KPMG Cyber Threat Intelligence Platform

Panchan Botnet – Proliferating through SSH

Making its debut in March 2022, Panchan botnet is targeting Linux servers in the telecom and education sector which use weak SSH credentials. Panchan's primary motive is to hijack victims' computational resources to mine cryptocurrencies. The first appearance of the botnet has been seen in Japan followed by affecting Asia, Europe, America and Africa. Notably, the admin panel is written in Japanese language indicating the origin of the threat actor from Japan.

Panchan botnet is an SSH worm that targets random IP addresses & attempts dictionary attacks to gain initial access, post which it harvests existing SSH keys to further spread itself. After successful SSH login, the malware copies itself into a hidden folder and deploys two fileless miners which are memory-mapping to the miner binary to avoid any disk presence. The malware then connects to a Discord webhook via an HTTP-POST operation which serves as C2. Panchan creates a systemd service under "/bin/systemd-worker" to masquerade as legitimate service and ignores two of the three linux process termination strings making it difficult to terminate. The botnet also continuously watches out for process monitoring commands and terminates itself intermittently to avoid monitoring. Interestingly, all of Panchan's peer-to-peer traffic is over plaintext on TCP port 1919. The malware also features built in "godmode" which is a private key protected admin panel that provides information such as configuration, host status, peer statistics, and miner settings.

Despite employing multiple novel techniques compared to other botnets, Panchan can be easily mitigated owing to its primary infection vector being SSH. Implementing multi-factor authentication (MFA) clubbed with network segmentation and access control is key in preventing organizations from falling victim to such threats.

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 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 face any 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: +9122 3989 6000, Fax: +9122 3983 6000.

© 2022 KPMG Assurance and Consulting Services LLP, a 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

Panchan Botnet – Proliferating through SSH

Indicators of Compromise: IP Addresses	
2.12.51[.]56	60.131.39[.]171
1.23.82[.]72	182.159.96[.]81
36.75.75[.]75	65.77.155[.]137
21.15.46[.]55	112.85.121[.]51
108.9.44[.]34	174.161.15[.]50
91.189.91[.]43	187.66.107[.]58
38.47.52[.]180	167.156.42[.]76
121.76.34[.]54	143.108.29[.]100
18.22.55[.]243	125.187.193[.]19
91.189.91[.]42	171.225.237[.]183
138.112.25[.]25	117.101.242[.]112
55.28.233[.]229	109.202.202[.]202

Indicators of Compromise: Domains	
submit[.]org	2fgithub[.]com
click[.]zero	click[.]compare
click[.]talk	continue[.]email
click[.]open	click[.]discover
signup[.]team	repository[.]click

Indicators of Compromise: Hashes
c8bc258ce1efd1acfb561b4bcf1680e6
6c8f1cfc42ec1dd0a01d73a3e97627ef
bae688df9d297afac98e2d254e912ada
95b24126db31ea8693c0fe5ea9f53b65
83356e17066d336d1803024138ecb683
830bf802470ec6c9c5800c99d8e57445
6c2cfda7c41396fcc31a4db759a42b94
3c64268131793aa297119a343c19e345
18e31c8a9b2271332466133162a4aa0d
16ed2b4ff7de02663b7c606309695916
1686089f6d540cd2deeaec60ee43ecf7
10f8ab3fbc5ebe989a36a05f79d48f32

