KPMG Cyber Threat Intelligence Platform

BlackCat Ransomware - Known for its sophistication

BlackCat Ransomware aka ALPHAV, first seen in November 2021 – written in Russian, quickly rose to prominence due to its sophistication and innovation. The malware is among the first to use Rust programming language which enables easy compilation across various operating system architectures and facilitates the capability to pivot and individualize attacks. Following an aggressive approach, they listed over a dozen victims on their leak sites in just over a month.

The Ransomware gang uses a triple extortion technique; steal sensitive data, encrypt the servers and threatens to launch distributed denial-of-service (DDoS) attack if the demands are not met. The ransomware group has been actively recruiting ex-REvil, BlackMatter & DarkSide operators, offering them remunerative affiliate payout of 90% and have targeted organizations across US, Europe & Philippines to name a few. The ransomware has also been linked to the attack on German oil companies, causing serious disruptions across hundreds of gas stations and impacted the fuel-distribution systems forcing the companies to reroute their supplies.

The ransomware uses common tools like Mimikatz, LaZagne and WebBrowserPassView to gain access to stored passwords, MEGAsync to extract data, anti-forensics tools like Fileshredder. The executable of ransomware provides extensive customization like encryption extension, ransom notes, auto-termination of services/processes and path/types of files to be excluded. Domain credentials can also be configured that can be effectively used to spread the ransomware and encrypt other devices on the network. The executable will then extract PSExec and use it to copy the ransomware to other devices on the network and execute it to encrypt the remote Windows machine.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

BlackCat Ransomware - Known for its sophistication

Indicators of Compromise: Domains
zujgzbu5y64xbmvc42addp4lxkoosb4tslf5mehnh7pvqjpwxn5gokyd[.]onion
sty5r4hhb5oihbq2mwevrofdiqbgesi66rvxr5sr573xgvtuvr4cs5yd[.]onion
mu75ltv3lxd24dbyu6gtvmnwybecigs5auki7fces437xvvflzva2nqd[.]onion
id7seexjn4bojn5rvo4lwcjgufjz7gkisaidckaux3uvjc7l7xrsiqad[.]onion
htnpafzbvddr2llstwbjouupddflqm7y7cr7tcchbeo6rmxpqoxcbqqd[.]onion
aoczppoxmfqqthtwlwi4fmzlrv6aor3isn6ffaiic55wrfumxslx3vyd[.]onion
alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad[.]onion
2cuqgeerjdba2rhdiviezodpu3lc4qz2sjf4qin6f7std2evleqlzjid[.]onion
b6v4ojs7jfvftvcoagjxp7qz33yeljydqy6afzsh26vqbzcjwz4b3zad[.]onion
odf3dt34tkqndw5h2l5gt2gwwd3jct5rwwjusbd3vlin2jueyv2qkgid[.]onion
y4722ss64vel5hmph75te7lx2x5xz463322ypjirm5ytxviijtdpybid[.]onion
rfosusl6qdm4zhoqbqnjxaloprld2qz35u77h4aap46rhwkouejsooqd[.]onion
xqoykemmcivwtpxh3a6pu3w7sstr2y7hapxdiv4caaxidurmwwbjx2id[.]onion
b4twqa2mvob3s6uvuyfra5xk3qgps2v5kkt7k2qnb7rpdu3j4fkntead[.]onion
l37tauvuvjzsl7grehyvzg2nvvcyx7fjvvduifdxxw5hg6eqcxnf6oad[.]onion
xnsbsjciylsg23zfmrv6ocuyh7ha5zexeouchlr3zsi5suda4arpeyqd[.]onion
74tutyjtwhxssfw7eax7gkb5upyo5dkmfxwzypk4sd3f3334z6anziyd[.]onion
43nk37hlzlc6w4fyqlco3w4ue34pocmzzliiy2ibkzc3tec7vqcdqsid[.]onion
pwvzjyle6fjb5rnqmqgt4uq4xoy54qk2jumss2wmt2wwczd4j4rsquyd[.]onion
wvbd67q3iuli2gdhtn7dloxaat72fzat6v2kytqgpupcvfmam4x3uwad[.]onion

Indicators of Compromise: Hashes
187bff96e7c4580f65c74bf5a6cc752d
dbeac48687a38094ee6f230f39283c5d
ac440698d3b8aa4cb9682ad92c56c4cc
01d1009e3f1a1b5c7159f84474d9e87e
d41d8cd98f00b204e9800998ecf8427e
085b8046d0c3958d78751b6825052d66
7d5c8fad34f0bbe5bc805b592737443a
b1c67f120df6d0dbe4bba7d4e180571e
eec96fa3f1b419efebfdbf7950736890
a63597e9f6e6b8e63ae4fe33942b1592
edca2cecac7ab6150a401f7c20f890b4

