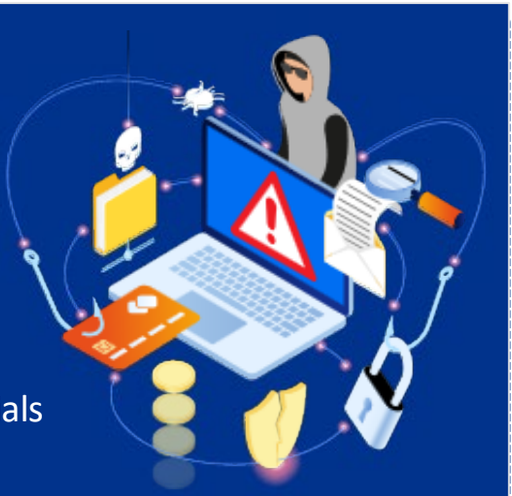
KPMG Cyber Threat Intelligence Platform

Cuttlefish Malware – Exploiting Routers and Sniffing Cloud Credentials



Cuttlefish, a sophisticated packet-sniffing malware, targets small office/home office (SOHO) routers. Active since at least July 27, 2023, with a possible earlier start, it employs a stealthy zero-click method to stealthily capture data from users and devices. Cuttlefish primarily focus their attacks on Turkey, with a limited number of victims extending to satellite phone providers and data center services in the USA.

While the initial access vector infecting routers remains unclear, it likely involves exploiting vulnerabilities or brute-forcing credentials. After gaining access to a router, a bash script collects host data (directory listings, running processes, active connections, mounts) and uploads it to an actor-controlled domain. The script downloads and executes the Cuttlefish payload (".timezone"), loading it into the tmp directory and deleting the uploaded file. Upon execution, a packet filter detects specific data and performs actions based on rulesets from the attacker's C2 server. HTTP and DNS hijackingis used for private IP connections, remaining dormant until activated by predefined rules. Its packet sniffer captures authentication data, focusing on public cloud-based services. The payload establishes a secure RSA-encrypted connection to the C2 for rule updates, configuring parameters, managing heartbeats, and monitoring network traffic. After intercepting traffic, the threat actor creates a VPN or proxy tunnel to the compromised router to weaponize stolen tokens and access cloud data, gaining a foothold in the cloud ecosystem. Once a log file of filtered traffic reaches a specified size, Cuttlefish exfiltrates it to the C2 server using a peer-to-peer VPN (n2n) or proxy tunnel (socks_proxy).

Cuttlefish's targeting of cloud-based authentication material ensures long-term persistent access to compromised systems, highlighting the urgent need for effective mitigation strategies.

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

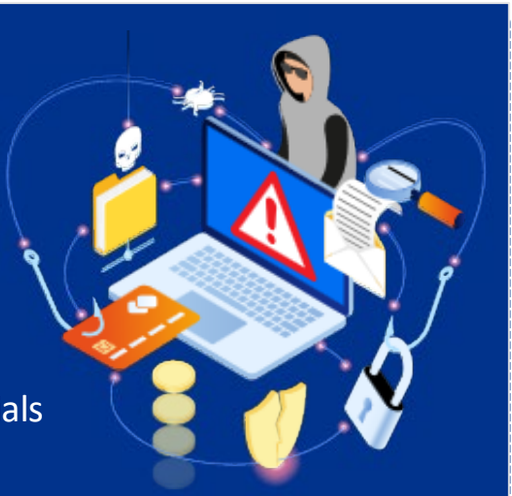
home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cuttlefish Malware – Exploiting Routers and Sniffing Cloud Credentials



Indicators of Compromise: IP Addresses	
198.98.56[.]93	107.189.28[.]251
209.141.49[.]178	205.185.122[.]121

