THREAT BULLETINS

Joint Cybersecurity Advisory: New Sandworm Malware Cyclops Blink Replaces VPNFilter

TLP:WHITE

Feb 23, 2022

The United Kingdom National Cyber Security Centre (NCSC), the United States Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) have identified that the actor known as Sandworm or Voodoo Bear is using a new malware, referred to here as Cyclops Blink.

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.

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).

Health-ISAC is issuing a threat bulletin regarding this alert, with additional technical details, indicators of compromise (IOCs), and remediations strategies attached. The original alert, AA22-054A: New Sandworm Malware Cyclops Blink Replaces VPNFilter, can be accessed here.

VPNFilter

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 a blog post that exposed VPNFilter and the US Department of Justice linked the activity to Sandworm and announced efforts to disrupt the botnet.

Cyclops Blink

The NCSC, CISA, the FBI, and NSA, along with industry partners, have now identified a large-scale modular malware framework that 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.

Post exploitation, Cyclops Blink is generally deployed as part of a firmware ‘update’. 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. 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), using individually generated keys and certificates. Sandworm manages Cyclops Blink by connecting to the C2 layer through the Tor network

Analysis

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
- A series of disruptive attacks against Georgia in 2019

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.

Reference(s)	NCSC, Gov.UK, US Department of Justice

Recommendations

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.

A variety of non-associated 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.

Sources
Alert (AA22-054A): New Sandworm Malware Cyclops Blink Replaces VPNFilter

BleepingComputer: US, UK Link New Cyclops Blink Malware to Russian State Hackers

The Record: US and UK Expose New Russian Malware Targeting Network Devices

Alert ID 1f8be291

View Alert

Tags Voodoo Bear, Cyclops Blink, Russian APT, Sandworm (Threat Actor), Sandworm hacking group, National Cyber Security Centre (NCSC) UK, NCSC Alert, National Cyber Security Centre (NCSC), National Security Agency (NSA), Sandworm, NCSC, National Cyber Security Centre, Cybersecurity And Infrastructure Security Agency, National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA)

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

CISA CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

FBI The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts may be identified at www.fbi.gov/contact-us/field. Contact CyWatch by telephone at 855-292-3937 or by email at CyWatch@fbi.gov.

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.