KPMG

KPMG Cyber Threat Intelligence Platform

Snatch Ransomware - Exploiting Safe Mode for Stealthy Intrusion

Snatch, formerly known as Team Truniger, has been operational since 2018 and has specifically targeted organizations in the United States since 2019. Their targets encompass critical industries such as the Defense Industrial Base (DIB), Food and Agriculture, and Information Technology. In June 2023, Snatch expanded its operations to include data theft and double extortion tactics. They have been observed purchasing data from other ransomware groups and leveraging this information to compel victims to pay ransoms, thereby avoiding data exposure on Snatch's extortion platform.

Initial access is achieved by exploiting Remote Desktop Protocol (RDP) vulnerabilities & brute forcing administrator credentials. Post access, it establish persistence through compromised admin accounts and connects to its C2 server via port 443. They abuse Windows Safe Mode to circumvent detection by antivirus or endpoint protection. Tools like PowerShell, Metasploit, and Cobalt Strike are used to perform Data discovery and lateral movement. It persists for over three months in the network, systematically exploiting network vulnerabilities, executing lateral movement, and actively collecting data for exfiltration. Disable antivirus software's and execute a file called "safe[.]exe," using a hexadecimal filename matching the SHA-256 hash to avoid rule-based detection. After activation, it alters registry keys, utilizes Windows tools for enumeration, creates processes to execute specific batch (.bat) files, deletes volume shadow copies. Also, Attaches hexadecimal characters to file and folder names, along with ransom notes prompting communication via email or Tox communication platform.

Snatch's brute forcing and RDP based threats calls for actions like limiting exposure, enforcing multi-factor authentication, segmenting networks, enhancing monitoring & employee training to minimize risk.

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

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 endeavor 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 josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Snatch Ransomware - Exploiting Safe Mode for Stealthy Intrusion

Indicators of Compromise: IP Addresses	
193.188.22[.]29	45.147.228[.]91
193.188.22[.]26	67.211.209[.]151
193.188.22[.]25	185.61.149[.]242
37.59.146[.]180	94.140.125[.]150

Indicators of Compromise: Domains
snatch24uldhpwrm[.]onion
snatch6brk4nfczg[.]onion
mydatasuperhero[.]com
mydatassuperhero[.]com

Indicators of Compromise: Hashes
3d29e9cdd2a9d76e57e8a3f9e6ed3643
395dad45c4761490c6480308a8359c06
304f8f54fb79bb470f3ccddd2befc5da
f9bf364f42f6e4d4bdc2cae74d6ca4cc
2202e846ba05d7f0bb20adbc5249c359
c95c81ca4e6b8153b458d29186e696bc
3a24a7b7c1ba74a5afa50f88ba81d550
6d9d31414ee2c175255b092440377a88
54fe4d49d7b4471104c897f187e07f91
891708936393b69c212b97604a982fed
3d33a19bb489dd5857b515882b43de12
3e36d3dc132e3a076539acc9fcd5535c
55310bb774fff38cca265dbc70ad6705
5ac9ad8a4be54a74aa117b2cf52824f8
e7b9147adc95c965e20ed9549bf01f8e
92926564df146ba4c8703171870ede9e
a9e612d1aadef0603f2e0a06a3f4f8bb
0e1a7ceb1cecc302a879b8fd77d5b926
8a6ba8c536b5986d7e8a477f35555d37
29738dd9b52dcd61cd791b6d805929c1
32de66a467db22cf0f5b65d1a9f4e19c

KPMG

KPMG Cyber Threat Intelligence Platform

Snatch Ransomware - Exploiting Safe Mode for Stealthy Intrusion

Indicators of Compromise: Hashes
601c6f6b1d98a9627ce8c372a9a2a969
d985a6610213773a43584afe1107dbd9
dc00d58e8d3d0ff58614c9a1d2b709de
c19cc2b8394ef302e154e0bb4882c29e
5a9ae5f51c41f2de4f3eca94ddb4ccfd
b7da210b885c6636de70c0129da48a66
46406680a5825b6d1622acb984d4a41d
58beaa9058c8fc4e3be97806566ab495
26e46fc3dff7635d2f538545e8fe5209
8ec25ab72b7ccc119b60156236827d52
5ad94f5303aed57a9d4f0055f15076454840064a
050304668d55e64f6088b407836cffd31d4b3414
c7cfc5a1b4dee08427bc11d202be13723ff19b9b
b3759d5a6412d085556fb081fd710ce62f18687f
c8a0060290715f266c89a21480fed08133ea2614
4115d2d15614503456aea14db61d71a756cc7b8c
f97f8f78abb205dda329d89143aae34ba04d13df
5da4de1dbba55774891497297396fd2e5c306cf5
c24aee8fa0a81a82fe73bf60e0282b1038d6ea80
18f963dbee830e64828991d26a06d058326c1ddb
5b86cf095fe515b590d18b2e976d9e544c43f6ca
0882f2e72f1ca4410fe8ae0fa1138800c3d1561d
89be35c19a65b9e6f7a277e1a9f66ab76d024378
cb8d76e9fd38a0b253056e5f204dab5441fe932b
7da13058dfcbd20817c19dbecacf6e2e32e80674
14d8276b1fdeff10622096f2f8eba4e1e29da7e7
ab7a4a75dc706d902490f59869f0f78857261904
4a420fcf3c4639b395c6d8b86cfeed9d6748caec
3097a10d0b1ae5874a998fd073dd8bf29d3ece04
a255d57f3ab5e0716d4a73ab4ab97783ec20e4f2
b226a60f03c7036f6bcbce400ad40ebe7f527925
cdb5c200cba7da3f6e80e868ef7df380ac1259c2
1ebd755618055ceac4ae1c139182b2c0997d05f1
4e743e81dcb4df6e21aacd0ad2918a5b20586127

