PROFILE

ALPHV (BlackCat) RANSOMWARE

ZEROFOX INTELLIGENCE

P-2023-03-10a

Classification: TLP:CLEAR
Criticality: Moderate
Intelligence Requirements: PII & Fraud, Deep Dark Web & Criminal Underground

March 10, 2023

Scope Note

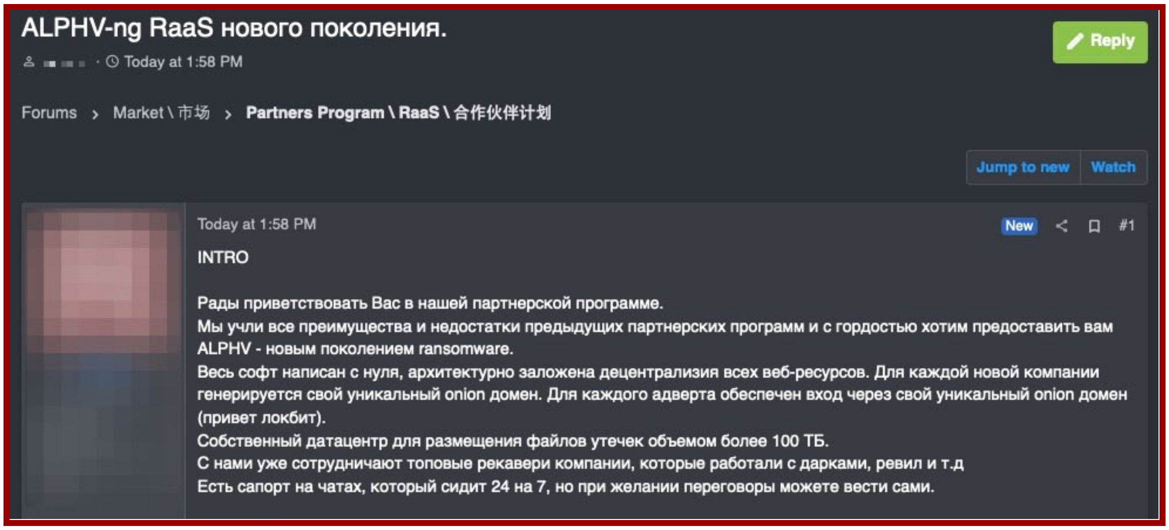
ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 9:00 AM (EST) on March 1, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

ALPHV (BlackCat) Ransomware

Also Known As: BlackCat and Noberus
Status: Active
First Observed: November 2021
Origin: Likely Russia; Russian-speaking
Motivation: Financial; claims to be apolitical
Targeted Industries: Manufacturing, Professional Services, Retail, Technology, Legal Services
Leak Site:
hXXp://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion

Background

ALPHV ransomware, identified as early as November 2021, is one of the most prolific ransomware strains on the market. It follows the ransomware-as-a-service (RaaS) model, which has been extensively used by threat actors to infect and extort victims. In Q4 2022, the strain accounted for at least 11% of global ransomware incidents. ALPHV operator tactics mirror other ransomware collectives and exfiltrate sensitive corporate data before encrypting devices and leverage double-extortion, threatening to release the data if the ransom demands are not met. Operators also experiment with novel extortion tactics, such as providing victim data in an open and searchable format and cloning victims' websites to leak stolen data. ALPHV is coded in Rust programming language, making the strain customizable for both Linux and Windows operating system targets, and also aids detection evasion due to Rust's relative obscurity. On December 9, 2021, ZeroFox Intelligence observed the active promotion and distribution of ALPHV through an affiliate program announced on the dark web RAMP ransomware forum by a user named "ransom."



ALPHV-ng RaaS нового поколения.

