JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA23-353A
December 19, 2023

#StopRansomware: ALPHV Blackcat

SUMMARY

Note: *This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known IOCs and TTPs associated with the ALPHV Blackcat ransomware as a service (RaaS) identified through FBI investigations as recently as Dec. 6, 2023.

Actions to take today to mitigate against the threat of ransomware:

- ✓ Routinely take inventory of assets and data to identify authorized and unauthorized devices and software.
- ✓ Prioritize remediation of known exploited vulnerabilities.
- ✓ Enable and enforce multifactor authentication with strong passwords.
- ✓ Close unused ports and remove applications not deemed necessary for day-to-day operations.

This advisory provides updates to the FBI FLASH BlackCat/ALPHV Ransomware Indicators of Compromise released April 19, 2022. Since previous reporting, ALPHV Blackcat actors released a new version of the malware, and the FBI identified over 1000 victims worldwide targeted via ransomware and/or data extortion.

FBI and CISA encourage critical infrastructure organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of ALPHV Blackcat ransomware and data extortion incidents.

In February 2023, ALPHV Blackcat administrators announced the ALPHV Blackcat Ransomware 2.0 Sphynx update, which was rewritten to provide additional features to affiliates, such as better defense

---

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at fbi.gov/contact-us/field-offices. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at report@cisa.dhs.gov.

evasion and additional tooling. This ALPHV Blackcat update has the capability to encrypt both Windows and Linux devices, and VMWare instances. ALPHV Blackcat affiliates have extensive networks and experience with ransomware and data extortion operations. According to the FBI, as of September 2023, ALPHV Blackcat affiliates have compromised over 1000 entities—nearly 75 percent of which are in the United States and approximately 250 outside the United States—, demanded over $500 million, and received nearly $300 million in ransom payments.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 14. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

ALPHV Blackcat affiliates use advanced social engineering techniques and open source research on a company to gain initial access. Actors pose as company IT and/or helpdesk staff and use phone calls or SMS messages [T1598] to obtain credentials from employees to access the target network [T1586]. ALPHV Blackcat affiliates use uniform resource locators (URLs) to live-chat with victims to convey demands and initiate processes to restore the victims' encrypted files.

After gaining access to a victim network, ALPHV Blackcat affiliates deploy remote access software such as AnyDesk, Mega sync, and Splashtop in preparation of data exfiltration. After gaining access to networks, ALPHV Blackcat affiliates use legitimate remote access and tunneling tools, such as Plink and Ngrok [S0508]. ALPHV Blackcat affiliates claim to use Brute Ratel C4 [S1063] and Cobalt Strike [S1054] as beacons to command and control servers. ALPHV Blackcat affiliates use the open source adversary-in-the-middle attack [T1557] framework Evilginx2, which allows them to obtain multifactor authentication (MFA) credentials, login credentials, and session cookies. The actors also obtain passwords from the domain controller, local network, and deleted backup servers to move laterally throughout the network [T1555].

To evade detection, affiliates employ allowlisted applications such as Metasploit. Once installed on the domain controller, the logs are cleared on the exchange server. Then Mega.nz or Dropbox are used to move, exfiltrate, and/or download victim data. The ransomware is then deployed, and the ransom note is embedded as a file.txt. According to public reporting, affiliates have additionally used POORTRY and STONESTOP to terminate security processes.

Some ALPHV Blackcat affiliates exfiltrate data after gaining access and extort victims without deploying ransomware. After exfiltrating and/or encrypting data, ALPHV Blackcat affiliates communicate with victims via TOR [S0183], Tox, email, or encrypted applications. The threat actors then delete victim data from the victim's system.

ALPHV Blackcat affiliates offer to provide unsolicited cyber remediation advice as an incentive for payment, offering to provide victims with "vulnerability reports" and "security recommendations" detailing how they penetrated the system and how to prevent future re-victimization upon receipt of ransom payment.

MITRE ATT&CK TACTICS AND TECHNIQUES

See Table 1 through Table 3 for all referenced threat actor tactics and techniques in this advisory.

Table 1: ALPHV Blackcat/ALPHV Threat Actors ATT&CK Techniques - Reconnaissance

Technique Title	ID	Use
Phishing for Information	T1598	ALPHV Blackcat affiliates pose as company IT and/or helpdesk staff using phone calls or SMS messages to obtain credentials from employees to access the target network.

