



Threat Level

 **Red**

 **CISA: AA23-353A**

HiveForce Labs

THREAT ADVISORY



ATTACK REPORT

BlackCat's Resurgence Despite Law Enforcement Disruptions

Date of Publication

February 28, 2024

Admiralty Code

A1

TA Number

TA2024080

Summary

Attack Began: November 2021

Targeted Countries: Worldwide

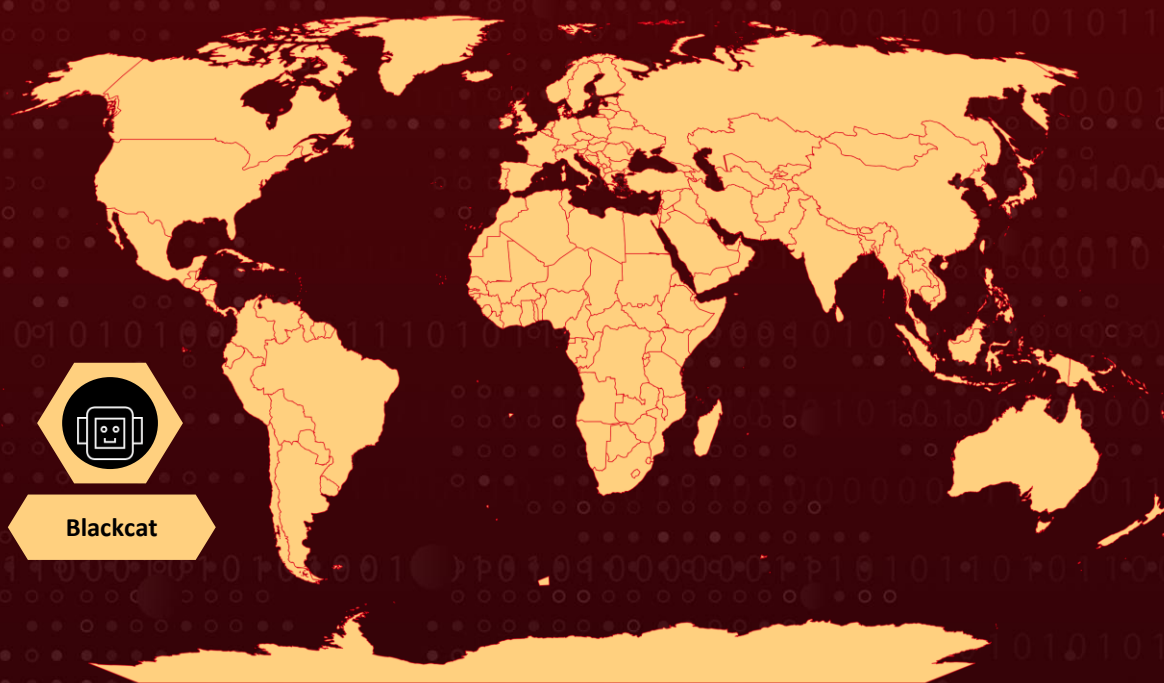
Targeted Industries: Healthcare, Oil and gas, Education, Petroleum, Chemical, Energy, Logistics, Finance, Manufacturing, Legal services, Technology, Transport, Engineering, Professional services, Construction and Retail

Malware: Blackcat Ransomware (aka ALPHV, AlphaV, AlphaVM, ALPHV-ng, or Noberus)



















Affected Platform: Windows, Linux, and VMware ESXi

Attack: Blackcat, a sophisticated Ransomware-as-a-Service operation, infiltrates networks using advanced social engineering and remote access tools, offering triple extortion tactics and cyber remediation advice for ransom payment, and resurged after a December 2023 disruption, causing widespread disruptions in U.S pharmacies.

🔪 Attack Regions



© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin
Powered by Bing

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2016-0099	Microsoft Windows Secondary Logon Service Privilege Escalation Vulnerability	Microsoft Windows			
CVE-2019-7481	SonicWall SMA100 SQL Injection Vulnerability	SonicWall SMA100			
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability	Microsoft Exchange Server			
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server			
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server			
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect			

Attack Details

#1

BlackCat aka AlphaV, was discovered in November 2021 as a suspected rebrand of the DarkSide and BlackMatter ransomware operations. BlackCat is the first known ransomware written in RUST which not only helps the attackers to evade detection but also improves stability and allows it to run on non-windows operating systems like Linux, VMware, etc.

#2

BlackCat operates as a Ransomware-as-a-Service (RaaS), meaning they lease their infrastructure and tools to other cybercriminals, known as affiliates. BlackCat is extremely customizable and can be tailored to create targeted executables, which makes it one of the most sophisticated RaaS operations to date. Its 90% payout has been luring affiliates from other RaaS groups.

#3

ALPHV Blackcat affiliates employ sophisticated social engineering tactics and open-source research to infiltrate targeted company networks. They masquerade as IT or helpdesk personnel to trick employees into revealing credentials via phone calls or SMS messages.

