KPMG Cyber Threat Intelligence Platform

Magniber - The Single Client Ransomware

Magniber is a recently identified Uncommon and Unlikely ransomware group targeting Windows home users instead of fleet of devices or large organizations by masquerading as software updates. These updates are launched under various names like Win10.0_System_Upgrade_Software.msi etc. and they trick users to update their systems thus resulting in successful installation of the ransomware in the targeted system. The threat actor is also suspected to distribute the malware as windows 10 update through a network of malicious websites.

The infection chain starts by downloading a zip file from an attacker owned website. The zip file contains a JavaScript file which disguises itself as an important anti-virus or software security update. Further, DotNetToJScript technique is used which enables the attacker in loading ".NET" executable in memory which bypasses detection of file writing to disk. Once the ."NET" code is done with the decoding of shellcode, the code is injected into another process. The ransomware then runs from the injected process and starts off by deleting shadow copy files. In order to restrict the ability of the victim to recover their data, the threat actor uses the user account control bypass provided the logged in user is part of the administrator's group. After disabling the windows backup and recovery features, the encryption routine begins and the files in the victim's machine are encrypted leaving a ransom note thereafter.

Provided the complexity with which Magniber has been targeting individual users, it still poses threat to large organizations. In order to avoid significant damage, individual users should be apprised of the importance of installing updates only from trusted sources in order to cope up through such cyber 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

KPMG Cyber Threat Intelligence Platform

Magniber - The Single Client Ransomware

Indicators of Compromise: IP Addresses	
totwo[.]pw	orhung[.]space
catat[.]site	actsred[.]site
pirlay[.]fun	tinpick[.]online
ittakes[.]fun	buyaims[.]online

Indicators of Compromise: Hashes
41f2bb0eb5c97319317488894c8bba581
5523c42788189336b50e00338676dc31
7822d28811afd739006b73db15d2b5a2
30665fb2dffafe5d7e3cfab4cf4d79dc
b6169c34b6eef8ebe21ae10904967385
0dfe349ff646b008b7ce6a8104f6e8c5
5efae9ad4bc66f7be01eca20277858aa
30a5ef2f39530eb3ffe61cb8153650e2
56cabf4dcdc963c8efd8dd4969825724
406e382d80ce29d0f0f02a9b1a258d40
166402b5dfa0717dfdc00702910ff354
fd4c042ef1e26410121b069744daf19d
1c09a97b26fff2465692df0a5cafc4e0
74d3f742a0110d11786e27ea3c6a4b59
78412c65ac9a1954f373961c0ddbc9ef
d9a63429fefa067c0ece510e6e22e1a4
dfdddf236603918bf4359716412c97fb
d417420973f452e41d9d5709fc76f8dd
f49194f0e8ced22850d91f231829d877
93425b7d09d179450b92f91b0942ef0b
37ebfc01406f7cde2741b3b73e77b991
b3ece680f2d56d0ce3d95f97dd36487b
6155453a58b0ba360fd18a32d838c4452fec374c364824b50447500c8fd12e80
5b2a5ac50977f41ac27590395bb89c1afd553e58f2979b680d545bff1530a17b
79590d91e9131918df458221e8fcb9c5e33d0200f05f9704dcf88167a5515b3f
7064eab88837bc68b8c5076300170cd73dbea046c9594b588779082396dbfe4c
a292ff42e0e1b58b13c867d2c94da2a5d34caa2e9c30b63610f7e12be5e7d3d9

