Threat Advisory: Cyclops Blink

blog.talosintelligence.com/2022/02/threat-advisory-cyclops-blink.html

This post is also available in:

日本語 (Japanese)

Українська (Ukrainian)

Update Mar. 17, 2022

Today, Asus released a product security advisory listing their products affected by Cyclops Blink. While the investigation is currently ongoing, this advisory provides guidance on taking necessary precautions via a checklist for the affected product versions.

Update Feb. 25, 2022

In our ongoing research into activity surrounding Ukraine and in cooperation with Cisco Duo data scientists Talos discovered compromised MikroTik routers inside of Ukraine being leveraged to conduct brute force attacks on devices protected by multi-factor authentication. This continues a pattern we have seen since our investigation into VPNFilter involving actors using MikroTik routers. While it may not be Cyclops Blink specifically -- we can't know without a forensic investigation -- it was yet another MikroTik router passing malicious traffic, a vendor widely abused by VPNFilter in the past.

Cisco Talos is aware of the recent reporting around a new modular malware family, Cyclops Blink, that targets small and home office (SOHO) devices, similar to previously observed threats like VPNFilter. This malware is designed to run on Linux systems and is compiled specifically for 32-bit PowerPC architecture. The modular nature of this malware allows it to be used in a variety of ways, including typical reconnaissance and espionage activity. It leverages modules to facilitate various operations such as establishment of C2, file upload/download and information extraction capabilities.

Details of modular Cyclops Blink malware

Cyclops Blink is a Linux ELF executable compiled for 32-bit PowerPC architecture that has targeted SOHO network devices since at least June 2019. The complete list of targeted devices is unknown at this time, but WatchGuard FireBox has specifically been listed as a target. The modular malware consists of core components and modules that are deployed as child processes using the Linux API fork. At this point, four modules have been identified that download and upload files, gather system information and contain updating mechanisms for the malware itself. Additional modules can be downloaded and executed from the command and control (C2) server.

The core component has a variety of functionality. Initially, it confirms that it's running as a process named 'kworker[0:1]' which allows it to masquerade as a kernel process. If that is not the case, it will reload itself as that process name and kill the parent process. The core component then adjusts the iptables to allow additional access via a set of hard-coded ports that are used for C2 communication. The C2 communication is conducted through multiple layers of encryption including a TLS tunnel with individual commands encrypted using AES-256-CBC.

Module details

The four known modules perform a variety of functions and tasks associated with initial access and reconnaissance. This could be the basis to deploy additional modules, but at this point, we cannot confirm any additional modules.

The system reconnaissance module (ID 0x8) is designed to gather various pieces of information from the system at regular intervals, initially set to occur every 10 minutes.

The file upload/download module (ID 0xf) is designed to upload and download files. These instructions are sent by the core component and can include downloads from URLs or uploads of files to C2 servers.

