KPMG

KPMG Cyber Threat Intelligence Platform

Jester Stealer – Not a Joke

Jester stealer, .Net Based malware, first came into light in July 2021, as Information Stealer malware which is distributed as Malware as a service and capable of stealing credentials, browser authentication tokens, cryptocurrency wallets, messengers, and gaming application information. In black market, Russian sold Jester malware that targeted ukrainians. After its initial release, it was upgraded seven times with new features and provides customization.

The broad campaign begins with a phishing link in an email with the subject “Chemical attack”. Once the link has been clicked, a macro-embedded excel file gets downloaded from the compromised resources. As soon as document opens, Macro gets executed and downloads a malicious executable “Jester Stealer”. Multi-functional jester stealer checks for anti-sandbox, anti-debug, anti-VM mode to avoid any detection from security tools. Jester is capable of stealing system information, login credentials, browser cookies, credit card details and targets the messenger, VPN, crypto currency wallets and Gaming applications. It steals all the data and saves it into their respective created text files in the memory. Stolen data exfiltrated to Telegram Bot in the form of logs via TOR proxy through AES-CBC-256 encrypted communication and in any failure, will send to anonymous file sharing platform. It makes sure to infect the machine only single time by adding a value in registry. After its successful operation, it deletes itself from the system to remove the footprints.

Phishing mails & macro embedded excel as initial access vector, it is recommended for the organization and people to be aware in clicking any suspicious attachment. Disable default execution of macros. Block all the malicious URLs & monitor the beacon activity for any type of data exfiltration activity in the organization network.

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.

© 2022 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Jester Stealer – Not a Joke

Indicators of Compromise: IP Addresses
92.38.240[.]149
157.112.183[.]47

Indicators of Compromise: Domains
igshop[.]net
dcshost[.]net
marmaris[.]com.ua
autodoka[.]com.ua
wasabiwallet[.]online
jesterdcuxzbey4xvlwwheoecpltru5be2mzuk4w7a7nrhckdjjhrbyd[.]onion
lightnogu5owjjllyo4tj2sfos6fchnmcidlgo6c7e6fz2hgryhfhoyd[.]onion

Indicators of Compromise: Hashes
8879ae061540ce3de496adec3683b0fe
a30d170412986b90ce293b5a8ff7dfd8
9196e0e3234ef664e828eba9628f468d
c73c7c93101d4d741c79127a37d13d3a
7989d8fb3ec96482016acd52d56ea7f8
3986844f88921ccaba28a173a843c27a
26e71a30d1e8b43be1f16d3483d1d44c
9378111ed1b30ad23d37d7d7c33345d1
952cd4334dc6b9c1a3e0d0ab64d5afb2
90257b4f1de0e70235b2ff7419803afa
2cd2390f2138b725f4176343784c7705
d5c9fd40738ac33f59467811c1ceb30b
d80f1d64e07909d29d7a2a1888931af9
4742c9d0a6b5b3b10ae7eb8f6b3e2fe6
70ef45cb31af0b6f37be051de4170839
8f32a69ecd777f99d67bd18363afa25d
31600c8891e3902a0fe2d2985d25ca34
4b5f73578a49ca01cc2ba7b414bcf1edfbefa079
a2d08c50f4adf4dabe5118ba390523e83b6ab246
486d766fda3ad882d1cdb62e38de15f3041d0874

