KPMG

KPMG Cyber Threat Intelligence Platform

Alphv/BlackCat – A Formidable Cross Platform Adversary

ALPHV/BlackCat ransomware aka ALPHV-ng, Noberus is a highly sophisticated ransomware group that emerged in November 2021 and is suspected to be a rebrand of BlackMatter. They employ triple-extortion strategy involving data theft, file encryption, and DDoS attacks on their victim. Written in Rust, the Windows variant packs advanced privilege escalation techniques, while the Linux variant dubbed "Sphynx" also packs the ability to target ESXI hypervisors. More creative attack tactics are being concocted by the group which includes deploying its custom Linux VM 'Munchkin' on victim host to distribute malware.

Initial access involves malvertising with social engineering, exploiting vulnerabilities in network devices like VPN gateways & Firewall and misusing credentials through exposed RDP services. To navigate host security constraints ALPHV deploys custom 'Munchkin' VM as an ISO via VirtualBox. Based off Alpine OS, it packs in a wealth of python scripts & tools to dump credentials, build the encryptor, distribute itself to other systems and configure attack parameters for minimal manual intervention. This allows the attacker to encrypt remote SMB and CIFS shares. Windows tactics include abuse of PowerShell, WMIC & fsutil, UAC bypass via COM interface elevation and payload execution via 'PsExec'. ESXI behavior includes leveraging 'esxcli' to enumerate & kill all VMs and deletion of all snapshots to inhibit recovery. ALPHV uses multiple Remote Access tools & registry Run keys for persistence. Cobalt Strike beacons are used as C2 which are deployed by '.pyc' scripts that run in memory. All of the above is done while using SpyBoy 'Terminator' utility to tamper/disable EDR & anti-virus solutions.

ALPHV's adoption of 'EDR killers' & VM for malware deployment exemplify the continuous evolution of tactics to bypass & evade defensive measures, underscoring the need for increased vigilance.

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Alphv/BlackCat – A Formidable Cross Platform Adversary

Indicators of Compromise: IP Addresses	
45.13.119[.]81	42.119.82[.]160
141.98.6[.]56	193.42.32[.]143
166.0.95[.]43	45.66.230[.]215
47.154.86[.]24	162.33.179[.]114
193.42.32[.]58	206.188.196[.]78
45.12.253[.]50	167.88.164[.]141
45.12.253[.]51	172.86.123[.]127
45.81.39[.]175	172.86.123[.]226
45.81.39[.]176	104.234.11[.]236
84.54.50[.]116	157.254.195[.]83
45.154.138[.]39	104.234.11[.]226
67.216.143[.]42	85.217.144[.]233
167.88.164[.]40	193.149.187[.]213
45.66.230[.]240	157.254.195[.]108
167.88.164[.]91	104.234.147[.]134

Indicators of Compromise: Domains	
temp[.]sh	bigallpack[.]com
gofile[.]io	maker-events[.]com
winsccp[.]com	closeyoueyes[.]com
4shared[.]com	firstclassbale[.]com
onemakan[.]ml	azurecloudup[.]online
privacy[.]sexy	airplexacrepair[.]com
anydeesk[.]net	cuororeresteadntno[.]com
storjshare[.]io	aleagroupdevelopment[.]com
devnetapp[.]com	events.drdivyaclinic[.]com
situotech[.]com	cloudupdateservice[.]online
alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad[.]onion	

Indicators of Compromise: Hashes
29efd64dd3c7fe1e2b022b7ad73a1ba5
44eee3d7f6d60f3390c68ad3f1cb1b77
4b940893856bbde6c7c587d7e10ec4d1

