UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00223

NEW BOTENAGO MALWARE TARGETS IOT DEVICES

DATE ISSUED: 17th November 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Written in Google's Golang programming language, the newly discovered BotenaGo malware targets Internet of Things (IoT) devices, commonly known as Smart devices, and network devices such as routers. Modems and Network Attached Storage (NAS) using 33 different exploit functions to infect victims.

BREAKDOWN

AT&T Labs have published research disclosing the vulnerabilities able to be targeted by this botnet and new strain of malware, that starts by creating a backdoor on to the device which lies in wait to receive attack instruction from a remote operator through port 31421 and 19412 or similar. It is unclear at this stage where BotenaGo has originated and at this stage the malware is able to go unrecognized by antivirus solutions – often being mistaken for a Mirai variant. The attack begins by initialising global infection counters and searching for the 'dlrs' folder to ascertain whether the device can be compromised. If the folder is missing, the attack is abandoned and if detected the function 'scannerInitExploits' is initiated to map all offensive functions with its relevant string representing the targeted system. If a device is found to be vulnerable to attack, BotenaGo proceeds with a "get" request to map attack functions to system signatures. By gaining access to vulnerable connected devices on a corporate network, attackers can use this as a launchpad for other attacks, such as further malware infection, Remote Code Execution (RCE), or Dedicated Denial of Service (DDoS) attacks or to move laterally across an internal network environment.

REMEDIATION STEPS

- Update IoT device and network device firmware and software to latest versions.
- Use network segmentation to isolate IoT devices where possible.
- Use network monitoring software to detect and alert on anomalous internal network activity.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/routers-iot-open-source-malware/176270/
Bleeping Computer https://www.bleepingcomputer.com/news/security/botenago-botnet-targets-millions-of-iot-devices-with-33-exploits/amp/