مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

New Cuttlefish Malware Targets Routers to Steal Credentials

Tracking #:432315822

Date:06-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new malware called Cuttlefish has emerged, targeting routers used by businesses (enterprise and SOHO) to steal login credentials for cloud services and potentially compromise internal traffic.

TECHNICAL DETAILS:

A new malware called Cuttlefish infects routers to steal login credentials for cloud services and internal resources. It can bypass traditional security measures and remain undetected for long periods.

Capabilities:

- Steals credentials (usernames, passwords, tokens) from cloud services like Alicloud, AWS, DigitalOcean, CloudFlare, and BitBucket.
- Monitors network traffic for specific data patterns.
- Creates a proxy or VPN tunnel for data exfiltration.
- Performs DNS and HTTP hijacking within private IP spaces.

Delivery: Infection vector unknown, but may involve exploiting vulnerabilities or brute-forcing credentials.

Targets:

- Router architectures including ARM, i386, i386_i686, i386_x64, mips32, and mips64.
- Cloud-based resources.

Active Since: July 2023 (at least).

Attribution: Unconfirmed, possible link to HiatusRat malware.

Impact

- Compromised cloud resources and data breaches.
- Lateral movement within the network.
- Bypassing security measures like network segmentation and endpoint monitoring.

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

- 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.
- Implement strong password policies: Enforce complex passwords with minimum length requirements and regular password changes
- Enable multi-factor authentication (MFA): MFA adds an extra layer of security by requiring a second verification factor beyond a username and password.
- Monitor for unusual logins, particularly from residential IPs.
- Secure traffic with TLS/SSL encryption.

- Regularly inspect devices for suspicious files or processes.
- Use certificate pinning for secure remote connections.
- Apply latest firmware updates from the router vendor.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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