Mphasis
The Next Applied

# New Cuttlefish Malware Hijacks Router Connections, Sniffs for Cloud Credentials

Date: 02nd May 2024 | Severity: High

## Summary

- A new malware called Cuttlefish is targeting small office and home office (SOHO) routers with the goal of stealthily monitoring all traffic through the devices and gather authentication data from HTTP GET and POST requests.
- “This malware is modular, designed primarily to steal authentication material found in web requests that transit the router from the adjacent local area network (LAN),” the Black Lotus Labs team at Lumen Technologies said in a report published today.
- Cuttlefish has been active since at least July 27, 2023, with the latest campaign running from October 2023 through April 2024 and predominantly infecting 600 unique IP addresses associated with two Turkish telecom providers.

## Attack Vectors

- It subsequently downloads and executes the Cuttlefish payload from a dedicated server depending on the router architecture (e.g., Arm, i386, i386_i686, i386_x64, mips32, and mips64).It is important to note that the main purpose of the passive network packet sniffing is to identify authentication data related to public cloud services like BitBucket, Amazon Web Services (AWS), Digital Ocean, CloudFlare, and Alicloud by generating an extended Berkeley Packet Filter (eBPF).
- The malware can either hijack communication going to a private IP address or, if specific conditions are fulfilled, start a sniffer function for traffic going to a public IP address with the intention of stealing credentials. This functionality is controlled by a ruleset. The hijack rules, for their part, are retrieved and updated from a command-and-control (C2) server set up for this purpose after establishing a secure connection to it using an embedded RSA certificate.
- The malware is also equipped to act as a proxy and a VPN to transmit the captured data through the infiltrated router, thereby allowing the threat actors to use the stolen credentials to access targeted resources. It has the ability to perform route manipulation, hijack connections, and employ passive sniffing capability. With the stolen key material, the actor not only retrieves cloud resources associated with the targeted entity but also gains a foothold in that cloud ecosystem.

# Indicator of compromise

| INDICATOR TYPE | INDICATORS |
|---|---|
| Hashes | • 10a4edbbb852a1b01fc6fbf0aa1407bc8589432bddb2001ae62702f18d919e89<br>• 94812d391160e4fce821701b944cfd8f5fd9454b3cbb8e8974d1dc259310e500<br>• 4aa23fbdc27d317c6e54481b6d884b962adf6e691a4731c859ddaf9af09822c6<br>• 1168e97ccf61600536e93e9c371ee7671bae4198d4bf566550328b241ec52e89<br>• 44b769be0c2a807082a9bfd2f33fdc744552c5c7ca88a812ef4bd0393a50f132<br>• 6295d5cb21c441066d2da81a76440bcac9bd5a7830fc9faea9668bd0b2015046<br>• eb7a7ab952080f66c82fe8350da131ce0d7766f203bd4d97b0798b4f59283a27<br>• 99d5cf32f8198e99c530be4f5e05487e280bacdb8ef26aaf38dc20e301aad75f<br>• 3d9ee05c0841ad65547c0cc8516d092cff48dad5e7bbf97c99ddd44ee94a24bc<br>• 2ed174523bd80a93b7d09940d375f9c0d71e1ce8ecffb2320e02a78f4b601408<br>• 23c2e7ff2602e5f76b3f2c354761ef39966facb3b12ed05551816f482d4d5608 |
| C&C servers with URLs | • hxxp://209.141.49[.]178/s<br>• hxxp://209.141.49[.]178/dajfdsfadsfa/arm<br>• hxxp://209.141.49[.]178/dajfdsfadsfa/i386<br>• hxxp://209.141.49[.]178/dajfdsfadsfa/i386_i686<br>• hxxp://209.141.49[.]178/dajfdsfadsfa/i386_x64<br>• hxxp://209.141.49[.]178/dajfdsfadsfa/misp32<br>• hxxp://209.141.49[.]178/dajfdsfadsfa/misp64<br>• hxxp://209.141.49[.]178/r/s.sh<br>• hxxp://209.141.49[.]178/r/arm_sniff<br>• hxxp://209.141.49[.]178/r/i386_i686_sniff<br>• hxxp://209.141.49[.]178/r/i386_sniff<br>• hxxp://209.141.49[.]178/r/i386_x64_sniff<br>• hxxp://209.141.49[.]178/r/mips32_sniff<br>• hxxp://209.141.49[.]178/r/mips64_sniff<br>• hxxps://198.98.56[.]93:443/rules<br>• hxxps://198.98.56[.]93:443/rulesinit<br>• hxxps://198.98.56[.]93:443/upload |

# Recommendation

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Eliminate weak credentials, monitoring for unusual logins, securing traffic with TLS/SSL.
- Inspect devices for abnormal files.
- It is recommended to reboot the devices regularly,
- Apply the latest available firmware updates,
- Change default passwords,
- Block remote access to the management interface and replace them when they reach end-of-life (EoL).

**NOTE:** The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

# Reference Links

- New Cuttlefish Malware Hijacks Router Connections, Sniffs for Cloud Credentials (thehackernews.com)
- Cuttlefish Malware Targets Routers, Harvests Cloud Authentication Data - SecurityWeek
- https://github.com/blacklotuslabs/IOCs/blob/main/Cuttlefish_IOCs.txt#L28