KPMG

KPMG Cyber Threat Intelligence Platform

BlackCat Ransomware - Known for its sophistication

Indicators of Compromise: Hashes
18a0d9e2af4ca21b5043970b83cadb53
49f861dd4ba8e7729af5ccc1572b402b
70b8bc74f381c9d7d1016006c3950f85
79fea7f741760ea21ff655137af05bd0
7a34b6a3c558492c04f3418d726b86a8
81d7c2d1dca5da7eef2896a76768d142
8e1f22dd9e809ead5e19b340b0c80cae
aea5d3cced6725f37e2c3797735e6467
bb266486ee8ac70c0687989e02cefa14
ed075c4718fd98efcbc845db00677065
fe16fa500584cb241532dc7cb75c1f53
ff56e700d15f3d944424c295eae926d9
087497940a41d96e4e907b6dc92f75f4a38d861a
11203786b17bb3873d46acae32a898c8dac09850
2a53525eeb7b76b3d1bfe40ac349446f2add8784
45212fa4501ede5af428563f8043c4ae40faec76
57a6dfd2b021e5a4d4fe34a61bf3242ecee841b3
5869820f261f76eafa1ba00af582a9225d005c89
5c6ca5581a04955d8e4d1fa452621fbc922ecb7b
655c2567650d2c109fab443de4b737294994f1fd
783b2b053ef0345710cd2487e5184f29116e367c
89060eff6db13e7455fee151205e972260e9522a
9146a448463935b47e29155da74c68d16e0d7031
94f025f3be089252692d58e54e3e926e09634e40
a186c08d3d10885ebb129b1a0d8ea0da056fc362
c1187fe0eaddee995773d6c66bcb558536e9b62c
ce5540c0d2c54489737f3fefdbf72c889ac533a9
d65a131fb2bd6d80d69fe7415dc1d1fd89290394
da1e4a09a59565c5d62887e0e9a9f6f04a18b5f4
e17dc8062742878b0b5ced2145311929f6f77abd
e22436386688b5abe6780a462fd07cd12c3f3321
f466b4d686d1fa9fed064507639b9306b0d80bbf
79802d6a6be8433720857d2b53b46f8011ec734a237aae1c3c1fea50ff683c13
3a08e3bfec2db5dbece359ac9662e65361a8625a0122e68b56cd5ef3aedf8ce1

KPMG

KPMG Cyber Threat Intelligence Platform

BlackCat Ransomware - Known for its sophistication

Indicators of Compromise: Hashes
5121f08cf8614a65d7a86c2f462c0694c132e2877a7f54ab7fcefd7ee5235a42
9802a1e8fb425ac3a7c0a7fca5a17cfcb7f3f5f0962deb29e3982f0bece95e26
e7060538ee4b48b0b975c8928c617f218703dab7aa7814ce97481596f2a78556
f7a038f9b91c40e9d67f4168997d7d8c12c2d27cd9e36c413dd021796a24e083
f8c08d00ff6e8c6adb1a93cd133b19302d0b651afd73ccb54e3b6ac6c60d99c6
0c6f444c6940a3688ffc6f8b9d5774c032e3551ebbccb64e4280ae7fc1fac479
13828b390d5f58b002e808c2c4f02fdd920e236cc8015480fa33b6c1a9300e31
15b57c1b68cd6ce3c161042e0f3be9f32d78151fe95461eedc59a79fc222c7ed
1af1ca666e48afc933e2eda0ae1d6e88ebd23d27c54fd1d882161fd8c70b678e
2587001d6599f0ec03534ea823aab0febb75e83f657fadc3a662338cc08646b0
28d7e6fe31dc00f82cb032ba29aad6429837ba5efb83c2ce4d31d565896e1169
2cf54942e8cf0ef6296deaa7975618dadff0c32535295d3f0d5f577552229ffc
38834b796ed025563774167716a477e9217d45e47def20facb027325f2a790d1
3d7cf20ca6476e14e0a026f9bdd8ff1f26995cdc5854c3adb41a6135ef11ba83
4e18f9293a6a72d5d42dad179b532407f45663098f959ea552ae43dbb9725cbf
59868f4b346bd401e067380cac69080709c86e06fae219bfb5bc17605a71ab3f
5bdc0fb5cfbd42de726aacc40eddca034b5fa4afcc88ddfb40a3d9ae18672898
658e07739ad0137bceb910a351ce3fe4913f6fcc3f63e6ff2eb726e45f29e582
7154fdb1ef9044da59fcfdbdd1ed9abc1a594cacb41a0aeddb5cd9fdaeea5ea8
722f1c1527b2c788746fec4dd1af70b0c703644336909735f8f23f6ef265784b
731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161
7b2449bb8be1b37a9d580c2592a67a759a3116fe640041d0f36dc93ca3db4487
7e363b5f1ba373782261713fa99e8bbc35ddda97e48799c4eb28f17989da8d8e
9f6876762614e407d0ee6005f165dd4bbd12cb21986abc4a3a5c7dc6271fcdc3
aae77d41eba652683f3ae114fadec279d5759052d2d774f149f3055bf40c4c14
b588823eb5c65f36d067d496881d9c704d3ba57100c273656a56a43215f35442
bd337d4e83ab1c2cacb43e4569f977d188f1bb7c7a077026304bf186d49d4117
be8c5d07ab6e39db28c40db20a32f47a97b7ec9f26c9003f9101a154a5a98486
c3e5d4e62ae4eca2bfca22f8f3c8cbec12757f78107e91e85404611548e06e40
c5ad3534e1c939661b71f56144d19ff36e9ea365fdb47e4f8e2d267c39376486
cda37b13d1fdee1b4262b5a6146a35d8fc88fa572e55437a47a950037cc65d40