KPMG Cyber Threat Intelligence Platform

Anubis Ransomware - Weaponizing Wipers for Extortion

TLP : Clear

KPMG. Make the Difference.

Anubis, initially branded as "Sphinx" is a newly identified Ransomware-as-a-Service (RaaS) group that emerged in December 2024. It stands out for its use of double-extortion tactics and a unique file-wiping feature that makes encrypted data permanently unrecoverable. The group operates with a flexible affiliate model and monetizes through access sales and data extortion. They target Windows, Linux, NAS, and ESXi systems across sectors like healthcare, construction, engineering, and hospitality in countries such as Australia, Canada, Peru, France, and the US.

Initial access is achieved via spearphishing emails containing malicious links or attachments that impersonate trusted sources, leading to payload execution upon user interaction. Once executed, the ransomware leverages configurable parameters to tailor its behavior to the compromised environment. The malware checks for administrative privileges, attempts SYSTEM-level escalation if found, or relaunches with elevated rights using legitimate accounts, confirming access by opening raw disk devices. They perform file and directory discovery, scanning for data while excluding critical system folders and developer tool directories to maintain stability and avoid early detection. Before encryption, they delete Volume Shadow Copies via vssadmin and disable services like backup, security, and database tools to block recovery. Files are encrypted using the Elliptic Curve Integrated Encryption Scheme (ECIES), renamed with a .anubis extension, visually marked by icon changes and wallpaper replacement, and a ransom note (RESTORE FILES.html) is dropped, threatening double extortion. Additionally, they use the /WIPEMODE parameter that enables a wiper feature that permanently deletes file contents, preventing recovery.

Anubis ransomware's irreversible destruction makes prevention and immutable backups essential, underscoring the need for robust mitigation strategies.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Patch your Windows environment with the latest version asper the OEM and secure it 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

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

Anubis Ransomware - Weaponizing Wipers for Extortion

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
38.134.148[.]20	195.133.67[.]35
5.252.177[.]249	212.224.107[.]203

Indicators of Compromise: Hashes
a1765503f1405b24b77a16071e6ea6f6
d2410703e93be61a652b92efcf42789d
0a5f3fc92af7aa3e448ac7b84e495fc6
271998018494403a9b5d0d4b01eb0c44
8a12e997e672b80319c5b852b237e5a9
f71d8db7fda7659718330efcbd0776f0
0f1b8aa83e5f9c40ad32561a95ed2c67
71ce395e8bb531ec3623b94387de8392
284d536dab5865150873e927a29cb0ae
a4b88bf440613390cd32e045a59fd7b0
c66022aa8b77a95c9b78a8743657f830
24eae2bb569d97018d343fff50112dab
f8a242fa6a8df6eafded0a6987a5ac09
1b701df9e6b5252feef3d1d8dcfe12f5
d9a053e54be4003cc28b41fe30790349
994a0c3e3e1390d972b1bdd8e8f2a449
4f178cefbf3fc66baed13b3c4fa897d4
054d432e231e8ee6e301675ef2bd598d
832feae0378a9b36c4958812735b6d81
241d01f08172a117268eb0f223348e47
a2d853247d939106231314bc5b233bda
5334cbddd1128f87308c0725d2cb012e

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Anubis Ransomware - Weaponizing Wipers for Extortion

