KPMG Cyber Threat Intelligence Platform

Shikitega - Stealthy Sophisticated Malware

Targeting the Linux operating systems, Shikitega is a recent addition to the malware family that infects vulnerable endpoints while taking full control over the system. The said malware is a sophisticated malware as it leverages polymorphic shellcode to evade AV products, exploits vulnerabilities for privilege escalations, and a meterpreter to gain access to the compromised system. The malware is specially designed to gain full control of the IoT devices and execute a cryptocurrency miner to extract transactional data.

Shikitega malware starts with a multistage infection chain where each module acts on the provided payload and downloads and executes the next one. Stealthy Shikitega downloads an obfuscated payload hosted on reputed cloud service encoded by Shikata Ga Nai polymorphic encoder and executes it. The executed payload connects to C2 and further downloads the next module containing Mettle. Mettle, is a Metasploit framework that can steal credentials, deploying multiple reverse shells, and taking webcam control onto the victim's system. Shikitega leverages unpatched bugs to spread its control over vulnerable IoT devices. It exploits two major privilege escalation vulnerabilities, CVE-2021-4034 and CVE-2021-3493 to obtain admin root access and downloads crypto-mining XMRig software which is used by the attackers to penetrate the compromised machines and mine for cryptocurrencies.

Provided the malware has a high disguise capability, users must update their firmware with the latest patches. Organizations should regularly perform an antivirus scan on all endpoints using an updated anti-malware application and the firmware must be extracted before running an anti-virus scan on IOT device's server file systems.

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

Shikitega - Stealthy Sophisticated Malware

Indicators of Compromise: Domains	
dash.cloudflare[.]ovh	main.cloudfronts[.]net

Indicators of Compromise: Hashes
347cfe81b13bd6d985a34a339f671458
b035f85870bb17380b25189bd97b8e65
7b229d73b7c5c55fda0e1f57ceaaf118
f105102404cda7e7de2ac1ae54d9a78c
932df67ea6b8900a30249e311195a58f
6e6845896222ee7d48e76ea2bf11b97d
6b13e69cc37757b1f2dbc2a1c8f806f1
557bdc5602b301d5584a34b27328b019
0f1f2d4a6fc26df7cf5d5a8c65ac8578
da193f6bf387f9884d88ace9c04278a0
7a34ca9c59cde0af620ffa30783348a9
2f56a330fb253a1520e00668c6f94e47
8e3e276e650e6ea21bea16c8c2f3e8c3
593e9551a4a9b49323a1fda81fe1dd5e
fd3bc823d9e6b1aa0622c36ebd5e69f2
d1cd3293ac4b312e0b3218e80376bd88
04ad59ff2b2b8461a6d990af16bc5ca7
dfd3d0154a8b49588136230bcb8abf77
029dbe8df57f3d89ee1f1fe7f50fbf4519ee9522
a046a2ddb1d4baa6cbc6611a3d072a28ff893e1f
8ff5bcf2c69056780f0a7b51c96bba243dca2201
d6b7c2388a75c2c3b71d5ad7130f1d3dfeb7fd83
6f89acd56678b4c9b929794334777fd8d93e6cd0
01364dc40e5f1005fd7cd6e087368d64b35896f7
6acba32a32d4d0dd01ad17db719d0d0bc26b551d
9eeef2f22ae1f96b49e45989a8e935c825be92ad
c193d71ab61054ea7b5445a5a7a5745624171cf8
74d584862b851fbf54605c205f447fc5cfb517ee
8ef509c2b25e6475dbdc92f14117c7592af70b88
e483074bbe5e41cacbe081f290d7e6b0c3184c7f
f437d04482e90d459c4bb6722cbec928f7317871