KPMG

KPMG Cyber Threat Intelligence Platform

Panchan Botnet – Proliferating through SSH

Indicators of Compromise: Hashes
086e2abe64e9101112af53b95d2d90b9
682e9645f289292b12561c3da62a059b
f4dcb2dd842efcd7509728c5517317be8e28ef30
98f82fb253eb3b65ea6452565041dccd7057de77
d3ebb5f3606708a0662ebf7afc93c579e9f6eda5
c2198bfad64989b47fec7c26f06b7f651b3ff7eb
cbc585180e7b4d33f383f8761b322bc5015287e9
b9e643a8e78d2ce745fbe73eb505c8a0cc49842803077809b2267817979d10b0
a819b4a95f386ae3bd8f0edc64e8e10fae0c21c9ae713b73dfc64033e5a845a1
6f445252494a0908ab51d526e09134cebc33a199384771acd58c4a87f1ffc063
00411a05a7374d64ce8be4ef85999c1434d867cd8db46c38cd03f76072c91460
fc928db3c8185d34278fc398f1e7fdbfdfca16e96b36f0128207a593771d273d
e52390ecaf833fca9c3815aa93c0b1bb7c8e02bac9daea52b009ad00e5ef9089
d38c7d2990587a334feeccc5933b22125fa56c67973147e4fbb028187ad7d11a
95901bf697ac513d5138a87b3a3eb159ea6a17ab4a3b2772f772b6556ea9f0de
74688d67fafcd99b0b4682864b9dd3f0080ee53dbd4f7eb8fcf0f1d0c245462c
58336c119bc551a11c13959f5205d1114ca4609c6ff545fb28e118f47c3bb4ec
485d6a5ccbb1eeae9c86b616b4870b531f6f458e8bd5c309c40280dc4f51defb
31c731ee82652e525692f7242575832c915df90f8029890faa452f82d758da1a
2aab88e016c474eae260c94542b6bcaccc633ba283a0da093165cd5f82fe0521
274a51ceb0c2cbce0c39f63a457287a9e4c9a99a4a635ff09231b4ecbac5d849
23e7cfb50e352611bddb1408bdc9e0a3d83e724a90ff75d2ab3fb98f29578381
23567f024fec7be53e6dea9bfb5a33690bc541a3a0224a6714d46e6b0a8d36b6
1051914dad61f7ff061aaa9c02cb41defae4b75160140bfc7331f896cab28bb8
0061c84d8ac52c810ded5a25f2e9e09dddbbf865e6d1bf54c2c6a33f6e7e6bf8
03ec1f033ffb2bd2b6c24f087a5d855a2cac38a81779c4d0f27b21a4b34475cf
0593f86978073dce3e51c5aa128a3f003f8764cf133de4ea954532cfb5b98666
688befaeb8d39562f64d1224afb2bd80ef56f29ebb23ef431fd04c672cb2c223
dc3fc52d08d02b62d1ca3f6fd17a978591fc4294d8adef75b118a892adf74321
c1b7d03c96e80f57dfb34795ad98b4adc0cf62f7f4936da9a5f11eea10ad4460
7b65530c68d46a2527014a53643e820442b5d1acf78a2ef2763a14cdf1bf8005
38b2993f7e2174586de759f1f8fd51f2a5b0e8bcf2c19b1d1ef014f85bd591f8
c2ec468efaefe413427efd2d10cdb174dbeca323c9480c45370db4a851db4b1e
18b2d2037ec83bc6afb6d28948975ff4f8866ea470bea3e9b44be333214197b7

KPMG

KPMG Cyber Threat Intelligence Platform

Panchan Botnet – Proliferating through SSH

Indicators of Compromise: Hashes
099a70c4a097ea7dc05a5c8db39f3eb355f6f6bf805920fdec07f6be6309fcdd
16d054526e15a6fc911c401545dc6dfcba7a6302e5620a5f8f26ccf9ff283dfa
19c7ee4706ac0e90244b042aab094fb87bf9e694b4c28083c5284a01e28fba82
24df4071ad03e859968f69feddc2432b5a0742ff6126d6779cc9ae9764f951b6
2bab38c9663f1dd95ebd455e9c7ba83a3929dfda2fedc8cc31d01611029ce999
351f55b27168d02f922d3eb3c557f4b351b9b4de854cae6bcc107a077f35fa6b
3a0391e0cef344bbbfa5aec1d59b719ed50b0112c7615519571b0471d6f365c5
d30933dcd928c73fb002ee86ebc5572286bb1b4a1ee4b910a89189285e055755
596e0a054f2e79b61a17bdc568eb4504ab8129ea0d62b832c7dc83310c59b373
48aa973e4a9d2bd7c0b1eed0f2ff74175abe0808959b40a8605fb3412655f026
e7469a5876f19fd60b5a0b183b329a59c77fbefff00802a162a3fe34cea42d66
f7ce60a4f88120e1c84cc4819a81ad866d618a9b80da8273f3e715fb0a89ee05
6609f29725f1563760d7b8b80ca00b095b7f1815f3594d3bd0a47ce484251c9a
61adc93ea26fd284bc7b2edb90318ae9a8915398bae4b0846400147c5d4e1da5
6ccb79588b79cbe22570712b02ee994d9eecf89fa4b56990c8b029fb921c5b50
43d16b507023d88580ae4a22a7e9a6b1dae3baabae1f62c5ba608e28fe2089c3
05b0a7d5dfc04120b25bcbf4c8fcffd7017b2ace7aff1f553d60d8d3987ae41c
14dcb69e5f49e60dcc1b939322386617c3f1779f320b44111b1b470a225711ab
458aabe8161c043e23b57f18e8fac219d3a9fb0c1b07998efe513c6196d3ea85
6fea9fb816a2643c6d7170cd9ea1d336418a10f4af420c1f95539343ad565a4f