KPMG Cyber Threat Intelligence Platform

RapperBot – Swiftly building upon Mirai

The Mirai-based botnet, RapperBot, originally discovered in May 2021 made its destructive appearance infecting Linux servers through SSH brute-forcing. The botnet re-emerged with its Distributed Denial of Service (DDos) attacks tailored to attack against IoT devices and servers hosting online games. Borrowing capabilities from the original Mirai code, the new RapperBot is known to target the technology domain including IT and gaming sectors with its brute force attacks.

SSH servers that support DH 768-bit / 2048-bit keys and AES128-CTR data encryption must be weary about this new menace. RapperBot brute forces against a list of common SSH credentials fetched from C2 & reports back valid credentials along with details like the target architecture, protocol and utility that it was spread with. Once inside, it downloads the payload binary via common pre-installed linux utilities such as ftpget, wget, curl, tftp, etc and executes it. The payload then establishes persistence by replacing the "/.ssh/authorized_keys" file with attacker's SSH key to defend against password reset & malware removal. Further, a superuser named "suhelper" is added by modifying "etc/shadow" & "etc/passwd" files. An hourly cronjob for the same is also set-up. Finally, with C2 communication successfully set-up, the infected devices are ready to support commands for multiple types of DoS attacks such as TCP SYN/ACK/STOMP floods, GRE floods and & UDP based SA:MP flood that targets the infamous GTA San Andreas game servers.

The malware is observed to leverage thousands of compromised devices as botnets to execute of Distributed DoS attack on its targets. The organizations must ensure the use of firewall for all the network devices in order to inculcate an additional layer of security.

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

KPMG Cyber Threat Intelligence Platform

RapperBot – Swiftly building upon Mirai

Indicators of Compromise: IP Addresses	
2.58.149[.]116	194.31.98[.]244
31.44.185[.]235	185.216.71[.]149
185.225.73[.]196	

Indicators of Compromise: Hashes
5630ee34393ce22d317c3a11a91b5bb2
30ce66fa45abddf278dbb3eccf87ddad
2e9740382e75ebb7c8f4a0cdf2c36500
927b2162032a3a89a6e17f9769155985
75181839d4eca01c095f5976cfe06f71
72c70d37a714ecf026cdea998c36a069
6faeac8f2269c3d86606b34de90607fd
669a8e0683154f594a110d129d96a068
64e0ddc2aa51350b355434ffd1a4d6b6
5e10e46ccd75627df169976de506029d
ee73067c97e7015dc3f805fd3f66f3db
e70f70c91670ac3fc8d3d7963f6fb8a6
e4b3a9f9e5e90ce3912665ffb7e0f6f8
bda8d5c2665f47877ab571728f07c65a
ab96e594403ed957ed2ec6c992513abf
ce1a980265811fd257b36a449b987702
9d8cd6a75e40c2022abca1e58c88b40f
94c9ae3ab4319954a302d819e8a608ec
5d7d2618e09ea3c84f5a484553e0ea65
5ab947f7cae22fa65398c591e1aed268
5a2fe024029c7b8894885ded5f08e42e
1bdfcca7b35ad31a41fba5d6dc88b276
1318afe218cf3a86f71aa6936df33ee7
5aa801ffe8d362bcb64a0575aea778082a4ddc54
5c5066d748f0ef4ef8fe4125434dd20cee566d65
564ce63b3939e10fd8ae3df1bc764083582707bc
52489a148462acc8b8633c09f3ba3ce5e9f27063
4f00520407a40ef18f144b4ac2c03657bc7a65b6

