KPMG Cyber Threat Intelligence Platform

Vice Society – Low Effort, High Impact Ransomware

Admittedly operating since 2021, Vice Society ransomware has had a keen affinity on picking easy & weakly funded targets in education, healthcare, manufacturing & local government sectors in regions like US, UK, Spain, France and Brazil to stay off the radar. Vice Society has amassed a reputation for its low-effort, high-impact approach owing to its use of encryptors borrowed from other ransomware gangs like Zepllin, HelloKitty & Five Hands. However, since July 2022, the group has been seen adopting its new 'PolyVice' encryptor which extensively borrows code from Chilly & SunnyDay ransomwares.

Vice Society uses various techniques for initial access which includes phishing emails, compromised RDP credentials and exploiting internet facing applications. Post access, attacker enumerates target system, attempts to access backups & probes network to gather information about AD using various tools. SMB shares and tools like CobaltStrike, SystemBC, etc., are used to laterally move through the environment. To gain elevated privileges, the group exploits PrintNightmare vulnerability or performs Kerberoast attack on AD. PowerShell scripts then aid the attacker to create new accounts & to add them to local admin & RDP user groups to maintain persistence. Further, passwords of legitimate accounts are also changed in few cases. Vice Society has several tricks to evade defenses including AMSI bypass, process injection along with disabling security solutions, clearing event viewer logs & RDP session traces through windows registry keys.

Vice Society uses multiple techniques like SMB shares, direct C2 transfer via PowerShell, and cloud storage/transfer services for data exfiltration. By borrowing toolsets, quickly adopting techniques & avoiding high-profile targets, Vice Society is here to stay for long.

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

Vice Society – Low Effort, High Impact Ransomware

Indicators of Compromise: IP Addresses	
5.255.99[.]59	146.70.41[.]133
5.161.136[.]176	198.252.98[.]184
194.34.246[.]90	

Indicators of Compromise: Domains
57thandnormal[.]com
vsociethok6sbprvevl4dlwbqrzyhxcxaqpvcqt5belwvsuxaxsutyad[.]onion
qu5dci2k25x2imgki2dbhcwegqqsqsrjj5d3ugcc5kpsgbtj2psaedqd[.]onion
wavbeudogz6byhnardd2lkp2jafims3j7tj6k6qnywchn2csngvtffqd[.]onion
gunyhng6pabzcurl7ipx2pbmjxpvqnu6mxf2h3vdeenam34inj4ndryd[.]onion

Indicators of Compromise: Hashes
fb91e471cfa246beb9618e1689f1ae1d
ddee92c23a182d69884422c1e8a3df1b
b455171462f0c30d3635bddad47bab44
a3cb3b02a683275f7e0a0f8a9a5c9e07
9fda237668200542b7a524afd59c6b48
3e711336ec93bd7c026a198512fb3820
31ac6a2cd36783540f0d0fc1f6eafb57
a0ee0761602470e24bcea5f403e8d1e8bfa29832
3122ea585623531df2e860e7d0df0f25cce39b21
41dc0ba220f30c70aea019de214eccd650bc6f37
c9c2b6a5b930392b98f132f5395d54947391cb79
d241df7b9d2ec0b8194751cd5ce153e27cc40fa4
d3c0510bf108a2a7c387c7edea77af7642222e56
9e9da169e7d37fe4e6151bd2c016cf7618f47c51
9c5a188cfb37d9b715afa2bdd5a2c8213565ddd6
605674a0e28e6c431a977800c5a9dd97dbedf75c
56e4739efcc0ded77a251ad7b4844d8536fe30d5
342c3be7cb4bae9c8476e578ac580b5325342941
0e79780baf6597a86faf8f2550f0f50418a1d4c6
6f191f598589b7708b1890d56b374b45c6eb41610d34f976f0b4cfde8d5731af
f51bb4637f429a2c2cd3b8d27c83cdfaab2349148865fe3d83a50f531021c4d4

KPMG

KPMG Cyber Threat Intelligence Platform

Vice Society – Low Effort, High Impact Ransomware

Indicators of Compromise: Hashes
f366e079116a11c618edcb3e8bf24bcd2ffe3f72a6776981bf1af7381e504d61
da0332ace0a9ccdc43de66556adb98947e64ebdf8b3289e2291016215d8c5b4c
cdb82be1b9dd6391ed068124cfdf2339d71dd70f6f76462a7e4a0fdadd5a208a
94bc7b115bce0eba58ffdcc58e37d79b6fe15b22ad347aea00fe3a1641725027
890736d072ff1e983333c6b248e9fbd7380a84dce5c175192dd8bbc9b5e917b5
7c26041f8a63636d43a196f5298c2ab694a7fcbfa456278aa51757fd82c237d4
6e7b4d2ca25630c88d5af6d61cd57d3084e0f266d13f576a6b3cafdda6a9b85e
49d01f2e32808e24dc8129d3c1ebe444f71792ddec2efabee354335fc6d6f64c
3aef9575f8467e6ffe1eaae358569095554808b57a4abee9eb8011b1c390fa6d
1df9b68a8642e6d1fcb786d90a1be8d9633ee3d49a08a5e79174c7150061faa8
78efe6f5a34ba7579cfd8fc551274029920a9086cb713e859f60f97f591a7b04
754f2022b72da704eb8636610c6d2ffcbdae9e8740555030a07c8c147387a537
24efa10a2b51c5fd6e45da6babd4e797d9cae399be98941f950abf7b5e9a4cd7
307877881957a297e41d75c84e9a965f1cd07ac9d026314dcaff55c4da23d03e
ab440c4391ea3a01bebbb651c80c27847b58ac928b32d73ed3b19a0b17dd7e75
aa7e2d63fc991990958dfb795a0aed254149f185f403231eaebe35147f4b5ebe
bafd3434f3ba5bb9685e239762281d4c7504de7e0cfd9d6394e4a85b4882ff5d