Table 2: ALPHV Blackcat/ALPHV Threat Actors ATT&CK Techniques – Resource Development

Technique Title	ID	Use
Compromise Accounts	T1586	ALPHV Blackcat affiliates use compromised accounts to gain access to victims' networks.

Table 3: ALPHV Blackcat/ALPHV Threat Actors ATT&CK Techniques – Credential Access

Technique Title	ID	Use
Obtain Credentials from Passwords Stores	T1555	ALPHV Blackcat affiliates obtain passwords from local networks, deleted servers, and domain controllers.
Adversary-in-the-Middle	T1557	ALPHV Blackcat/ALPHV affiliates use the open-source framework Evilginx2 to obtain MFA credentials, login credentials, and session cookies for targeted networks.

INCIDENT RESPONSE

If compromise is detected, organizations should:

1. Quarantine or take offline potentially affected hosts.
2. Reimage compromised hosts.
3. Provision new account credentials.
4. Collect and review artifacts such as running processes/services, unusual authentications, and recent network connections.

5. Report the compromise or phishing incident to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870). State, local, tribal, or territorial government entities can also report to MS-ISAC (SOC@cisecurity.org or 866-787-4722).
6. To report spoofing or phishing attempts (or to report that you've been a victim), file a complaint with the FBI's Internet Crime Complaint Center (IC3), or contact your local FBI Field Office to report an incident.

MITIGATIONS

FBI and CISA recommend organizations implement the mitigations below to improve your organization's cybersecurity posture based on threat actor activity and to reduce the risk of compromise by ALPHV Blackcat threat actors. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

> These mitigations apply to all critical infrastructure organizations and network defenders. The FBI and CISA recommend that software manufactures incorporate secure-by-design and -default principles and tactics into their software development practices limiting the impact of ransomware techniques, thus, strengthening the security posture for their customers.
>
> For more information on secure by design, see CISA's Secure by Design webpage and joint guide.

- Secure remote access tools by:
  - **Implementing application controls** to manage and control execution of software, including allowlisting remote access programs. Application controls should prevent installation and execution of portable versions of unauthorized remote access and other software. A properly configured application allowlisting solution will block any unlisted application execution. Allowlisting is important because antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation.
  - Applying recommendations in CISA's joint Guide to Securing Remote Access Software.
- **Implementing FIDO/WebAuthn authentication or Public key Infrastructure (PKI)-based MFA** [CPG 2.H]. These MFA implementations are resistant to phishing and not susceptible to push bombing or SIM swap attacks, which are techniques known be used by ALPHV Blackcat affiliates. See CISA's Fact Sheet Implementing Phishing-Resistant MFA for more information.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting ransomware, implement a tool that logs and reports all network traffic [CPG 5.1], including lateral movement activity on a network. Endpoint detection and response (EDR) tools are useful for detecting

lateral connections as they have insight into common and uncommon network connections for each host.

- **Implement user training on social engineering and phishing attacks** [CPG 2.I]. Regularly educate users on identifying suspicious emails and links, not interacting with those suspicious items, and the importance of reporting instances of opening suspicious emails, links, attachments, or other potential lures.
- **Implement internal mail and messaging monitoring**. Monitoring internal mail and messaging traffic to identify suspicious activity is essential as users may be phished from outside the targeted network or without the knowledge of the organizational security team. Establish a baseline of normal network traffic and scrutinize any deviations.
- **Implement free security tools** to prevent cyber threat actors from redirecting users to malicious websites to steal their credentials. For more information see, CISA's Free Cybersecurity Services and Tools webpage.
- **Install and maintain antivirus software.** Antivirus software recognizes malware and protects your computer against it. Installing antivirus software from a reputable vendor is an important step in preventing and detecting infections. Always visit vendor sites directly rather than clicking on advertisements or email links. Because attackers are continually creating new viruses and other forms of malicious code, it is important to keep your antivirus software up to date.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA recommends exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. CISA recommends testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 1-3).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA and FBI recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.

- Resource to reduce the risk of a ransomware attack: #StopRansomware Guide.
- No-cost cyber hygiene services: Cyber Hygiene Services and Ransomware Readiness Assessment.

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. CISA and FBI do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA and FBI.

VERSION HISTORY

December 19, 2023: Initial version.