KPMG Cyber Threat Intelligence Platform

Alphv/BlackCat – A Formidable Cross Platform Adversary

Indicators of Compromise: Hashes
60cf9dfc495e4bd99e31b2b6079f654e
61b13d54c8dda98b7aa13e75abfdbd12
7f4c0d171e104eea3c48e03ade1ec68a
825e125eb34abb8197178ed10d5452d5
adc52a4c68173dce2733dbfe45c5ebe9
bbeb9589a0f406d0d4921df68641ccf1
cc51281a38bdc87a7ad0e4b612181ced
d2848456bc6fc3bdccf6998befeced4b
ed6cb54d34f1cc8c9095c201f3173a06
21e13f2cb269defeae5e1d09887d47bb
8cb0be47cfe2eca8a4958375cacdb4a1
1c939f39a93aa425f857f76a8072ef0e43153ed0
48579f02785e022db5d31c229be8b9a098134d95
6f464abe5f9591b3786f21ef911fc6cd1f717131
9d966e90c1c6bc7100e9b089fe6c8ce52a6b379c
a9ed0ca8e08cf1e7569fcda769351850c748d681
b6da15fb313b3c7d66923f6144bac69aa19e74d1
bd53bd285071966d8799e5d9ceaa84a0b058a4fb
d278d06db4e1b8a6379308a797c0304676a30e10
d34043b44a7405e1359ef5f4dbebd09f324d9645
e3b6ea8c46fa831cec6f235a5cf48b38a4ae8d69
eb410e312adadda3a3d13c608b8bb5ef7ecb812c
e5db80c01562808ef2ec1c4b8f3f033ac0ed758d
cfbde85bdb62054b5b9eb4438c3837b9f1a69f61
3b14559a6e33fce120a905fde57ba6ed268a51f1
aae1b17891ec215a0e238f881be862b4f598e46c
c82b28daeb33d94ae3cafbc52dbb801c4a5b8cfa
d2663fc6966c197073c7315264602b4c6ba9c192
c7568d00ae38b3a4691a413ed439a0e3fb5664b1
61e41be7a9889472f648a5a3d0b0ab69e2e056c5
69ffad6be67724b1c7e8f65e8816533a96667a36
c1516915431cb55703b5a88d94ef6de0ac67190a
a7b1853348346d5d56f4c33f313693a18b6af457
ac8e3146f41845a56584ce5e8e172a56d59aa804

Indicators of Compromise: Hashes
e5d434dfa2634041cdbdac1dec58fcd49d629513
42da9e9e3152c1d995d8132674368da4be78bf6a
5cbb6978c9d01c8a6ea65caccb451bf052ed2acd
a9310c3f039c4e2184848f0eb8e65672f9f11240
5e36a649c82fa41a600d51fe99f4aa8911b87828
5263a135f09185aa44f6b73d2f8160f56779706d
75d02e81cc326e6a0773bc11ffa6fa2f6fa5343e
9d85cb2c6f1fccc83217837a63600b673da1991a
2f2eb89d3e6726c6c62d6153e2db1390b7ae7d01
7d500a2cd8ea7e455ae1799cb4142bb2abac3ae1
0362c710e4813020147f5520a780a15ef276e229
fb2ef2305511035e1742f689fce928c424aa8b7d
7874d722a6dbaef9e5f9622d495f74957da358da
06e3f86369046856b56d47f45ea2f7cf8e240ac5
36b454592fc2b8556c2cb983c41af4d2d8398ea2
337ca5eefe18025c6028d617ee76263279650484
e862f106ed8e737549ed2daa95e5b8d53ed50f87
2a85cdfb1c3434d73ece7fe60d6d2d5c9b7667dd
d883be0ee79dec26ef8c04e0e2857a516cff050c
ec4e4760b04d51e4b6f7acaf5a6e86b8620eb8df
16d7ecf09fc98798a6170e4cef2745e0bee3f5c7
59922fbf94425834d9cbbcfc4f089570b069e2d2
3a08e3bfec2db5dbece359ac9662e65361a8625a0122e68b56cd5ef3aedf8ce1
5121f08cf8614a65d7a86c2f462c0694c132e2877a7f54ab7fcefd7ee5235a42
9802a1e8fb425ac3a7c0a7fca5a17cfcb7f3f5f0962deb29e3982f0bece95e26
e7060538ee4b48b0b975c8928c617f218703dab7aa7814ce97481596f2a78556
f7a038f9b91c40e9d67f4168997d7d8c12c2d27cd9e36c413dd021796a24e083
f8c08d00ff6e8c6adb1a93cd133b19302d0b651afd73ccb54e3b6ac6c60d99c6
140bcad5397858a7fa35a79dba4cd83decd4ae2927a22983218b3a0efebd8b9e
1c2fbab9c849db1e8d8f26d217a7434aad3cab45b6f3c6c2de81b548220779fd
20529bcdc538cc28303300bab95b9daeb07264cf7ccdef837f87e26ea2a4f23f
234f8d70d92dde7d8f5edee2d3b3152214ef0b86c8e7c30274371fa9880243e6
243e1d202848ae99d8ee7a13f08316a8f0d37db93379df2fcbae7ff82754d89e
25e6fef0dce4e0f6260442b164ce7305561223429771b96f7448db8f337955cb

