KPMG Cyber Threat Intelligence Platform

Clop Ransomware – Honing its techniques

Clop Ransomware, akin to the Russian affiliated CryptoMix ransomware family was discovered in Feb 2019. While known for its numerous high-profile attacks targeting Windows Operating System, instances of a nascent Linux variant making rounds have been identified recently. The group majorly targets US, Spain, Brazil, Turkey, etc. focusing on sectors like healthcare, finance, media, energy and educational institutions.

Clop targets organizations rather than individuals and employs multiple methods for initial access. These include using spear-phishing, maldocs, exposed RDP/SMB/WinRM services & malware droppers like Get2 and TrueBot to deliver payloads. Further, the necessary tools are downloaded using the initial loader payloads. FlawedAmmyy RAT is used to extract system information such as processes, registries, antivirus, networks, etc. and to communicate with C2 for next stage. Persistence is achieved by writing itself to Run registry. Admin shares/SMB vulnerabilities are then leveraged to laterally move to compromise AD server for maximum impact. Also, Cobalt Strike & TinyMet are used for post-exploitation C2 activities. The main ransomware executable is distributed to all systems & detonated via AD admin account by running remote WMI commands PowerShell scripts. It also evades detection by utilizing application shimming technique and deletes shadow copies to prevent recovery. The encryption routine involves encryption of each file with a unique key and in-turn encrypting those keys with another key.

Clop is known to use extensive extortion techniques which hinges on data exfiltration through tools like DEWMODE web shell and Teleport. With Clop becoming cross-platform and constantly evolving attack vectors, organizations must secure their network by frequently patching vulnerabilities and by ensuring constant monitoring.

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

KPMG Cyber Threat Intelligence Platform

Clop Ransomware – Honing its techniques

Indicators of Compromise: IP Addresses	
185.99.133[.]153	103.232.123[.]160

Indicators of Compromise: Domains
rsv-box[.]com
gl-box[.]com
ekbgzchl6x2ias37[.]onion
6v4q5w7di74grj2vtmikzgx2tnq5eagyg2cubpcnqrvvee2ijpmprzqd[.]onion
santat7kpllt6iyvqbr7q4amdv6dzrh6paatvyrzl7ry3zm72zigf4ad[.]onion

Indicators of Compromise: Hashes
0403db9fcb37bd8ceec0afd6c3754314
0571bb4ecf3dbf5d5185eabd7d03d455
160fd326a825271e9bd71653ba6f3ee1
1b6e1afbacc63096e4418badb6dec7fa
227a9f4931342f8b49cb3044f66dbf05
279f5beee9d4bf8c54026e78acba61b1
31e0439e6ef1dd29c0db6d96bac59446
35792c5501760071d461e9455aa50730
39ae516ed2cd6bdbc58c2ad2740c9883
3fe02fdd243979106f6d91ae2df8ccff
4431b6302b7d5b1098a61469bdfca982
4eab23668cfc12818d05ccc4b7042a22
569d3ed52f17b12729cef26018c81fb9
592a37d9d808f97c43f45ee515e9c914
5e52f75d17c80dd104ce0da05fdfc362
738314aa6e07f9a625e4774ac1243a79
73fbfbb0fb34e2696e5f3d9a9d2f6d46
8752a7a052ba75239b86b0da1d483dd7
8bd774fbc6f846992abda69ddabc3fb7
8fc09cb1540a6dea87a078b92c8f2b0a
91b05a8c97429ef315ddb7e00613f133
949670dcded69c76760d87f2271e0631
9ca31cf03258d8f02ab4cd8fccbf284b

KPMG

KPMG Cyber Threat Intelligence Platform

Clop Ransomware – Honing its techniques

Indicators of Compromise: Hashes
a93b3daa9460c64c631ad076d8ed126e
ae0c9765cc0bc9f4d2ed8970ff77a8d1
ae5cb860f043caa84bf4e11cec758616
afe7f87478ba6dfca15839f958e9b2ef
b65646fd89d5860c470112417a54fb2f
be3dde8959f32c547fd83bc1f794e726
c41a0e1ddeb85b6326a3dc403a5fd0fa
d8df0eee17fa5a361e26d67c43e10f28
dd5cee48cdd586045c5fb059a1120e15
f59d2a3c925f331aae7437dd7ac1a7c8
09b4c74c0cf18533c8c5022e059b4ce289066830
0a7ab8cc60b04e66be11eb41672991482b9c0656
16f48624ea2a575e1bdceb4ac6151d97d4de80b6
21bdec0a974ae0f811e056ce8c7e237fd7c220c1
2950a3fcdd4e52e2b9469a33eee1012ef58e72b6
2a870e331c2322ed00b22d418173e57c87db71bf
37269b8d4115f0bdef96483b1de4593b95119b93
37a62c93ba0971ed7f77f5842d8c9b8a4475866c
3c8e60ce5ff0cb21be39d1176d1056f9ef9438fa
40b7b386c2c6944a6571c6dcfb23aaae026e8e82
46b02cc186b85e11c3d59790c3a0bfd2ae1f82a5
4d885d757d00e8abf8c4993bc49886d12c250c44
4fa2b95b7cde72ff81554cfbddc31bbf77530d4d
51e0095668356f13b652d25a89aa2f67259e3299
57d589642b57f034cd1439fee637f0325cf5b4da
6eeef883d209d02a05ae9e6a2f37c6cbf69f4d89
77ea0fd635a37194efc1f3e0f5012a4704992b0e
7d97a6b6a8d171c251a7f9d236399ae5518efa52
87e8d54eb7a494649724804f5cb8f4276090068d
98fe0eb11fcccef4785e433f8c837371ae6eec41
9d59ee5fc7898493b855b0673d11c886882c5c1d
a1a628cca993f9455d22ca2c248ddca7e743683e
a6e940b1bd92864b742fbd5ed9b2ef763d788ea7
a71c9c0ca01a163ea6c0b1544d0833b57a0adcb4