KPMG

KPMG Cyber Threat Intelligence Platform

Magniber - The Single Client Ransomware

Indicators of Compromise: Hashes
dfa32d8ed7c429b020c0581148a55bc752c35834d7a2b1bae886f2b436285c94
c1d1402226179c66570d66290dff2238b6a9f918c81267a61d58f4807f0d911c
56fb0d5e2e216f2b4d9846517d9ed23b69fba4f19f2bad71cdce47d9081642eb
92ec900b0aa0f8a335cf63d4f313729da2831ffc7d15985adf2d98f2c85c3783
c7729a7817a3d63f71d6c9066bd87192d07992ae57fc3d3e6d0e67c5ab9fb213
9d665f87440c22e3ae209308e3712a83a67932643be019e18b1ae00dc4ab8cbd
b12461bdd88bb2a7f56d11324272ae2a766d560371b2725be6f9d3175fb32f8c
abeec5267f6eb9fc9f01f4688a53e83c87898845767b8cd8599c75dbce1766a8
aeee31c3649724686cb9ad17fe1ee2b70b1ad1b6cd77cb8b1997aa6e75d49cc5
1eba630a870ce1aa840219d77e280cfd05d3d5e5cdea6f382c1c2b8b14ddf04d
54a5b06060639a483a8f6c80c8f095fb41e3eb5e7c02c3ad4ba29ee3a9ed7aab
76c012f134e81138fb37ac3638488f309662efcc9bb4011ff8e54869f26bb119
56d301fe7a6b1a9e21898162b0dada9ff12878c539591052919fabcc36d28541
4936cf896d0e76d6336d07cc14fbe8a99fbe10ad3e682dbc12fdfe7070fd1b24
6a68217b951f9655e4a7ed13fcfc4696ac5d231450fe7d2be8b6a1d71425752c
05cf26eaea577417804075a2458ac63f58a56b7612653d3a4c2ce8fa752bd418
266f930572d3006c36ba7e97b4ffed107827decd7738a58c218e1ae5450fbe95
9095bbb4b123a353a856634166f193124bdc4591cb3a38922b2283acc1d966d6
98d96f56deaec6f0324126fcdd79fd8854d52ac2996d223d0cb0ab4cff13ff7c
0c5956b7f252408db7e7b0195bb5419ad3b8daa45ec1944c44e3ec1cca51920f
c4f9dbff435d873b4e8ecbab8c1b7d2dbdb969ac75af4b1d325e06eb4e51b3ad
5472bce876d0758fb1379260504b791a3b8c95b87fc365f5ce8c3a6424facd34
d0375fc9cbb564fb18e0afea926c7faf50464b9afb329913dd5486c7cbb36e2e
ad89fb8819f98e38cddf6135004e1d93e8c8e4cba681ba16d408c4d69317eb47
99f0e7f06831c6283f5f4dc261a7bcbe4109b4a6717b534c816ca65cd2f05dc4
b81f76bd5c6e66b9b3a4f2828e58d557091475bed656c9a8d13c8c0e4b7f3936
c6f1da2490fe78b1f281a98c32d6fa88d675598e658d4e660274047e36f1b189
dd30688a0e5ac08fc547f44b60f13ef664654c9a8977f7a5f8f619b08c09620b
c0bf9153ce1641791b357fdb5c2c596fbbf15991a86f510cc444bdb477574d44
bf50794c33eebc9dc2ce3902fe29f683a37da50de3654a2775baa74d0bbd1188
b8e76ad7c7857d9985b15dcd064664d198db7201cb9eb6a0e53d81b6002f7d29
cc1ce8c687450b082dd19a6c5d868f5798e52422172f91ee4b70cb5ffd9f6fcd
a587172f1bbe665cdfc0cbcec54e72d8b9048c77f344ba5076a17fbf620597de
c4560eee4b02dc0ef087e48848cc83b270068d167f613f04d43a64025e72c09f

KPMG

KPMG Cyber Threat Intelligence Platform

Magniber - The Single Client Ransomware

Indicators of Compromise: Hashes
82fcea3c48509a1724c0a6ded9e3d3cab775a86588119c35b79355105bd828c4
e993e4ddd05007e62e6e2d00e70927933446ff4bcae2b559bb6be3bc5e4ad2d8
5b513dfd8f94f9b6e962eb691caa56d52ab4453369108ae3b572e2ee7f9b555d
d2d3fbfa73dfeb73a6f5c59fefab8dd99dcff58cefeb0d3b3b1c1a8854178933
d80d90ef631bb60b773bf1211f3c53c1cac043674c85eb65dbc457656ba5d4cc
757cd5b65155cd115b71021685fcc52a42ee80aca247ea68f41aa0d82dc20fc0
bba85d79db69db1b638e24e0a426ccccdc5c95875b8c3a26aa959cce3f6c8575
beb5e1c5ba835f29e272b2942b27b63f6f15647f3da51754fcf53c277e0eccf7
f41ec94f9d0c7480df2196b3fc5493599d50de222d2c903b173db3e7caff8747
397aa7bcc4a574dc30f0a491e03be15da55fa898624c7b15d0197e72802d048d
6b18a287aa2c170605409a4675fd600d0597623d174445aaea5a2279bee0c145
46d8d6230083254fa324299fc609125ee404e4bbdd3936ddc0235ae21479b655
e8663c5c28d8591f06eb7995e0f22b7ae7909f9431786f8557f2c081e0e79fad
d3f626d3e533f3b4aa0599c231210d53f709c46f0cfc3d28f0303df544a39b1b
814061567356daf6306eb673cfb97cab264c798320bf1b432d396b66393adf83
2c93879d024238d23270fab734a5ba530bfba2d35b44d265c8be3c93ff8cf463
3055baf30466f1c0f4cd5b78d05fe32ef7fd406dead3ecfcbdef464fdee551b8
568e1e3d55a6146f0f899159c3a5183362b8b13304109b49f7394a9fe8c69ea7
932d2330dc3c1366a8e956183858246c4052027cae1590d2211186be648fdcf4
dfabd6462ab2ecb9fb0cea7caa257841a751c1e91118168ef5a082cf8a25210f
fbd69303e6255aae830daba957c8ef62eb6d23340274eb8058826a08e82773db
123d7744a407af376b4ee4402ff8bee588b40540bcfba22fb64768d1de8c1861
934cfeb5ee3d2ba49831d76dffb1a2658326e1cd90b50779d6670eb2fbdc7ed1
10b9b1d8f6bafd9bb57ccfb1da4a658f10207d566781fa5fb3c4394d283e860e
36417f0ea6d948cbd7e003b3cefbb603d886849a8c80e0999c7969b03f2b9c28
66c4f54da6542339de036872e80306f345b8572a71e782434245455e03541465
77d3b1cf6d5a0a07090cdb078dce6e3849465c9acde7e1ba66c3893fefc73d4b
9a6584a163d8c378e6f873c5544794274cce2532e91fc079b79fd73399447b03