Hive Pro

THREAT ADVISORY

Sandworm Team using a new modular malware Cyclops Blink	TA2022059
Threat Level RED	**Publish Date –** Mar 16, 2022 **Updated Date –** April 7, 2022

The National Cyber Security Centre (NCSC) in the United Kingdom, the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) have discovered that the **Sandworm actor** is employing a new malware known as Cyclops Blink. Cyclops Blink looks to be a replacement framework for the VPNFilter virus, which was first discovered in 2018 and targeted network equipment such as SOHO routers and network attached storage (NAS) devices.

Cyclops Blink is a malicious Linux ELF program that has been developed for the PowerPC (big-endian) 32-bit architecture. It can maintain persistence all throughout the legitimate device firmware update process. The malware has implemented a modular architecture with a core component and is able to execute additional modules as child processes. It has built in modules for downloading or uploading data, extracting device information, and updating the virus and run upon startup. Underneath TLS, a custom binary protocol for command and control (C2) communication is used, and messages are individually encrypted. WatchGuard thinks the threat actor exploited a previously identified and fixed vulnerability (**CVE-2022-23176**) that was only available when firewall appliance management policies were set to enable unlimited management access from the Internet.
The vulnerability was resolved in these Fireware releases: Fireware v12.8, Fireware v12.7 Update 1, Fireware v12.7.2 Update 1 or later, Fireware v12.5.7 Update 3 or later, and Fireware v12.1.3 Update 5 or later.

The Mitre TTPs used by **Cyclops Blink** malware are:
TA0002 - Execution
TA0003 - Persistence
TA0005 - Defense Evasion
TA0007 - Discovery
TA0011 - Command and Control
TA0010 - Exfiltration
T1059.004: Command and Scripting Interpreter: Unix Shell
T1037.004: Boot or Logon Initialization Scripts: RC Scripts
T1542.001: Pre-OS Boot: System Firmware
T1562.004: Impair Defenses: Disable or Modify
T1036.005: Masquerading: Match Legitimate Name or Location
T1082: System Information Discovery
T1132.002: Data Encoding: NonStandard Encoding
T1008 Fallback Channels
T1071.001: Application Layer Protocol: Web Protocols
T1573.002: Encrypted Channel: Asymmetric Cryptography
T1571: Non-Standard Port
T1041: Exfiltration Over C2 Channel

Hive Pro

THREAT ADVISORY

Actor Details

Name	Origin	Target Locations	Target sectors	Motive
Sandworm Team (ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, VOODOO BEAR)	Russia	Azerbaijan, Belarus, France, Georgia, Iran, Israel, Kazakhstan, Kyrgyzstan, Lithuania, Poland, Russia, Ukraine	Education, Energy, Government, Telecommunications	Sabotage and destruction

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-23176	Watchguard Fire ware versions up to 11.7.1, 12.0.0-12.1.2and 12.2.0-12.5.6	cpe:2.3:o:watchguard :fireware:*:*:*:*:*:*: *:*	WATCHGUARD FIREBOX/XTM MANAGEMENT ACCESS CONTROL	CWE-269

Indicators of Compromise (IoCs)

Type	Value
MD5	D01e2c2e8df92edeb8298c55211bc4b6, Bbb76de7654337fb6c2e851d106cebc7, 3c9d46dc4e664e20f1a7256e14a33766, 3f22c0aeb1eec4350868368ea1cc798c
SHA-1	3adf9a59743bc5d8399f67cab5eb2daf28b9b863, C59bc17659daca1b1ce65b6af077f86a648ad8a8, 7d61c0dd0cd901221a9dff9df09bb90810754f10, 438cd40caca70cafe5ca436b36ef7d3a6321e858
SHA-256	50df5734dd0c6c5983c21278f119527f9fdf6ef1d7e808a29754ebc5253e9a86, c082a9117294fa4880d75a2625cf80f63c8bb159b54a7151553969541ac35862, 4e69bbb61329ace36fbe62f9fb6ca49c37e2e5a5293545c44d155641934e39d1, Ff17ccd8c96059461710711fcc8372cfea5f0f9eb566ceb6ab709ea871190dc6, 88e568afd69fbc944a8d8268e41f2f6100e8bb007083175884ea4149033f4fcf, cc3d51578a9dcc7e955061881490e54883904956f5ca5ee2918cd3b249415e59, d186f553ad6b38951fdebabfe7ecb4ca6d86ac702a9e8c90a338ad668afdf490, fc1e50172c0ce221452b967d1ef705f11bbfe2d54c533d68bd2a7a094605df2d, 82c3f5092d45ce0e19ac42adaf6632b954b8e78d399f673724956a89c1826d7b, 6f4ee4e05483ca3db54040506ac21a2b49d2bd12379cafad54764907be228556, 4ec5e0c5dccc5891d39ea76e3c3d3e26d8830d7aa4d63db6084dbfbec6f0d211, 3830213049d64b09f637563faa470b0f2edd0034aa9e92f7908374bd1d6df116, 36b3a9dcb283fb0f9fd45f4a371006228d206ec0bdd9e3392eb2d07e72f8d7b0
Filename	rootfs_cfg
IPs	100.43.220[.]234, 96.80.68[.]193, 188.152.254[.]170, 208.81.37[.]50, 70.62.153[.]174,

Indicators of Compromise (IoCs)

Type	Value
IPs	2.230.110[.]137, 90.63.245[.]175, 212.103.208[.]182, 50.255.126[.]65, 78.134.89[.]167, 81.4.177[.]118, 24.199.247[.]222, 37.99.163[.]162, 37.71.147[.]186, 105.159.248[.]137, 80.155.38[.]210, 217.57.80[.]18, 151.0.169[.]250, 212.202.147[.]10, 212.234.179[.]113, 185.82.169[.]99, 93.51.177[.]66,

Patch

Fireware Release Notes - Upgrade to Fireware v12.7 Update 1 (watchguard.com)

References

https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf
https://techsearch.watchguard.com/KB?type=Article&SFDCID=kA16S000000SOCGSA4&lang=en_US