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

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

February 15, 2024

Press Release

A January 2024 court-authorized operation has neutralized a network of hundreds of small office/home office (SOHO) routers that GRU Military Unit 26165, also known as APT 28, Sofacy Group, Forest Blizzard, Pawn Storm, Fancy Bear, and Sednit, used to conceal and otherwise enable a variety of crimes. These crimes included vast spearphishing and similar credential harvesting campaigns against targets of intelligence interest to the Russian government, such as U.S. and foreign governments and military, security, and corporate organizations. In recent months, allegations of Unit 26165 activity of this type has been the subject of a private sector cybersecurity advisory and a Ukrainian government warning.

This botnet was distinct from prior GRU and Russian Federal Security Service (FSB) malware networks disrupted by the Department in that the GRU did not create it from scratch. Instead, the GRU relied on the "Moobot" malware, which is associated with a known criminal group. Non-GRU cybercriminals installed the Moobot malware on Ubiquiti Edge OS routers that still used publicly known default administrator passwords. GRU hackers then used the Moobot malware to install their own bespoke scripts and files that repurposed the botnet, turning it into a global cyber espionage platform.

The Department's court-authorized operation leveraged the Moobot malware to copy and delete stolen and malicious data and files from compromised routers. Additionally, in order to neutralize the GRU's access to the routers until victims can mitigate the compromise and reassert full control, the operation reversibly modified the routers' firewall rules to block

remote management access to the devices, and during the course of the operation, enabled temporary collection of non-content routing information that would expose GRU attempts to thwart the operation.

“The Justice Department is accelerating our efforts to disrupt the Russian government’s cyber campaigns against the United States and our allies, including Ukraine,” said Attorney General Merrick B. Garland. “In this case, Russian intelligence services turned to criminal groups to help them target home and office routers, but the Justice Department disabled their scheme. We will continue to disrupt and dismantle the Russian government’s malicious cyber tools that endanger the security of the United States and our allies.”

“For the second time in two months, we’ve disrupted state-sponsored hackers from launching cyber-attacks behind the cover of compromised U.S. routers,” said Deputy Attorney General Lisa Monaco. “We will continue to leverage all of our legal authorities to prevent harm and protect the public — whether the hackers are from Russia, China, or another global threat.”

“Russia’s GRU continues to maliciously target the United States through their botnet campaigns,” said FBI Director Christopher Wray. “The FBI utilized its technical capabilities to disrupt Russia’s access to hundreds of routers belonging to individuals in addition to small and home offices. This type of criminal behavior is simply unacceptable, and the FBI, in coordination with our federal and international partners, will not allow for any of Russia’s services to negatively impact the American people and our allies.”

“In this unique, two-for-one operation, the National Security Division and its partners disrupted a botnet used by both criminal and state-sponsored actors,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division. “Notably, this represents the third time since Russia’s unjustified invasion of Ukraine that the Department has stripped the Russian intelligence services of a key tool used to further the Kremlin’s acts of aggression and other malicious activities. We will continue to use our legal authorities and cutting-edge techniques, and to draw on the strength of our partnerships, to protect the public and our allies from such threats.”

“This is yet another case of Russian military intelligence weaponizing common devices and technologies for that government’s malicious aims,” said U.S. Attorney Jacqueline C. Romero for the Eastern District of Pennsylvania. “As long as our nation-state adversaries continue to threaten U.S. national security in this way, we and our partners will use every tool available to disrupt their cyber thugs — whomever and wherever they are.”

“Operation Dying Ember was an international effort led by FBI Boston to remediate over a thousand compromised routers belonging to unsuspecting victims here in the United States, and around the world that were targeted by malicious, nation state actors in Russia to facilitate their strategic intelligence collection,” said Special Agent in Charge Jodi Cohen of

the FBI Boston Field Office. “The FBI’s strong partnerships with the private sector were critical to identifying and addressing this threat which targeted our national security interests here and abroad. This operation should make it crystal clear to our adversaries that we will not allow anyone to exploit our technology and networks.”

As described in court documents, the government extensively tested the operation on the relevant Ubiquiti Edge OS routers. Other than stymieing the GRU’s ability to access to the routers, the operation did not impact the routers’ normal functionality or collect legitimate user content information. Additionally, the court-authorized steps to disconnect the routers from the Moobot network are temporary in nature; users can roll back the firewall rule changes by undertaking factory resets of their routers or by accessing their routers through their local network (e.g., via the routers’ web-based user interface). However, a factory reset that is not also accompanied by a change of the default administrator password will return the router to its default administrator credentials, leaving the router open to reinfection or similar compromises.

The FBI Philadelphia and Boston Field Offices and Cyber Division, U.S. Attorney’s Office for the Eastern District of Pennsylvania, and the National Security Division’s National Security Cyber Section led the disruption effort. The Criminal Division’s Computer Crime and Intellectual Property Section and Office of International Affairs, Shadowserver Foundation, Microsoft Threat Intelligence, and other partners provided valuable assistance.

The FBI is working with internet service providers to provide notice of the operation to owners and operators of SOHO routers covered by the court’s authorization. If you believe you have a compromised router, please visit the FBI’s Internet Crime Complaint Center.

To better protect themselves, the FBI advises all victims to conduct the following remediation steps:

1. Perform a hardware factory reset to flush the file systems of malicious files;
2. Upgrade to the latest firmware version;
3. Change any default usernames and passwords; and
4. Implement strategic firewall rules to prevent the unwanted exposure of remote management services.

The FBI strongly encourages router owners to avoid exposing their devices to the internet until they change the default passwords.

Updated February 15, 2024

Attachment
redacted_warrant_and_affidavit.pdf [PDF,]
Topic

National Security

Press Release Number: 24-179