KPMG

KPMG Cyber Threat Intelligence Platform

RapperBot – Swiftly building upon Mirai

Indicators of Compromise: Hashes
4b6524d0a3f1ffeac80c1251ad63601274896eb0
4698a9f872bde68f504e875cf02c87cd53a4b445
40434f00734ccd0d55edd135c50b7595de2bc66b
3f563eb47e096ff02f43795f8e4964f217c3b8f4
33cf1b18c99a43ea76c4b87c92b73a769acd24ad
d9c3051c61aedd87c530123ece2fdc5123f04ec8
d833bcb845db2ca88e0ae6cb72961b4a1ed6a21a
d68e46e4cd4f8fc7af2b82be7e3dea9be3ade56a
c8e50331f951ea848b36a35751988b9f00336071
bbd8f413be3abe8df87cd2ed6c58e68f4bb505ce
94d51c338af676e51cb22f8d169a5aa867259118
8b9f2892a5fe32fe4ffe65c97b7ba0bb2f58bcf9
887da60a3146abc39b33bdedadbba1e0818e37ba
781160ca6c18a0875dc2c3269cfa97398f36f27c
679010f52909c909bde9aa34645c5ac0044df453
e8f05a1c719b0348a490afd6b0c213b53d9835ca
92ae77e9dd22e7680123bb230ce43ef602998e6a1c6756d9e2ce5822a09b37b4
a31f4caa0be9e588056c92fd69c8ac970ebc7e85a68615b1d9407a954d4df45d
e8d06ac196c7852ff71c150b2081150be9996ff670550717127db8ab855175a8
23a415d0ec6d3131f1d537836d3c0449097e98167b18fbdbf2efca789748818a
c83f318339e9c4072010b625d876558d14eaa0028339db9edf12bbcafe6828bb
05c78eaf32af9647f178dff981e6e4e43b1579d95ccd4f1c2f1436dbfa0727ad
88bbb772b8731296822646735aacbfb53014fbb7f90227b44523d7577e0a7ce6
e8f1e8ec6b94ea54488d5f714e71e51d58dcdfe4be3827c55970d6f3b06edf73
23256f231f3d91b0136b44d649b924552607a29b43a195024dbe6cde5b4a28ad
77b2e5fb5b72493bde35a6b29a66e6250b6a5a0c9b9c5653957f64a12c793cd5
dcdeedee4736ec528d1a30a585ec4a1a4f3462d6d25b71f6c1a4fef7f641e7ae
ebb860512a55c1cdc8be1399eec44c4481aedb418f15dbda4612e6d38e9b9010
9d234e975e4df539a217d1c4386822be1f56cea35f7dd2aa606ae4995894da42
1975851c916587e057fa5862884cbac3fa1e80881ddd062392486f5390c86865
8380321c1bd250424a0a167e0f319511611f73b53736895a8d3a2ad58ffcd5d5
f5ff9d1261af176d7ff1ef91aa8c892c70b40caa02c17a25de22539e9d0cdd26
2298071b6ba7baa5393be064876efcdbd9217c212e0c764ba62a6f0ffc83cc5a
2479932a6690f070fa344e5222e3fbb6ad9c880294d5b822d7a3ec27f1b8b8d5

KPMG

KPMG Cyber Threat Intelligence Platform

RapperBot – Swiftly building upon Mirai

Indicators of Compromise: Hashes
1d5e6624a2ce55616ef078a72f25c9d71a3dbc0175522c0d8e07233115824f96
746106403a98aea357b80f17910b641db9c4fedbb3968e75d836e8b1d5712a62
ddf5aff0485f395c7e6c3de868b15212129962b4b9c8040bef6679ad880e3f31
e56edaa1e06403757e6e2362383d41db4e4453aafda144bb36080a1f1b899a02
55ff25b090dc1b380d8ca152428ba28ec14e9ef13a48b3fd162e965244b0d39b
8e9f87bb25ff83e4ad970366bba47afb838028f7028ea3a7c73c4d08906ec102
ff09cf7dfd1dc1466815d4df098065510eec504099ebb02b830309067031fe04
d86d158778a90f6633b41a10e169b25e3cb1eb35b369a9168ec64b2d8b3cbeec
d86d158778a90f6633b41a10e169b25e3cb1eb35b369a9168ec64b2d8b3cbeec
3d5c5d9e792e0a5f3648438b7510b284f924ab433f08d558b6e082e1d5414a03
4aa9175c1846557107ec197ea73d4cc8dbe6d575a8fd86ae214ff9b3a00e438b
7afcac5f71e9205879e0e476d3388898a62e7aa4a3e4a059884f40ea36cfd57f
8ec79a35700f6691f0d88d53647e9f2b75648710ecd119e55815331fc3bdd0b5
a12ad4bc394d60bc037271e1c2df1bd2b87bdaaba85f6c1b7d046341f027cc2d
f000bf482040b48595badee1fc56afb95449ac48b5dc35fe3a05542cbf18f658
f98261eb7dc122449c158118cc9c660683206983a9e90ff73eb88c4705e0c48e