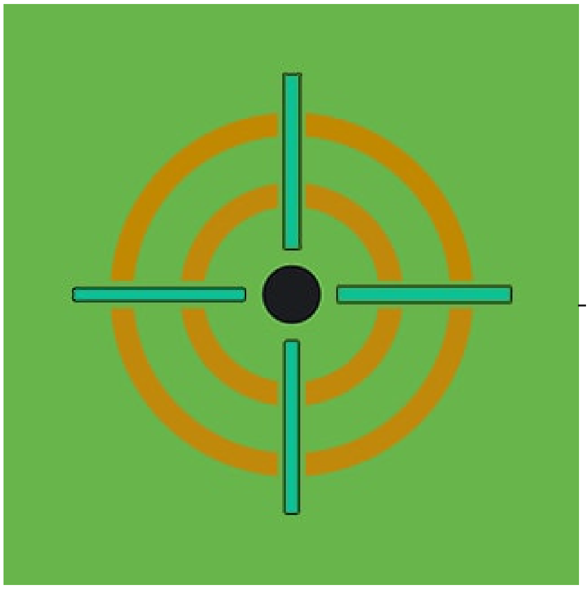
STRT-TA03 CPE - Destructive Software

April 15, 2022



By Splunk Threat Research Team April 15, 2022

The Splunk Threat Research Team is monitoring several malicious payloads targeting Customer Premise Equipment (CPE) devices. These are defined as devices that are at customer (Commercial, Residential) premises and that provide connectivity and services to the internet backbone. Examples include:

- Cable Modems

- Internet Gateways
- Satellite Modems
- Firewalls
- Home routers, cable set-top boxes, DSL modems
- VOIP telephones

The above devices are prevalent and fundamental for internet connectivity. Malicious actors can target these devices to build very powerful botnets which in combination with tactical payloads, can potentially exert a significant effect on critical internet infrastructure or even Operational Technologies devices. CPE devices are generally not very powerful in terms of processing or functionality, however, when hundreds of thousands of these devices are compromised and work in aggregation via Command and Control they can cause significant damage. An example of this type of payload is VPNFilter discovered by Cisco Talos and said to have compromised 500,000 devices worldwide.

Based on the current, ongoing geopolitical events and the recent takedown of a similar malicious payload by the FBI named “Cyclops Blink” and attributed to Russian Federation’s Main Intelligence Directorate (GRU). The Splunk Threat Research Team has developed specific analytics to detect this type of malicious code, including Cyclops Blink, and AcidRain.

The main malicious functions of these malicious payloads can be resumed in:

- System discovery and footprinting
- In some cases resists removal/reboot
- Destroys infected equipment (Wipes flash memory, sd, memory card, and block devices)
- Modification of routing traffic rules
- Ability to download and install additional payloads
- Obfuscated multiple C2 callback failover (TOR, VPS, Geolocation)

Another common thing about these payloads is that they target popular commercial CPE brands. This speaks of the intention of targeting critical infrastructure to gain access, implant malicious payloads, and hoard as many compromised devices as possible that can be used for subsequent attacks.

Due to the ability to download additional payloads, these additional payloads may likely be implemented based on tactical objectives (DDoS, Destruction, Espionage, Lateral Movement, etc). It is important to notice that many of these devices are not just commercial, industrial, or military but used in civilian networks, which exposes the general population to these attacks and presents a direct threat to civilian infrastructure and livelihood.

For specific make and model of affected devices please refer to the reference section at the end of this advisory.

The following are the detections crafted for these payloads.

Cyclops Blink

Name	Technique ID	Tactic	Description
Linux Iptables Firewall Modification	T1562.004	Defense Evasion	This analytic looks for suspicious command lines that modify the iptables firewall setting of a Linux machine.
Linux Kworker Process CommandLine	T1036.004	Defense Evasion	This analytic looks for suspicious process kworker command lines in a Linux machine.
Linux Stdout Redirection To Dev Null File	T1562.004	Defense Evasion	This analytic looks for suspicious command lines that redirect the stdout or possible stderr to dev/null file.

AcidRain

Name	Technique ID	Tactic	Description
Linux High Frequency Of File Deletion In Etc Folder(New)	T1485, T1070.004	Defense Evasion, Impact	This analytic looks for a high frequency of file deletion relative to process name and process id /etc/ folder.
Linux Deletion Of Init Daemon Script(New)	T1485, T1070.004	Defense Evasion, Impact	This analytic looks for deletion of the init daemon script in a Linux machine.
Linux Deletion of SSL Certificate(New)	T1485, T1070.004	Defense Evasion, Impact	This analytic looks for deletion of the SSL certificate in a Linux machine.
Linux deletion Of SSH Key(New)	T1485, T1070.004	Defense Evasion, Impact	This analytic looks for deletion of an ssh key in a Linux machine.
Linux Deletion Of Services(New)	T1485, T1070.004	Defense Evasion, Impact	This analytic looks for deletion of services in a Linux machine.
Linux Deletion Of Cron Jobs(New)	T1485, T1070.004	Defense Evasion, Impact	This analytic looks for deletion of cron jobs in a Linux machine.

The above searches will be available at research.splunk.com, the Splunk Threat Research Team (STRT) security content repository, and the Splunk ES Content Update (ESCU) application at Splunkbase.