KPMG

KPMG Cyber Threat Intelligence Platform

Snatch Ransomware - Exploiting Safe Mode for Stealthy Intrusion

Indicators of Compromise: Hashes
37f1d40f3d1c7805e1027b08a5141b6d4a974c60
7610f95738a8cde9474145f1cc0ff4e054acd77b
f74893ac96c66a778d7b95e1ff279624d70553d1
7199988d0a50b024ca69c6b567496920b0eecd3f
e6d8b1715daa1502ca622ba57bbc48561bac6fe8
ed481af02c2909cca3b7a6bb7eb855bf92bb10c2
edda359ef29f0a2c93353ea0d3cb5af995d72a05
f88063e198e15dbaca60416a56acdf34dbabd714
5950b4e27554585123d7fca44e83169375c6001201e3bf26e57d079437e70bcd
b998a8c15cc19c8c31c89b30f692a40b14d7a6c09233eb976c07f19a84eccb40
84e1476c6b21531de62bbac67e52ab2ac14aa7a30f504ecf33e6b62aa33d1fe5
510e9fa38a08d446189c34fe6125295f410b36f00aceb65e7b4508e9d7c4e1d1
7018240d67fd11847c7f9737eaaae45794b37a5c27ffd02beaacaf6ae13352b3
6992aaad3c47b938309fc1e6f37179eb51f028536f8afc02e4986312e29220c0
ed0fd61bf82660a69f5bfe0e66457cfe56d66dd2b310e9e97657c37779aef65d
fc31043b5f079ce88385883668eeebba76a62f77954a960fb03bf46f47dbb066
0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f
28e82f28d0b9eb6a53d22983e21a9505ada925ebb61382fabebd76b8c4acff7c
a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae
2155a029a024a2ffa4eff9108ac15c7db527ca1c8f89ccfd94cc3a70b77cfc57
6c9d8c577dddf9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7
a80c7fe1f88cf24ad4c55910a9f2189f1eedad25d7d0fd53dbfe6bdd68912a84
3295f5029f9c9549a584fa13bc6c25520b4ff9a4b2feb1d9e935cc9e4e0f0924
251427c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30d
1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d
eebc57e9e683a3c5391692c1c3afb37f3cb539647f02ddd09720979426790f56
78816ea825209162f0e8a1aae007691f9ce39f1f2c37d930afaf5ac3af78e852
80cc8e51b3b357cfc7115e114cecabc5442c12c143a7a18ab464814de7a66ab4
ebcded04429c4178d450a28e5e190d6d5e1035abcd0b2305eab9d29ba9c0915a
fe8ba1eaf69b1eba578784d5ab77e54caae9d90c2fb95ad2baaaef6b69a2d6cb
28125dae3ab7b11bd6b0cbf318fd85ec51e75bca5be7efb997d5b950094cd184
0ce4c4af321ff02928aacf105f03dead87e85003080586615755f278770f5adb
36a4311ef332b0b5db62f8fcabf004fdcfbbde62f791839a8be0314604d814c4
d0ddc221b958d9b4c7d9612dd2577bec35d157b41aa50210c2ae5052d054ff33

KPMG Cyber Threat Intelligence Platform

Snatch Ransomware - Exploiting Safe Mode for Stealthy Intrusion

Indicators of Compromise: Hashes
e8931967ed5a4d4e0d7787054cddee8911a7740b80373840b276f14e36bda57d
ae9cdbb717625506ed0df7af153dc2741395655aeb1da2f91079e3ea616af6a1
5f24536e48f406177a9a630b0140baadff1e29f36b02095b25e7e21c146098bb
c0f506e98f416412b3a9dcd018341afab15e36b15bac89d3b02ff773b6cc85a6
8c9fab558b3e9e21936a91422d9e2666f210c5fd7d9b0fd08d2353adb64a4c00
329f295b8aa879bedd68cf700cecc51f67feee8fd526e2a7eab27e216aa8fcaa
ab6b0d00ba8f8553c015743b9da8761a9b1fca750d3f73bda573a8fbc47dafa1
63c2c1ad4286dbad927358f62a449d6e1f9b1aa6436c92a2f6031e9554bed940
d22b46ea682838e0b98bc6a1e36fd04f0672fe889c03d227cdeb5dcc5d76ae7c