KPMG Cyber Threat Intelligence Platform

8220 Gang - Unleashing Crypto Chaos on Windows and Linux

The 8220 Gang, aka "8220 Mining Group," is a Chinese threat group active since 2017. They target cloud and container vulnerabilities to deploy cryptocurrency miners on Linux and Windows. Their recent campaign demonstrates a shift to more sophisticated tactics, exploiting well-known vulnerabilities like CVE-2021-44228 and CVE-2022-26134. They use tools like Tsunami malware and XMRIG cryptominer to compromise systems, with attacks exploiting vulnerabilities such as CVE-2017-3506 in Oracle WebLogic.

Initial access is achieved by scanning the internet for vulnerable Linux applications using masscan and utilizing novel file and C2 servers for Windows, executing PowerShell scripts to download payloads. They employ shell scripts with base64 encoding for Linux and PowerShell for Windows to download and execute AES encrypted, Gzip compressed payloads. Persistence is established through services and cron jobs in Linux and via startup entries and directories in Windows. To avoid detection, they disable SELinux, bypass firewalls on Linux, and utilize fileless attacks, UAC bypass, and DLL sideloading on Windows. They exploit vulnerabilities and use SSH brute force attacks for credential theft. On Linux, they scan for SSH ports, while on Windows, they parse command history files for SSH connections, aiding lateral movement. The group automates SSH connections and payload execution on various hosts for network spread and communicates with C2 servers for instructions, payload downloads, and data exfiltration. Additionally, they gather information on compromised systems and networks to identify potential targets for further exploitation.

The group's evolving strategies and sophisticated techniques have raised significant concerns, emphasizing the need for robust defenses and proactive threat intelligence to mitigate & prevent future attacks.

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

8220 Gang - Unleashing Crypto Chaos on Windows and Linux

Indicators of Compromise: IP Addresses	
5.42.67[.]29	79.137.203[.]156
185.17.0[.]19	201.71.165[.]153
51.255.171[.]23	179.43.155[.]202
89.185.85[.]102	185.106.94[.]146
194.38.23[.]170	217.182.205[.]238
45.142.122[.]11	159.223.201[.]180
178.62.234[.]229	163.123.142[.]210

Indicators of Compromise: Domains	
dw.bpdeliver[.]ru	dw.c4kdeliver[.]top
fbi.su1001-2[.]top	

Indicators of Compromise: Hashes
f162522851b01256bd3fda3832824abf
74d4e0b04e390a5812686f216af1e86d
6b90414017bbd93115e55aa853bd7f30
05e45080d540858523c79696815c07f7
7e0ad4d0a2eb8e59579236f90499e2b6
8c60e957f2bf8d3bef3b710377a098e0
996bb2c31eb116d82147737e202b83c7
5f5785bb3af4b000e03e11cb961fb815
3b3ede235ff38972126e5907cd40cb8e
24e41d283346621a92ad2723aae6a024
77e3046e6271f2871ed34497a06ce770
c5dad0cddb066f02cdbb6b9073bce05a
4e9c1e438d5728fcb478450e94a2dc5d
c0703b08be76644d49dd9cc054fe8bd6
1905b587d04ee38d42267fe145fb0f62
44fe52818d466432ebe55e6e277823eb
9de62417afc3e41786a63b89a6d9e7f9
5bf0ed7b9000b965ae2a58f891f1fe1e

