US disrupts Russian Cyclops Blink botnet before being used in attacks

bleepingcomputer.com/news/security/us-disrupts-russian-cyclops-blink-botnet-before-being-used-in-attacks/

Sergiu Gatlan

By
Sergiu Gatlan

- April 6, 2022
- 11:46 AM
- 0

US government officials announced today the disruption of the Cyclops Blink botnet controlled by the Russian-backed Sandworm hacking group before being used in attacks.

The malware, used by Sandworm to create this botnet since at least June 2019, is targeting WatchGuard Firebox firewall appliances and multiple ASUS router models.

Cyclops Blink enables the attackers to establish persistence on the device through firmware updates, providing remote access to compromised networks.

This malware is modular, making it easy to upgrade to target new devices and tap into new pools of exploitable hardware.

"We are announcing today [..] the disruption of a global botnet controlled by the Russian military intelligence agency, commonly known as the GRU," US Attorney General Merrick Garland said.

"The Russian government has recently used similar infrastructure to attack Ukrainian targets. Fortunately, we were able to disrupt this botnet before it could be used.

"Thanks to our close work with international partners we were able to detect the infection of thousands of network hardware devices. We were then able to disable the GRU's control over those devices before the botnet could be weaponized."

Watch Video At:

https://youtu.be/lwJpfC2a3qM

Malware removed from infected Watchguard and Asus devices

Following this US Justice Department operation's initial March 18 court authorization, the malware was removed from all remaining identified Watchguard devices acting as command and control servers.

The FBI has also notified owners of compromised devices in the United States and abroad through foreign law enforcement partners before removing the Cyclops Blink malware. US victims whose contact info was not found were contacted by their providers following notices issued by the FBI.

FBI Director Chris Wray said the botnet was disrupted following close cooperation with Watchguard while analyzing the malware and developing detection tools and remediation techniques.

"I should caution that as we move forward, any Firebox devices that acted as bots, may still remain vulnerable in the future until mitigated by their owners. So those owners should still go ahead and adopt Watchguard's detection and remediation steps as soon as possible," FBI Director Chris Wray added.

"Sandworm strung them together to use their computing power in a way that would obfuscate who was really running the network and let them launch malware or to orchestrate distributed denial of service attacks, like the GRU has already used to attack Ukraine."

WatchGuard has shared detailed instructions on how to restore compromised Firebox appliances to a clean state to remediate the infection and update them to the latest Fireware OS version to prevent future infections.

> WatchGuard played an important role in eliminating the threat posed by Cyclops Blink, with the rapid release of detection and remediation tools to protect its partners and customers following the government disclosure of the malware, and by cooperating with the U. S. Department of Justice in its effort to disrupt the botnet. The company's close collaboration with its partner and customer communities was instrumental in mitigating this sophisticated state-sponsored threat, which affected less than 1% of WatchGuard appliances. — WatchGuard spokesperson

The Sandworm Russian-backed threat group

Sandworm (also tracked as Voodoo Bear, BlackEnergy, and TeleBots), the group behind the Cyclops Blink botnet, is a Russian-sponsored hacking group active since the mid-2000s.

Its operators are believed to be Russian military hackers part of Unit 74455 of the Russian GRU's Main Center for Special Technologies (GTsST).

Sandworm was linked to the BlackEnergy malware behind blackouts in Ukraine in 2015 and 2016 [1, 2, 3], the KillDisk wiper attacks against Ukrainian banks, and highly destructive NotPetya ransomware used to inflict billions worth of damage to companies worldwide starting with June 2017.

"Sandworm is the premier Russian cyber attack capability and one of the actors we have been most concerned about in light of the invasion," John Hultquist, Mandiant VP of Intelligence Analysis, told BleepingComputer.

"We are concerned that they could be used to hit targets in Ukraine, but we are also concerned they may hit targets in the West in retribution for the pressure being placed on Russia."

Related Articles:

US, UK link new Cyclops Blink malware to Russian state hackers

REvil ransomware returns: New malware sample confirms gang is back

US and allies warn of Russian hacking threat to critical infrastructure

US eases sanctions that may lead to Russia's Internet isolation

FTC fines Twitter $150M for using 2FA info for targeted advertising