IOC:

Filename	Size	Sha256
acid_rain.elf	22656 bytes (22 KiB)	9b4dfaca873961174ba935fddaf696145afe7bbf5734509f95feb54f3584fd9a
cyclopblink1	2332316 bytes (2277 KiB)	4ec5e0c5dccc5891d39ea76e3c3d3e26d8830d7aa4d63db6084dbfbec6f0d211
cyclopblink2	7346456 bytes (7174 KiB)	fc1e50172c0ce221452b967d1ef705f11bbfe2d54c533d68bd2a7a094605df2d

Mitigations

The above detections were crafted under a Linux environment and can be used as guidelines for other architectures such as MISP or PowerPC. The key to implementing these types of detections is the ability to monitor via a logging mechanism (i.e syslog).

Addressing the threat of these types of payloads can be very difficult as many of these devices do not allow for the implementation of centralized logging which impairs monitoring and defense. Considering that many enterprises have had remote work programs since the pandemic started, their perimeter may likely have a device affected by these payloads, in which case the best course of action is to disconnect, discard and replace them. Some other mitigation options are:

- Discard affected hardware as payload resists removal, and rebooting.
- Implement integrity validation mechanisms on CPEs software and hardware
- Upgrade and harden CPE devices, discard them if the device has reached the end of life (EOL). If a device cannot be monitored, the device must be discarded.
- Consult with vendors, ISP on how to improve security on CPE devices
- Enable logging of these devices to implement detections
- Follow CISA Home Network Security Guide (ST15-002)
- Follow CISA Securing Network Infrastructure Devices (ST18-001)

It is also important to consider that an advanced adversary as the aforementioned has likely devised other ways of access, exploitation or persistence that may be yet unknown and that may target these devices after remediation. This is why prevention, monitoring, and detection are fundamental to defend against these threats.

Reference

- CISA Alert (AA22-054A): https://www.cisa.gov/uscert/ncas/alerts/aa22-054a
- Watchguard advisory: https://detection.watchguard.com
- NCSC Password Administration for System Owners Guide: https://www.ncsc.gov.uk/collection/passwords
- NCSC Cyclops Blink Malware Analysis Report: https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf
- CISCO how to harden IOS Devices: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html
- CISA advises D-LINK users to take vulnerable routers offline: https://blog.malwarebytes.com/exploits-and-vulnerabilities/2022/04/cisa-advises-d-link-users-to-take-vulnerable-routers-offline/
- Cisco Talos VPNFilter advisory and affected devices: https://en.wikipedia.org/wiki/VPNFilter#cite_note-ars-9
- Cyclops Blink affected devices: https://www.zdnet.com/article/cyclops-blink-botnet-launches-assault-against-asus-routers/
- Sentinel One AcidRain analysis: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe
- NSA - Protecting VAST Communications: https://media.defense.gov/2022/Jan/25/2002927101/-1/-1/0/CSA_PROTECTING_VSAT_COMMUNICATIONS_01252022.PDF
- ASUS security bulletin: https://www.asus.com/content/ASUS-Product-Security-Advisory/

Learn More

You can find the latest content about security analytic stories on GitHub and in Splunkbase. Splunk Security Essentials also has all these detections available via push update. In the upcoming weeks, the Splunk Threat Research Team will be releasing a more detailed blog post on this analytic story. Stay tuned!

For a full list of security content, check out the release notes on Splunk Docs.

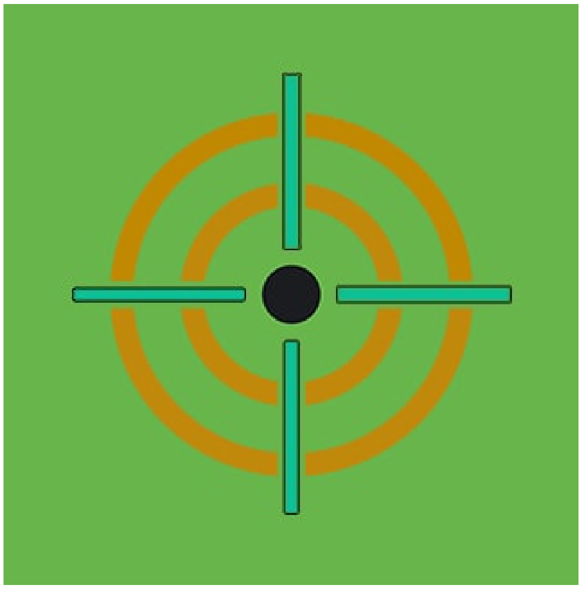
Feedback

Any feedback or requests? Feel free to put in an issue on GitHub and we'll follow up. Alternatively, join us on the Slack channel #security-research. Follow these instructions If you need an invitation to our Splunk user groups on Slack.

We would like to thank the following for their contributions to this post.

- Teoderick Contreras
- Rod Soto

- Jose Hernandez
- Patrick Barreiss
- Lou Stella
- Mauricio Velazco
- Michael Haag
- Bhavin Patel
- Eric McGinnis



Posted by

Splunk Threat Research Team

The Splunk Threat Research Team is an active part of a customer's overall defense strategy by enhancing Splunk security offerings with verified research and security content such as use cases, detection searches, and playbooks. We help security teams around the globe strengthen operations by providing tactical guidance and insights to detect, investigate and respond against the latest threats. The Splunk Threat Research Team focuses on understanding how threats, actors, and vulnerabilities work, and the team replicates attacks which are stored as datasets in the Attack Data repository.

Our goal is to provide security teams with research they can leverage in their day to day operations and to become the industry standard for SIEM detections. We are a team of industry-recognized experts who are encouraged to improve the security industry by sharing our work with the community via conference talks, open-sourcing projects, and writing white papers or blogs. You will also find us presenting our research at conferences such as Defcon, Blackhat, RSA, and many more.

Read more Splunk Security Content.