KPMG

KPMG Cyber Threat Intelligence Platform

8220 Gang - Unleashing Crypto Chaos on Windows and Linux

Indicators of Compromise: Hashes
6f1d8ee2d7a591f416bd91b5998623ba
cc370b929b8849dce02f0c7e5a41dd8a
558c75fe6823c4ee9d066a4d9d1aff4c
2efefcc01367d598d50de06fa98b1694
490e83b54f48901cbca652603d2fa315
d54f3aae7090f5b56ed185d52d878f8bea215e3e
197d29f1937851c47c143f8ec6f5392c98bbbb00
574179950c0881faa9bfaefe0fbcfff5e9decb46
80cd8a8f1813fb47c5235e4847c26c6debdaf192
12642a19d8960e0dfaf53fe94369a2c209c29014
2a829a50aa0557acf22896d9b4318f4e3b9cd1c5
0d9c7cf737839a7aaedc39421c033d3a5d2f8f5a
49e4797468e916e53dd28acafc4397368e442e73
a91d1143eb01c9445de6d6c1f1cf954ce5f98a9a
0a863729c844a4da3a1ef994628e855ddc7a8d49
c7496e3a98ab018901d3de0cdff8742aa4d0d373
4d52b71959559782f8d52d72bb88604a38e8c3ee
b8a0a9b54c6a5bc62a4ddde02c938c519f189fc6
ac176986392d9672ed98859ab0246daf2afe83dc
2cbe796425c2184ffad2e826f7bfd5b260358b86
144b8c52f63191301652bd5aeed7bdbd62c314d2
3e973e4cfb8182fcff69ad7fd6f3bcc1b52570a2
d1bb8b614ca754be3e1aec283c0eb978749ec35d
4ce4d988c686bace1aa8e64ed2b6f86e475ec9c9
00ec71262d6c7556ecede5f10cd1637f7375b9bb
103330645e380adf4a9ca46137c166834bdb1fea
a966af08dcb4e94e7432ee744aaa7c13c27332aa
cc09ef95d4a3f6ef6e130e0daaf7117bce3b6613
b60d2d8aebd4c58a16f57ffa7137cc0235e60815
44255b59172806d7f5b814b84a2d70f14d16c82b
897e8f7b27c5042208170fe69686e87d4951139b
dbe7d445b346bae7551e9074d1a7f8c60d10f219
8f25564a40863c5edff7746bc437d1a27d794574
79d2a06fc476c94b1cdff782bc885268415190e2

KPMG

KPMG Cyber Threat Intelligence Platform

8220 Gang - Unleashing Crypto Chaos on Windows and Linux

Indicators of Compromise: Hashes
7abb0dd26419c875bd2831686613a858a95f10de
28047c2dfb40b06d83f24598ba5687a260d87b33
efe375a5d14f8581e80a303cad47a12f7c3a2450
01ca22966c2a26b90d192978b20cf54b8eaf811e
e52f2ebeba91510fd5f60f4fabc2fdcd41936fe4
b7629c823461e55c461a21a36f19616148fdc7ebac8c74bedb38c625fb4d94c5
f295fac3c85545188388ea80457d61b2fe0f62476a5b8f681c6110f0ff002aab
7822d8d9d1bab1ad4ba3a0366c18df11bed661c70c9f88db00c33daddf71c9b4
7994b4e514d3b0a33c975b921d9bd7e9d2ef06d30adac0489c198fa3575b8dbf
3394734ea39a406475159c425fe187297fe4cc6dc9e1867ea3ecfe55a4911760
ff47fb01a09359d7fb2c7ffca42ea8de496b78f01dcb856da2b9a597f1606247
f476017cc9052b36d7326a5e3083dc9c76048e2fb9eada0032c5e40c036544f1
bcca7dc3d3ece544d700eb5fbfdb055c2f2b05a06aaa1e4485eba0ce7399f59e
0db1c107fe9bb37aac6f548c2ad9c25d339f0a3e7770a47f13760db87ad0405f
fa4de2e35f04292a043294ae88ec3a7bbd7694e32b91e9e94a17e8d7aa32b284
cedb99c61221e174c7ed8bf283d4342e6b0ba5792a6f85d0e24db7037bab2cf7
9f8aeda646b376e1c71fe7166207b0a0c6a265fc7900f73cdbfb4f97a976b5c4
0021c7388be9ebc3a911b0a04a5722bc94af243c4f426924bbdd6bf9609e0515
0a30d3b6f4c64101ea41dd8132c9075351da4a3b11fd8ce7a5265ac0ec8f7649
9a598c1b86d08d48166100a09e1ccfa1f848403a004da22fce9852df5421fca0
f6f10836612e7e0c27091494ab67ac8cb95203aed23a8bd0ba9c7230e18644ef
8bf0af857be974c445353978820661dc496167e044d05f07e45808bd7d72fb7e
9cde5a31c450ff6e4128010c1496c237fbd225ca6624181445475d1aa55ea39c
e9308e2976836ae26bfbb92106525c33282f0c56b97b0b297155abb4882f8d27
be6d1c864b7784f3db710cd1f32d813470489ef275e1ae359c57370248bf1f0a
b3d5206fae479e6aa88bf135da867ae984aec2b30b5581c54c0dd88e97b8aca0
6aea8f96dc013105ef3e2641fcb650065e4d5c0c0a8f7ca4e93b68c1f3695a08
6a47571c3e4311c11d5717d02ad696ff96e61fceeea5730d61aa5a1175a08f7e
af5ab11e9a1578c62246d40d47bd017fa9897912be1a725bb41c56e3fc64c1eb
0b74f0d40ff3c743811fcf8f92e9ab1cf5af4c532d7392e0a6f2c36b25414247
6d0507b35f70e8e3377d584552f91b2c3ba782c40e189849fc0a70bace824393
0c69a6a5497c8bd3ed6b9db4b5036b6ed3d069edd7100d8988803366477d715f
d579057e3f4da79bb722fe18dfd7b0328355a1c48d0b3cdb2514954ebed24eb5
dfd1ac49e99ebaa61196262da41877b6afaf631384e71114836a2609519402f2

