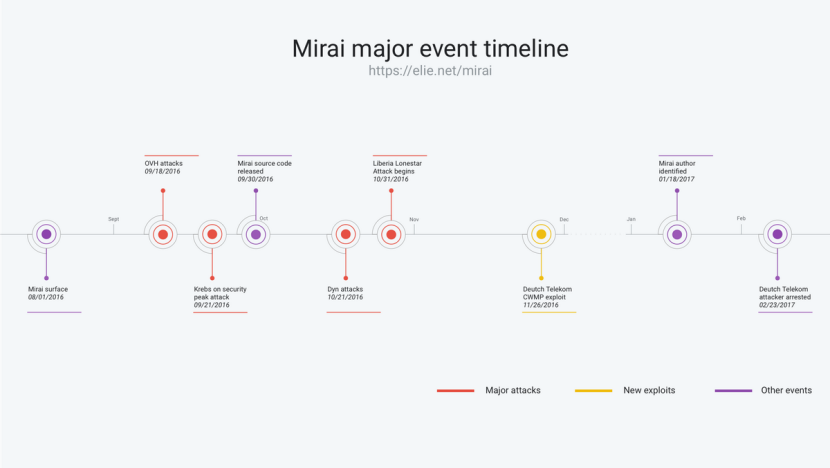
Northern Arizona University

Cybersecurity

CYB 410 - Software Security

Analyzing Mirai
a *Nix-Focused Attack



Author:
Akiel Aries

Supervisor:
Prof. Sareh Assiri

October 9, 2022

Introduction

Mirai is a piece of malware targeting Linux based systems first discovered in 2016 by a malware research group MalwareMustDie and gaining more popularity when cybersecurity journalist, Brian Krebs, had his website attacked. The goal being to control nodes part of a botnet running large-scale attacks. From previous research on attack history most victims include consumer grade devices such as local home routers and IP cameras, which are known to be insecure and attack-prone. The bot has been used in very large- scale DDoS (Distrubuted Denial of Service) atacks targeting many users machines and taking place accross the globe. Mirai's networking agent is written in C and its controller interface written in Go. It utilizes computer numerical control (CNC) which is a quite genius way to control the operation and functionality of a machine through injection of software. Mirai went on to spawn many variations, much like pieces of malware, that exploited zero-day's in some pieces of software for effecient and malicious operation.

Scale

hello

Running the Bug

Requirements:

- 2 servers: 1 for CNC + mysql, 1 for scan receiver, and 1+ for loading

Setup

- 2 VPS and 4 servers
- 1 VPS with extremely bulletproof host for database server
- 1 VPS, rootkitted, for scanReceiver and distributor
- 1 server for CNC (used like 2
- 3x 10gbps NForce servers for loading (distributor distributes to 3 servers equally)

Static Analysis/Debugging

Final Notes

Sources

https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/
https://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html