Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

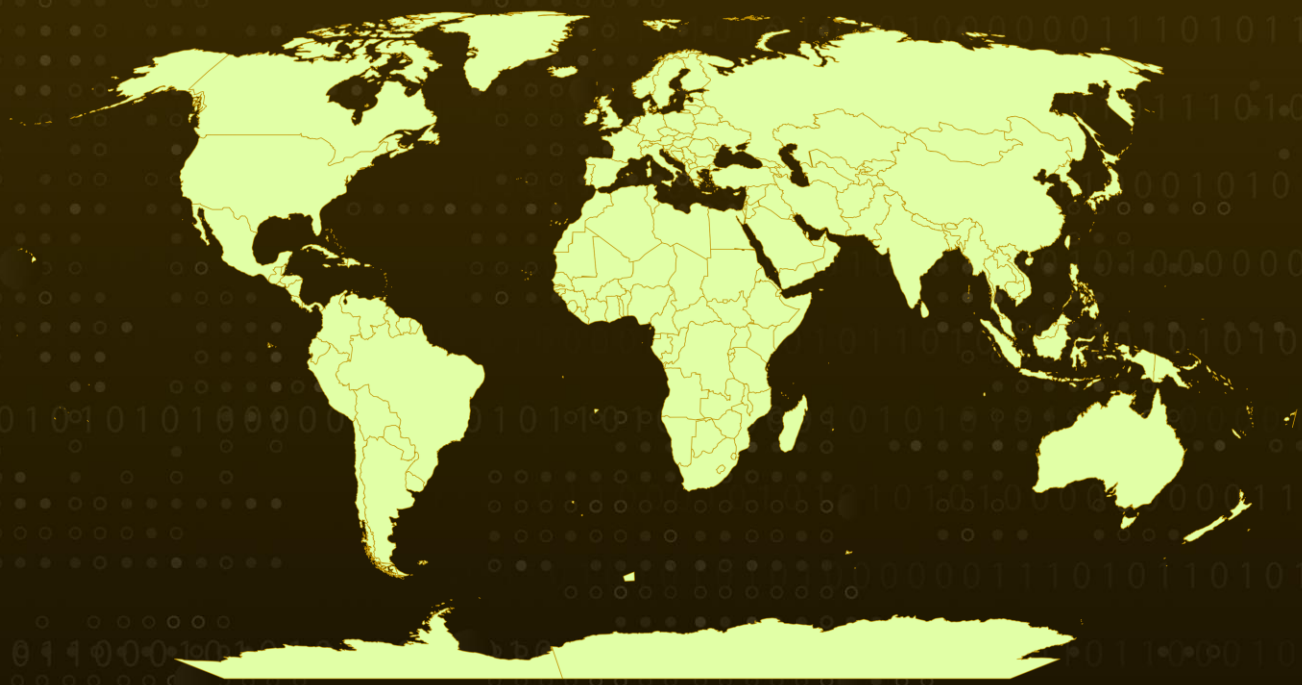
Cuttlefish Malware Silent Stalkers of Router Traffic

Date of Publication	Admiralty Code	TA Number
May 7, 2024	A1	TA2024175

Summary

Active Since: July 27, 2023
Malware: Cuttlefish
Attack Region: Worldwide
Attack: A newly identified malware, named 'Cuttlefish', has been detected infiltrating enterprise-level and small office/home office (SOHO) routers, secretly monitoring data transmissions and stealing authentication credentials. Cuttlefish has been active since at least July 2023, with its latest campaign running from October 2023 to April 2024.

Attack Regions



Attack Details

#1 A newly discovered malware named 'Cuttlefish' has been found infiltrating both enterprise-grade and small office/home office (SOHO) routers, aiming to secretly monitor data transmissions and steal authentication credentials. Cuttlefish has been active since at least July 27, 2023, with its most recent campaign spanning from October 2023 to April 2024.

#2 Using a zero-click approach, this malware seamlessly intercepts data passing through the compromised network's periphery, thereby exposing any transmitted information. What sets Cuttlefish apart is its proficiency in executing HTTP and DNS hijacking, specifically targeting connections to private IP addresses.

#3 The exact method of initial router infection remains unclear, although it likely exploits known vulnerabilities or employs brute-force credential attacks. While Cuttlefish shares certain code similarities with HiatusRat, which has previously been associated with campaigns linked to Chinese state interests, no definitive connections between the two have been established.

