UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00138

MIRAI INSPIRED GAFGYT BOTNET DDOS

DATE ISSUED: 27th April 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

Also known as Bashlite, the Gafgyt Linus-based botnet malware family have recently upgraded by incorporating code from the Mirai botnet to target Internet of Things (IoT) or Smart device such as routers to launch large scale DDoS attacks.

BREAKDOWN

Targeting device such as Huawei and Realtek routers, GPON and ASUS devices, Gafgyt is exploiting known vulnerabilities such as CVE-2017-17215, CVE-2014-8361, and CVE-2018-10561 to download payloads in order to infect IoT devices. With Mirai modules now incorporated into the malware, new attack methods are possible including HTTP flooding, UDP flooding, TCP flood attacks and an STD module to carry out DDoS style attacks. Uptycs discovered that infected devices are being turned into bots to target specific IP addresses in the DDoS attacks and brute-forcing over Telnet. By exploiting the Remote Code Execution (RCE) vulnerabilities listed above, Gafgyt uses the 'wget' command to fetch the payload and provide execution permissions using the 'chmod' command. CVE-2018-10561 is an authentication bypass that is used in a similar fashion to achieve the same results. Gafgyt uses the Tor network to cloak its activities.

REMEDIATION STEPS

- Ensure Operating Systems are up to date with the latest version and security patches applied.
- Use network monitoring software to detect, alert on and remediate anomalous behaviours.
- Remove and replace any devices that are unable to support the latest patches and updates.
- Isolate devices behaving abnormally on your network,
- Invest in DDoS protection through your ISP.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/gafgyt-botnet-ddos-mirai/165424/
Trend Micro	https://www.trendmicro.com/vinfo/fr/security/news/vulnerabilities-and-exploits/patch-now-new-mirai-gafgyt-variants-target-16-flaws-via-multi-exploits
F5 Labs	https://www.f5.com/labs/articles/threat-intelligence/gafgyt-targeting-huawei-and-asus-routers-and-killing-off-rival-iot-botnets