KPMG Cyber Threat Intelligence Platform

BlackCat Ransomware: Unleashing the Nitrogen Threat

TLP : Clear

KPMG. Make the Difference.

Emerging in November 2021, BlackCat (ALPHV/Noberus) is a rapidly evolving and persistent ransomware group that offer RaaS. Built in Rust it encrypts Windows, Linux, VMware ESXi, ReadyNAS, and Synology NAS devices, using advanced social engineering and malvertising like the "Nitrogen" campaign. BlackCat targets major industries, especially healthcare, across regions like the US, Australia, Canada, China, France, Germany, India, Italy, Japan, Romania, Spain, Taiwan, and the UK.

Users may download malware posing as "Advanced IP Scanner" via deceptive Google ads, initiating a "Nitrogen campaign" with a ZIP file containing a disguised executable that side-loads a modified "python311.dll" to trigger the Nitrogen code. Persistence is achieved via registry run keys and scheduled tasks, such as "OneDrive Security," which executes every five minutes. They use "Py-Fuscate" to obfuscate remote access tools like "Sliver" and "Cobalt Strike," using API unhooking and bypassing AMSI, WLDP, and ETW for evasion. Over eight days, attackers use tools like "PowerView" and "BloodHound" for extensive network mapping, identifying admins, computers, and AD trusts. They move laterally using "WMI," "RDP," and "Pass-the-Hash," often leveraging dumped LSASS credentials. Sensitive data is exfiltrated using the open-source tool "Restic," which encrypts and transfers files to remote servers. Finally, BlackCat is deployed via SMB and PsExec, forcing systems to restart in "Safe Mode" with Networking, using a compromised account for auto-login to enable widespread file encryption. They deploy batch scripts to reset passwords, modify boot configurations, enable auto-login, delete shadow copies to hinder recovery, and leave ransom notes on compromised systems..

BlackCat's evolving ransomware tactics expose critical industries to severe data risks, stressing the necessity for continuous threat intelligence and strong encryption defenses.

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.

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

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

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

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

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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

KPMG Cyber Threat Intelligence Platform

BlackCat Ransomware: Unleashing the Nitrogen Threat

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses

5.199.168[.]24	94.156.67[.]180
91.92.242[.]55	94.156.67[.]185
141.98.6[.]195	194.180.48[.]42
193.42.33[.]14	91.92.240[.]194
194.49.94[.]18	91.92.241[.]117
194.49.94[.]21	91.92.242[.]182
194.49.94[.]22	91.92.245[.]174
91.92.242[.]39	91.92.247[.]123
91.92.245[.]26	91.92.247[.]127
91.92.250[.]60	91.92.249[.]110
91.92.250[.]65	91.92.250[.]148
91.92.250[.]66	91.92.250[.]158
91.92.254[.]193	91.92.251[.]240
94.156.67[.]175	185.73.124[.]238
94.156.67[.]188	194.180.48[.]165
91.92.245[.]175	195.123.226[.]84
91.92.240[.]175	194.169.175[.]134

Indicators of Compromise: Domains

pcrendal[.]com	resources.docusong[.]com

Indicators of Compromise: Hashes

341d43d4d5c2e526cadd88ae8da70c1c
34aac5719824e5f13b80d6fe23cbfa07
eea9ab1f36394769d65909f6ae81834b

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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.

KPMG Cyber Threat Intelligence Platform

BlackCat Ransomware: Unleashing the Nitrogen Threat

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
379bf8c60b091974f856f08475a03b04
ebca4398e949286cb7f7f6c68c28e838
c04c386b945ccc04627d1a885b500edf
824d0e31fd08220a25c06baee1044818
8738b8637a20fa65c6e64d84d1cfe570
944153fb9692634d6c70899b83676575
61804a029e9b1753d58a6bf0274c25a6
83deea3b61b6a734e7e4a566dbb6bffa
0b1882f719504799b3211bf73dfdc253
1329384dfdcfde2228da94e2a042f2b4
19e29534fd49dd27d09234e639c4057e
1be7fe8e20f8e9fdc6fd6100dcad38f3
3a4fdbc642a24a240692f9ca70757e9f
4232c065029eb52d1b4596a08568e800
637fb65a1755c4b6dc1e0428e69b634e
72a589da586844d7f0818ce684948eea
7a1e7f652055c812644ad240c41d904a
7a4cb8261036f35fd273da420bf0fd5e
c737a137b66138371133404c38716741
d6828e30ab66774a91a96ae93be4ae4c
dbf5f56998705c37076b6cae5d0bfb4d
e0d1cf0abd09d7632f79a8259283288d
e20fc97e364e859a2fb58d66bc2a1d05
eb64862f1c8464ca3d03cf0a4ac608f4
f176ba63b4d68e576b5ba345bec2c7b7
f27a9b7c29960aaf911f2885b40536c2

