KPMG Cyber Threat Intelligence Platform

RansomHub Ransomware: The RaaS Powerhouse Wreaking Havoc

TLP : Clear

KPMG. Make the Difference.

RansomHub, aka Cyclops and Knight, is a RaaS launched in February 2024 targeting Windows, Linux, and ESXi systems using malware written in Go and C++. Leading Q3 2024 attacks, it offers a high 90% commission to lure seasoned affiliates. Using double extortion, it partners with groups such as Scattered Spider. It targets I.T., government services, healthcare, aviation, food, transportation, finance, manufacturing, and communications across nations such as Mexico, USA, Turkey, Canada, Germany, and Italy.

RansomHub ransomware affiliates gain initial access by exploiting known vulnerabilities, using phishing emails, or employing password spraying against compromised accounts. Once inside the network, they execute the ransomware by deploying it under innocuous file names to avoid detection. They ensure persistence by creating new user accounts and reactivating previously disabled ones, maintaining ongoing access. Affiliates then escalate privileges using tools like Mimikatz to extract credentials from memory, allowing them to gain elevated permissions and control over the system. To evade detection, they rename the ransomware executable, clear system logs, and disable antivirus and endpoint detection systems. Following this, they use tools like AngryIPScanner and Nmap for network reconnaissance, moving laterally through the network via RDP and executing commands on remote systems with tools such as PsExec, along with leveraging penetration testing tools like Cobalt Strike and Metasploit. Communication with victims occurs through unique .onion URLs on the Tor network for ransom negotiations. Finally, they exfiltrate data using tools like WinSCP and Rclone, transferring stolen information to their controlled environments before encryption.

RansomHub ransomware poses a serious threat, employing advanced tactics for compromise and extortion, highlighting the urgent need for stronger cybersecurity 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

KPMG

KPMG Cyber Threat Intelligence Platform

RansomHub Ransomware: The RaaS Powerhouse Wreaking Havoc

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
8.211.2[.]97	45.134.140[.]69
45.95.67[.]41	193.124.125[.]78
188.34.188[.]7	193.233.254[.]21
45.135.232[.]2	193.106.175[.]107
89.23.96[.]203	

Indicators of Compromise: Domains	
40031[.]co	samuelelena[.]co
12301230[.]co	banccosanlanber[.]site

Indicators of Compromise: Hashes
f17ceae8c5066608b5c87431bac405a9
407dcc63e6186f7acada055169b08d81
da3ba26033eb145ac916500725b7dfd5
57556d30b4d1e01d5c5ca2717a2c8281
03b9b7bc71c22d078987b2640190b655
de8e14fdd3f385d7c6d34b181903849f
676259a72f3f770f8ad20b287d62071b
0cd57e68236aaa585af75e3be9d5df7d
719ba3d7051173982919d1e4e9e9a0ec
ff1eff0e0f1f2eabe1199ae71194e560
5075f994390f9738e8e69f4de09debe6
229d24b004c9f8abaf76aa25e49bf08f
4677cc44ee1c005b5f156aefb4c56959
73191bc793deef595be84a4d6b389d82

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

RansomHub Ransomware: The RaaS Powerhouse Wreaking Havoc

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
b962b36c3194976bfa8fe18c99e70fb6
49ef1d6c0b367ae82449d4f307566edc
f2828e09b7b33122f74857a6833058c6
d08e82f2b16f3fe2d0f4ff23429f7a5c
b724e4bc22d5f782a6f991d67fb00fb6
241a8786b63d84c7c69d3d56e8e14a6d
5885e000140360787bff99b6616d68a2
9404fa51d497626bbaa99cfb51897e25
73b1cfb93eac9de5764c1c1dde2d28e2
0798aa30f12682c97f4292c2be3710b1
a3256c9495e248197c5271b4351aecf0
076c4581f79b90229edbb3854674e7f3
6dc730f1726f298108e229d29ca00b05
497b441e9dd963aac97eb61ebebaafd6
a71c1d94f130c6f168b2456f5a9bcbd3f455ac77
094e160d68026861491e2746299437d0a00baf96
a34ab11f41ad5b8c0b20434f4eb6042e5d182811
03c8dde484a939837478252674c7535973882c4e
5c62a7f5b11cb5fc97e9bff2173b7ec17dfdac63
de1241a592760cc1d850be8f41beebcd460b66ec
189c638388acd0189fe164cf81e455e41d9629d6
2d3a95e91449a366ccf56177a4542cc439635768
6764ddb2e5b18bf5d0c621f3078d7ac72865c1c3
77daf77d9d2a08cc22981c004689b870f74544b5
86cdb729094c013e411ac9b4c72485a55a629e5d
8de2d38d33294586b4758599fdf65f1a265e013b