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
ed2510198b03435570d72ce274bc245c
9ef845add689fc71cae33686139efbb0
f1b5f6edfba8bf1312f65e7f2787c72f
982c6db5e35382ec49e57f4b0855f820add9a213
d74004bd257f4274bdfab89e0f781aaee91ed56b
6480ca1b4ef8ee7074be143cc103c655c107b038
c1ff775ce01d756e778513a5bd40ace004576ab1
d11a0b8b22869c004247e1888ac5ebe6b207c1d7
3647c15e9b4d500ed2944e82285dd597c5c8f25d
e1ebdf56163f177f861d4d4583e55ed7183ab795
a63ad4c104c79f400867e0ee73a50b3619bb5a6a
15e1210c4b07503d17caf7d5e7ade2d32a3c3bec
d7e93057251e1fbf08c4e3b17841e79452b0be66
7353de0aa950726c57245932fb6a21da7beb0a4e
d0362adb0cc9140859e14cd129cfe605105a5cef
cffa3967ce585ab127346a68b38cd8bd1f3a640c
33e2230bc30f8da47f61ad26b2ace02d6312aadf
4a6c37e07b055a58e0d9535df4e6c92d7615dc5d
9fed1f0aab3fa121a73a6a35be5c4e3af4b9cd6f
abdcc5e1efbacd8bfe791edde922a44e6927de78
3a2328d1794752177f4e1ce5c7c8824f425cbf6a
73470da480a65fe768691c43c4756641f515ff7c
2cc2c4a6e55db1cdb96e15a29eaec90f1a3b04e9
b3a683e5c18aaa741aee2fb35ec7fb3e0ad91f66
7d38a2de7e7ce9c169885c9465b8d0cebb4428ae
7cfcd32d2cd839adf08e6052f64e9dd561306a15

KPMG

KPMG Cyber Threat Intelligence Platform

Anubis Ransomware - Weaponizing Wipers for Extortion

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
ed9a73f4f1f8bb43a110697d9eab9c386a568f0c
9c40267f7a3003219ec11567241a6d966ef46971
96b9f84cc7bf11bdc3ce56c81cca550753790b3021aa70ec63b38d84b0b50f89
e5255d5f476784fcef97f9c41b12665004c1b961e35ad445ed41e0d6dbbc4f8e
03a160127cce3a96bfa602456046cc443816af7179d771e300fec80c5ab9f00f
5203f2667ab71d154499906d24f27f94e3ebdca4bba7fe55fe490b336bad8919
1c486702b74550c0abe3f5e353f52b1d4c737bfc253b4db3fcdd9caf6612c98a
447433baf4fabb5b4271e16fc35c8b26b794759789b1abf37d3e3087046ad058
a30ce9c01652a044920ee121c9b56231d35594ca31d1ada10f5c65c7cd69f6d2
500c9ec95e931f6df9418b709379df4f83519a76fbbab4bb86db36a35a62cb42
6d999b3e3b5a9e3826d483b3ae0c8ad3203bcfab0c3701f6e5399fd7201fe57d
97193c63a3dd04816007ca71c9e29d560733453136c3ffe5764014dc9c586305
88e9e2810590d3126a518630460e4179f2a4c8cb956abc6886c663b0749382f2
45383c88da59fcf6a69a84536b0488f4b7a8910a3ff76bf47424e21973c17dca
3b22cb5a35d0ea6fe967791ca4f7b3b0f2326cf757579dad3bd3ddaee0751697
9039fb7b875ddbeb39cbde09a78f82102cd6d6270fa9e6a994e84005dba68b70
52e0171d1e88c2e21a0309cb91e1261c8c7c1097d8066dcde486bc85316fd898
0bfc2b5594e9563b60bdce2deb8d1bd3766a8a574bbc5dc604f4eaad5723fcf4
ac402ab656a315e412c6ad8bcd41de3fee5058ef08befcc4fd0bddfb2e2ba6bd
d764287198865dae880e7f2ffeca531d5d827f7828d495aa6f08da7c8ecad059
036aa36f994c7ef36f79d38692079039afb20b2381fc71ff448b405a24df4ebb
48fa4d2a7fa3aba03305ee0a6edd5d8e8e3fb2e978436f23419f83204a42e6e5
46087c924131351976831d38a4f8a2beb722eac0b47026bb0961f01caf7a50f9
d84f3eed419573ea0d790d2557b57eb59c064a0db605e17ef4b2a4c3f31a3aee
7cba150646b812549c6f17c8bb622bee49fc115b04c67b87d30179c492a12f55
40ea161cc38d2849964d2a3c047b4dcc161242f5e7ffab40667a7d02160a49df