[redacted] · Today at 1:58 PM

Reply
Forums › Market \ 市场 › Partners Program \ RaaS \ 合作伙伴计划
Jump to new
Watch
New
#1

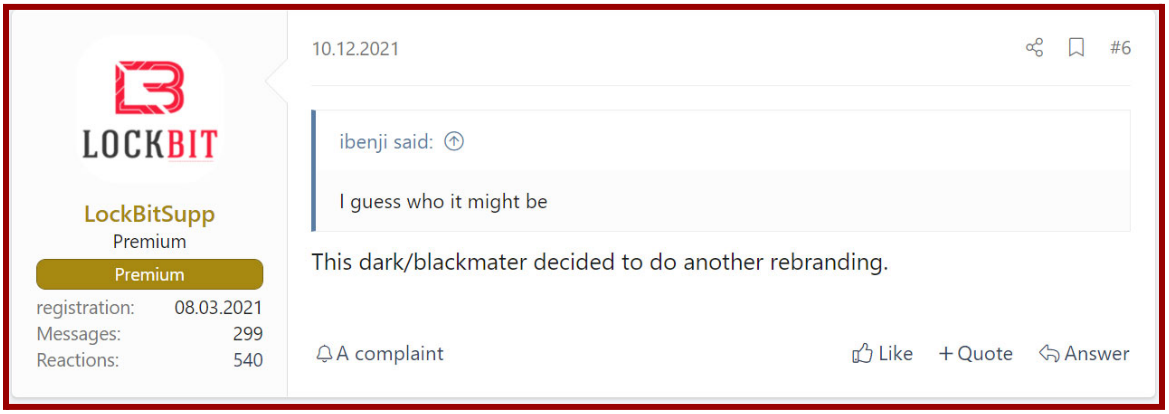
Today at 1:58 PM

INTRO

Рады приветствовать Вас в нашей партнерской программе.
Мы учли все преимущества и недостатки предыдущих партнерских программ и с гордостью хотим предоставить вам ALPHV - новым поколением ransomware.
Весь софт написан с нуля, архитектурно заложена децентрализия всех веб-ресурсов. Для каждой новой компании генерируется свой уникальный onion домен. Для каждого адверта обеспечен вход через свой уникальный onion домен (привет локбит).
Собственный датацентр для размещения файлов утечек объемом более 100 ТБ.
С нами уже сотрудничают топовые рекавери компании, которые работали с дарками, ревил и т.д
Есть сапорт на чатах, который сидит 24 на 7, но при желании переговоры можете вести сами.

Source: ZeroFox Intelligence

Since its emergence, researchers have linked ALPHV to BlackMatter, which was a rebrand of Darkside, used in the attack on the Colonial Pipeline. ZeroFox Intelligence also observed the same rhetoric across cybercriminal communities. In December 2021, the founder of the Lockbit affiliate program also wrote that ALPHV is a rebrand of Dark Side/Black Matter.



registration:	08.03.2021
Messages:	299
Reactions:	540

10.12.2021 #6

> ibenji said:
>
> I guess who it might be

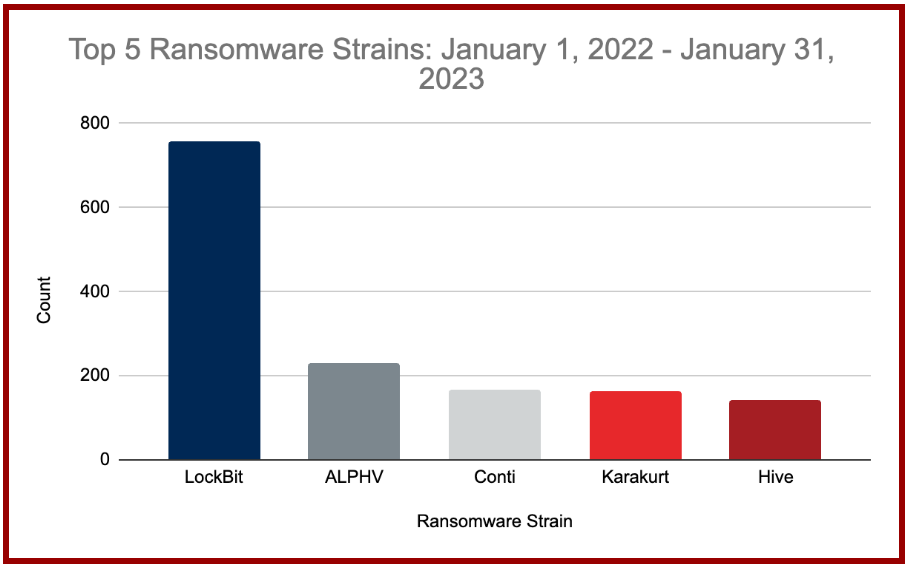
This dark/blackmater decided to do another rebranding.

