December 17, 2019

Momentum botnet spotted in the wild

Doug Olenick

Follow @DougOlenick

A new botnet dubbed Momentum has been found targeting Linux systems running on a variety of different processors and pushing a list of well-known backdoors with the goal of being able to launch DDoS attacks.

Trend Micro reported Momentum has been found launching Mirai, Kaiten and Bashlite variants in a series of attacks that use a multitude of vulnerabilities on routers and web services to download and execute shell scripts.

“The main purpose of this malware is to open a backdoor and accept commands to conduct various types of DoS attacks against a given target,” Trend Micro wrote.

Once injected into a device the malware achieves persistence by modifying the rc files and then connecting to the command and control server and joins an internet relay chat channel named #hellboy to register and begin accepting commands. The chat channel is used to command the botnet devices.

Momentum has in its arsenal 36 different methods for creating a denial of service situation. A typical attack sees the malware spoofing the victim’s source IP addresses to services run on publicly accessible servers, provoking a flood of responses to overwhelm the victim’s address,” Trend Micro wrote.

The best defense against Momentum is to not just trust the factory setting and instead make certain your Linux device is properly secured.

TOPICS: BOTNET DDOS