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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

KPMG Cyber Threat Intelligence Platform

BlackCat Ransomware: Unleashing the Nitrogen Threat

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
f4febc55ea12b31ae17cfb7e614afda8
1376ac8b5a126bb163423948bd1c7f861b4bfe32
3dd0f674526f30729bced4271e6b7eb0bb890c52
d6d442e8b3b0aef856ac86391e4a57bcb93c19ad
6b52543e4097f7c39cc913d55c0044fcf673f6fc
004ba0454feb2c4033ff0bdb2ff67388af0c41b6
380f941f8047904607210add4c6da2da8f8cd398
fba4652b6dbe0948d4dadcebf51737a738ca9e67
9648559769179677c5b58d5619ca8872f5086312
e6ab3c595ac703afd94618d1ca1b8ebce623b21f
f5f56413f81e8f4a941f53e42a90ba1720823f15
3a78ce27a7aa16a8230668c644c7df308de6cf33
448892d5607124fdd520f62ff0bc972df801c046
6f43e6388b64998b7aa7411104b955a8949c4c63
794203a4e18f904f0d244c7b3c2f5126b58f6a21
79818110abd52ba14800cdff39eca3252412b232
a3e4fb487400d99e3a9f3523aeaa9af5cf6e128b
b39c244c3117f516ce5844b2a843eff1e839207c
c4cde794cf4a68d63617458a60bc8b90d99823ca
430bd437162d4c60227288fa6a82cde8a5f87100
bd9edc3bf3d45e3cdf5236e8f8cd57a95ca3b41f61e4cd5c6c0404a83519058e
1f5e4e2c78451623cfbf32cf517a92253b7abfe0243297c5ddf7dd1448e460d5
3670dd4663adca40f168f3450fa9e7e84bc1a612d78830004020b73bd40fcd71
af28b78c64a9effe3de0e5ccc778527428953837948d913d64dbd0fa45942021
bbfe7289de6ab1f374d0bcbeecf31cad2333b0928ea883ca13b9e733b58e27b1
732e24cb5d7ab558effc6dc88854f756016352c923ff5155dcb2eece35c19bc0

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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 Cyber Threat Intelligence Platform

BlackCat Ransomware: Unleashing the Nitrogen Threat

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
b3b1ff7e3d1d4f438e40208464cebfb641b434f5bf5cf18b7cec2d189f52c1b6
4ef1009923fc12c2a3127c929e0aa4515c9f4d068737389afb3464c28ccf5925
5dc8b08c7e1b11abf2b6b311cd7e411db16a7c3827879c6f93bd0dac7a71d321
9514035fea8000a664799e369ae6d3af6abfe8e5cda23cdafbede83051692e63
5f7d438945306bf8a7f35cab0e2acc80cdc9295a57798d8165ef6d8b86fbb38d
5fac60f1e97b6eaae18ebd8b49b912c86233cf77637590f36aa319651582d3c4
726f038c13e4c90976811b462e6d21e10e05f7c11e35331d314c546d91fa6d21
d15cab3901e9a10af772a0a1bdbf35b357ee121413d4cf542d96819dc4471158
25172a046821bd04e74c15dc180572288c67fdff474bdb5eb11b76dce1b3dad3
3298629de0489c12e451152e787d294753515855dbf1ce80bfcded584a84ac62
39ec2834494f384028ad17296f70ed6608808084ef403714cfbc1bfbbed263d4
4ee4e1e2cedf59a802c01fae9ccfcfde3e84764c72e7d95b97992addd6edf527
5d1df950b238825a36fa6204d1a2935a5fbcfe2a5991a7fc69c74f476df67905

Follow us on:
kpmg.com/in/socialmedia

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 endeavour 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.