#4

Once inside, they utilize various remote access tools like AnyDesk or Splashtop to prepare for data theft. The creation of a user account named "aadmin" and utilization of legitimate remote access tools aid in lateral movement within the network. Additionally, they leverage frameworks like Evilginx2 to acquire multifactor authentication credentials and passwords from various sources within the network.

#5

They employ a [triple extortion](#) tactic, demanding payment for decrypting encrypted files, threatening to publish the data if the ransom is not paid. It utilizes a signed kernel driver for defense evasion, these drivers are employed to gain privileged-level access and impair security measures on targeted systems.

#6

To avoid detection, they utilize whitelisted applications like Metasploit and clear logs on critical servers. Data exfiltration is facilitated through services like Mega.nz or Dropbox, followed by the deployment of ransomware and embedding ransom notes in affected systems. Some affiliates opt to extort victims without deploying ransomware by exfiltrating data and threatening exposure. Communication with victims occurs through various encrypted channels such as TOR, Tox, or email.

#7

They offer cyber remediation advice as an incentive for ransom payment, promising vulnerability reports and security recommendations. Files encrypted by ALPHV Blackcat follow a specific naming convention: RECOVER-(seven-digit extension) FILES.txt.

#8

In December 2023, a collaborative effort by international law enforcement agencies, including the US FBI, disrupted ALPHV Blackcat's operations. The FBI released a decryption tool, allowing some victims to recover their files without paying the ransom. However, they have resurfaced, causing disruptions at US pharmacies. Security researchers have linked the outage at a UnitedHealth Group unit, via the [ScreenConnect vulnerability \(CVE-2024-1709\)](#), which led to nationwide disruptions.

Recommendations



Keep Software Up-to-Date: Ensure that all software, including operating systems, applications, and security tools, is regularly updated with the latest patches and security updates. This helps to address known vulnerabilities that attackers may exploit.



Conduct Regular Data Backups and Test Restoration: Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom. Regularly test the restoration process to verify the integrity and availability of backups.



Patch Management: Maintain a rigorous patch management process to ensure that all software, including operating systems, web browsers, and security applications, is up-to-date with the latest security patches. Promptly apply patches released by software vendors to mitigate known vulnerabilities.



Endpoint Protection: Deploy advanced endpoint protection solutions that include anti-malware, anti-phishing, and behavior-based detection capabilities. Ensure that endpoint security software is configured to detect and block malicious activities, including attempts to exploit vulnerabilities.



Network Segmentation: Implement network segmentation to restrict the lateral movement of attackers within the network. Segment critical systems and sensitive data from less secure areas of the network to minimize the impact of a successful breach.



Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0002 Execution	TA0008 Lateral Movement	TA0004 Privilege Escalation
TA0011 Command and Control	TA0042 Resource Development	TA0005 Defense Evasion	TA0040 Impact
TA0001 Initial Access	TA0006 Credential Access	T1569 System Services	T1027 Obfuscated Files or Information
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1110 Brute Force	T1562 Impair Defenses

T1588 Obtain Capabilities	T1564 Hide Artifacts	T1486 Data Encrypted for Impact	T1210 Exploitation of Remote Services
T1078 Valid Accounts	T1505 Server Software Component	T1021 Remote Services	T1068 Exploitation for Privilege Escalation
T1040 Network Sniffing	T1041 Exfiltration Over C2 Channel	T1046 Network Service Scanning	T1047 Windows Management Instrumentation
T1106 Native API	T1119 Automated Collection	T1553 Subvert Trust Controls	T1105 Ingress Tool Transfer
T1598 Phishing for Information	T1555 Credentials from Password Stores	T1558 Steal or Forge Kerberos Tickets	T1557 Adversary-in-the-Middle
T1562.001 Disable or Modify Tools	T1562.009 Safe Mode Boot	T1489 Service Stop	T1057 Process Discovery
T1649 Steal or Forge Authentication Certificates	T1588.003 Code Signing Certificates	T1529 System Shutdown/Reboot	T1566 Phishing

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	944153fb9692634d6c70899b83676575, efc80697aa58ab03a10d02a8b00ee740, c90abb4bbbfe7289de6ab1f374d0bcbe, 341d43d4d5c2e526cadd88ae8da70c1c, 34aac5719824e5f13b80d6fe23cbfa07, eea9ab1f36394769d65909f6ae81834b, 379bf8c60b091974f856f08475a03b04, ebca4398e949286cb7f7f6c68c28e838, c04c386b945ccc04627d1a885b500edf, 824d0e31fd08220a25c06baee1044818
Domains	resources.docusong[.]com, Fisa99.screenconnect[.]com
IPv4	5.199.168[.]24, 91.92.254[.]193