Source: ZeroFox Intelligence

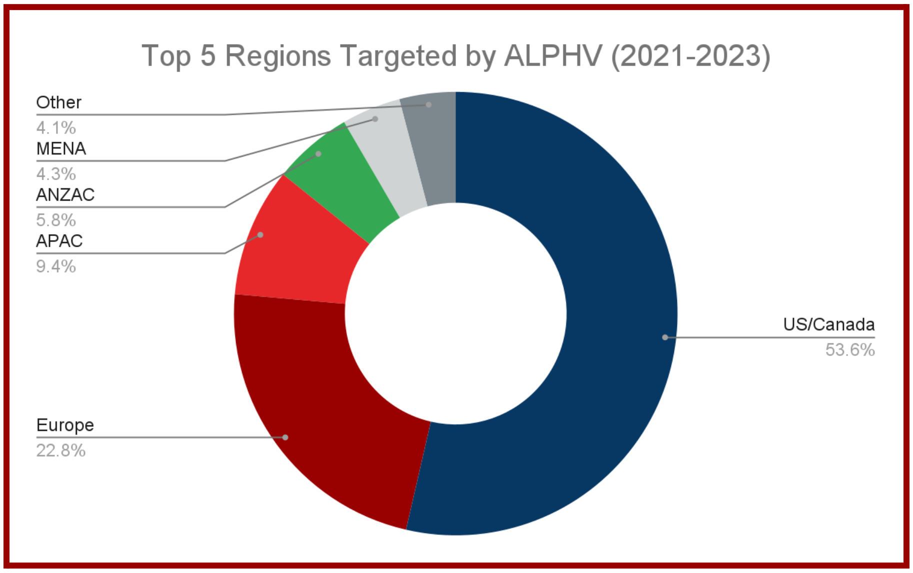
Targeting

Between January 1, 2022, and January 31, 2023, ALPHV accounted for the second-highest number of ransomware incidents among the most notable strains, leveraged in the targeting of at least 200 organizations globally across multiple industries. Although the number of ALPHV victims fell in 2022, ZeroFox Intelligence observed an increase in activity towards the end of the year, a resurgence exceeding the small increase in global ransomware and digital extortion threat. By Q4 2022, ALPHV was leveraged in at least 11% of all ransomware attacks.

More than 75 percent of ALPHV victims are based in North America and Europe, although ZeroFox Intelligence has observed a recent increase in ALPHV affiliates targeting the North America and APAC regions, judging from ZeroFox internal data holdings. ZeroFox has identified no evidence to suggest that ALPHV affiliates disproportionately target ANZAC organizations.

