KPMG Cyber Threat Intelligence Platform

BlackSuit Ransomware - Rebranded Threat Targeting Enterprises Worldwide

TLP : Clear

KPMG. Make the Difference.

BlackSuit Ransomware, identified in April/May 2023, is recognized as a rebranding of the Royal ransomware due to notable code similarities. BlackSuit introduces a novel multi-pronged strategy, targeting both large enterprises and small to medium-sized businesses. Its attacks predominantly affect sectors such as healthcare, education, IT, government, retail, and manufacturing, with a focus on regions including USA, Canada, UK, Italy, South Korea, and Brazil.

Initial access is gained through phishing emails, third-party frameworks (e.g., Empire, Metasploit, Cobalt Strike), or malicious torrent files. Once inside, they use tools like SharpShares and SoftPerfect NetWorx for network enumeration and repurpose legitimate Windows software and open-source tools to strengthen their foothold and further intrusion. For lateral movement, they use RDP, PsExec, and SMB, employing an admin account that deactivates the antivirus by logging in the domain controller via SMB and modifying Group Policy Objects. Credential-stealing tools (Mimikatz) and Nirsoft's password harvesting tools are employed, along with PowerTool and GMER to kill system processes. Data is exfiltrated using repurposed penetration testing tools and malware derivatives. Payloads on Windows and Linux use AES for data encryption, with intermittent encryption options. Batch files execute the ransomware, monitor the encryption process, delete files and event logs upon completion, while Volume Shadow Copies are removed to prevent file recovery and compel ransom payment.

BlackSuit's utilization of advanced tools, coupled with its extortion tactics, necessitates robust network defenses and effective backup protocols to counter these threats.

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

KPMG

KPMG Cyber Threat Intelligence Platform

BlackSuit Ransomware - Rebranded Threat Targeting Enterprises Worldwide

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
89.251.22[.]32	147.78.47[.]178
5.181.234[.]58	180.131.145[.]85
193.37.69[.]116	180.131.145[.]61
137.220.61[.]94	138.199.53[.]226
45.141.87[.]218	184.166.211[.]74
135.148.67[.]84	185.190.24[.]103
137.220.61[.]94	143.244.146[.]183

Indicators of Compromise: Domains	
abbeymathiass[.]com	hourlyprofitstore[.]com
turnovercheck[.]com	

Indicators of Compromise: Hashes
748de52961d2f182d47e88d736f6c835
9656cd12e3a85b869ad90a0528ca026e
9495672a47fcaa5ce6f9f1bd86a56b79
92283d4d0e7e730c3f4f5485bfa48cb6
5cae01aea8ed390ce9bec17b6c1237e4
5cb9d80f82f674b065c3d80816a370c4
c1d6a5a9a9952583809ccf9ee7e67888
43250dd7f3a01c689131849c39f36482
4ac7f6cb9119fa684f57edeaa42eef46
3b080e25e0f37677c9fea6b8cf28528e
ed44877077716103973cbbebd531f38e
fa40a83774c126982696e8f8e380a49a
75b55bb34dac9d02740b9ad6b6820360

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

BlackSuit Ransomware - Rebranded Threat Targeting Enterprises Worldwide

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
bd288b5a4b86c32a74525927a9f3b5b1
aee6801792d67607f228be8cec8291f9
96e49160a2a64c833382bf9981530879
be7b13aee7b510b052d023dd936dc32f
772b6bae6862a79bbff035151972cec9
57bd8fba4aa26033fa080f390b31ed0e
50cc3a3bca96d7096c8118e838d9bc16
f42cc960e4ad9c27d2dd3e991a55a423
f88b66d108b050ea7c1552df33f0aa34
9d024548f5ae659770a041b10e92a1cd
4701be2d303bdb0b3a8d8c98ee0a44da
4f813698141cb7144786cdc6f629a92b
2902e12f00a185471b619233ee8631f3
30cc7724be4a09d5bcd9254197af05e9fab76455
861793c4e0d4a92844994b640cc6bc3e20944a73
790d40cd16fb458bf99e3600bce29eca06d40b56
a51b1f1f0636bff199c0f87e2bb300d42e06698b
d93f1ef533e6b8c95330ba0962e3670eaf94a026
1206bd44744d61f6c31aba2234c34d3e35b5bac7
b286b58ed32b6df4ecdb5df86d7d7d177bb7bfaf
b1605c73cce540effd015b22ef4e4b26e93f7eb2
fa09b4a336139acc85b12ae92b2dfbcdd05f7074
6e2dd5ec1c86a2e1d3f7c5964010127e9c4609a3
9ebb247b701f0e9f580f2d11c4eb6b6b86a64a3b
69feda9188dbebc2d2efec5926eb2af23ab78c5d
7e7f666a6839abe1b2cc76176516f54e46a2d453