#4 Once it gains a foothold, Cuttlefish deploys a bash script to extract host data, including contents from /etc, active processes, network connections, and mounted devices, subsequently sending this information to a domain controlled by threat actors.

#5 A notable aspect of Cuttlefish is its passive packet sniffing capability, specifically designed to intercept authentication data related to public cloud services such as Alicloud, Amazon Web Services (AWS), Digital Ocean, CloudFlare, and BitBucket, achieved through the creation of an extended Berkeley Packet Filter (eBPF).

#6 Data that meets specified criteria is logged locally and, upon reaching a predetermined threshold (1048576 bytes), is exfiltrated to the command and control (C2) server via a peer-to-peer VPN (n2n) or a proxy tunnel (socks_proxy) established on the compromised device. Cuttlefish epitomizes the latest iteration of passive eavesdropping malware targeting edge networking infrastructure.

Recommendations

Enhancing Router Security: Apply the latest firmware updates provided by the manufacturer to patch known vulnerabilities and strengthen device security. Additionally, changing default passwords to unique, strong alternatives helps effectively prevent unauthorized access.

Implement Certificate Pinning: Employ certificate pinning techniques, particularly when remotely connecting to high-value assets like cloud resources, to thwart potential hijacking attempts by threat actors.

Continuous Monitoring and Analysis: Implement continuous monitoring and analysis of network traffic and system logs. This proactive approach can help identify anomalies and potential threats before they escalate.

End-of-Life Replacement: Plan to replace SOHO routers once they reach end-of-life (EoL) and are no longer supported by the manufacturer to ensure continued security against evolving threats.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	T1543 Create or Modify System Process	T1055 Process Injection
T1552 Unsecured Credentials	T1098 Account Manipulation	T1040 Network Sniffing	T1056 Input Capture
T1212 Exploitation for Credential Access	T1090 Proxy	T1110 Brute Force	T1087 Account Discovery
T1010 Application Window Discovery	T1135 Network Share Discovery	T1018 Remote System Discovery	T1016 System Network Configuration Discovery
T1560 Archive Collected Data	T1041 Exfiltration Over C2 Channel	T1030 Data Transfer Size Limits	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	07df37d8168e911b189bbe0912b4842fa1fe48d5264e99738ad3247f9c818478, 10a4edbbb852a1b01fc6fbf0aa1407bc8589432bddb2001ae62702f18d919e89, 1168e97ccf61600536e93e9c371ee7671bae4198d4bf566550328b241ec52e89, 23c2e7ff2602e5f76b3f2c354761ef39966facb3b12ed05551816f482d4d5608, 2ed174523bd80a93b7d09940d375f9c0d71e1ce8ecffb2320e02a78f4b601408, 2f0911fb892d448910c36a37c9fbdec8c73ccfecc274854b1fa053fb1cc2369b, 3d9ee05c0841ad65547c0cc8516d092cff48dad5e7bbf97c99ddd44ee94a24bc, 44b769be0c2a807082a9bfd2f33fdc744552c5c7ca88a812ef4bd0393a50f132, 4aa23fbdc27d317c6e54481b6d884b962adf6e691a4731c859ddaf9af09822c6, 6295d5cb21c441066d2da81a76440bcac9bd5a7830fc9faea9668bd0b2015046, 70693211cd0b14a7463b39b2fa801ce1fdefc85c7f3e003772d1b4deeb78efde, 73cf20675639c18c04381b5efd7d628736d149734280988f55358e301c1d9bb8, 94812d391160e4fce821701b944cfd8f5fd9454b3cbb8e8974d1dc259310e500, 99d5cf32f8198e99c530be4f5e05487e280bacdb8ef26aaf38dc20e301aad75f, Eb7a7ab952080f66c82fe8350da131ce0d7766f203bd4d97b0798b4f59283a27
URLs	hxxp://209[.]141[.]49[.]178/dajfdsfadsfa/arm, hxxp://209[.]141[.]49[.]178/dajfdsfadsfa/i386, hxxp://209[.]141[.]49[.]178/dajfdsfadsfa/i386_i686, hxxp://209[.]141[.]49[.]178/dajfdsfadsfa/i386_x64, hxxp://209[.]141[.]49[.]178/dajfdsfadsfa/misp32, hxxp://209[.]141[.]49[.]178/dajfdsfadsfa/misp64, hxxp://209[.]141[.]49[.]178/r/arm_sniff, hxxp://209[.]141[.]49[.]178/r/i386_i686_sniff, hxxp://209[.]141[.]49[.]178/r/i386_sniff, hxxp://209[.]141[.]49[.]178/r/i386_x64_sniff, hxxp://209[.]141[.]49[.]178/r/mips32_sniff, hxxp://209[.]141[.]49[.]178/r/mips64_sniff,