KPMG

KPMG Cyber Threat Intelligence Platform

Shikitega - Stealthy Sophisticated Malware

Indicators of Compromise: Hashes
009639d09c5955ae5fda4a5e1c161579a684b514
3ea957516c02bc2e57ce17401b56e5f2f0288725
c49bd909be55892f75d81b174588b5af15d2a6ff
159810f29358d6231c0ea0c0ba998376104f22cd
17f8cca0d941ed633acc69746eef6fdd1db6dd8b
0233dcf6417ab33b48e7b54878893800d268b9b6e5ca6ad852693174226e3bed
05727581a43c61c5b71d959d0390d31985d7e3530c998194670a8d60e953e464
3ce8dfaedb3e87b2f0ad59e1c47b9b6791b99796d38edc3a72286f4b4e5dc098
59f0b03a9ccf8402e6392e07af29e2cfa1f08c0fc862825408dea6d00e3d91af
623e7ad399c10f0025fba333a170887d0107bead29b60b07f5e93d26c9124955
64a31abd82af27487985a0c0f47946295b125e6d128819d1cbd0f6b62a95d6c4
9ca4fbfa2018fe334ca8f6519f1305c7fbe795af9eb62e9f58f09e858aab7338
cbdd24ff70a363c1ec89708367e141ea2c141479cc4e3881dcd989eec859135d
e8e90f02705ecec9e73e3016b8b8fe915873ed0add87923bf4840831f807a4b4
130888cb6930500cf65fc43522e2836d21529cab9291c8073873ad7a90c1fbc5
29aafbfd93c96b37866a89841752f29b55badba386840355b682b1853efafcb8
2b305939d1069c7490b3539e2855ed7538c1a83eb2baca53e50e7ce1b3a165ab
4dcae1bddfc3e2cb98eae84e86fb58ec14ea6ef00778ac5974c4ec526d3da31f
4ed78c4e90ca692f05189b80ce150f6337d237aaa846e0adf7d8097fcebacfe7
6b514e9a30cbb4d6691dd0ebdeec73762a488884eb0f67f8594e07d356e3d275
7c70716a66db674e56f6e791fb73f6ce62ca1ddd8b8a51c74fc7a4ae6ad1b3ad
8462d0d14c4186978715ad5fa90cbb679c8ff7995bcefa6f9e11b16e5ad63732
fc97a8992fa2fe3fd98afddcd03f2fc8f1502dd679a32d1348a9ed5b208c4765
b9db845097bbf1d2e3b2c0a4a7ca93b0dc80a8c9e8dbbc3d09ef77590c13d331
d318e9f2086c3cf2a258e275f9c63929b4560744a504ced68622b2e0b3f56374
d5bd2b6b86ce14fbad5442a0211d4cb1d56b6c75f0b3d78ad8b8dd82483ff4f8
e4a58509fea52a4917007b1cd1a87050b0109b50210c5d00e08ece1871af084d
ea7d79f0ddb431684f63a901afc596af24898555200fc14cc2616e42ab95ea5d
f7f105c0c669771daa6b469de9f99596647759d9dd16d0620be90005992128eb
600d319d935ded4e2bcf9d339c81be8f5c7451b9e9ae1ee65ce6a5e0037254b1
f71c565db6730392855d6fabc85a763fcbac91e9893145f62f21ae2b0dc369c0
b30305f6c2b47c52ea8947602d93ee3122711b39861711e621f522b3511502a9
f4319955980f712e994a5be651d90d9a065d6677999f38952b337f18d4e63d9d
2e3af22bc5e9698d8480cddc4f7616f33473ffcd0590c5093d09990c2f54c504

KPMG

KPMG Cyber Threat Intelligence Platform

Shikitega - Stealthy Sophisticated Malware

Indicators of Compromise: Hashes
7b12fbb705207471b5aed77531b21c5c8b448314650f6f6bbb83001164c3c993
db550ff9f9855132d84cfe8b3fd4b3799c30f61ef0e451d61f285e55a25e8f29
285bad58550c1465e53c5c05ba3de542934e3385910fb099273638b1b06cab60
b57f720cf39f7597c49e539e8e64d25ab43336cecdc32c09e4c48cadcfd1e0db
8fe7f489f0329abdd20401bf61feeb801044d0a589c31bdc8a8d198833a63b0b
cded658a65911737c54b6aa0b96cf34600cf55d7c9553c667780813e65cd0bf1
acb2488101bf160da1c1bcf7de82d9f955e913ab37c4254dbeececdf69c20856
0277e6d43c2ad919081aba176e99921b1621387db0695c06797fd9710b9e7dda
592cb7c1995d0fc5dbc4cbbad831ae3b705271e5c3be9d91cc8880a72b291c06
9e59f7acb753d43682656c8c6aadd0b361dea3d687658b1b2859b674011fd1b4
accfda452a9514c0b4c1aa2d9d06dff1b9033d4186272c87f5cb1a2af1479092
a740e447ea8389cb1defae24971c08963e348e5db822b27dcb41ef6781c206ea
e89450147e2fdabbcfadfe1d8bd77514259f61b535790c9b2576db21b9d186cf
a4ad70467739628c3c5bfa07ce0715c641aad24260d91beaafbae460d5495d35
6fb75f94b55512e7462a384c6a7d683b91410567352bffc66a2708dc9b9c58b8
b0530aa5f2811fed2b88a34b97dadf07e3cf60ccc3b809b2ab876f9f560e5497
73f25c2694d57eb45611a9d3912b999a93b4fca6f4b7e79491050d8aa1859a18
573a19864de03558d0319f2c47db412e7377156e1c8723934faf3456441174a8
20e5f62649fd92909c8cd66838ad11918fdba9326910290af66b028a9214d7c0
948b23f78a793bd043dd485d9d78cfb16a97210c4745a436d00b3cd5871d65fb
d72549eeebcda3fcee673e3915ab1c0352a30a8dd8cce0e0ee7065eb4f7239d8
2f7aa2a78a0b633e645649ad0cd0c3e083863aa380e2bfa784aeeb03880dea4d
6b2f5f2aca2900fe890e73d5cc56cd3f6925cfaa74f326643ed19b5023a1057a
8439e7d14f3e03943fa9a828fc2f60532fce0c3a5c75d81c4c288a4f477b82fd
109dbb5efc00d093d88d403b9cc97a24a7e9faef6366587cfa3b46e5ed00d8be
bb6ad49c7d59a09d4c8cbe543578eb6330616b104cbc894de8281e6b12a25ce8
669296c495f6bd0bcd7a3e84a0bfc15ca4a57e0d83f97a191c31da3381be1709
72d739451d13597ca0500cbf7c216c2dc6aed19cbd2319edb66058af1afa5609
7a0631a44ba2c7c29922d57c45966d4b55eb6a4538e7891f82015054a4d58488
54038c2a1917821b5bb3bcb9cb14218dd238f138410f9c3536ae261da3022291
75bade44dda9e5a460a57346eef1a01d3e3c1482f529ee5d62b6d0609d969321
1821f453d80efdf374c66597ff33a388fff71b0a47c1cee798dc2626f43eadab
61ec836ef41c22390b79371717eae49531a44def39f764d1fab6136165eebe36
02b4a8199206e6af7dbdf003fe7e35347e12942ad6d1d446fd9285d2c0b76046