Cyber Threat Advisory

ALPHV

Threat Actor Ransomware

CATEGORY

Ransomware

SEVERITY

High

Platforms

Windows & Linux

IMPACT

- **Data Encryption and Ransom Demands**
- **Operational Disruption**
- **Propagation Across Networks**
- **Financial Losses**
- **Data Breaches and Leakage**
- **Increased Security Expenditures**
- **Impact on Various Sectors**

Description

ALPHV

ALPHV, also known as BlackCat or Noberus, is a ransomware family utilized in Ransomware as a Service (RaaS) operations. Written in Rust, ALPHV is compatible with Windows, Linux-based operating systems (including Debian, Ubuntu, ReadyNAS, Synology), and VMWare ESXi. Although marketed as ALPHV on cybercrime forums, security researchers commonly refer to it as BlackCat due to a black cat icon on its leak site. ALPHV has been involved in ransomware attacks since November 18, 2021. It can encrypt files using either AES or ChaCha20 algorithms. To maximize the amount of ransomed data, ALPHV can delete volume shadow copies, stop processes and services, and halt virtual machines on ESXi servers. Additionally, ALPHV can propagate itself across a local network by using PsExec to remotely execute on other hosts.

Indicator of compromise

SHA-256

1d3e573d432ef094fba33f615aa0564feffa99853af77e10367f54dc6df95509

307c3e23a4ba65749e49932c03d5d3eb58d133bc6623c436756e48de68b9cc45

48e3add1881d60e0f6a036cfdb24426266f23f624a4cd57b8ea945e9ca98e6fd

4db89c39db14f4d9f76d06c50fef2d9282e83c03e8c948a863b58dedc43edd31

356adc348e9a28fc760e75029839da5d374d11db5e41a74147a263290ae77501

e7175ae2e0f0279fe3c4d5fc33e77b2bea51e0a7ad29f458b609afca0ab62b0b

e4e3a4f1c87ff79f99f42b5bbe9727481d43d68582799309785c95d1d0de789a

2cd2e79e18849b882ba40a1f3f432a24e3c146bb52137c7543806f22c617d62c

78109d8e0fbe32ae7ec7c8d1c16e21bec0a0da3d58d98b6b266fbc53bb5bc00e

ede6ca7c3c3aedeb70e8504e1df70988263aab60ac664d03995bce645dff0935

5b8b732d0bb708aa51ac7f8a4ff5ca5ea99a84112b8b22d13674da7a8ca18c28

4e73e9a546e334f0aee8da7d191c56d25e6360ba7a79dc02fe93efbd41ff7aa4

05236172591d843b15987de2243ff1bfb41c7b959d7c917949a7533ed60aafd9

edfd3ae4def3ddffb37bad3424eb73c17e156ba5f63fd1d651df2f5b8e34a6c7

827448cf3c7ddc67dca6618f4c8b1197ee2abe3526e27052d09948da2bc500ea

0e11a050369010683a7ed6a51f5ec320cd885128804713bb9df0e056e29dc3b0

0980aa80e52cc18e7b3909a0173a9efb60f9d406993d26fe3af35870ef1604d0

5d1df950b238825a36fa6204d1a2935a5fbcfe2a5991a7fc69c74f476df67905

3670dd4663adca40f168f3450fa9e7e84bc1a612d78830004020b73bd40fcd71

1f5e4e2c78451623cfbf32cf517a92253b7abfe0243297c5ddf7dd1448e460d5

e594dc53d2bf4518632e9ca4308a11a0b10409f035554255bbdc7e3f577fe585

afd0c82318a32f3a82bbc8320e03e33ee84e3fb3c8a64b3fe06a48fc37682dae

03b9ee39f5316efe71b0c915374da7d3d4b393ed402d4fe6b57cbc38ac60783b

a39d9b1b41157510d16e41e7c877b35452f201d02a05afa328f1bcd53d8ee016

1362e6d43b068005f5d7c755e997e6202775430ac15a794014aa9a7a03a974e7

fa131238c3c35efe99cde59dd409c0436fd642b6bf5d56f994f52ab3a62bae4e

e3401d7699cc5067620e43bd24e8ccd437832c16f2fa7d5baaad8c170383cc92

cc13b5721f2ee6081c1244dd367a9de958353c29e32ea8b66e3b20b293fabc55

8e51de4774d27ad31a83d5df060ba008148665ab9caf6bc889a5e3fba4d7e600

86b5d7dd88b46a3e7c2fb58c01fbeb11dc7ad350370abfe648dbfad45edb8132

47d83461ee57031fd2814382fb526937a4cfa9a3eea7a47e4e7ee185c0602b27

3a659609850664cbc0683c8c7b92be816254eb9306e7fb12ad79d5a9af0fb623

11d2dde6c51e977ed6e3f3d3e256c78062ae41fe780aefecfba1627e66daf771

ce26642327aa55c67a564f695ae3038d5afee9b8d14bb5146bf30dd0f1af24e5

SHA-256

64f8ac7b3b28d763f0a8f6cdb4ce1e5e3892b0338c9240f27057dd9e087e3111

2d39a58887026b99176eb16c1bba4f6971c985ac9acbd9e2747dd0620548aaf3

8cfb05cde6af3cf4e0cb025faa597c2641a4ab372268823a29baef37c6c45946

72fd2f51f36ba6c842fdc801464a49dce28bd851589c7401f64bbc4f1a468b1a

6cba6d8a1a73572a1a49372c9b7adfa471a3a1302dc71c4547685bcbb1eda432

1dab85cf02cf61de30fcda209c8daf15651d649f32996fb9293b71d2f9db46e1