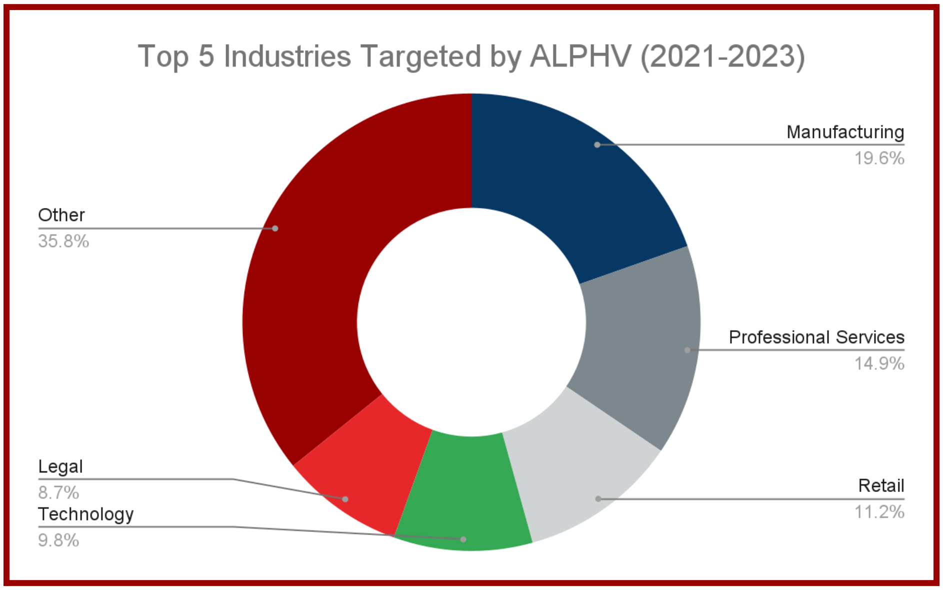


Source: ZeroFox Intelligence



Source: ZeroFox Intelligence

ALPHV has been leveraged to target organizations of all sizes in almost all industries globally. Threat actors deploying the strain have shown a propensity to target organizations within the manufacturing, professional services, and retail sectors. While manufacturing targets make up the largest proportion of the strain's victims, ZeroFox Intelligence notes that ALPHV affiliates targeted retail, technology, and professional services organizations more frequently in 2022 than the global average. Almost 20 percent of ALPHV attacks in Q4 2022 targeted manufacturing.

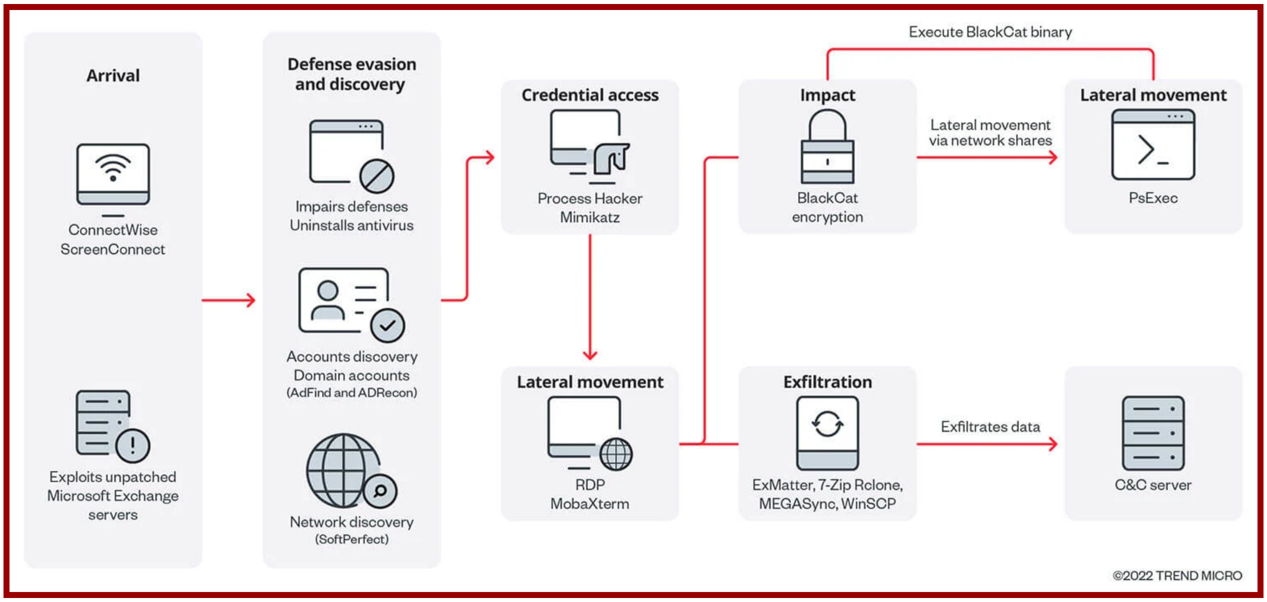


Source: ZeroFox Intelligence

It is notable that the ransomware is capable of infecting both Windows and Linux systems, which means that a broad range of organizations may be vulnerable to this threat. ALPHV has self-imposed restrictions on its targeting, prohibiting attacks on nations belonging to the Commonwealth of Independent States (CIS), as well as government, healthcare, and educational institutions. While it is unclear why the group has chosen to adopt these restrictions, as it considers itself "apolitical", it is worth noting that if an entity belonging to one of these sectors is attacked, ALPHV claims that it will provide free decryption and ban the offending affiliate.

