Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU)

justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation

April 6, 2022

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, April 6, 2022

Operation Copied and Removed Malware Known as "Cyclops Blink" from the Botnet's Command-And-Control Devices, Disrupting the GRU's Control Over Thousands of Infected Devices Worldwide. Victims Must Take Additional Steps to Remediate the Vulnerability and Prevent Malicious Actors From Further Exploiting Unpatched Devices.

The Justice Department today announced a court-authorized operation, conducted in March 2022, to disrupt a two-tiered global botnet of thousands of infected network hardware devices under the control of a threat actor known to security researchers as Sandworm, which the U.S. government has previously attributed to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (the GRU). The operation copied and removed malware from vulnerable internet-connected firewall devices that Sandworm used for command and control (C2) of the underlying botnet. Although the operation did not involve access to the Sandworm malware on the thousands of underlying victim devices worldwide, referred to as "bots," the disabling of the C2 mechanism severed those bots from the Sandworm C2 devices' control.

“This court-authorized removal of malware deployed by the Russian GRU demonstrates the department’s commitment to disrupt nation-state hacking using all of the legal tools at our disposal,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “By working closely with WatchGuard and other government agencies in this country and the United Kingdom to analyze the malware and to develop detection and remediation tools, we are together showing the strength that public-private partnership brings to our country’s cybersecurity. The department remains committed to confronting and disrupting nation-state hacking, in whatever form it takes.”

“Through close collaboration with WatchGuard and our law enforcement partners, we identified, disrupted and exposed yet another example of the Russian GRU’s hacking of innocent victims in the United States and around the world,” said U.S. Attorney Cindy K. Chung for the Western District of Pennsylvania. “Such activities are not only criminal but also threaten the national security of the United States and its allies. My office remains committed to working with our partners in the National Security Division, the FBI, foreign law enforcement agencies and the private sector to defend and maintain our nation’s cybersecurity.”

“This operation is an example of the FBI’s commitment to combatting cyber threats through our unique authorities, capabilities, and coordination with our partners,” said Assistant Director Bryan Vorndran of the FBI’s Cyber Division. “As the lead domestic law enforcement and intelligence agency, we will continue pursuing cyber actors that threaten the national security and public safety of the American people, our private sector partners and our international partners.”

“The FBI prides itself on working closely with our law enforcement and private sector partners to expose criminals who hide behind their computer and launch attacks that threaten Americans’ safety, security and confidence in our digitally connected world,” said Special Agent in Charge Mike Nordwall of the FBI’s Pittsburgh Field Office. “The FBI has an unwavering commitment to combat and disrupt Russia’s efforts to gain a foothold inside U.S. and allied networks.”

On Feb. 23, the United Kingdom’s National Cyber Security Centre, the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency, the FBI and the National Security Agency released an advisory identifying the Cyclops Blink malware, which targets network devices manufactured by WatchGuard Technologies Inc. (WatchGuard) and ASUSTek Computer Inc. (ASUS). These network devices are often located on the perimeter of a victim’s computer network, thereby providing Sandworm with the potential ability to conduct malicious activities against all computers within those networks. As explained in the advisory, the malware appeared to have emerged as early as June 2019, and was the apparent successor to another Sandworm botnet called VPNFilter, which the Department of Justice disrupted through a court-authorized operation in 2018.

The same day as the advisory, WatchGuard released detection and remediation tools for users of WatchGuard devices. The advisory and WatchGuard's guidance both recommended that device owners deploy WatchGuard's tools to remove any malware infection and patch their devices to the latest versions of available firmware. Later, ASUS released its own guidance to help compromised ASUS device owners mitigate the threat posed by Cyclops Blink malware. The public and private sector efforts were effective, resulting in the successful remediation of thousands of compromised devices. However, by mid-March, a majority of the originally compromised devices remained infected.

Following the initial court authorization on March 18, the department's operation was successful in copying and removing the malware from all remaining identified C2 devices. It also closed the external management ports that Sandworm was using to access those C2 devices, as recommended in WatchGuard's remediation guidance (a non-persistent change that the owner of an affected device can reverse through a device restart). These steps had the immediate effect of preventing Sandworm from accessing these C2 devices, thereby disrupting Sandworm's control of the infected bot devices controlled by the remediated C2 devices. However, WatchGuard and ASUS devices that acted as bots may remain vulnerable to Sandworm if device owners do not take the WatchGuard and ASUS recommended detection and remediation steps. The department strongly encourages network defenders and device owners to review the Feb. 23 advisory and WatchGuard and ASUS releases.

The operation announced today leveraged direct communications with the Sandworm malware on the identified C2 devices and, other than collecting the underlying C2 devices' serial numbers through an automated script and copying the C2 malware, it did not search for or collect other information from the relevant victim networks. Further, the operation did not involve any FBI communications with bot devices.

Since prior to the Feb. 23 advisory, the FBI has been attempting to provide notice to owners of infected WatchGuard devices in the United States and, through foreign law enforcement partners, abroad. For those domestic victims whose contact information was not publicly available, the FBI has contacted providers (such as a victim's internet service provider) and has asked those providers to provide notice to the victims. As required by the terms of the court authorization, the FBI has provided notice to the owners of the domestic C2 devices from which the FBI copied and removed the Cyclops Blink malware.

The efforts to disrupt the Cyclops Blink botnet were led by the FBI's Pittsburgh, Atlanta and Oklahoma City Field Offices, the FBI Cyber Division, the National Security Division's Counterintelligence and Export Control Section, and the U.S. Attorney's Office for the Western District of Pennsylvania. Assistance was also provided by the Criminal Division's Computer Crime and Intellectual Property Section and Office of International Affairs, as well as the U.S. Attorney's Office for the Eastern District of California.

If you believe you have a compromised device, please contact your local FBI Field Office for assistance. The FBI continues to conduct a thorough and methodical investigation into this cyber incident.