KPMG Cyber Threat Intelligence Platform

Alphv/BlackCat – A Formidable Cross Platform Adversary

Indicators of Compromise: Hashes
61c0810a23580cf492a6ba4f7654566108331e7a4134c968c2d6a05261b2d8a1
85ba48604d680d2786f485d70a6892dcf059c646e28b0a9befe530f9e3e459a5
b6bb576e3dd58f09218cf455d94e4db253af5f244f70f88abd78af0dc29c1246
bfa3cf521eefaaecc5d54028b3c12ea571033d4fe98e94d0031912b55071357b
c97641412ba384933dae4d4de377bc57bd0c9cd6d17b52a9a38c7c9a6eadd64c
da8c1976b9756cfb9afdcb4eaca193f411f96cee65835a87b3efb3423b33810b
df1f54952d918b1ddabf543ac50c2dafbca7aad2e5681824c0d1a44416da9c1d
e7e8a15588225ae93f2ebc91769352de0d48bfdcfcb93718e66119eb23dee976
f51166cf076d96c47b5c2ba22e65903b21e4d6735e585e1c51f796108a0a54f9
b4dd6e689b80cfcdd74b0995250d63d76ab789f1315af7fe326122540cddfad2
41c0b2258c632ee122fb52bf2f644c7fb595a5beaec71527e2ebce7183644db2
2e808fc1b2bd960909385575fa9227928ca25c8665d3ce5ad986b03679dace90
25467df66778077cc387f4004f25aa20b1f9caec2e73b9928ec4fe57b6a2f63c
4a4d20d107ee8e23ce1ebe387854a4bfe766fc99f359ed18b71d3e01cb158f4a
13090722ba985bafcccfb83795ee19fd4ab9490af1368f0e7ea5565315c067fe
8859a09fdc94d7048289d2481ede4c98dc342c0a0629cbcef2b91af32d52acb5
bacbe893b668a63490d2ad045a69b66c96dcacb500803c68a9de6cca944affef
c7a5a4fb4f680974f3334f14e0349522502b9d5018ec9be42beec5fa8c1597fe
3ce4ed3c7bd97b84045bdcfc84d3772b4c3a29392a9a2eee9cc17d8a5e5403ce
21e7bcc03c607e69740a99d0e9ae8223486c73af50f4c399c8d30cce4d41e839
0c6f444c6940a3688ffc6f8b9d5774c032e3551ebbccb64e4280ae7fc1fac479
13828b390d5f58b002e808c2c4f02fdd920e236cc8015480fa33b6c1a9300e31
15b57c1b68cd6ce3c161042e0f3be9f32d78151fe95461eedc59a79fc222c7ed
1af1ca666e48afc933e2eda0ae1d6e88ebd23d27c54fd1d882161fd8c70b678e
2587001d6599f0ec03534ea823aab0febb75e83f657fadc3a662338cc08646b0
28d7e6fe31dc00f82cb032ba29aad6429837ba5efb83c2ce4d31d565896e1169
2cf54942e8cf0ef6296deaa7975618dadff0c32535295d3f0d5f577552229ffc
38834b796ed025563774167716a477e9217d45e47def20facb027325f2a790d1
3d7cf20ca6476e14e0a026f9bdd8ff1f26995cdc5854c3adb41a6135ef11ba83
4e18f9293a6a72d5d42dad179b532407f45663098f959ea552ae43dbb9725cbf
59868f4b346bd401e067380cac69080709c86e06fae219bfb5bc17605a71ab3f
5bdc0fb5cfbd42de726aacc40eddca034b5fa4afcc88ddfb40a3d9ae18672898
658e07739ad0137bceb910a351ce3fe4913f6fcc3f63e6ff2eb726e45f29e582
7154fdb1ef9044da59fcfdbdd1ed9abc1a594cacb41a0aeddb5cd9fdaeea5ea8