Tactics, Techniques, and Procedures

ALPHV affiliates leverage a variety of intrusion vectors, including exploiting known vulnerabilities in Microsoft Exchange servers and firewalls, as well as previously compromised user credentials for Remote Desktop Protocol (RDP) and Virtual Private Networks (VPNs).


Arrival
ConnectWise ScreenConnect
Exploits unpatched Microsoft Exchange servers
Defense evasion and discovery
Impairs defenses Uninstalls antivirus
Accounts discovery Domain accounts (AdFind and ADRecon)
Network discovery (SoftPerfect)
Credential access
Process Hacker Mimikatz
Lateral movement
RDP MobaXterm
Execute BlackCat binary
Impact
BlackCat encryption
Lateral movement via network shares
Lateral movement
PsExec
Exfiltration
ExMatter, 7-Zip Rclone, MEGASync, WinSCP
Exfiltrates data
C&C server
©2022 TREND MICRO

Source:
hXXps://www.trendmicro[.]com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat

ALPHV is also known to compromise Active Directory accounts with user or administrator privileges and leverages Windows Task Scheduler to deploy payloads via malicious Group Policy Objects. In some cases, threat actors leveraged PowerShell commands to download and execute Cobalt Strike beacons and used a post-exploitation tool called Brute Ratel– a tool that became increasingly popular with malware operators towards the end of 2022 and enables arbitrary command execution to perform lateral movement, privilege escalation, and establish persistence. Brute Ratel can generate shellcode that is undetected by many endpoint detection and response (EDR) and antivirus (AV) services. During compromise, ALPHV also makes use of Windows administrative tools and Microsoft Sysinternals tools. ALPHV exfiltrates victim data prior to the execution of the ransomware, either from local systems or cloud services. According to open sources, PowerShell scripts observed include[1]:

- start.bat - launches the ransomware executable with required arguments
- est.bat - copies the ransomware to other locations
- drag-and-drop-target.bat - launches the ransomware executable for the MySQL Server
- run.bat - executes a callout command to an external server using SSH - file names may change
- depending on the company and systems affected
- Runs1.ps1 – PowerShell script to disable McAfee

[1] hXXps://www.ic3[.]gov/Media/News/2022/220420.pdf

ALPHV ransomware is highly customizable. Using Rust programming language, the malware authors can easily compile their malware to target multiple operating system architectures. This is due to Rust's inherent flexibility, which allows the group to easily adapt and customize their attacks as needed.

ZeroFox Intelligence observed ALPHV affiliates implementing various extortion techniques in addition to file encryption and ransom demand. ALPHA operators exfiltrate sensitive corporate data before encrypting devices and leverage double-extortion tactics by threatening to release the exfiltrated data if the ransom demands are not met. Operators also experiment with additional–and in some cases novel–extortion tactics, such as providing victim data in an open and searchable format, cloning victims' websites to leak stolen data, and threatening the victim with Distributed Denial of Service (DDoS) attacks if they do not comply with ransom demands.

Indicators of Compromise[2]