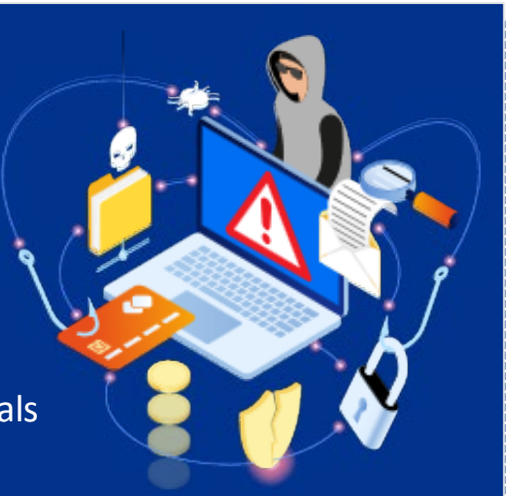
Indicators of Compromise: **Domains**
kkthreas[.]com

Indicators of Compromise: Hashes
2abe840c10755c2571bddf2abea537f2
b2ca9e24000c6b5846ffecd70083a850
c123c4426418dd329d6f306582ac9dd5
9b7a35a728924ca782e77a68d281c777
edfebb4e48c4681c89b3ac6b370cf88b
3cc56b4d78fcec8df6c53ce20d407156
d9d0b7c110bc09843f18ed37f7cd0d3d
4e5c0ba24772747c2fd43b98f06d082b
1a44c96440ea260a958062493386fb21
d5826bf1a5d87799ced9a0519260327b
9b9346d728da0b0a9a14d083192bdc6c
52fbd93433973d6b033f2d7aa9d0c085
114419df7296c38dda5b7c52fab3e16e89c472ba
8c92790a1a630d8e27a33bcfbb634b2f56f5dcd1
eb6b765180c8b46fddc1a43d2c9a82591b6d2ea9
b6195aec010f77a8b53a74a3caa161fdc06dcf32
2773ee18bc041f6d8e95af46bc5212529853a347
5476ea7f5d0d2326d4b5f58aba3f6943fd98b81a
1b36cb75602c0de8afdf5cdd8f67b7f96f317abc
f093856fef5a0ce37c9ca403ffdd3fcd2c9ea6cc
200230cd020bbd5ec20d65fc306093f377ce1fec
8528d36654f30ce280aedb3b3f0e70287a050ab3
545403c9a119dbe7639695a1b0e662cd7e40c0cc
0f0d0326110288f38d134befdb56540ed112ca0e
73cf20675639c18c04381b5efd7d628736d149734280988f55358e301c1d9bb8

KPMG

KPMG Cyber Threat Intelligence Platform

Cuttlefish Malware – Exploiting Routers and Sniffing Cloud Credentials



Indicators of Compromise: Hashes
10a4edbbb852a1b01fc6fbf0aa1407bc8589432bddb2001ae62702f18d919e89
94812d391160e4fce821701b944cfd8f5fd9454b3cbb8e8974d1dc259310e500
4aa23fbdc27d317c6e54481b6d884b962adf6e691a4731c859ddaf9af09822c6
1168e97ccf61600536e93e9c371ee7671bae4198d4bf566550328b241ec52e89
70693211cd0b14a7463b39b2fa801ce1fdefc85c7f3e003772d1b4deeb78efde
2f0911fb892d448910c36a37c9fbdec8c73ccfecc274854b1fa053fb1cc2369b
07df37d8168e911b189bbe0912b4842fa1fe48d5264e99738ad3247f9c818478
44b769be0c2a807082a9bfd2f33fdc744552c5c7ca88a812ef4bd0393a50f132
6295d5cb21c441066d2da81a76440bcac9bd5a7830fc9faea9668bd0b2015046
eb7a7ab952080f66c82fe8350da131ce0d7766f203bd4d97b0798b4f59283a27
99d5cf32f8198e99c530be4f5e05487e280bacdb8ef26aaf38dc20e301aad75f
3d9ee05c0841ad65547c0cc8516d092cff48dad5e7bbf97c99ddd44ee94a24bc
2ed174523bd80a93b7d09940d375f9c0d71e1ce8ecffb2320e02a78f4b601408
23c2e7ff2602e5f76b3f2c354761ef39966facb3b12ed05551816f482d4d5608
e48c250c47dd071dcee984a8e9f27b170004ff81c3f0da6a50364fdecf800fd3