Cyclops Blink

Threat: **Malware**

Author: **Jeffrey Farnan** Date Originally Published: **May 31th, 2022**

1. SUMMARY

- Cyclops Blink is a new malware targeting network hardware with the goal of adding the targeted device to a botnet for command and control. This malware targets routers and firewall devices sold by the companies WatchGuard and ASUS. This new sophisticated malware is an advanced persistent threat botnet attributed to a Russian nation-state threat group called Sandworm. This malware is a multi-stage, modular platform with versatile capabilities to support both intelligence-collection and potentially destructive cyber-attack operations.

2. MALWARE FAMILY

- **Type** = Malware.
- **Sub-type** = Botnet.

- **Malware:** The Cyclops Blink malware comes in the form of a firmware update which abuses WatchGuard's standard firmware upgrade to install the malicious firmware. This malware targets vulnerable internet-connected firewall devices used for command-and-control (C2) of the underlying botnet. While it originally targeted WatchGuard firewall appliances, it now extends to Asus and other router manufacturers.
- **Botnet:** A botnet is a collection of private computers infected with malicious software and controlled as a group without the owner's knowledge. The Cyclops Blink botnet was created in an attempt to build an infrastructure for future attacks on high value targets.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = Russia.
- **First seen date/period** = February 2022.
- **Still active** = Yes.

4. MALWARE HISTORY

- Cyclops Blink was first reported in February of 2022, after a number of security agencies disclosed its presents in the wild. It’s designed to infect routers and other networked devices to steal data or compromise them for further attacks on other targets.
- Cyclops Blink is a botnet attributed to Sandworm, a Russian nation-state threat group. Sandworm group has been known to target Ukrainian companies and government agencies. They were held responsible for destroying entire Ukrainian networks, triggering blackouts by targeting electrical utilities in Ukraine.
- The Cyclops Blink malware appears to have been existed since 2019 and believed to be the successor to another similar botnet called VPNFilter, which also belonging to Sandworm. The VPNFilter botnet was previously used by the threat actor to redirect and manipulate traffic and infected devices and also used to maintain persistence on victim networks.

5. MALWARE DESCRIPTION

- Cyclops Blink malware is a multi-stage, modular platform with versatile capabilities to support both intelligence-collection and potentially destructive cyber-attack operations.
- **Malware:** Cyclops Blink is a new malware targeting network hardware with the goad of adding the targeted device to a botnet for command and control (C&C). This malware targets routers and firewall devices sold by the companies WatchGuard and ASUS. These network devices are often located on the perimeter of a victim's computer network, thereby providing Sandworm with the potential ability to conduct malicious activities against all computers within those networks.
- **Functionality:** The malware has basic core functionality to send information from the compromised device to a server controlled by the hackers, as well as allowing files to be downloaded and executed. The modules are specifically developed to upload/download files to and from its command and control server, collect device information, and update the malware. Additional functionality allows new modules to be added as the malware executes, causing Sandworm to add new features to an attack as needed.
- **Development:** The developers have reverse engineered the WatchGuard Firebox firmware update process and have identified a specific weakness in this process, namely the ability to recalculate the HMAC value used to verify a firmware update image. They have taken advantage of this weakness to enable them to maintain the persistence of Cyclops Blink throughout the legitimate firmware update process.
- **Botnet:** The devices infected by Cyclops Blink have been incorporated into a large-scale botnet operated by the threat actor, which appears to have first become active as early as June 2019. Once established on targeted devices, the Cyclops Blink provides backdoor access to the compromised networks for the Sandworm hackers. The invasive features of the threat are spread through specifically designed modules. Some of the most notable harmful functions of the malware include the ability to fetch additional files, exfiltrated chosen files, collect and transmit device information and get updates from the operations of the Command-and-Control (C2) server. A significant amount of attention has been given to ensuring that the C2 communications are difficult to detect and track.
- The presence of a Cyclops Blink infection does not mean that an organization is the primary target, but its machines could be used to conduct attacks on others.

6. POTENTIAL CUSTOMER DEFENSE

- The good news is that the US Justice Department has announced that the FBI has disrupted the Cyclops Blink botnet of thousands of infected network hardware devices. The FBI neutralized the threat before the slave computers could be weaponized.
- The Cyclops Blink malware can't be flushed from infected devices by simply rebooting the device, so owners of WatchGuard and ASUS devices are advised to check whether they have been compromised and, if they have, to perform a set of actions to clean up the device. To remove the malware detection and remediation tools have been released along with guidelines on how to remove the malware. It is critical whether infected or not, to upgrade the appliance to the latest version.
- The threat is still active and attacks could prove disastrous for affected organizations, so here is some useful recommendations:
    - Protect your devices and networks by keeping them up to date using the latest supported versions, apply security patches issued by different manufacturers, make use of anti-malware and schedule regular scans to protect against new and known malware threats.
    - Make use of multi-factor authentication to mitigate the impact of passwords that may be compromised.
    - Do not expose network device management interfaces (router, switch, firewall, etc.) to the Internet.
    - Prevent and detect lateral movement in your organization's networks.

Research Sources:

- https://www.theguardian.com/world/2022/feb/23/russia-hacking-malware-cyberattack-virus-ukraine
- https://gbhackers.com/cyclops-blink-malware/
- https://www.cisa.gov/uscert/ncas/alerts/aa22-054a
- https://chowdera.com/2022/03/202203211426551405.html
- https://thehackernews.com/2022/04/fbi-shut-down-russia-linked-cyclops.html
- https://blog.malwarebytes.com/threat-spotlight/2022/02/cyclops-blink-malware-us-and-uk-authorities-issue-alert/

Disclaimer: All opinions expressed in this article are the opinions solely of the author.