KPMG

KPMG Cyber Threat Intelligence Platform

RansomHub Ransomware: The RaaS Powerhouse Wreaking Havoc

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
e187d58f59e0444f7ef9ddefec88d2b11b96e734
e38082ae727aeaef4f241a1920150fdf6f149106
3b035da6c69f9b05868ffe55d7a267d098c6f290
a3fad01a0c10fde5b38267188860ea1da649697d
4d37e7fe6a48de25926fb97adc978fa4c780e1eb
c998899e9c3671d1103b0ee774eba0e19c7030ce
dff0977e0c43ff254289c4ac00efd1c291fd97aa
b3d7565c555056980d25e2681a215d720c90c571
b019c09e482c405b6c4c00a4be20c3657854aaed
22a56e9ed057e945d97ce77ffb222aa428804a89
0ecdb7a9f22ab0aa2d2e91f5299455d257ff6a10
97e1f54f9cf51fc0055235e473782ab89e9031e6
3b9b94c686823c80e06c23d767ddbc54f918d17c
1103e687cd961ecb9558db0ad3d43a8b5d84cb8e
2e14fca60b7d3b8b49ae5766f32ca8f45afad9e2
f2d314a29093554196bea7473c1df1c1d61b8e4f
311247e2cde7034dd2f727efbf539f472e670052
6f425f3dcb1ae96e535926e40ccbe7e94c1f5964
b0e16773b7a068a81b2c44e3f6ed32373c9bd1bd
966cac7e63e8c75292249c66bf502c639d705274
d40f677732135c2ebaede0229b53ca2097090a440f0b833bb63326d3d0c03df2
e4fbf178411b45b9e881d3072097a5388964aa9e133fe0f5054492d51af6589d
edd824432b3967538229b06101c83aad67daef286c41b26574f5e43396763b7f
d3e052004dba62484477f5c2e7e8d77055dd067f916dd150d1199d45647b8d3e
7f3c6e98b039213cb241f99f26e328647efa7a683cdee8dfd6f5d5db11161ae2
30abbbeedeeb268435899a7697f7a72f37a38e60ae2430e09bc029c7a8aa7001

KPMG

KPMG Cyber Threat Intelligence Platform

RansomHub Ransomware: The RaaS Powerhouse Wreaking Havoc

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
bfbbba7d18be1aa2e85390fa69a761302756ee9348b7343af6f42f3b5d0a939c
bd70882f67da03836f372172f655456ce19f95878d70ec39fcc6c059f9ef4ca0
b2a2e8e0795b2f69d96a48a49985fb67d22d1c6e8b40dadd690c299b9af970d4
f982dfc0a0984f317460ca6d27d72ad6b3274b58cb7cf984e1c3e6f001e1edf8
46ff164e066a3a88dad76cad25c6ea42c7da6890bcba3fa3ccd4c6e93a3272d0
869758de8334c2b201a07cfbfc0a903105a113080dde0355857de46b3eaae08e
d9a8c4fc94655f47a127b45c71e426d0f2057b6faf78fb7b86ee2995f7def41d
d1347f4dccebf2fcd672dcef9c66c91b9d3f12b9881e3e390626927718fda616
2d823c8b6076e932d696e8cb8a2c5c5df6d392526cba8e39b64c43635f683009
467e49f1f795c1b08245ae621c59cdf06df630fc1631dc0059da9a032858a486
0e31d6dcf5e519f0126c2256ce58b9fccec75b6dd6d5ad320f7b707339cd38be
1b9fc1d47cd53724ed9ea20f118db57ac53953744f54184d30566c587cae155d
27ca9c2d6359d54f59cbe362b20b0556128b063baf1db166696cd41684fa46d1
340c67b9436c1d9c7243cd5f6297aae94edf6873117fbb0458f2b877fd90f28b
4b697ad035c370e1e8d74f5017247f37fb8abc0d84ff061a25a193e41d60aa25
554b54dd18ef35af4bfe0f065f0310a29a3ae19bfc518bc50be481744aaa01fe
627611f37a051dc649065489cf39e9666701b2c235ac3f8d43712ddd723dd710
73bff01c6a0221d976aa45d9b15f4b2d210cf46bee93b4ffa80233e9ca322cdc
8ff5e1d3b77757508111ecb54f48fb39b58dc1a54531a62ad4fbaa9eab5f44a3
959d13a29b6a671c60b2eb11e0a403612e226efd32088b3f16961935a3fb43f3
98f867eae6642bd6da41f357945367d401d0f07678e01ca2741a0fdac631146e
a03d487a6ceec70c8ff273f148025b8f72d7418b60103384aa9d27f4371224b0
a1ff7b99688dd4c591d7ff7fa7fb053e7eb0fdb386a7395fb82a7559d02e8c65
ad91c11b510357bd3d4eddc55b2542b648ca5219e04fe6e2a84ecf10e5a01d3d
c6e0bee98c312f99534380619ac048909b05785aaf14549e9d3b0d61f57c3b31
d3e9982ac4906f3a70839db4b1ef4459ed98c9708bf7b88ed70438b37fb9f399