KPMG Cyber Threat Intelligence Platform

Alphv/BlackCat – A Formidable Cross Platform Adversary

Indicators of Compromise: Hashes
722f1c1527b2c788746fec4dd1af70b0c703644336909735f8f23f6ef265784b
731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161
7b2449bb8be1b37a9d580c2592a67a759a3116fe640041d0f36dc93ca3db4487
7e363b5f1ba373782261713fa99e8bbc35ddda97e48799c4eb28f17989da8d8e
9f6876762614e407d0ee6005f165dd4bbd12cb21986abc4a3a5c7dc6271fcdc3
aae77d41eba652683f3ae114fadec279d5759052d2d774f149f3055bf40c4c14
b588823eb5c65f36d067d496881d9c704d3ba57100c273656a56a43215f35442
bd337d4e83ab1c2cacb43e4569f977d188f1bb7c7a077026304bf186d49d4117
be8c5d07ab6e39db28c40db20a32f47a97b7ec9f26c9003f9101a154a5a98486
c3e5d4e62ae4eca2bfca22f8f3c8cbec12757f78107e91e85404611548e06e40
c5ad3534e1c939661b71f56144d19ff36e9ea365fdb47e4f8e2d267c39376486
c8b3b67ea4d7625f8b37ba59eed5c9406b3ef04b7a19b97e5dd5dab1bd59f283
cda37b13d1fdee1b4262b5a6146a35d8fc88fa572e55437a47a950037cc65d40
cefea76dfdbb48cfe1a3db2c8df34e898e29bec9b2c13e79ef40655c637833ae
d767524e1bbb8d50129485ffa667eb1d379c745c30d4588672636998c20f857f
f837f1cd60e9941aa60f7be50a8f2aaaac380f560db8ee001408f35c1b7a97cb
847fb7609f53ed334d5affbb07256c21cb5e6f68b1cc14004f5502d714d2a456
35415d97038e091744e9cab3b88c78c1a7ca87f78d2b4a363f72f2c28d65932b
543991ca8d1c65113dff039b85ae3f9a87f503daec30f46929fd454bc57e5a91
120695e966f4ad588acd5fa4ac08cf1b1be9c901382d8b4da536ce2e74883cf0
120695e966f4ad588acd5fa4ac08cf1b1be9c901382d8b4da536ce2e74883cf0
8412b3eaaffd2241fab4491972f08f6737360146aa9e0eea9bdff3a1b1833203
6fed4ecc00c512fd389c7caab46f6767f4617fa3f4b2a57cb6807a2977ab11c2
9867fb9f609e8cfd9b15e2301c75050b76e069cd550f4a7528d9e7bd498df727
e074e9670abdf738be73c194a64b1cd8eb2775e9c2bdce14ee49f84390d1bfb4
f01e3aada6dbe347cf8eea37f88d603339507f18b1cb9695867714c20dbd2fdc
cf6453e6f2dc9523d1970f66c8383bd2fbb63f18e5feb1f85df68fac0981c549
a5807f4faf0fb0b541cc0a62a7ab9bac8167522e386e19b74e0420d56b41bb80
386b1c2def7334f4106c6f906486b35c71b200ace05f80c69906c2de682fd03e
541963093ea9025ad581c359dd85777ddd46327b2382ff0376aacd674e651ebe
dcdb6a70df8b1d5654956e00c0025dc7382771c7e073ea113f32fd90866ea55c
f61a6d3f0c618e9a0b5ccba092159ebff2197635bf985c04a1c923f769bd7352