New Sandworm Malware Cyclops Blink Replaces VPNFilter

cisa.gov/uscert/ncas/alerts/aa22-054a

Summary

The Sandworm actor, which the United Kingdom and the United States have previously attributed to the Russian GRU, has replaced the exposed VPNFilter malware with a new more advanced framework.

The United Kingdom's (UK) National Cyber Security Centre (NCSC), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) in the U.S. have identified that the actor known as Sandworm or Voodoo Bear is using a new malware, referred to here as Cyclops Blink. The NCSC, CISA, and the FBI have previously attributed the Sandworm actor to the Russian General Staff Main Intelligence Directorate's Russian (GRU's) Main Centre for Special Technologies (GTsST). The malicious cyber activity below has previously been attributed to Sandworm:

Cyclops Blink appears to be a replacement framework for the VPNFilter malware exposed in 2018, and which exploited network devices, primarily small office/home office (SOHO) routers and network attached storage (NAS) devices.

This advisory summarizes the VPNFilter malware it replaces, and provides more detail on Cyclops Blink, as well as the associated tactics, techniques and procedures (TTPs) used by Sandworm. An NCSC malware analysis report on Cyclops Blink is also available.

It also provides mitigation measures to help organizations defend against malware.

Click here for a PDF version of this report.

Technical Details

VPNFilter

The malware was first exposed in 2018

A series of articles published by Cisco Talos in 2018 describes VPNFilter and its modules in detail. VPNFilter was deployed in stages, with most functionality in the third-stage modules. These modules enabled traffic manipulation, destruction of the infected host device, and likely enabled downstream devices to be exploited. They also allowed monitoring of Modbus SCADA protocols, which appears to be an ongoing requirement for Sandworm, as also seen in their previous attacks against ICS networks.

VPNFilter targeting was widespread and appeared indiscriminate, with some exceptions: Cisco Talos reported an increase of victims in Ukraine in May 2018. Sandworm also deployed VPNFilter against targets in the Republic of Korea before the 2018 Winter Olympics.

In May 2018, Cisco Talos published the blog that exposed VPNFilter and the U.S. Department of Justice linked the activity to Sandworm and announced efforts to disrupt the botnet.

Activity since its exposure

A Trendmicro blog in January 2021 detailed residual VPNFilter infections and provided data which showed that although there had been a reduction in requests to a known C2 domain, there was still more than a third of the original number of first-stage infections.

Sandworm has since shown limited interest in existing VPNFilter footholds, instead preferring to retool.

Cyclops Blink

Active since 2019

The NCSC, CISA, the FBI, and NSA, along with industry partners, have now identified a large-scale modular malware framework (T1129) which is targeting network devices. The new malware is referred to here as **Cyclops Blink** and has been deployed since at least June 2019, fourteen months after VPNFilter was disrupted. In common with VPNFilter, Cyclops Blink deployment also appears indiscriminate and widespread.

The actor has so far primarily deployed Cyclops Blink to WatchGuard devices, but it is likely that Sandworm would be capable of compiling the malware for other architectures and firmware.

Note: *Note that only WatchGuard devices that were reconfigured from the manufacturer default settings to open remote management interfaces to external access could be infected*