TYPE	VALUE
SHA256	c64300cf8bacc4e42e74715edf3f8c3287a780c9c0a38b0d9675d01e7e231f16, 1f5e4e2c78451623cfbf32cf517a92253b7abfe0243297c5ddf7dd1448e460d5, 3670dd4663adca40f168f3450fa9e7e84bc1a612d78830004020b73bd40fcd71, af28b78c64a9effe3de0e5ccc778527428953837948d913d64dbd0fa45942021, bbfe7289de6ab1f374d0bcbeecf31cad2333b0928ea883ca13b9e733b58e27b1, 5d1df950b238825a36fa6204d1a2935a5fbcfe2a5991a7fc69c74f476df67905, bd9edc3bf3d45e3cdf5236e8f8cd57a95ca3b41f61e4cd5c6c0404a83519058e, 732e24cb5d7ab558effc6dc88854f756016352c923ff5155dcb2eece35c19bc0
SHA1	3dd0f674526f30729bced4271e6b7eb0bb890c52, d6d442e8b3b0aef856ac86391e4a57bcb93c19ad, 6b52543e4097f7c39cc913d55c0044fcf673f6fc, 004ba0454feb2c4033ff0bdb2ff67388af0c41b6, 430bd437162d4c60227288fa6a82cde8a5f87100, 1376ac8b5a126bb163423948bd1c7f861b4bfe32, 380f941f8047904607210add4c6da2da8f8cd398

Recent Breaches

unitedhealthgroup.com
verbraucherzentrale-hessen.de
emtek.es
scpllp.com
angelesmentalhealth.com
worthenind.com
familyhealthcenter.com
andfla.ro
hardemanhealth.org
worthenind.com
www.khss.com
austenconsultants.com
vspdental.com
prudential.com
loandepot.com
asaelectronics.com
tnpi.ca
www.thesource.ca
www.procopio.com

herrs.com
arcisgolf.com
newindycontainerboard.com
sercide.com
lvenergy.com
rushenergyservices.com
rushenergyservices.com
maddockhenson.com
graceluthfound.com
jewishhome.org
vailsummitortho.com

Patch Links

<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-032>

<https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0016>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473>

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523>

<https://screenconnect.connectwise.com/download>

References

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a>

<https://www.cisa.gov/news-events/alerts/2024/02/27/cisa-fbi-and-hhs-release-update-stopransomware-advisory-alphv-blackcat>

<https://www.crn.com/news/security/2024/blackcat-ransomware-linked-with-screenconnect-recent-health-care-attacks-us?itc=refresh>

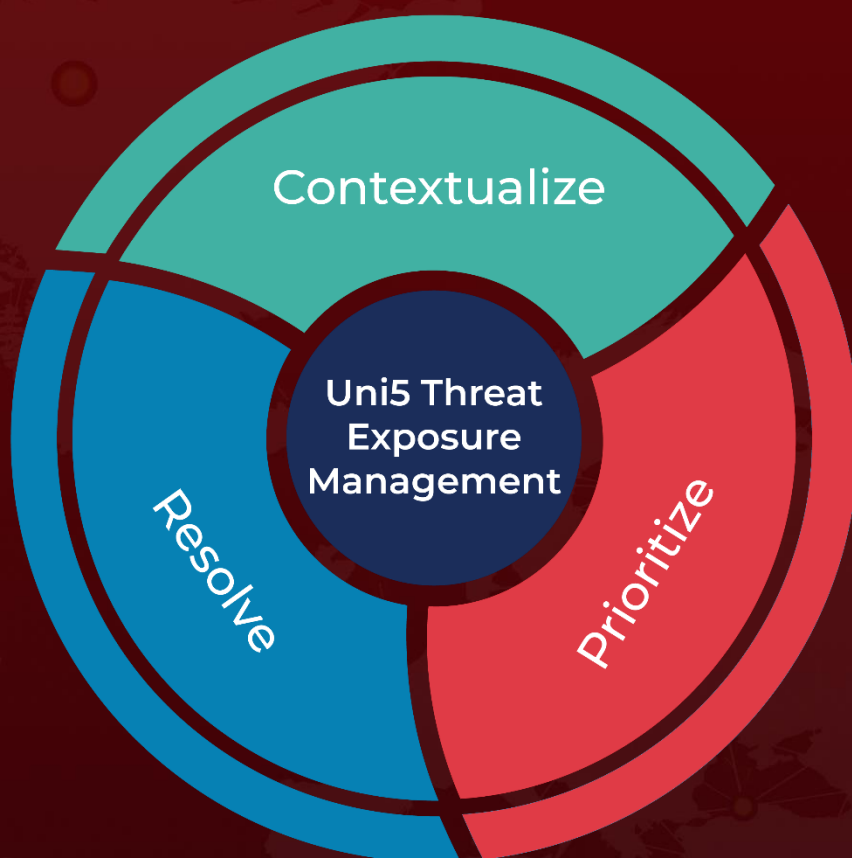
<https://www.hivepro.com/threat-advisory/critical-vulnerabilities-in-screenconnect-under-active-exploitation/>

<https://www.hivepro.com/threat-advisory/advanced-blackcat-ransomware-using-triple-extortion-tactics-and-signed-kernel-driver/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

February 28, 2024 • 7:30 AM

© 2024 All Rights are Reserved by Hive Pro®



More at www.hivepro.com