SECURITY ADVISORY

CYBER STASH

May, 2024

Cuttlefish Packet-Sniffing Malware

Context

A new strain of malware, known as Cuttlefish, has surfaced, targeting small office and home office (SOHO) routers. This sophisticated threat is designed to clandestinely monitor all traffic passing through these routers, specifically honing in on HTTP GET and POST requests to extract authentication data. What sets Cuttlefish apart is its modular nature, tailored to intercept web requests and pilfer authentication credentials.

By masquerading as a DNS and HTTP proxy, Cuttlefish can execute man-in-the-middle attacks, redirecting pilfered credentials to designated command-and-control (C2) infrastructure controlled by malicious actors. This poses a significant risk, especially as more organizations adopt hybrid work models, with employees working remotely for a portion of the week.

While initial infections have been concentrated in Turkey, primarily through two telecommunications providers and potentially linked to Chinese-backed advanced persistent threat (APT) groups, CyberStash foresees a proliferation of copycat attacks in the near future. As such, it's imperative for organizations to proactively address this threat by treating home offices as an extension of their network and implementing robust risk mitigation measures.

Mitigation

Defending against the Cuttlefish and similar malware necessitates more than just patching vulnerabilities. It involves actively limiting the attack surface of SOHO routers by:

Admin Interface Access Control: Implement proactive network traffic blocking measures, including the restriction of suspicious IPs, domains, and connections from high-risk Autonomous System Numbers, Top-Level Domains, and countries. Preferably block all traffic to the admin interface.

SOHO Router Security: Apply best-practice security controls to the SOHO router: Disable unnecessary services, keep firmware updated, restrict admin access, and enforce strong passwords.

Audit Suspected Compromised Routers: check for listening port 61235 and examine the router's file system for files named co.tmp.tar.gz, /tmp/log.txt, and directory /tmp/.Pg88s51gQG4tFyImFsT9qy6ZM5TeTF8.so.

Technical Details

The method for the initial infection of routers remains undetermined, although it likely involves exploiting known vulnerabilities or employing brute-force techniques to breach router credentials. This initial access represents a critical stage in the deployment of the Cuttlefish malware.

Upon gaining access to a compromised router, a bash script named "s.sh" is deployed to initiate the reconnaissance phase. This script is responsible for gathering host-based data essential for further exploitation. It systematically collects information such as directory listings, running processes, and active network connections, providing the attackers with valuable insights into the compromised system's configuration and operation.

Following reconnaissance, the primary Cuttlefish payload, denoted by the filename ".timezone," is downloaded and executed by the bash script. Notably, this payload is designed to evade detection by loading directly into memory, thereby circumventing traditional file-based antivirus detection mechanisms. Furthermore, to cover their tracks and maintain stealth, the downloaded payload is promptly wiped from the file system after execution.

Cuttlefish malware is available in multiple builds tailored to support various router architectures, including ARM, i386, i386_i686, i386_x64, mips32, and mips64. Upon execution, Cuttlefish employs a packet filter to monitor all connections passing through the device. When specific data is detected, it triggers actions based on regularly updated rulesets fetched from the attacker's command and control (C2) server. The malware passively scans packets for "credential markers," including usernames, passwords, and tokens, particularly targeting those associated with public cloud-based services such as Alicloud, AWS, Digital Ocean, CloudFlare, and BitBucket.

Tactics, Techniques and Procedures

The notable TTPs related to the Cuttlefish Malware are:

T1190 - Exploit Public-Facing Application: Adversaries exploit known vulnerabilities in routers to gain initial access. This may involve exploiting unpatched vulnerabilities or default credentials to compromise router devices.

T1064 - Scripting: Upon gaining access to a compromised router, Cuttlefish deploys a bash script ("s.sh") to execute commands and collect host-based data. This script may be responsible for tasks such as reconnaissance and payload execution.

T1070 – File Deletion: After executing the primary Cuttlefish payload, the malware promptly deletes the downloaded file from the file system to evade detection and cover its tracks. This tactic aims to minimize the malware's footprint and hinder forensic analysis.

Cyber Threat Intelligence

The Black Lotus Labs team at Lumen Technologies is tracking a malware platform they've named Cuttlefish. Cuttlefish has been active since at least July 27, 2023, with the latest campaign observed from October 2023 to April 2024. It predominantly targeted 600 unique IP addresses associated with two Turkish telecom providers.

Although there is evidence suggesting overlaps with another known activity cluster called HiatusRAT, no shared victimology has been observed to date.

References

Related IOC's & Yara Rules:

- https://github.com/blacklotuslabs/IOCs/blob/main/Cuttlefish_IOCs.txt
- https://otx.alienvault.com/pulse/6633687c8b2b019953cb8eff

Public Intelligence:

- https://blog.lumen.com/eight-arms-to-hold-you-the-cuttlefish-malware/
- https://www.bleepingcomputer.com/news/security/new-cuttlefish-malware-infects-routers-to-monitor-traffic-for-credentials/
- https://thehackernews.com/2024/05/new-cuttlefish-malware-hijacks-router.html
- https://therecord.media/cuttlefish-malware-routers-turkey
- https://www.darkreading.com/cloud-security/cuttlefish-zero-click-malware-steals-private-cloud-data