مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

"RustoBot" Botnet Targeting TOTOLINK and DrayTek Devices

Tracking #:432317105

Date:22-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new botnet, named "RustoBot," has been discovered targeting vulnerabilities in TOTOLINK and DrayTek devices.

TECHNICAL DETAILS:

FortiGuard Labs has identified a new botnet dubbed “RustoBot”, targeting vulnerable TOTOLINK and DrayTek networking devices. This malware is distinct in its implementation—written in the Rust programming language—and is spreading via known command injection vulnerabilities. Once infected, devices become part of a botnet capable of launching high-volume DDoS attacks using multiple protocols.

Affected Platforms:

TOTOLINK Routers:

- N600R V4.3.0cu.7570_B20200620
- A830R V5.9c.4729_B20191112
- A3100R V4.1.2cu.5050_B20200504
- A950RG V4.1.2cu.5161_B20200903
- A800R V4.1.2cu.5137_B20200730
- A3000RU V5.9c.5185_B20201128
- A810R V4.1.2cu.5182_B20201026

DrayTek Routers:

- Vigor2960
- Vigor300B (Firmware version 1.5.1.4)

Vulnerabilities Exploited:

- **TOTOLINK cstecgi.cgi:**
  - CVE-2022-26186
  - CVE-2022-26187
  - CVE-2022-26188
  - CVE-2022-26189
  - CVE-2022-26210
- **DrayTek apmcfgupload:**
  - CVE-2024-12987

Malware Analysis of RustoBot

- **Language:** Written in Rust, allowing for cross-platform compatibility.
- **Distribution:** Distributed via multiple downloader scripts (wget and tftp).
- **Target Architectures:** Targets arm5, arm6, arm7, mips, mpsl, and x86 architectures.
- **Obfuscation:** Employs XOR encryption and numerous calculations to obfuscate its configuration and operation.
- **Communication:** Uses DNS-over-HTTPS (DoH) to resolve C2 server domains, blending malicious traffic with legitimate HTTPS requests.
- **DDoS Capabilities:** Launches DDoS attacks using Raw IP, TCP, and UDP protocols, triggered by commands from the C2 server.

Indicators of compromise:
Attached File

RECOMMENDATIONS:

1. **Apply Patches:** Ensure that all TOTOLINK and DrayTek devices are updated with the latest firmware patches to address the identified command injection vulnerabilities.
2. **Network Segmentation:** Implement network segmentation to isolate IoT devices from critical network resources, limiting the impact of potential compromises.
3. **Firewall Configuration:** Configure firewalls to block traffic to and from known malicious IP addresses and domains associated with the RustoBot botnet.

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://www.fortinet.com/blog/threat-research/new-rust-botnet-rustobot-is-routed-via-routers?lctg=232952123