SHA256

847fb7609f53ed334d5affbb07256c21cb5e6f68b1cc14004f5502d714d2a456
0ea5dfd5682892d6d84c9775f89faad0c3c8ecce89dfbba010a61a87b258969e
f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb
731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161
80dd44226f60ba5403745ba9d18490eb8ca12dbc9be0a317dd2b692ec041da28
C50bca08a8e80850ec18d258ff937b7b72a500d9027c730c86b05aa73c938b5d
3a08e3bfec2db5dbece359ac9662e65361a8625a0122e68b56cd5ef3aedf8ce1
5121f08cf8614a65d7a86c2f462c0694c132e2877a7f54ab7fcefd7ee5235a42
9802a1e8fb425ac3a7c0a7fca5a17cfcb7f3f5f0962deb29e3982f0bece95e26
e7060538ee4b48b0b975c8928c617f218703dab7aa7814ce97481596f2a78556
f7a038f9b91c40e9d67f4168997d7d8c12c2d27cd9e36c413dd021796a24e083
F8c08d00ff6e8c6adb1a93cd133b19302d0b651afd73ccb54e3b6ac6c60d99c6
67d1f4077e929385cfd869bf279892bf10a2c8f0af4119e4bc15a2add9461fec
0a609fa2db910615b2c1ad235ca46562ff4034800c44802a63a28826669a7eee
cda37b13d1fdee1b4262b5a6146a35d8fc88fa572e55437a47a950037cc65d40
bacedbb23254934b736a9daf6de52620c9250a49686d519ceaf0a8d25da0a97f

SHA1

d241df7b9d2ec0b8194751cd5ce153e27cc40fa4
4831c1b113df21360ef68c450b5fca278d08fae2
fce13da5592e9e120777d82d27e06ed2b44918cf
3f85f03d33b9fe25bcfac611182da4ab7f06a442

[2] Actual indicators might vary per attack.

37178dfaccbc371a04133d26a55127cf4d4382f8
1b2a30776df64fbd7299bd588e21573891dcecbe
53489b26fcceff4ef3240b2efcbfb38a78d24c4d

MD5

Db7a7403e5e248d0e96efe67cef73449
861738dd15eb7fb50568f0e39a69e107
9f60dd752e7692a2f5c758de4eab3e6f
09bc47d7bc5e40d40d9729cec5e39d73
F5ef5142f044b94ac5010fd883c09aa7
84e3b5fe3863d25bb72e25b10760e861
9f2309285e8a8471fce7330fcade8619
6c6c46bdac6713c94debbd454d34efd9
E7ee8ea6fb7530d1d904cdb2d9745899
994de6a3f96bd710d620e1396e1bec92

