UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00255

SANDWORM & CYCLOPS BLINK BOTNET HUNT ASUS ROUTERS

DATE ISSUED: 22nd March 2022

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

The 'Cyclops Blink' botnet that has been linked to the same Advanced Persistent Threat (APT) group associated with the NotPetya wiper attacks (Sandworm) which is now hunting down ASUS routers for reasons which are not yet clear.

BREAKDOWN

While the botnet has been around since 2019, the recent surge in activity and links to the Russian-speaking group have researchers and experts worried they may be ramping up for Distributed Denial of Service (DDoS) attacks on a large scale or something more sinister. "The more routers that are compromised, the more sources of powerful data collection – and avenues for further attacks – become available to attackers." The group is also known by other names including Voodoo Bear and Telebots and have been linked to series of high-profile, state-sponsored attacks as well as the VPNFilter Internet of Things (IoT) botnet. Researchers have also discovered that some of the devices assessed had been infected for years. The module targeting ASUS routers is built to replace the routers flash memory and can read and write from this memory that contains the Operating System (OS), configuration and file systems. Once the connection to the C2 server is established the module then harvest the devices' Linux version, memory consumption information, SSD storage information, network interfaces information and the contents of the following files: /etc/passwd, /etc/group, /etc/mounts, /proc/partitions. It also downloads a further module that can download files via the internet using DNS over HTTPS.

REMEDIATION STEPS

- Routers are a popular target due to a lack of regular patching. Check your firmware and updates and apply all outstanding patches.
- Check you have strong passwords on devices and access is only granted to administrators who require it
- If you discover your router has been compromised, replacement of the hardware is the best option as performing a factory reset will not fix any alterations to the OS completed by attackers to establish persistence.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/sandworm-asus-routers-cyclops-blink-botnet/178986/