KPMG Cyber Threat Intelligence Platform

Chalubo Malware – Exploiting Routers Across the Globe

Chalubo (ChaCha-Lua-bot), which emerged in 2018, is a commodity remote access trojan (RAT) drawing code from Xor.DDoS and Mirai bot. Initially designed for DDoS assaults, it has expanded its scope to sabotage routers through malicious firmware updates. Recent versions showcase enhanced evasion tactics like ChaCha stream cipher encryption. Primarily targeting SOHO/IoT devices, especially routers, Chalubo's impact extends across global telecommunications infrastructure. Notable affected regions include the United States, Brazil, and China.

Conducts reconnaissance by gathering information about potential target IP addresses through the ISPs ASN, then gains initial access through SSH brute-forcing vulnerable devices, thereby injecting the malware into the system. Following successful access, a malicious script is executed which fetches and executes a second malicious script initiating the infection process. The second script connects to a payload server to download and execute the primary loader, directly into memory. The primary loader retrieves and executes the main payload "Chalubo", directly into memory to elude detection. C2 communication is securely encrypted using ChaCha20 encryption. Post-execution, the malware diligently erases its files from the system and disguises its process to avoid detection, ensuring prolonged access to the compromised device. The attacker controls the infected devices through Lua scripts, facilitating actions such as data exfiltration, module downloads, and the introduction of new payloads. The malware incorporates evasion tactics such as a 30-minute delay upon execution, to thwart sandbox detection and evade automated analysis.

Chalubo's targeted approach and specific ASN focus distinguish it from broad attacks on multiple router models and networks, necessitating a strategic and precise countermeasure.

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

Chalubo Malware – Exploiting Routers Across the Globe

Indicators of Compromise: IP Addresses	
45.10.90[.]89	107.148.88[.]123
38.54.27[.]204	45.116.160[.]100
2.59.222[.]102	104.233.167[.]62
2.59.223[.]226	141.193.159[.]10
2.59.223[.]253	104.233.210[.]118
38.54.27[.]204	104.233.210[.]119
103.84.84[.]250	103.117.145[.]106
103.244.2[.]218	216.118.241[.]204
103.244.2[.]170	

Indicators of Compromise: Domains	
cu6s[.]com	m.aiguoba[.]com
m.isanyin[.]com	

Indicators of Compromise: Hashes
1e6e664d0669f1d625fcba5b12f43c6c
28827aba3675e1a802bb7d8113701615
b7765c4b6c9d3501722dfaef806317b6
2bc04862bb2b0815fa7d114bcfb9cd96
5e585c116fce92f2ec46c691e8094413
f07748badfc0150911bb43be6725c56b
73784e0fcd98104f9f4425ff54007791
c550c13575fa3aee3364fb3ba433824a
ff4bb9013f3e93d1d72e42997bca92af
c4dbd53e08afead45b175e211dc65d1f
e8ab3d465bcc12364b4a7944377af73a
081984e73a4809f61cb736b6ab387cd2
bcbb1b2590ae28a110963b3bcfd3c189
ac0a8a2ef031117d295c958b7cba7ace
a7d937a946b83573f4c439cdb117597d
154fcf08e5040f6c79cbeed8f7a781b2
5e15f06e5ef13f2da034b8a510065eae

KPMG

KPMG Cyber Threat Intelligence Platform

Chalubo Malware – Exploiting Routers Across the Globe

Indicators of Compromise: Hashes
443c043c9d45cf854637afe29bb618d5
7707838b50dfb08bbbbffa1e6b51fc75
76a35bbb40c30ea564b8fd013545bbcc
e7a8a9a54f97213dc3476fa647998ee7
ef2194957349faac259b1cff2de38a87
27dc61dd0bb9a53799ae29c6927f38d98ccdb27b
0ab35c25ece1d53456828da394a846602f028bf0
6abff93ddb4fb96a134e028839279b7147f701d7
aeeac998e1626dae4ae3ece55414f0cc7a7c7d66
851da211a48eda4fb1bb9914bc6afe2adae82da0
6b84a17e061a07585c9f4dd799c0be96911a85d1
183fa84e35bb498efb4dfb05d2a4997cd66e2f0f
b5d1cbd4e4e4f57c06e66131daedc2c9f18ca4ba
7376220218fb31881c1445bd7972285ace8b8bbe
2c8665a143cd12b90510120d7db10cabed3cce1d
da6f203d42d6641c12c6f1b10ab5da1bee3077d7
a40dc05d181ae2824decb3b911ba232d6d62f2fd
2d90cbd7acd159a42636e77a93f34324b2ca35b2
5ef3777f3bbca8743dd035e61527630b3f9511a6
c7a01b871438472ff0291700dc5d78f3c505a197
b003841b89d2b37633ba2b0ff9f260096c0aac8d
0fc4991ac19d3f3181670c1a2404462aa5f62e42
69a24bbbd1ff96afb3079a255d5e683107d3c314
965df8823c2aa6ae75ca406eb4646fb5ac081804
65856181fa5787c6d73e2474326c388e94c3b633
17f4c04dc19ae0c98f55fb642340efc29e540eaa
8a53fbe90923fb7c2c0440a49a9c514e467e6555
6a536b3d58f16bbf4333da7af492289a30709e77
a0feff9dc365941cddcc6eec3c1ff0d0da3349d2
145deb4c042aa508d4250badccd974c2715007ca
57d5cc52038b5fccc452a36b934458611fb94a68
4ca3b06c76f369565689e1d6bd2ffb3cc952925d
887f3eb6970176580a4e3f8d0cf39ae45c8cd1f2
0d218c2e0f4a7ae9b5e1997fc8ed47297f0e9558