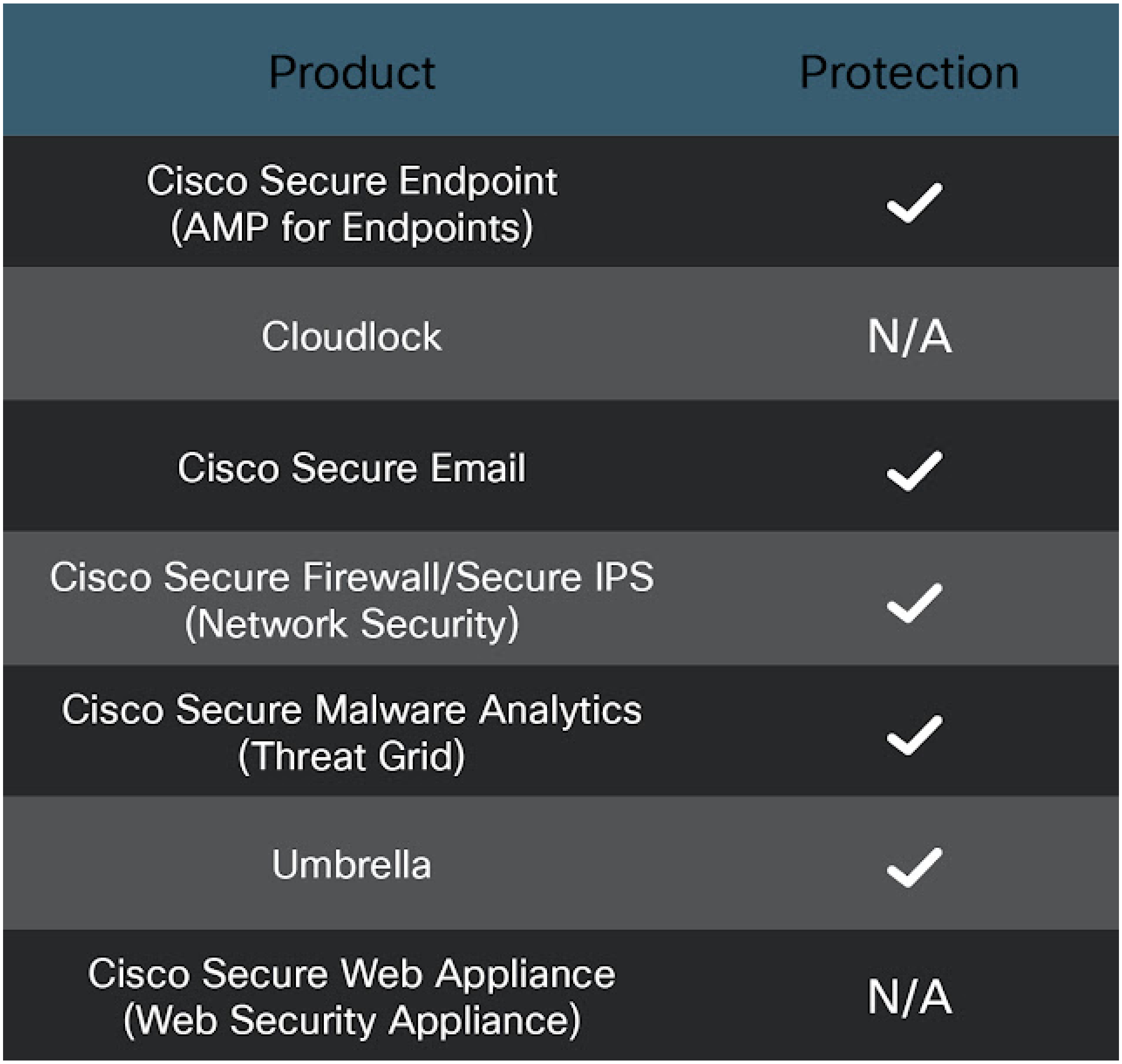
The C2 server list module (ID 0x39) is used to store and/or update the list of IP addresses used for C2 activity. The list is loaded and passed to the core component and when updates are received from the core component it is passed into this module to be updated.

The Update/Persistence module (ID 0x51) installs updates to Cyclops Blink or ensures its persistence on the system. The update process leverages the firmware update process on the device. The persistence is handled via a subprocess to this module and involves overwriting legitimate executables with modified versions allowing the firmware update process to be manipulated to update Cyclops Blink.

Complete details on the modules and core components can be found in NCSC's report.

Coverage

Ways our customers can detect and block this threat are listed below.



Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	N/A

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Malware Analytics (formerly Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Firepower Threat Defense (FTD), Firepower Device Manager (FDM), Threat Defense Virtual, Adaptive Security Appliance can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

Meraki MX appliances can detect malicious activity associated with this threat.

Umbrella, Secure Internet Gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Orbital Queries

Cisco Secure Endpoint users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click here.

Snort SIDs: **59095-59098**

The following ClamAV signatures available for protection against this threat:

Unix.Backdoor.CyclopsBlink

Umbrella SIG customers will be protected from this threat if configured to leverage IPS or Malware Analytics capabilities.

IOCs

50df5734dd0c6c5983c21278f119527f9fdf6ef1d7e808a29754ebc5253e9a86
c082a9117294fa4880d75a2625cf80f63c8bb159b54a7151553969541ac35862
4e69bbb61329ace36fbe62f9fb6ca49c37e2e5a5293545c44d155641934e39d1
ff17ccd8c960594617107111fcc8372cfea5f0f9eb566ceb6ab709ea871190dc6