KPMG Cyber Threat Intelligence Platform

Jester Stealer – Not a Joke

Indicators of Compromise: Hashes
ed8558d02259f5766db38e04cc3a0397a2ca78be
6ea8fc4269d1d6914337c922faf9b5b689a5b818
83eb4a253e3199a8647e74caeebd96a4a3079657
bbc0a01fc29f04a0b291222fe31cceeb7477aa80
5b6f37fb27d502f6c50ecac13bef06dcf597f0a9
8e76ad772450473e469e4423375d3caa1968bb9a
60cebe074e8303abf2c344a99c2e83bad5a0d9c3
e9309eda5a0b8d4a52da226089edc79278dec8b4
3168f18432106cfaf21f48598c1b26b1026de7a0bac69ae548c79dec67be7853
cdbed3a79d37d581fc5be268df61e13aaafa5c88a001f4e8b298d77c4b37ae13
6dd7f4652faa45c4e124cdeb6582262b8572f5ed8bd7fbdb2967ee5dce01d8e0
a4a81d6a903411ebca75c1f2d85f6db8ef65cd6e4e5fdbaa9b8fafc093d42970
83315459c10621aa4965545a36ec5fb0b803ec0dcd5a1fa3b3a2266db9165714
ee5e8737168f71747990cce9802470c6d9d484ebd51225fd972408f4909c92fc
28b7bab024147403bc3988850009c6e5120686292c8927056b521bb9b0cc0337
ecb44ba0a108abc5f5c4d6e22fcd46e6d9608f7b72ea0fe603f2f0918b542937
ceb1a94e9366a84f75948fbe56576945abeb7b2ecb578b00aeaa22b7896bf6fb
a679ee3c33f24010f2b794bb76e0f4b11bbca6c4f87240820e308ea1d5b442cf
b61663582da089a5ba37ad833149864a99ce60d8f2d9106d02aa26baa7b14106
010207d4463874eabd3808b12355e24acab67ff55c93c075625c2a05e481fd31
63c6a046117b72d93b4e7080112efeef75a56c70fc739337a0e58a24bc9b483c
6c696dfabef6726c984759bbd8ea68c048bf2a8efd056597bcbe0b179c3a9d89
e038cd85c9da66e9517bba1e3af819a7cb1cf068fe955b8e125273d1e0533c2b
cfa4a0acd6953e845c6dc4e7d66f1acd487c24814689a575190642c2be76852d
e9c0a925edadcabd11f20a9c44912b1f4be987998208d16a728fef8c3d0792d2
32c5f9a900171b2a12fa07e8bcccb91cb45433b59e34ba691bf6d3ba239c4268
69e395e78e1ad069f22269e0d3618706d95f174d6af411bec70e1e315308aff4
ecd4609a880cb82fce449a7d8e5919c7f2786f5918f6aa5d8a29438f4393547d
10c3846867f70dd26c5a54332ed22070c9e5e0e4f52f05fdae12ead801f7933b
0a5aa0a06a4d01dc423c4500d3278e61f03af07dd28ad299d29a6434026efebe
b1a4fb5177d642fb5647168070aa054f2eace2291c82361f0799ba0fbac38483
e4637b5597e15a276d2635c05ac4ea71a3d2ec3dee2435991868f12a09e45d58
2a9904c9776ebb1843cc43ab3f70fa13083a37f44ffe965cf688788d5895ab14
efe72384bb1fb454100492b73ba80496052816f8b40b0e26f3492dce9bea8938

KPMG

KPMG Cyber Threat Intelligence Platform

Jester Stealer – Not a Joke

Indicators of Compromise: Hashes
ffddc659a5a95a821eb8479124b67decce76249ee7ec734bd766c02bd2f9242b
2f6d1b66a3836d7eb9709592d530f2a1c8097b2c59ae7a51db9a5db8455d0294
81fcca2ba4b2af6081ff0291f7e5221ed811549b2b5e27e9456e19ed8f71c649
fda7f3bd7166684ae7b8b1d4e6212c73a4af21452c7d855675600c1cd064cbdd
5df051b418cd3d51cfcfe17685275e03b0efdf9a80ce237d2deccb3749576092
f963ed8559ade984e81a95238c4875d4c0a6ff14a7695630429bf98d4235d596
ef7ddd544267a8781c99f08146d455aa08beab867e0453b07f1131edcbef92b2
a2234ee40097fa832eb3a533840e86de3933cf216fbf8445d2946cb7b61c887b
da0de03004e3ec2711ddc71e119ecc252568b2c9300b98dd2434b8e83ce02dc9
f7477c153f861d8c57d47944814451344266d634b9f4ca58d4d8519c4b0cd0085