KPMG

KPMG Cyber Threat Intelligence Platform

Clop Ransomware – Honing its techniques

Indicators of Compromise: Hashes
ac71b646b0237b487c08478736b58f208a98eebf
ba5c5b5cbd6abdf64131722240703fb585ee8b56
c41749901740d032b8cff0e397f6c3e26d05df76
ccd147cea99c1b2e15f193a761f7a5be8da850e8
d613f01ed5cb636feeb5d6b6843cb1686b7b7980
e1fb096873ac5ca990dda56d381f676178159885
e38bca5d39d1cfbfbcac23949700fe24a6aa5d89
e473e5b82ce65cb58fde4956ae529453eb0ec24f
ec2a3e9e9e472488b7540227448c1794ee7a5be6
f4492b2df9176514a41067140749a54a1cfc3c49
09d6dab9b70a74f61c41eaa485b37de9a40c86b6d2eae7413db11b4e6a8256ef
0d19f60423cb2128555e831dc340152f9588c99f3e47d64f0bb4206a6213d579
102010727c6fbcd9da02d04ede1a8521ba2355d32da849226e96ef052c080b56
2f29950640d024779134334cad79e2013871afa08c7be94356694db12ee437e2
31829479fa5b094ca3cfd0222e61295fff4821b778e5a7bd228b0c31f8a3cc44
3320f11728458d01eef62e10e48897ec1c2277c1fe1aa2d471a16b4dccfc1207
35b0b54d13f50571239732421818c682fbe83075a4a961b20a7570610348aecc
389e03b1a1fd1c527d48df74d3c26a0483a5b105f36841193172f1ee80e62c1b
3ee9b22827cb259f3d69ab974c632cefde71c61b4a9505cec06823076a2f898e
408af0af7419f67d396f754f01d4757ea89355ad19f71942f8d44c0d5515eec8
46cd508b7e77bb2c1d47f7fef0042a13c516f8163f9373ef9dfac180131c65ed
6d115ae4c32d01a073185df95d3441d51065340ead1eada0efda6975214d1920
7ada1228c791de703e2a51b1498bc955f14433f65d33342753fdb81bb35e5886
7e91ff12d3f26982473c38a3ae99bfaf0b2966e85046ebed09709b6af797ef66
85c42e1504bdce63c59361fb9b721a15a80234e0272248f9ed7eb5f9ba7b3203
8e1bbe4cedeb7c334fe780ab3fb589fe30ed976153618ac3402a5edff1b17d64
929b7bf174638ff8cb158f4e00bc41ed69f1d2afd41ea3c9ee3b0c7dacdfa238
a9741b16f4169f56ae0f2e49c87f3c5360ed5ab4370e6d16bd86179999f11795
ad320839e01df160c5feb0e89131521719a65ab11c952f33e03d802ecee3f51f
af1d155a0b36c14626b2bf9394c1b460d198c9dd96eb57fac06d38e36b805460
bc59ff12f71e9c8234c5e335d48f308207f6accfad3e953f447e7de1504e57af
c150954e5fdfc100fbb74258cad6ef2595c239c105ff216b1d9a759c0104be04
c5f995d04720cd53f6d12364212231e05ea27ed2cff37abba22b87a73e9dac78
c793a9225d799150538f058c886e2806083f6bc33813a3bd8231ab2775b7ec2f

KPMG

KPMG Cyber Threat Intelligence Platform

Clop Ransomware – Honing its techniques

Indicators of Compromise: Hashes
cb36503c08506fca731f0624fda1f7462b7f0f025a408596db1207d82174796a
cf0a24f1cdf5258c132102841d5b13e1c6978d9316ba4005076606dc60ec761b
cff818453138dcd8238f87b33a84e1bc1d560dea80c8d2412e1eb3f7242b27da
d0cde86d47219e9c56b717f55dcdb01b0566344c13aa671613598cab427345b9
dd2f458a29b666bbfe5a5dbf6a36c906d0140e0ae15b599e8b4da1863e7e41ff
e19d8919f4cb6c1ef8c7f3929d41e8a1a780132cb10f8b80698c8498028d16eb
e48900dc697582db4655569bb844602ced3ad2b10b507223912048f1f3039ac6
eba8a0fe7b3724c4332fa126ef27daeca32e1dc9265c8bc5ae015b439744e989
f1b8c7b2d20040f1dd9728de9808925fdcf035a1a289d42f63e5faa967f50664
00e815ade8f3ad89a7726da8edd168df13f96ccb6c3daaf995aa9428bfb9ecf1