Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices

justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected

May 23, 2018

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, May 23, 2018

Additional action necessary worldwide to remediate the botnet.

The Justice Department today announced an effort to disrupt a global botnet of hundreds of thousands of infected home and office (SOHO) routers and other networked devices under the control of a group of actors known as the “Sofacy Group” (also known as “apt28,” “sandworm,” “x-agent,” “pawn storm,” “fancy bear” and “sednit”). The group, which has been operating since at least in or about 2007, targets government, military, security organizations, and other targets of perceived intelligence value.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney Scott W. Brady for the Western District of Pennsylvania, Assistant Director Scott Smith for the FBI’s Cyber Division, FBI Special Agent in Charge Robert Johnson of the Pittsburgh Division and FBI Special Agent in Charge David J. LeValley of the Atlanta Division made the announcement.

“The Department of Justice is committed to disrupting, not just watching, national security cyber threats using every tool at our disposal, and today’s effort is another example of our commitment to do that,” said Assistant Attorney General Demers. “This operation is the first step in the disruption of a botnet that provides the Sofacy actors with an array of capabilities that could be used for a variety of malicious purposes, including intelligence gathering, theft of valuable information, destructive or disruptive attacks, and the misattribution of such activities.”

“The United States Attorney’s Office will continue to aggressively fight against threats to our national security by criminals, no matter who they work for” said U.S. Attorney Brady. “This court-ordered seizure will assist in the identification of victim devices and disrupts the ability of these hackers to steal personal and other sensitive information and carry out disruptive cyber attacks. We will be relentless in protecting the people of Western Pennsylvania - from international corporations to local businesses to the elderly - from these threats.”

“Today's announcement highlights the FBI's ability to take swift action in the fight against cybercrime and our commitment to protecting the American people and their devices,” said Assistant Director Scott Smith. “By seizing a domain used by malicious cyber actors in their botnet campaign, the FBI has taken a critical step in minimizing the impact of the malware attack. While this is an important first step, the FBI's work is not done. The FBI, along with our domestic and international partners, will continue our efforts to identify and expose those responsible for this wave of malware.”

“The FBI will not allow malicious cyber actors, regardless of whether they are state-sponsored, to operate freely,” said FBI Special Agent in Charge Bob Johnson. “These hackers are exploiting vulnerabilities and putting every American’s privacy and network security at risk. Although there is still much to be learned about how this particular threat initially compromises infected routers and other devices, we encourage citizens and businesses to keep their network equipment updated and to change default passwords.”

“This action by the FBI, DOJ, and our partners should send a clear message to our adversaries that the U.S. Government will take action to mitigate the threats posed by them and to protect our citizens and our allies even when the possibility of arrest and prosecution may not be readily available,” said FBI Special Agent in Charge David J. LeValley. “As our adversaries’ technical capabilities evolve, the FBI and its partners will continue to rise to the challenge, placing themselves between the adversaries and their intended victims.”

The botnet, referred to by the FBI and cyber security researchers as “VPNFilter,” targets SOHO routers and network-access storage (NAS) devices, which are hardware devices made up of several hard drives used to store data in a single location that can be accessed by multiple users. The VPNFilter botnet uses several stages of malware. Although the second stage of malware, which has the malicious capabilities described above, can be cleared from a device by rebooting it, the first stage of malware persists through a reboot, making it difficult to prevent reinfection by the second stage.

In order to identify infected devices and facilitate their remediation, the U.S. Attorney's Office for the Western District of Pennsylvania applied for and obtained court orders, authorizing the FBI to seize a domain that is part of the malware's command-and-control infrastructure. This will redirect attempts by stage one of the malware to reinfect the device to an FBI-controlled server, which will capture the Internet Protocol (IP) address of infected devices, pursuant to legal process. A non-profit partner organization, The Shadowserver Foundation, will disseminate the IP addresses to those who can assist with remediating the VPNFilter botnet, including foreign CERTs and internet service providers (ISPs).

Owners of SOHO and NAS devices that may be infected should reboot their devices as soon as possible, temporarily eliminating the second stage malware and causing the first stage malware on their device to call out for instructions. Although devices will remain vulnerable to reinfection with the second stage malware while connected to the Internet, these efforts maximize opportunities to identify and remediate the infection worldwide in the time available before Sofacy actors learn of the vulnerability in their command-and-control infrastructure.

The FBI and the Department of Homeland Security have also jointly notified trusted ISPs. The Department and the FBI also encourage users and administrators to review the Cisco blog post on VPNFilter, available **HERE**, for recommendations and to ensure that their devices are updated with the latest patches.

The efforts to disrupt the VPNFilter botnet were led by the FBI's Pittsburgh and Atlanta Offices; FBI Cyber Division; Trial Attorney Matthew Chang of the National Security Division's Counterintelligence and Export Control Section; and Assistant U.S. Attorneys Charles Eberle and Soo C. Song of the Western District Pennsylvania. Critical assistance was also provided by Richard Green of the Criminal Division's Computer Crime and Intellectual Property Section and The Shadowserver Foundation.

Note: The documents filed by the Government as well as the court orders entered in this case are available as attachments below.