KPMG

KPMG Cyber Threat Intelligence Platform

BlackSuit Ransomware - Rebranded Threat Targeting Enterprises Worldwide

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
9e19afc15c5781e8a89a75607578760aabad8e65
9a92b147cad814bfbd4632b6034b8abf8d84b1a5
a4ef01d55e55cebdd37ba71c28b0c448a9c833c0
3288f6f98bc2445f4ad688b562fe12414893c1ac
3a80a49efaac5d839400e4fb8f803243fb39a513
dd37973be7e6ede23c131a48919a4f6e1fb49328
39ef662922463b913e84a338ad4832674219964d
3182cc12b54a95a2d0d7f6fb8a0e4662a53bfe81
817a45fcc809d5272a30ea369cd5d67dc7fbbe36
d55aa4bd977f3fb5c8abecb5c5548b7319ff0834
25a6f82936134a6c5c0066f382530b9d6bf2c8da6feafe028f166b1a9d7283cf
e3d7c012040962acd66f395d1c5c5f73f305aa1058f2111e8e37d9cb213b80c4
c798b2690c5f16eb2917a679af3117cfe9c7060fa8bc84ffc3159338ef33508e
3c8c1b1f53e0767b7291bb1ae605ffa62a93e9c8cc783e4ca47ac84b48320d59
ee6ec2810910c6d2a2957f041edd1e39dca4266a1cc8009ae6d7315aba9196f5
68c57daed0e5899c49b827042bcf3bbeba33b524bd83315a44d889721664dc34
bbb7404419f91f82cedfec915931a9339f04165b27d8878d63827c9ee421ed62
338228a3e79f3993abc102cbac2ff253c84965213d59ac30892538cdd9b0a22b
3041dfc13f356c2f0133a9c11a258f87cb7de1e17bc435e9b623d74bc5e1c6be
8f87a1542ee790623896bbaab933d1883484de02a7b3d65d6c791d50173a923d
f1684fb118d4d8fc56653fcc49e12a659b64c4459ba037fa94f21783235cc6ba
dede96fd44c0f78eb79ceb63b898874e8922efc59d8bfb9f86505b1992bc00a3
79ab73a0e9dd8eac045c00fd1bd172a7f359588901f93c83e6740157eb21e7df
d96ff4b3e188f7ff96ed28c1381a6318dd76bb1fbd6ca02c6ab0236e1c7f35aa
dede96fd44c0f78eb79ceb63b898874e8922efc59d8bfb9f86505b1992bc00a3
6a2e454942cfeebb1140e1a28cb05fd49461d07792e97663378399c719fbc9ee

KPMG

KPMG Cyber Threat Intelligence Platform

BlackSuit Ransomware - Rebranded Threat Targeting Enterprises Worldwide

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
8605dec4ae4bd9f51297d1f244d0647bc0637d6ce6a957a5f810c64ae63276cb
2adcf43d221de2f72ba5088dac3a3193219412882df711d095f04e3f5b40767c
6ac8e7384767d1cb6792e62e09efc31a07398ca2043652ab11c090e6a585b310
d47d4b52e75e8cf3b11ea171163a66c06d1792227c1cf7ca49d7df60804a1681
be030e685536eb38ba1fec1c90e90a4165f6641c8dc39291db1d23f4ee9fa0b1
f0197bd7ccd568c523df9c7d9afcbac222f14d344312322c04c92e7968859726
b987f738a1e185f71e358b02cafa5fe56a4e3457df3b587d6b40e9c9de1da410
85087f28a84205e344d7e8e06979e6622fab0cfe1759fd24e38cd0390bca5fa6
d47d4b52e75e8cf3b11ea171163a66c06d1792227c1cf7ca49d7df60804a1681
1c849adcccad4643303297fb66bfe81c5536be39a87601d67664af1d14e02b9e
1743494f803bbcbd11150a4a8b7a2c5faba1223da607f67d24b18ca2d95d5ba3
f805dafb3c0b7e18aa7d8c96db8e8d4e9301ff619622d1aecc8080e0ecd9ebbe
6332f189cc71df646ff0f1b9b02a005c9ebda3fe7b9712976660746913b030de
e813f8faf3aa2eb20e285596413f5088b2d7fd153fe9f72f3ff45735d0fddced
25a6f82936134a6c5c0066f382530b9d6bf2c8da6feafe028f166b1a9d7283cf
e3d7c012040962acd66f395d1c5c5f73f305aa1058f2111e8e37d9cb213b80c4
c798b2690c5f16eb2917a679af3117cfe9c7060fa8bc84ffc3159338ef33508e
3c8c1b1f53e0767b7291bb1ae605ffa62a93e9c8cc783e4ca47ac84b48320d59
ee6ec2810910c6d2a2957f041edd1e39dca4266a1cc8009ae6d7315aba9196f5
68c57daed0e5899c49b827042bcf3bbeba33b524bd83315a44d889721664dc34
bbb7404419f91f82cedfec915931a9339f04165b27d8878d63827c9ee421ed62
338228a3e79f3993abc102cbac2ff253c84965213d59ac30892538cdd9b0a22b
3041dfc13f356c2f0133a9c11a258f87cb7de1e17bc435e9b623d74bc5e1c6be
8f87a1542ee790623896bbaab933d1883484de02a7b3d65d6c791d50173a923d
f02af8ffc37d1874b971307fdec80e33e583b56d9ebabda78a4b8ad038bc3bf0
b028eaa0ec452c6844881dc34be813834813a40591b89ea9a57dd4fb4084e477