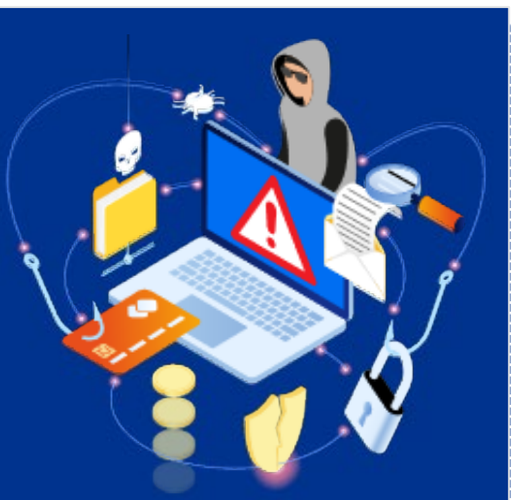
KPMG Cyber Threat Intelligence Platform

Raccoon Stealer Malware V2 - Resurging as a Stealthier Threat



Introduced as a malware-as-a-service in 2019, it quickly gained traction among cybercriminals due to its adaptability. However, in March 2022, its operators abruptly shut down. This hiatus proved temporary as Raccoon Stealer reemerged in June 2022 as version 2, sporting improved infrastructure, heightened capabilities, and enhanced password-stealing functions. Its primary focus is the theft of sensitive user data such as login details, credit card data, cryptocurrency wallets, as well as browser data encompassing history, cookies, and autofill information.

Like its forerunner, Raccoon Stealer v2 spreads via fake software installers or cracked versions of legitimate programs, often circulated through malicious websites or email attachments, tricking victims into downloading and executing them. Once executed, the malware first checks for the presence of other instances to avoid running multiple instances simultaneously. The malware hides essential details, such as configuration specifics and the C2 IP address, by obfuscating strings using methods like Base64 encoding and RC4 encryption. To evade detection by security tools that rely on static analysis, it dynamically resolves imports at runtime. This technique helps the malware avoid being flagged by identifying imported functions, allowing it to operate stealthily in different environments. It establishes communication with a remote C2 server, uses encrypted HTTP POST requests to transmit data such as victim's machine ID, username, and an RC4 decryption key. The C2 server responds with tailored instructions. Further, Raccoon Stealer v2 infiltrates systems, captures valuable information, maintains persistence via scheduled task, and transmits stolen data.

Raccoon Stealer operators can tweak C2 traffic, but unusual network behavior remains harder to hide. Detecting and responding autonomously is key for organizations to stop its advancement.

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 josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Raccoon Stealer Malware V2 - Resurging as a Stealthier Threat

Indicators of Compromise: IP Addresses	
2.58.56[.]247	55.195.166[.]184
89.39.106[.]64	185.225.19[.]190
109.236.82[.]58	51.195.166[.]175
136.244.65[.]99	178.128.94[.]180
94.158.247[.]24	45.133.216[.]170
179.43.154[.]171	142.132.180[.]233
192.248.184[.]34	

Indicators of Compromise: Domains	
roll-rave[.]site	main-soft[.]site
fall2sleep[.]xyz	heal-brain[.]xyz
tech-lover[.]xyz	violance-rave[.]site
cool-story[.]xyz	

Indicators of Compromise: Hashes
214add3ebdd5b429fda7c00e7f01b864
0cfa58846e43dd67b6d9f29e97f6c53e
1d7d285f77ed5460fe9aada4c04dcfcf
d28ba705f24c9e51564c46aefab26754
6844edfec32e4323ecfedc458f7d3b86
92d3194f6c3511b40def1b3c8f86e585
7a2ef36c5dbf72b92b1adfb52e1e5426
c5ce68e5feabffe94ce4309e9e278a91
b35cde0ed02bf71f1a87721d09746f7b
7894ab366f0b984ce78d7ef9724cec0d
9ea0905f02da6e6ef2e46d5e434ec2e9
7be14834721533240 66babf71c683045
6affeba1a78fcedc2d7dd78713a79a00
1e682d91b86e5d1059496ef5c9404a83
80b0745106a9a4ed3c18264ba1887bff
b71921298c866e9d17fe83becf9a2107
88a354d8d051d4dd8c741cdf3e986244

