مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

ShadowV2 IoT Malware Campaign

Tracking #:432318180

Date:26-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Researchers at FortiGuard Labs Threat Research have uncovered a Mirai-based botnet variant named 'ShadowV2' actively exploiting IoT vulnerabilities during a global disruption of AWS connections.

TECHNICAL DETAILS:

FortiGuard Labs identified widespread exploitation activity linked to a Mirai-based malware variant known as ShadowV2. The malware targeted vulnerable IoT and network devices across multiple vendors, industries, and geographic regions.

ShadowV2 leverages a collection of publicly known but still widely unpatched vulnerabilities to compromise devices and recruit them into a botnet. Once compromised, these devices can be remotely controlled by attackers and used for distributed denial-of-service (DDoS), lateral movement, scanning, or future coordinated attacks.

Although the observed activity window was limited and coincided with the AWS outage, analysis strongly suggests this campaign was a test deployment or rehearsal, likely intended to validate exploit chains and propagation efficiency ahead of future large-scale attacks.

Organizations with exposed IoT infrastructure should treat this advisory as urgent and take immediate mitigation steps.

Affected Platforms:

- **DDWRT:** CVE-2009-2765
- **D-Link:** CVE-2020-25506, CVE-2022-37055, CVE-2024-10914, CVE-2024-10915
- **DigiEver:** CVE-2023-52163
- **TBK:** CVE-2024-3721
- **TP-Link:** CVE-2024-53375

IOCs

Hosts
silverpath[.]shadowstresser[.]info 81[.]88[.]18[.]108 198[.]199[.]72[.]27
Files
Downloader 7dfbf8cea45380cf936ffdac18c15ad91996d61add606684b0c30625c471ce6a
ShadowV2 0408d57c5ded5c79bf1c5b15dfde95547e17b81214dfc84538edcdbef4e61ffe dfaf34b7879d1a6edd46d33e9b3ef07d51121026b8d883fdf8aced630eda2f83 6f1a5f394c57724a0f1ea517ae0f87f4724898154686e7bf64c6738f0c0fb7b6 5b5daeaa4a7e89f4a0422083968d44fdfe80e9a32f25a90bf023bca5b88d1e30 c0ac4e89e48e854b5ddbaef6b524e94cc86a76be0a7a8538bd3f8ea090d17fc2 499a9490102cc55e94f6a9c304eea86bbe968cff36b9ac4a8b7ff866b224739f bb326e55eb712b6856ee7741357292789d1800d3c5a6be4f80e0cb1320f4df74 24ad77ed7fa9079c21357639b04a526ccc4767d2beddbd03074f3b2ef5db1b69 80ee2bf90545c0d539a45aa4817d0342ff6e79833e788094793b95f2221a3834 cb42ae74216d81e87ae0fd51faf939b43655fe0be6740ac72414aeb4cf1fecf2 22aa3c64c700f44b46f4b70ef79879d449cc42da9d1fe7bad66b3259b8b30518

c62f8130ef0b47172bc5ec3634b9d5d18dbb93f5b7e82265052b30d7e573eef3

RECOMMENDATIONS:

- **Patch and Update Firmware**
  - Apply vendor security updates addressing the listed CVEs
  - Decommission unsupported or end-of-life IoT devices
- **Disable Default Credentials**
  - Remove factory-default usernames and passwords
  - Enforce strong, unique authentication on all devices
- **Restrict Network Exposure**
  - Remove IoT devices from direct internet access
  - Disable unused services (Telnet, UPnP, legacy admin panels)

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/shadowv2-casts-a-shadow-over-iot-devices