Mirai Botnet targets IoT Devices including routers

Dear Constituents,

A new variant of the Mirai IoT malware in the wild targeting two new classes of devices --smart signage TVs and wireless presentation systems. It includes devices such as routers, network storage devices, NVRs, and IP cameras and leverages various exploits in an attempt to compromise them. Security Researchers say this new Mirai botnet uses 27 exploits, 11 of which are new to Mirai altogether, to break into smart IoT (**Internet of Things**) devices and networking equipments.

This malicious payload was hosted at a compromised website in Colombia: an “Electronic security, integration and alarm monitoring” business.

In addition, this new variant of Mirai includes new exploits in its multi-exploit battery, as well as new credentials to use in brute force against devices.

List of Affected Devices targeted by Mirai Botnet

- LG Supersign TVs
- WePresent WiPG-1000 Wireless Presentation System
- Linksys E1500/E2500 Routers
- D-Link Routers
- Netgear Routers
- ZTE Routers

What to do

1. Set up password managers to store strong, complex passwords for all corporate devices, including IoT assets. Also changing default passwords on the IoT devices.
2. Ensure to fully patch vulnerable IoT devices and disclose any security events involving those products.

Reference

Paloalto Networks: https://unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.gov.to
web: www.cert.gov.to