National Cyber Security Centre
a part of GCHQ

Advisory.

New Sandworm malware Cyclops Blink replaces VPNFilter

Version 1.0

23 February 2022

New Sandworm malware Cyclops Blink replaces VPNFilter

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

Background

The 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 US 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, NSA and FBI have previously attributed the Sandworm actor to the Russian GRU's Main Centre for Special Technologies GTsST. The malicious cyber activity below has previously been attributed to Sandworm:

- The BlackEnergy disruption of Ukrainian electricity in 2015
- Industroyer in 2016
- NotPetya in 2017
- Attacks against the Winter Olympics and Paralympics in 2018[1]
- A series of disruptive attacks against Georgia in 2019[2]

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

[1]https://www.ncsc.gov.uk/news/uk-and-partners-condemn-gru-cyber-attacks-against-olympic-an-paralympic-games

[2] https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks

This advisory summarises the VPNFilter malware it replaces, and provides more detail about 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 and can be read in parallel.

It also points to mitigation measures to help organisations that may be affected by this malware.

VPNFilter

First exposed in 2018

A series of articles published by Cisco Talos in 2018[1] 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 protocol 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 US Department of Justice linked the activity[2] to Sandworm, and announced its disruption of the botnet.

Activity since its exposure

A Trendmicro[3] blog in January 2021 detailed residual VPNFilter infections and provided data showing a reduction in requests to a known C2 domain. Since the disruption in May 2018, Sandworm has shown limited interest in existing VPNFilter footholds, instead preferring to retool.

[1] https://blog.talosintelligence.com/2018/05/VPNFilter.html

[2] https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected

[3] https://www.trendmicro.com/en_gb/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html

Cyclops Blink

Active since 2019

The NCSC, CISA, FBI and NSA, along with industry partners, have now identified a large-scale modular malware framework which is affecting 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,[1] but it is likely that Sandworm would be capable of compiling the malware for other architectures and firmware.

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.

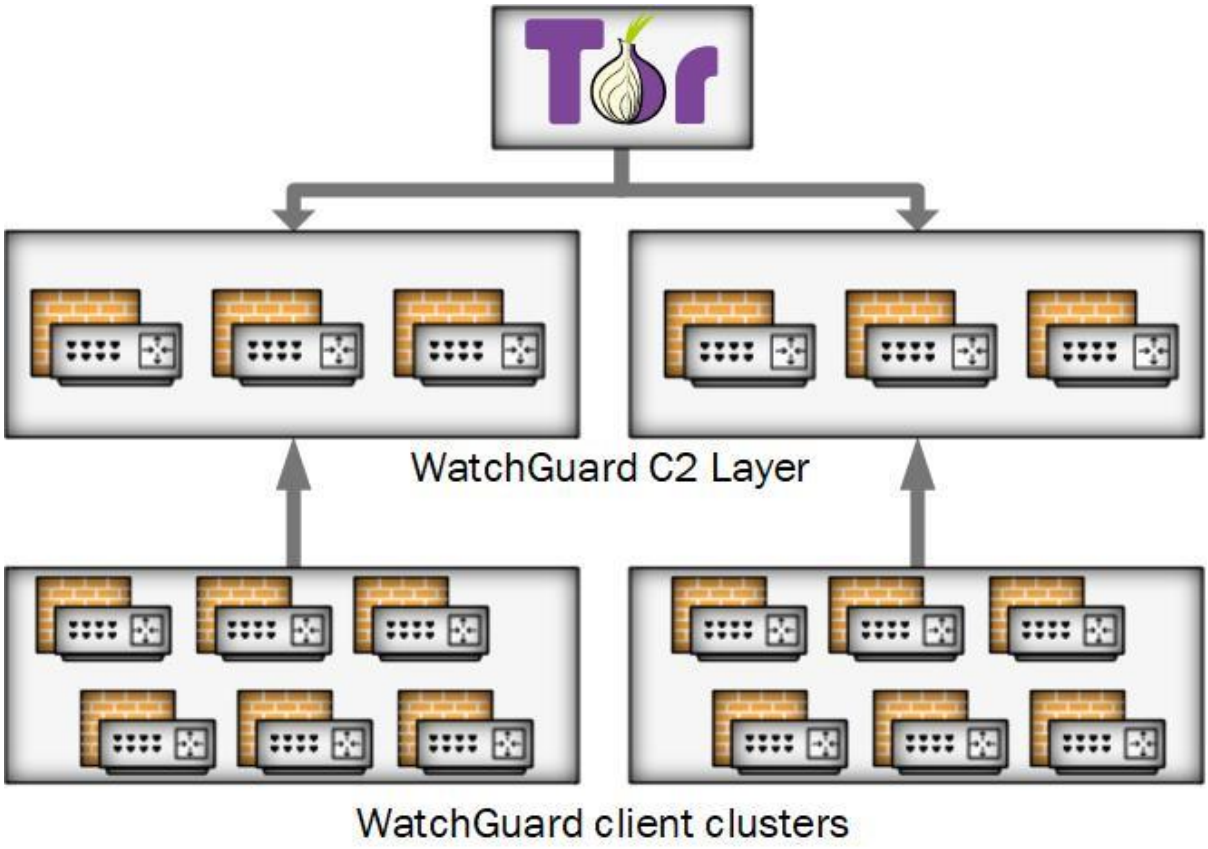
The NCSC has published a malware analysis report on Cyclops Blink which provides more detail about the malware.

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.

[1] Note that only WatchGuard devices that were reconfigured from the manufacture default settings to open remote management interfaces to external access could be infected.

Victim devices are organised 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:



Mitigation

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

WatchGuard has worked closely with the FBI, CISA 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.

WatchGuard tooling and guidance is available 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 organisations: https://www.ncsc.gov.uk/collection/passwords)
- 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 Initialisation Scripts: RC Scripts Cyclops Blink is executed on device startup, using a modified RC script
Defence 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

Conclusion

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

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

UK organisations affected by the activity outlined in this advisory should report any compromises to the NCSC via our website.

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 defence**. 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 analyse network intrusions. See NCSC guidance: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.
- **Prevent and detect lateral movement in your organisation'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' Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) and National Security Agency (NSA)

The United States' Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) and National Security Agency (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.

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