Malware overview

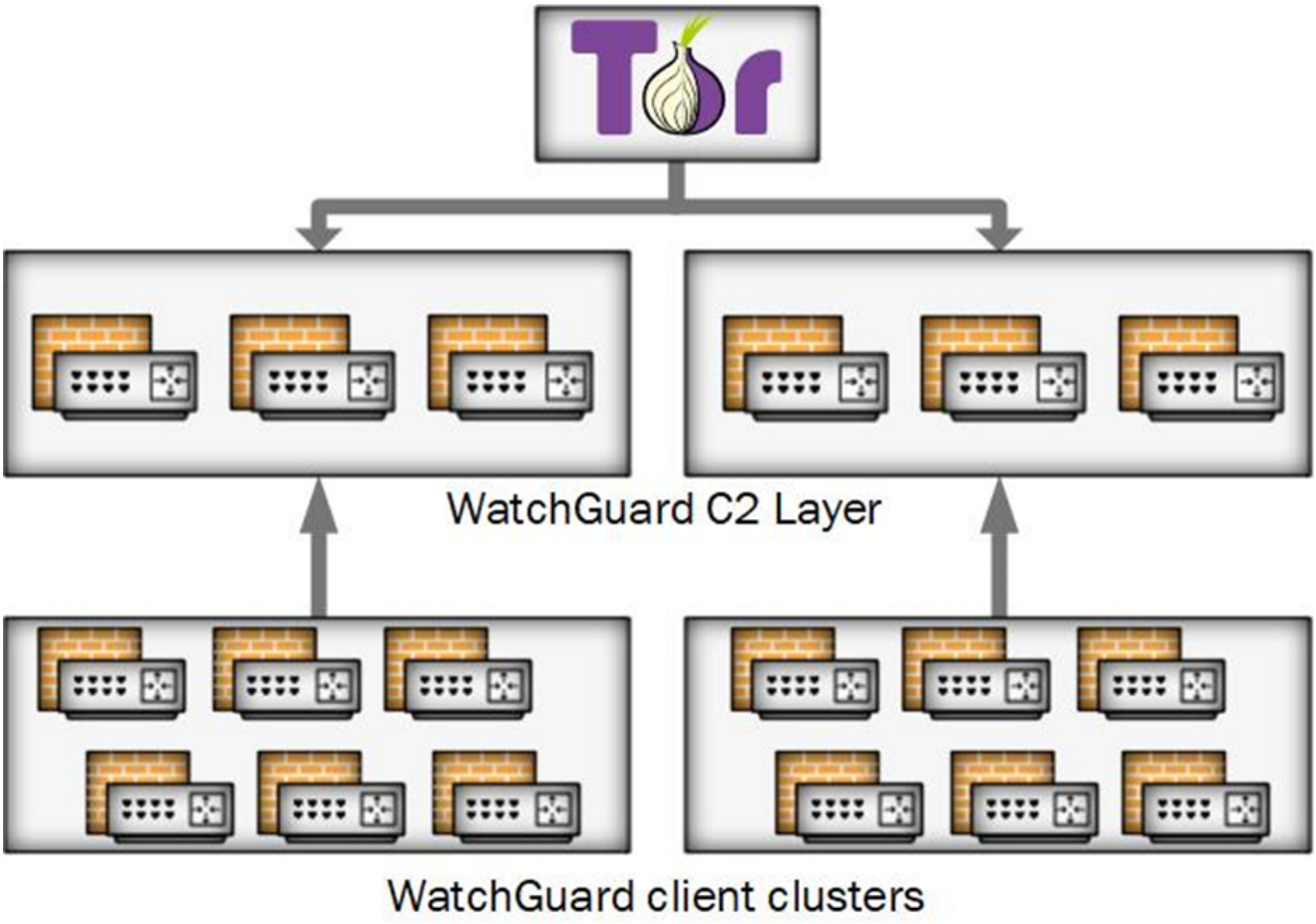
The malware itself is sophisticated and modular with basic core functionality to beacon (T1132.002) device information back to a server and enable files to be downloaded and executed. There is also functionality to add new modules while the malware is running, which allows Sandworm to implement additional capability as required.

The NCSC has published a malware analysis report on Cyclops Blink which provides more detail about the malware.

Post exploitation

Post exploitation, Cyclops Blink is generally deployed as part of a firmware 'update' (T1542.001). This achieves persistence when the device is rebooted and makes remediation harder.

Victim devices are organized into clusters and each deployment of Cyclops Blink has a list of command and control (C2) IP addresses and ports that it uses (T1008). All the known C2 IP addresses to date have been used by compromised WatchGuard firewall devices. Communications between Cyclops Blink clients and servers are protected under Transport Layer Security (TLS) (T1071.001), using individually generated keys and certificates. Sandworm manages Cyclops Blink by connecting to the C2 layer through the Tor network.



Mitigations

Cyclops Blink persists on reboot and throughout the legitimate firmware update process. Affected organizations should therefore take steps to remove the malware.

WatchGuard has worked closely with the FBI, CISA, NSA and the NCSC, and has provided tooling and guidance to enable detection and removal of Cyclops Blink on WatchGuard devices through a non-standard upgrade process. Device owners should follow each step in these instructions to ensure that devices are patched to the latest version and that any infection is removed.

The tooling and guidance from WatchGuard can be found at: https://detection.watchguard.com/.

In addition:

- If your device is identified as infected with Cyclops Blink, you should assume that any passwords present on the device have been compromised and replace them (see NCSC password guidance for organizations.
- You should ensure that the management interface of network devices is not exposed to the internet.