KPMG

KPMG Cyber Threat Intelligence Platform

Chalubo Malware – Exploiting Routers Across the Globe

Indicators of Compromise: Hashes
72651454d59c2d9e0afdd927ab6eb5aea18879ce
1ad309b7ad6a22cd5925c5dbd9f6975dd077ac09
1d6bacf15cd6f02b8725d4ee3f1ceb71e4e07525
00550d5c2ed14a445ae13cff8eff32ba7a7dd502d145481bcd18161cf1df540d
ce68c3687aae08b796e3e57d97d4f333991b6eba804581ae66f46dbd6ec7dae7
b9d31125782ca0f20162b9f86b034a34cdc6b3fe318ee990721dc7d7dae66d22
0c7c6926e854aac4dc4821be07f826157b576d0a217d74d5675d7b32eb78b50e
f9db9632ffd7e3bd5b700025fa9278420de0778029fe2eedb6ea7b3d7b999ef6
d9322af52b941e76bec3d2596a1c1be47dffc4fb161656da2c7c45b3d492cfd8
b5fc0c265eb192b2a2d778e66d6f076e876eeacf57c3927e406b4e1b72152038
b2e2193e49ee1240be30f5040dbb5e2c973cdfb02c3ea88ef4ffeda884de28c2
59437e986acd685ad3ce48bf010efff22aa866c0fa066b0e64e510ecb026dd1a
117bd27a209d6350b10f5c8f8cf841755c253276460be8c7681f5357e07d2e0c
619564061e62a6352f0ce1a06d2883d46eb69df16322b30e8a2a9c65e2d32f5f
bdef8e089ffa00794f40f14ad3cdb8f1629241a4ac313bef8fe3d38e08207e4c
2a65fdd8c44a6b7191c09702d9f747471564346c465a42b9abbb4dfa1bc5f7fb
6be5b4bc461f1ba931bfe773df66bf5f8052626adbdf2b1156a06d0da2d8d3d1
9b929bcc182c39540767a9b8237a8436c82997c68d4d2ba710241387c39c27f5
e5030083c101058f52394820420a372bf93bcac2d802902d4d4c91470c96b608
ed9511c16229f4bb41f461e90fff7964e79f2c2d27e7de2b107e4d003e9e0def
5fc8534d490312823a49e2a13afc8a7b6b026280c79db704465fddd8a1fdc376
5621cdb8d07900a333d022a9696c1a6f7e45d6cfc713558c462a3ace7c4b426f
5b7874b18e8365e07624946a33518988aea4c72478a285a36047b4ba554a7576
8f4b61975539dbfe903f448636a48168351018801f2581a63d97179c37cad979
7a81bbb1f7055cd3f30db8bb2a104b969914ccd520cf85c24b25ba5b0c720206
967289406b0da030a93cefaa2644b109260565f5f767b95ce2a5d96d49c57bf2
f5894f0cc7d9da2f188b740bb0596206038d9dba430c7d2a145d7454d9f1b4db
f35be9f432322555f682c13465b3428bc364b96fc02e4e7ac98fa49f20a1f1e8
f6503a9717614a9f4bf5db88bb912bc43462ede1a9627f4ba5c544f644f4ad31
fba737436bdbf1461b3092b79fea0770302aeaed79389eb60b5c45c3bfc9f693
fddeddae2bf1d0759d914bced1bd678a2191152c580f6ce86f87b0674b80bf8b
8fbd768368019df9a3bd05cfc83b3f00933440a8dadc88fe6d2af8a683b089b5
799400b6419b91fe8810456d9b32d124dfaad2c5626a07405f5a099679de29b5
ed44898c666b154111bcbe8d4940aebdaed09d735445f3cc85f2d6e29a850f23