TYPE	VALUE
URLs	hxxp://209[.]141[.]49[.]178/r/s[.]sh, hxxp://209[.]141[.]49[.]178/s, hxxps://107[.]189[.]28[.]251:443/rules, hxxps://198[.]98[.]56[.]93:443/rules, hxxps://198[.]98[.]56[.]93:443/rulesinit, hxxps://198[.]98[.]56[.]93:443/upload, hxxps://205[.]185[.]122[.]121/rules, hxxps://205[.]185[.]122[.]121/rulesinit, hxxps://205[.]185[.]122[.]121/upload, hxxps://kkthreas[.]com, hxxps://kkthreas[.]com/upload, hxxps://pp[.]kkthreas[.]com

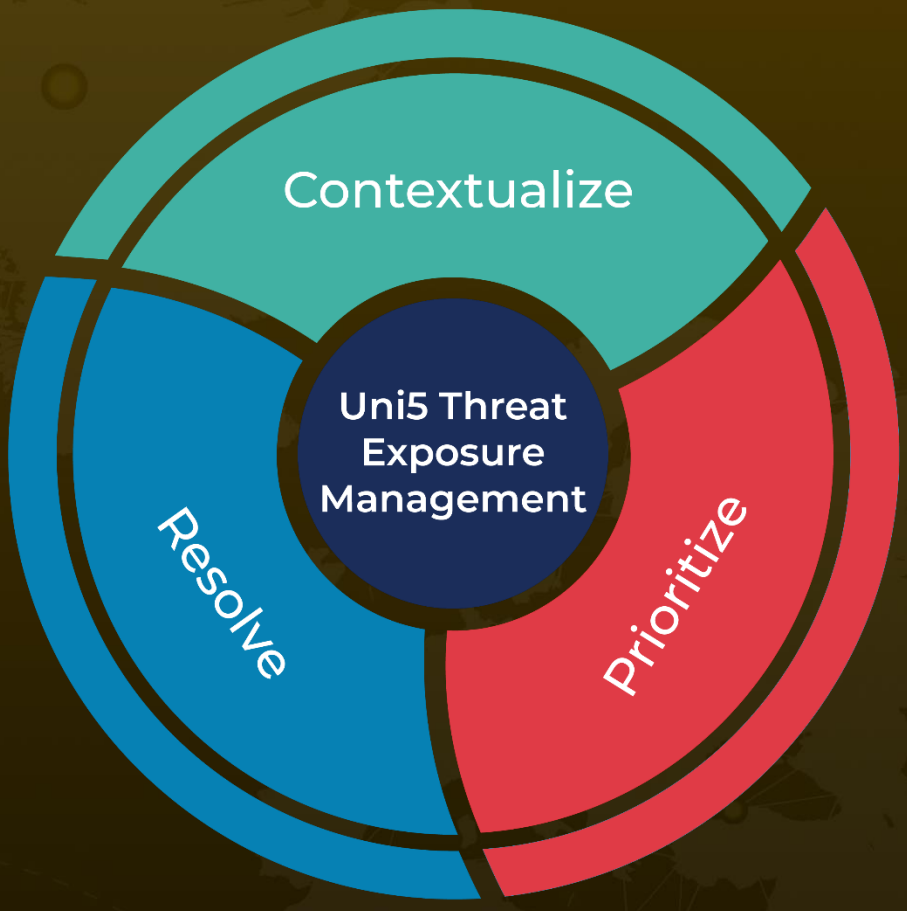
References

https://blog.lumen.com/eight-arms-to-hold-you-the-cuttlefish-malware/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 7, 2024 • 10:00 PM

More at www.hivepro.com