Indicators of Compromise

Please refer to the accompanying Cyclops Blink malware analysis report for indicators of compromise which may help detect this activity.

MITRE ATT&CK®

This advisory has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Tactic	Technique	Procedure
Initial Access	T1133	External Remote Services **The actors most likely deploy modified device firmware** images by exploiting an externally available service
Execution	T1059.004	Command and Scripting Interpreter: Unix Shell Cyclops Blink executes downloaded files using the Linux API
Persistence	T1542.001	Pre-OS Boot: System Firmware Cyclops Blink is deployed within a modified device firmware image

T1037.004	Boot or Logon Initialization Scripts: RC Scripts Cyclops Blink is executed on device startup, using a modified RC script	
Defense Evasion	T1562.004	Impair Defenses: Disable or Modify System Firewall Cyclops Blink modifies the Linux system firewall to enable C2 communication
	T1036.005	Masquerading: Match Legitimate Name or Location Cyclops Blink masquerades as a Linux kernel thread process
Discovery	T1082	System Information Discovery Cyclops Blink regularly queries device information
Command and Control	T1090	Proxy
T1132.002	Data Encoding: Non-Standard Encoding Cyclops Blink command messages use a custom binary scheme to encode data	
T1008	Fallback Channels Cyclops Blink randomly selects a C2 server from contained lists of IPv4 addresses and port numbers	
T1071.001	Application Layer Protocol: Web Protocols Cyclops Blink can download files via HTTP or HTTPS	

	T1573.002	Encrypted Channel: Asymmetric Cryptography Cyclops Blink C2 messages are individually encrypted using AES-256-CBC and sent underneath TLS
	T1571	Non-Standard Port The list of port numbers used by Cyclops Blink includes non-standard ports not typically associated with HTTP or HTTPS traffic
Exfiltration	T1041	Exfiltration Over C2 Channel Cyclops Blink can upload files to a C2 server

A Cyclops Blink infection does not mean that an organization is the primary target, but it may be selected to be, or its machines could be used to conduct attacks.

Organizations are advised to follow the mitigation advice in this advisory to defend against this activity, and to refer to indicators of compromise (not exhaustive) in the Cyclops Blink malware analysis report to detect possible activity on networks.

UK organizations affected by the activity outlined in should report any suspected compromises to the NCSC at https://report.ncsc.gov.uk/.

Further Guidance

A variety of mitigations will be of use in defending against the malware featured in this advisory:

- **Do not expose management interfaces of network devices to the internet:** the management interface is a significant attack surface, so not exposing them reduces the risk. See NCSC guidance: https://www.ncsc.gov.uk/guidance/acquiring-managing-and-disposing-network-devices.
- **Protect your devices and networks by keeping them up to date**: use the latest supported versions, apply security patches promptly, use anti-virus and scan regularly to guard against known malware threats. See NCSC guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware.

- **Use multi-factor authentication to reduce the impact of password compromises.** See NCSC guidance: https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services and https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa.
- **Treat people as your first line of defense.** Tell staff how to report suspected phishing emails, and ensure they feel confident to do so. Investigate their reports promptly and thoroughly. Never punish users for clicking phishing links or opening attachments. See NCSC guidance: https://www.ncsc.gov.uk/phishing.
- **Set up a security monitoring capability** so you are collecting the data that will be needed to analyze network intrusions. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.
- **Prevent and detect lateral movement in your organization's networks.** See NCSC guidance: https://www.ncsc.gov.uk/guidance/preventing-lateral-movement.

About This Document

This advisory is the result of a collaborative effort by United Kingdom's National Cyber Security Centre (NCSC), the United States' National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

CISA, FBI, and NSA agree with this attribution and the details provided in the report.

This advisory has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

Disclaimers

This report draws on information derived from NCSC and industry sources. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

Disclaimer of Endorsement: The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

For NSA client requirements or general cybersecurity inquiries, contact the Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov.

Contact Information

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory:

U.S. organizations contact your local FBI field office at fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by email at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov.

Australian organizations should report incidents to the Australian Signals Directorate's (ASD's) ACSC via cyber.gov.au or call 1300 292 371 (1300 CYBER 1).

U.K. organizations should report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hrs) or for urgent assistance, call 03000 200 973.

Revisions

February 23, 2022: Initial Version

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.