distributed Denial of Service (DDoS) attacks to extort ransom payments.	Filter network traffic [M1037] Monitor network traffic to identify possible denial-of-service attacks, and filter or block attack traffic. This service can be delivered by an ISP, CDN or other hosting provider. Prepare for denial-of-service attacks Take steps to prepare for, and mitigate the potential impact of denial-of-service attacks. For example: • Establish disaster recovery plans for critical systems.

		• Establish out-of-band communication procedures and contact points. • Partition critical online services (e.g. email) from services that are more likely to be targeted (e.g. web hosting). • Use cloud-based hosting from a major service provider, with high bandwidth and content delivery networks that cache static web content. See also: • Preparing for and Responding to Denial-of-Service Attacks

Document Change Log

Version	Date	Change summary
1	14 April 2022	First published.

ACSC Australian Cyber Security Centre

Traffic light protocol

TLP Level	Restriction on access and use
RED	**Not for disclosure, restricted to participants only.** Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
AMBER	**Limited disclosure, restricted to participant's organisations.** Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organisations involved. Recipients may only share TLP:AMBER information with members of their own organisation, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
GREEN	**Limited disclosure, restricted to the community.** Sources may use TLP:GREEN when information is useful for the awareness of all participating organisations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.
WHITE	**Disclosure is not limited.** Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.
Not classified	Any information received from the ACSC that is not classified in accordance with the Traffic light protocol must be treated as AMBER classified unless otherwise agreed in writing by the ACSC.