Hive Pro

THREAT ADVISORY

BlackCat Ransomware group attacks on the rise	TA2022035
Threat Level RED	**Publish Date –** Feb 16, 2022

The Blackcat Ransomware gang also known as ALPHV has targeted around 25 organizations belonging to multiple sectors globally since November 2021. The group has claimed responsibility for the recent cyber attack on Swissport which resulted in aircraft delays and service disruptions.

The current attack was carried out by first acquiring access via either leaked credentials or exposed vulnerable software. The attackers then disable defenses such as Windows Defender and increase the connection limit on remote connections for better data exfiltration. The Blackcat ransomware then terminates a series of pre-defined processes before beginning the encryption process with either AES or ChaCha20 encryption. Encrypted files have the extension ".sykffle" attached to them. Blackcat uses 7zip and Rclone to exfiltrate data, which is subsequently put on their website for sale if the ransom is not paid.

The notable capabilities of the ransomware written in rust include embedded PsExec, Powershell process migration capabilities, ability to infect VMWare ESXi service and also has built-in anti-recovery method that deletes the shadow volume copy using "vssadmin.exe".
The user can mitigate the risk by following the recommendations:

- Monitor the use of stolen credentials.
- Have an effective backup strategy that ensures the backup are inaccessible from the endpoint.
- Keep all operating systems and software up to date.
- Implement a user training program and phishing exercises.

The Techniques commonly used by Blackcat are:

TA0001: Initial Access
TA0002: Execution
TA0007: Discovery
TA0005: Defense Evasion
TA0040: Impact
TA0003: Persistence
TA0004: Privilege Escalation
TA0006: Credential Access
TA0011: Command and Control
TA0010: Exfiltration
T1027: Obfuscated Files or Information
T1007: System Service Discovery
T1059: Command and Scripting Interpreter
T1082: System Information Discovery
T1490: Inhibit System Recovery
T1485: Data Destruction
T1078: Valid Accounts
T1486: Data Encrypted For Impact
T1140: Encode/Decode Files or Information
T1202: Indirect Command Execution
T1543.003: Create or Modify System Process: Windows Service
T1550.002: Use Alternate Authentication Material: Pass the Hash
T1027.002: Obfuscated Files or Information: Software Packing

Hive Pro

THREAT ADVISORY

Actor Details

Name	Target Locations	Target sectors	Motive
BlackCats aka ALPHV	Worldwide	Construction and engineering, retail, transportation, commercial services, insurance, machinery, professional services, telecommunication, auto components and pharmaceuticals	Financial gain

Indicators of Compromise (IoCs)

Type	Value
SHA-256	0c6f444c6940a3688ffc6f8b9d5774c032e3551ebbccb64e4280ae7fc1fac479 13828b390d5f58b002e808c2c4f02fdd920e236cc8015480fa33b6c1a9300e31 15b57c1b68cd6ce3c161042e0f3be9f32d78151fe95461eedc59a79fc222c7ed 1af1ca666e48afc933e2eda0ae1d6e88ebd23d27c54fd1d882161fd8c70b678e 28d7e6fe31dc00f82cb032ba29aad6429837ba5efb83c2ce4d31d565896e1169 2cf54942e8cf0ef6296deaa7975618dadff0c32535295d3f0d5f577552229ffc 38834b796ed025563774167716a477e9217d45e47def20facb027325f2a790d1 3d7cf20ca6476e14e0a026f9bdd8ff1f26995cdc5854c3adb41a6135ef11ba83 4e18f9293a6a72d5d42dad179b532407f45663098f959ea552ae43dbb9725cbf 59868f4b346bd401e067380cac69080709c86e06fae219bfb5bc17605a71ab3f 731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161 74464797c5d2df81db2e06f86497b2127fda6766956f1b67b0dcea9570d8b683 7b2449bb8be1b37a9d580c2592a67a759a3116fe640041d0f36dc93ca3db4487 7e363b5f1ba373782261713fa99e8bbc35ddda97e48799c4eb28f17989da8d8e bd337d4e83ab1c2cacb43e4569f977d188f1bb7c7a077026304bf186d49d4117 c3e5d4e62ae4eca2bfca22f8f3c8cbec12757f78107e91e85404611548e06e40 c8b3b67ea4d7625f8b37ba59eed5c9406b3ef04b7a19b97e5dd5dab1bd59f283 cefea76dfdbb48cfe1a3db2c8df34e898e29bec9b2c13e79ef40655c637833ae f815f5d6c85bcbc1ec071dd39532a20f5ce910989552d980d1d4346f57b75f89 f8c08d00ff6e8c6adb1a93cd133b19302d0b651afd73ccb54e3b6ac6c60d99c6
SHA-1	087497940a41d96e4e907b6dc92f75f4a38d861a 11203786b17bb3873d46acae32a898c8dac09850 2a53525eeb7b76b3d1bfe40ac349446f2add8784 45212fa4501ede5af428563f8043c4ae40faec76 57a6dfd2b021e5a4d4fe34a61bf3242ecee841b3 5869820f261f76eafa1ba00af582a9225d005c89 5c6ca5581a04955d8e4d1fa452621fbc922ecb7b 655c2567650d2c109fab443de4b737294994f1fd 783b2b053ef0345710cd2487e5184f29116e367c 89060eff6db13e7455fee151205e972260e9522a 9146a448463935b47e29155da74c68d16e0d7031 94f025f3be089252692d58e54e3e926e09634e40 a186c08d3d10885ebb129b1a0d8ea0da056fc362 c1187fe0eaddee995773d6c66bcb558536e9b62c ce5540c0d2c54489737f3fefdbf72c889ac533a9 d65a131fb2bd6d80d69fe7415dc1d1fd89290394 da1e4a09a59565c5d62887e0e9a9f6f04a18b5f4 e17dc8062742878b0b5ced2145311929f6f77abd e22436386688b5abe6780a462fd07cd12c3f3321

Hive Pro

THREAT ADVISORY

Recent Breaches

https://www.swissport.com/en
https://www.moncler.com/en-gb/
https://www.oiltanking.com

References

https://www.bleepingcomputer.com/news/security/blackcat-alphv-claims-swissport-ransomware-attack-leaks-data/
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware
https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/blackcat-ransomware-as-a-service.html
https://www.cisa.gov/uscert/ncas/alerts/aa22-040a