KPMG

KPMG Cyber Threat Intelligence Platform

8220 Gang - Unleashing Crypto Chaos on Windows and Linux

Indicators of Compromise: Hashes
89b142345117l6f64b5f25660cdace4f183b1eedeccb201095cc5d29fbb87518
076d0e32e9233c101f7ef8489935bca861e3e3fbbc1962828bf469b7d4671263
2ff0aa3ee969020281dc099a8556ace53074f23021a8f3b7e3916364c266cb15
a1dad8768ab2cb89d883979a99d23cbe586539b69530345f4069a399ff2eedf6
dfa9e2ff880196a1070820b75eedf468f52a332b723e2dea9dd7cfe3a68c0148
039e8df99d1de3ff85181ca75130c69497b112b340a315c625812474105acf74
07ed5aaafaeb24c4237d0e4a2fa9706768768ad8cb895a326a328dd415037495
c65157c5f655986a3fb5933f2845a0d979267a75d8780521b890a1169e60df62
f6ed5506e5bff89852d6c5283594bc556a0273a57fcb117eb42d1b28285890a5
697f94b66d9520e6225266bc7954a5d8dfb800d352de7b88ad12e7e5d31bf8a3
cda6a3a92d746c0be30c1809c15b2f5e344b724dcecbda7729234a798fb5218b
28682cc7e703cf947ac6e43c9f624b0ac80247805eeb92192c276bb106b65dba
d4d8a166dd8cbca451cadab8fccb959d368ee2f661fcc5ee32baede11e043d6d
a978b12022427089a12323ec24b4babb7ab201c30fa15f0c1f5e109e1f536e73
e0b8d7e3cdd3aa6f1db434ae1cf9af518b1f2f4b39067949900d35a4002df503
9fb1688906adff5f6fd89bd97ecf4fe8211647b9e6b8eaa168dbfed39320fbed
cfbd2b113263e698e7adbdc9ece71af1719513be84315178123e6fcfb0f92131
dd344fe031fc97316be10505e872ce5280ef512bfe1c1caf324920dfe2c7b173
5f2486bfce763e8a93b216a8359c661a55a811708dceb40b1bbac99ccc1bce66
22878b86b6c2f101ca51f7107b485dc0a15937fd5a87f88ab8df75d085718960
6ac610fbda8436d4c4c104d996a18ced3e67a21544772330ac85de26a0fcd58a
ea6a9bdd8b106573a37f6b1b4214cab5a37d12fc39e5f78da5073c535c1b0f74
edc08a540181a77225792c123181456207c8fb7c2a662faad87aea993e88af23
5542c8f1927ed4872492abd0c99a8d9df2f9554a3e001248abc82e729731d3af
45140a0bd9805e0d14998e45c923e95886526b01a56404ae679bf5ec80c23814
0b3afeb03fe2b8fadad891812ffeda70f861ca313499e729baf7f67a3b200b0c
4643b1870fc85c74f54918df076798d2e30a2e750b48304196829d33956d7494
81d005d2ee691acdfc3c0e8425e061a4d826fe2892bcbc0946ea53ff47609e05
928be749aded14c117b6dc971175ff73b44b95fc895b5c7f8aff4bd7fee2d058
2aea86868c34d5f91acd31223c333250e0235bf2e654f964e9cbe79cfe3b55f7
b5fa13d8a03e9a38995e1a087f873e9f2e5d53d8ac713ffb951f62084c810a90
5183206bb4a1a5ad57ccf2d07c4cd1b34c16841e891e1742225213c47a751c0c
ee6b797484c6747550b0dbb7ff707554b64f5bd4abcef8a78ad33f6c2c8d53c8
4636a3c1f9c526c3a99b7e4abe187a4bd4261817f7472d765f11982b33176ce8