KPMG

KPMG Cyber Threat Intelligence Platform

Raccoon Stealer Malware V2 - Resurging as a Stealthier Threat

Indicators of Compromise: Hashes
16bae91061e6410ddf2c17b544939d87
0b4146abe7ab84bfa66e1bb9b947fee3
3e8a0b51131b8937ec9d36e96872a581
eca370e62443218965eb27b1a61bb7a0
7cead6f1e4c4b0824365268cdd5d168acf56265c
19d9fbfd9b23d4bd435746a524443f1a962d42fa
9c6e393d8b2eac432720518f8991c86ad8fa94b7
0c6bb0d8f2611775b495a019c63f95b1377f2054
465d756d89a18d40a2721e74d99b4df8dc9438a8
e9aaee23127a796285e3e227e4d92e3cf572c529
abe82a1405471258c72d031191846ea627f1c63c
ab272e68f0e09391e3675cf8cda344774ae98769
0cf266265f77e387a9d396888651240f2b458e0a
48ca383575fdc914ed3436d40201eae6bac55007
90acb6ca3f40b72a7ab601b2f781d43ddb5d2bb9
4436a1c572737a82494d4ddfe91929ce4cd836cd
3cd9f5678212e7465af460eb05b9a5c1899842a9
b997c212dee402190a4fe7562fa68f565c084711
b97787c5fb625d884b184b16266d58bcec1bdff1
7f224b87eeaa85417c2d1e4a254d907c44439dee
b47cc17316ef37a18919eedd0ec16908febac7a1
531b6c546b26eeb9e33560292bb756b47affbeaa
f88cb9e308c4de39ddbb0d50b71a28f04bc8bd85
589676a88d04977b651722dd061b158771a6435d
4e48d0c38e0a4543137cd381abb38e6bd17f17aa
0123b26df3c79bac0a3fda79072e36c159cfd1824ae3fd4b7f9dea9bda9c7909
022432f770bf0e7c5260100fcde2ec7c49f68716751fd7d8b9e113bf06167e03
048c0113233ddc1250c269c74c9c9b8e9ad3e4dae3533ff0412d02b06bdf4059
0c722728ca1a996bbb83455332fa27018158cef21ad35dc057191a0353960256
2106b6f94cebb55b1d55eb4b91fa83aef051c8866c54bb75ea4fd304711c4dfc
263c18c86071d085c69f2096460c6b418ae414d3ea92c0c2e75ef7cb47bbe693
27e02b973771d43531c97eb5d3fb662f9247e85c4135fe4c030587a8dea72577
2911be45ad496dd1945f95c47b7f7738ad03849329fcec9c464dfaeb5081f67e
47f3c8bf3329c2ef862cf12567849555b17b930c8d7c0d571f4e112dae1453b1

KPMG

KPMG Cyber Threat Intelligence Platform

Raccoon Stealer Malware V2 - Resurging as a Stealthier Threat

Indicators of Compromise: Hashes
516c81438ac269de2b632fb1c59f4e36c3d714e0929a969ec971430d2d63ac4e
5d66919291b68ab8563deedf8d5575fd91460d1adfbd12dba292262a764a5c99
62049575053b432e93b176da7afcbe49387111b3a3d927b06c5b251ea82e5975
7299026b22e61b0f9765eb63e42253f7e5d6ec4657008ea60aad220bbc7e2269
7322fbc16e20a7ef2a3188638014a053c6948d9e34ecd42cb9771bdcd0f82db0
960ce3cc26c8313b0fe41197e2aff5533f5f3efb1ba2970190779bc9a07bea63
99f510990f240215e24ef4dd1d22d485bf8c79f8ef3e963c4787a8eb6bf0b9ac
9ee50e94a731872a74f47780317850ae2b9fae9d6c53a957ed7187173feb4f42
bd8c1068561d366831e5712c2d58aecb21e2dbc2ae7c76102da6b00ea15e259e
c6e669806594be6ab9b46434f196a61418484ba1eda3496789840bec0dff119a
e309a7a942d390801e8fedc129c6e3c34e44aae3d1aced1d723bc531730b08f5
f7b1aaae018d5287444990606fc43a0f2deb4ac0c7b2712cc28331781d43ae27
00f673951e56b240628083558294b856e86402e7ee4a7490b5cf0ba9ef566c4a
02f4dadb5ddffaf16957363cbc50299829b1ba8d1d1b4d411596ff39d8633d95
0369bea9b737199511f30bb172e4aee892aec0daca70b29ce70da22f1f543ce0
03996f49944edb335f6320612127709551ab5e7b1f9acd352a2fd43520c5a60e
05acd1d4a4a5ac409a605b6f82e172c9b21a2d507a50a65384243f7217ce61ff
05afdcb00b307ba14cd4e74afcf2a0ab70eb8635f43d1ad5e27833cbe3171716
07f0ca5ef8919f72de4e64fd66f60b4f48a49594d9750e1d9428612bf12ffce0
09ee750816c082c9dba557874cb4a244dfffaa1737a0b918d937c27d2df0f36a
0b4964fec40013d6d87b85f6eb132b622fdb4f1b2582a31c4b21ec1d0313657a
e56df70cfd23a5e6921d676069e0fe264d15136250fa2776fb7afc22f3b024a8
0001093a633f5e2619932f3945e48bffd39d4fac3dd35ac8d93de154baa3b41b
0304f19f48dcc2cb38dc194ef6f2432769956e8abb8b6256d14e83f9cc9cf831
0325502958cf6111b78350207292984e34a990e4f64214a18a7b231c4c796fbd
0482228a35ec2e139460fb091b4cb94e88a2148f778c7a66b8a439534c1c7226
04fcbe38ce51213011460e0f6c85998a095e1330d673b04b06dcb0a97b495585
0580678f81e9801e3678c5d4cf1cfe674aa52ce95092e67908d6a7d4192a429b
063f8e5a99819843ef6fdae6dfb4cd836d92c426792639ecbba6da75a1f4fb0a
069494fedfdfd26cd90ee6614b3ce09884eb53c0bd8566f9e70d55243c44b5a6