Kaiji - a new strain of IoT malware seizing control and launching DDoS attacks

Smart Home
2 min read

Graham CLULEY
May 05, 2020

Kaiji, a new botnet campaign, created from scratch rather than resting on the shoulders of those that went before it, is infecting Linux-based servers and IoT devices with the intention of launching distributed denial-of-service (DDoS) attacks.

Kaiji,named by researcher MalwareMustDie after one of the function names they observed in the malware's code (but also the name of a series of Japanese manga comic books), is believed to have originated in China, but is now spreading slowly around the world infecting new devices.

```
    _main_Getjiechi(); // chk commands, to process below malicious actions:
    runtime_newproc() => _to_ddos_Runkit()
    runtime_newproc(); => _to_main_runprofile()
    runtime_newproc(); => _to_main_runkshell()
    runtime_newproc(); => _to_main_runghost()
    runtime_newproc(); => _to_main_rundingshi()
    runtime_newproc(); => _to_main_runshouhu()
    runtime_newproc(); => _to_main_runkaiji()
    runtime_newproc(); => _to_main_runkaiji()
    runtime_newproc(); => _to_main_runganran()
    runtime_newproc(); => _to_ddos_Rdemokill()
    runtime_newproc(); => _to_ddos_MSG_CHINESE()
    runtime_makechan(*(var_08 ));
GOTO_ERR:
```

In a technical blog post, security researchers at Intezer describe how Kaiji, which unusually for an IoT botnet is written in the Go programming language, does not attempt to compromise unpatched devices by exploiting security vulnerabilities.

Instead it targets servers and ‘smart’ internet-connected devices via SSH brute forcing, taking advantage of administrators who are using weak or recycled passwords.

Rather than target one specific server or IoT device with many different passwords, in Kaiji’s SSH brute-forcing attack it automatically tries one password against the ‘root’ user on countless thousands of systems that have left their SSH port open to the internet.

It’s not an effective technique if a hacker has a specific target in mind, but it will certainly do if you’re happy to attack many SSH servers in the hope that you might just gain remote access to one.

Once it has compromised the Linux server or IoT device, Kaiji can begin to launch DDoS attacks at the beck-and-call of its operators. It also steals any local SSH keys it finds, and launches further SSH brute-force attacks to infect other exposed devices on the internet.

The researchers at Intezer describe Kaiji as “simple” and “in its early stages.” Their explanation for this is that Kaiji was written from scratch, rather than reusing existing botnet code available on the internet.

The expectation, however, is that Kaiji may very well be developed further and become more sophisticated over time – potentially escalating the number of devices it could hijack and the level of disruption it could cause.

Furthermore, the security researchers believe that Kaiji confirms a growing trend for more online criminals to migrate to the Go language – sometimes referred to as GoLang – for their malware development rather than more common choices for IoT malware such as C and C++.

Indicators of Compromise (IoCs) for Kaiji have been published on Intezer’s blog.

It should go without saying that users would be wise to restrict SSH access to their servers and IoT devices wherever possible, and use unique, complex passwords.

TAGS

smart home

AUTHOR

blic speaker. He has