6f4a0cc0fa22b66f75f5798d3b259d470beb776d79de2264c2affc0b5fa924a2

679fad2fd86d2fd9e1ec38fa15280c1186f35343583c7e83ab382b8c255f9e18

e179a9e5d75d56140d11cbd29d92d8137b0a73f964dd3cfd46564ada572a3109

c64300cf8bacc4e42e74715edf3f8c3287a780c9c0a38b0d9675d01e7e231f16

bd9edc3bf3d45e3cdf5236e8f8cd57a95ca3b41f61e4cd5c6c0404a83519058e

bbfe7289de6ab1f374d0bcbeecf31cad2333b0928ea883ca13b9e733b58e27b1

c06e320ad2568e15baae155346c6fb92e18fc038e7465adfb5fc2a3f8af9caa5

8d5c521d7a52fd0b24d15c61c344a8f87b3b623a1ab3520ab55197b772377155

7ebe51d5a48cc3c01878e06c6db3f4f0189c4f9788bfe57b763b03f4ab910e26

6ec7a25adc9bf516e9150bebd773feafa64787769156ffbcb6eccabc579ee03a

4c1346eab3fb23ca0613d73bbd2dd87fedb6ca8b1ba7bf48d69a57868d05854d

19707b18f750bae0214e2a6d36735b6723549899bf83751d3650b9ec8125b91f

13d525588d2f6babe0b6de7d1456a6f3f39a0947128280a94b6f676dd5684201

09f7622eb9ed3bbd375575c8a190ff152ef3572a717a20c1b2dd5556b8cc9eba

005cfd8a4dd101c127bcb0f94f1fa143b24d91442ee9e1525b4c540c9fe88c63

af28b78c64a9effe3de0e5ccc778527428953837948d913d64dbd0fa45942021

732e24cb5d7ab558effc6dc88854f756016352c923ff5155dcb2eece35c19bc0

SHA -1

ffaa1f429e72ea875541a06294445d58d989c4cc

cc3d54fd20d3ddbc811b063f70b24ea4dda7807b

08750c05472cb9de2650ae800b6c790fe812b715

d6d442e8b3b0aef856ac86391e4a57bcb93c19ad

6b52543e4097f7c39cc913d55c0044fcf673f6fc

430bd437162d4c60227288fa6a82cde8a5f87100

3dd0f674526f30729bced4271e6b7eb0bb890c52

380f941f8047904607210add4c6da2da8f8cd398

1376ac8b5a126bb163423948bd1c7f861b4bfe32

004ba0454feb2c4033ff0bdb2ff67388af0c41b6

4d661f7dc3be493780ab5cdf655d7c42473ee5da

badd7a5231217749bf947e64390f73ac933cd4e8

9459f3499b90f90b17911cc1047b3fa625ad83b5

7f0ed21819595bb72dba05f6b7e6efdd9b9bed3f

36aa43055abadb7e7b37a5fb99125ac587e1c147

ef43f25a27e5f34ca748c4116f9fc607525228da

ffaa1f429e72ea875541a06294445d58d989c4cc

cc3d54fd20d3ddbc811b063f70b24ea4dda7807b

08750c05472cb9de2650ae800b6c790fe812b715

d6d442e8b3b0aef856ac86391e4a57bcb93c19ad

MD-5

f2590ece758eb32302c504ac3ff413f4

dd378ade8ce19f6585b2280de53779fb

f0a3499f83d2d9066ab19d39b9af6696

c04c386b945ccc04627d1a885b500edf

944153fb9692634d6c70899b83676575

824d0e31fd08220a25c06baee1044818

379bf8c60b091974f856f08475a03b04

341d43d4d5c2e526cadd88ae8da70c1c

34aac5719824e5f13b80d6fe23cbfa07

eea9ab1f36394769d65909f6ae81834b

ebca4398e949286cb7f7f6c68c28e838

af2b1882f7cc9c7ebbc7ff20e872c6d9

56bf47ebf4595ca4972af03332254d99

dd287eb11b2f9f034115edaa7aa33b10

b9bf8efb56cb3398e5fa149863cbb749

6e4f71e2c61fb671c6ade8c6f265928a

4e8f19da7c984434e4d718f45f6c9f4f

f2590ece758eb32302c504ac3ff413f4

dd378ade8ce19f6585b2280de53779fb

f0a3499f83d2d9066ab19d39b9af6696

Host Name

alternativebehavioralconcepts.org

birdarid.org

notione.my-apk.com

yogapets.xyz

cerisico.net

rollecoin.online

cloudmine.online

dns.artstrailreviews.com

kenparkmdpllc.com

sgacor.kenparkmdpllc.com

wipresolutions.com

minerclouds.xyz

resources.docusong.com

alternativebehavioralconcepts.org

birdarid.org

notione.my-apk.com

yogapets.xyz

cerisico.net

rollecoin.online

cloudmine.online

Remediation

- Isolate Infected Systems: Disconnect from the network to prevent spread.
- Identify and Analyze: Determine the ransomware variant and scope.
- Restore from Backups: Use clean, recent backups to restore data.
- Rebuild Systems: Rebuild or verify system integrity before reconnecting.
- Patch and Update: Apply all security patches and updates.
- Enhance Security: Implement EDR, strengthen firewalls, and update anti-malware solutions.
- Reset Credentials: Change passwords and enforce MFA.
- User Training: Educate employees on cybersecurity best practices.
- Block all IOCs on your XDR, EDR and other security tools.

THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

Cyber Threat Advisory

Secure your byte world

+1 (832) 271 2738

info@threatcure.net

https://threatcure.net/