Severity

Medium

Analysis Summary

BotenaGo is a malware developed in an open-source programming language “Go” created by Google. In October 2021, the source code for Botena malware was leaked, allowing additional versions to be created based on the original. Nozomi Networks Labs uncovered a new variant of BotenaGo and named it “Lilin Scanner” which particularly targets Lilin security camera DVR equipment. Lilin Scanner is extremely evasive, with a 0% detection rate. Its main purpose is to use a list of IP addresses as inputs to infect its victims with Mirai executables. It is incapable of self-propagation. Mirai payloads are downloaded and executed on vulnerable devices after they have been infected by the Lillin scanner. Still, because it exclusively targets gadgets from a single manufacturer, this new BotenaGo variant isn’t a huge danger.

Impact

- Password & identity theft
- Server Outage
- Data Loss

Indicators of Compromise

IP

- 136[.]144[.]41[.]169

MD5

- 348bf5500f09b0c5e76bf67ae2ae12e5
- 147d956e488d0c9636604f4185f8da61

SHA-256

- fdbd955959a8f42450af5ac2bf93efba180f4cbae64dd4dd852f65c2e2057f56
- ae0185189e463c6abddf8865972dac72630b6e515e79d3f7566f0983a0eae295

SHA-1

- f0b208cba041e57762d5962ba392857602d629b2
- 9ec10995c06fcd47347eccd0260c8e7ec75074ca

Remediation

- Upgrade your operating system.
- Don’t open files and links from unknown sources.
- Install and run anti-virus scans.