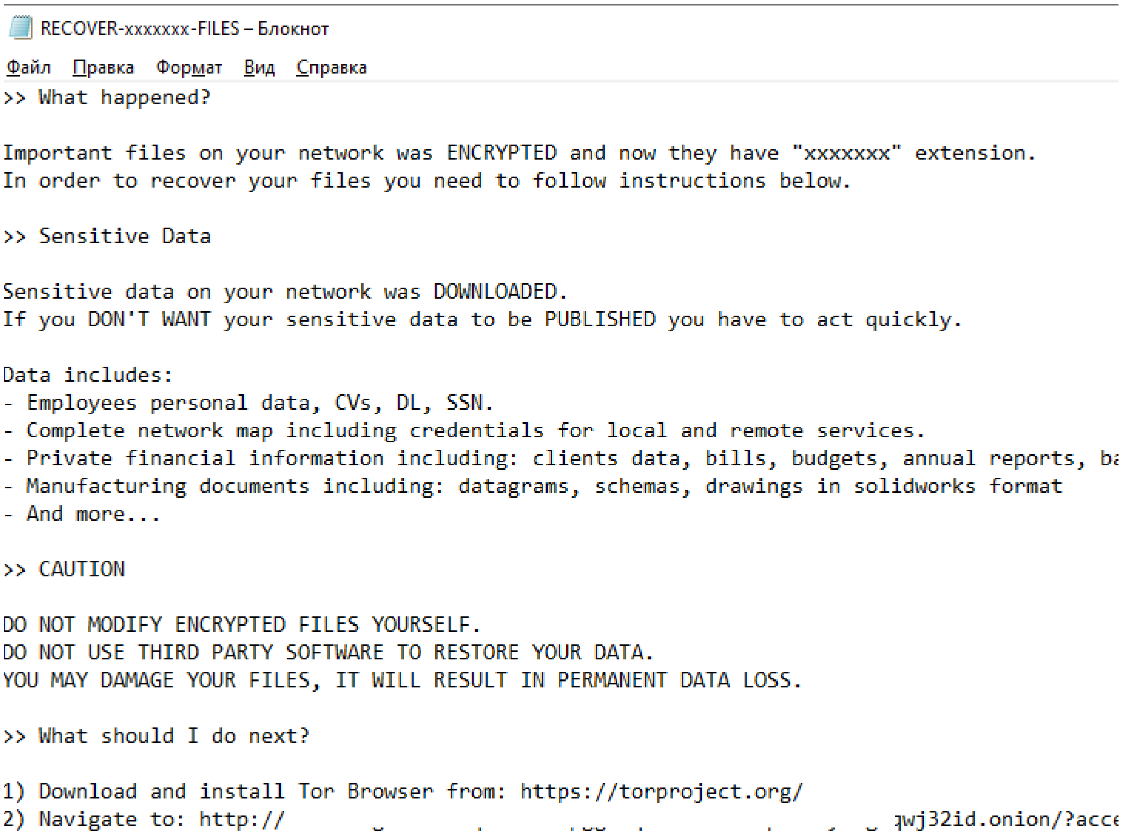
C2 IPs

89.44.9.243
142.234.157.246
45.134.20.66
185.220.102.253
37.120.238.58
152.89.247.207
198.144.121.93
89.163.252.230
45.153.160.140
23.106.223.97
139.60.161.161
146.0.77.15
94.232.41.155

Detection Name

Ransom.Win32.BLACKCAT.SMYXBLK
Ransom.Win32.BLACKCAT.YMCAE
Ransom.Win32.BLACKCAT.SMYXBLK

ALPHV Ransom Note



```
>> What happened?

Important files on your network was ENCRYPTED and now they have "xxxxxxx" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, ba
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?

1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to: http://                                          qwj32id.onion/?acce
```

Files Created

checkpoints-<Filename>.uhwuvzu
RECOVER-uhwuvzu-FILES.txt.png

Processes Spawned

cmd.exe /c “wmic csproduct get UUID”
cmd.exe /c “fsutil behavior set SymlinkEvaluation R2L:1”
cmd.exe /c “fsutil behavior set SymlinkEvaluation R2R:1”
cmd.exe /c “iisreset.exe /stop”
cmd.exe /c “vssadmin.exe Delete Shadows /all /quiet”
cmd.exe /c “wmic.exe Shadowcopy Delete”
cmd.exe /c “bcdedit /set {default}”
cmd.exe /c “bcdedit /set {default} recoveryenabled No”
cmd.exe /c for /F “tokens=*” %1 in (‘wevtutil.exe el’) DO wevtutil.exe cl %1

```
cmd.exe /c “reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f”
cmd.exe /c “arp -a”
```

TOX

3488458145EB62D7D3947E3811234F4663D9B5AEEF6584AB08A2099A7F946664BBA2B0D30BFC,16BF03E7266A1859E5032203EB546C1DFD1AF6D72A23A863B0100198354C9F7D330C2001EA1B

Jabber

username01@thesecure.biz

Recommendations

- Regularly back up critical data, including password-protected backup copies kept offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, or the cloud).
- Ensure proper network segmentation.
- Never download email attachments from unknown senders or click links from untrusted sources. Provide user training programs to fight against phishing or social engineering attacks used to obtain critical information that can lead to attacks.
- Enable secure multi-factor authentication wherever possible.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Patch disclosed vulnerabilities with updated software versions as quickly as practical.
- Secure PowerShell wherever possible to limit the possibility of operators employing lateral movement modules.
- Should your organization be impacted by this type of cyber event, engage with ZeroFox for support through our DarkOps and Incident Response teams by utilizing the RFI button in the ZeroFox platform.

Appendix: Traffic-Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**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.	**Sources may use TLP:** AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share TLP:** RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share TLP:** AMBER information with members of their own organization and only as widely as necessary to act on that information.

	Green	White
WHEN SHOULD IT BE USED?	**Sources may use TLP:** GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use TLP:** WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share TLP:** GREEN information with peers & partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share TLP:** WHITE information without restriction, subject to copyright controls.