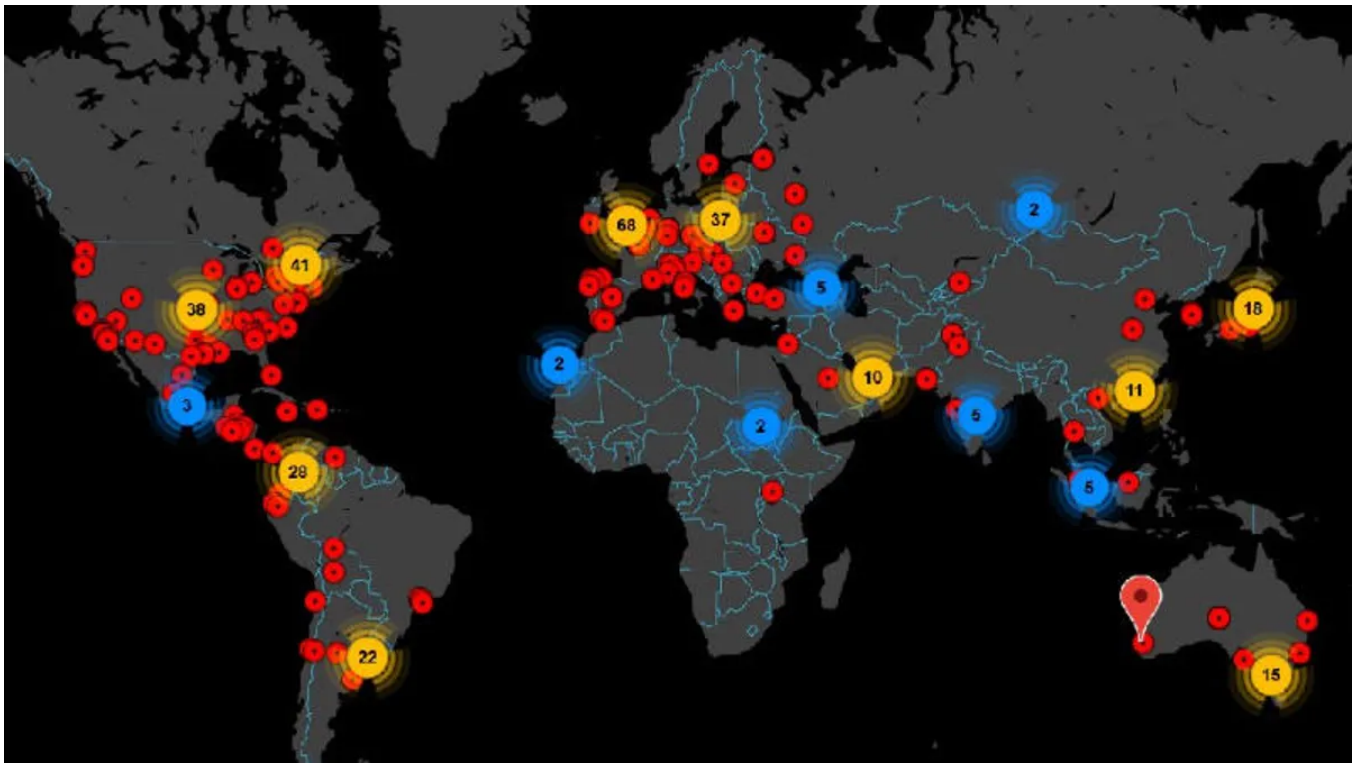
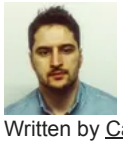
Naive IoT botnet wastes its time mining cryptocurrency

zdnet.com/article/naive-iot-botnet-wastes-its-time-mining-cryptocurrency/



Home Innovation Security

Operators of LiquorBot botnet waste their time trying to mine Monero on hacked SOHO routers.



Written by Catalin Cimpanu, Contributor on Jan. 8, 2020

-
-
-
-
-

Image: Peter Kruse

See als

10 dangerous app vulnerabilities to watch out for (free PDF)

Security researchers from Romanian antivirus vendor Bitdefender have discovered a botnet that infects home routers and other Internet of Things (IoT) smart devices and then attempts to mine for cryptocurrency.

This marks the third such IoT botnet that wastes its time by attempting to mine cryptocurrency on devices that clearly don't support these types of operations.

Short history of LiquorBot

Named LiquorBot, the botnet was first spotted in May 2019, according to a report Bitdefender published yesterday.

The botnet is nothing special in terms of technical capabilities. It works just like any other IoT botnet that's been documented over the past few years. Below is a short summary of LiquorBot's features:

- Uses the following exploits to infect routers and smart devices (mostly routers): CVE-2015-2051, CVE-2016-1555, CVE-2016-6277, CVE-2018-17173, CVE-2017-6884, CVE-2018-10562, CVE-2017-6077, CVE-2017-6334, CVE-2016-5679, CVE-2018-9285, CVE-2013-3568, CVE-2019-12780
- Uses a list of 82 username-password combinations to brute-force the SSH service of smart devices on which the default password has not been changed
- Can infect devices running on CPU architectures like ARM, ARM64, x86, x64, and MIPS
- Is controlled from a web-based command and control (C&C) server

About the only novel detail about LiquorBot is the fact that the malware is a version of the Mirai strain rewritten in the Go programming language -- but that's about it.

Wasting its time

Most IoT botnets today usually appear and disappear within weeks or months. LiquorBot is a strange case because it remained active throughout all 2019.

Bitdefender says the malware often received updates, usually in the form of new exploits. The most interesting update was, however, recorded in October.

The company says the LiquorBot code was expanded with a module that attempted to mine the Monero (XMR) cryptocurrency on infected devices.

The module, in itself, is quite useless, seeing that the entire botnet is predicated on infected routers, above anything else.

SOHO (Small Office Home Office) routers are cheap devices that lack the CPU and hardware capabilities to adequately mine cryptocurrency -- which is a very resource-heavy operation.

In the past, other IoT botnets have also wasted their time attempting to mine cryptocurrency on SOHO routers, with little success, and with all dropping any attempts within weeks, primarily due to the low yield the hacked devices were turning in.

The first IoT botnet to experiment with the feature was a Mirai-based botnet operated out of China, back in March 2017. The botnet experiment with a Bitcoin-mining module for a week, before dropping the module altogether.

The second was an IoT malware strain named Linux.MulDrop.14, detected by Dr.Web in June 2017. This botnet targeted Raspberry Pi devices, where it also attempted to mine Bitcoin. While Raspberry Pi devices have access to more hardware resources than your casual SOHO router, this botnet didn't break the bank either, stopping its experiments after a few weeks.

The discovery of these two botnets in 2017 encouraged researchers to look into the possibility of IoT botnets of being used as cryptocurrency mining farms. At the time, Errata Security estimated that if a Mirai botnet of 2.5 million bots mined cryptocurrency it would earn only a meager $0.25 per day, effectively dispelling the notion that IoT botnets could ever be used for cryptocurrency mining.

Apparently, the LiquorBot author didn't get the notice.

The most shocking of Shodan