Russian Botnet Disrupted in International Cyber Operation

Published: 2022-06-16 · Archived: 2026-04-07 02:08:28 UTC

Assistant U. S. Attorney Jonathan I. Shapiro (619) 546-8225

NEWS RELEASE SUMMARY – June 16, 2022

SAN DIEGO – The U.S. Department of Justice, together with law enforcement partners in Germany, the Netherlands and the United Kingdom, have dismantled the infrastructure of a Russian botnet known as RSOCKS which hacked millions of computers and other electronic devices around the world.

A botnet is a group of hacked internet-connected devices that are controlled as a group without the owner's knowledge and typically used for malicious purposes. Every device that is connected to the internet is assigned an Internet Protocol (IP) address.

According to a search warrant affidavit, unsealed today in the Southern District of California, and the operators' own claims, the RSOCKS botnet, operated by Russian cybercriminals, comprised millions of hacked devices worldwide. The RSOCKS botnet initially targeted Internet of Things (IoT) devices. IoT devices include a broad range of devices—including industrial control systems, time clocks, routers, audio/video streaming devices, and smart garage door openers, which are connected to, and can communicate over, the internet, and therefore, are assigned IP addresses. The RSOCKS botnet expanded into compromising additional types of devices, including Android devices and conventional computers.

"The RSOCKS botnet compromised millions of devices throughout the world," said U.S. Attorney Randy Grossman. "Cyber criminals will not escape justice regardless of where they operate. Working with public and private partners around the globe, we will relentlessly pursue them while using all the tools at our disposal to disrupt their threats and prosecute those responsible." Grossman thanked the prosecution team, the FBI and the Department of Justice Criminal Division's Computer Crimes and Intellectual Property Section for their excellent work on this case.

"This operation disrupted a highly sophisticated Russia-based cybercrime organization that conducted cyber intrusions in the United States and abroad," said FBI Special Agent in Charge Stacey Moy. "Our fight against cybercriminal platforms is a critical component in ensuring cybersecurity and safety in the United States. The actions we are announcing today are a testament to the FBI's ongoing commitment to pursuing foreign threat actors in collaboration with our international and private sector partners."

A legitimate proxy service provides IP addresses to its clients for a fee. Typically, the proxy service provides access to IP addresses that it leases from internet service providers (ISPs). Rather than offer proxies that RSOCKS had leased, the RSOCKS botnet offered its clients access to IP addresses assigned to devices that had been hacked. The owners of these devices did not give the RSOCKS operator(s) authority to access their devices in order to use their IP addresses and route internet traffic. A cybercriminal who wanted to utilize the RSOCKS platform could use a web browser to navigate to a web-based "storefront" (*i.e.*, a public web site that allows users to purchase

access to the botnet), which allowed the customer to pay to rent access to a pool of proxies for a specified daily, weekly, or monthly time period. The cost for access to a pool of RSOCKS proxies ranged from $30 per day for access to 2,000 proxies to $200 per day for access to 90,000 proxies.

Once purchased, the customer could download a list of IP addresses and ports associated with one or more of the botnet's backend servers. The customer could then route malicious internet traffic through the compromised victim devices to mask or hide the true source of the traffic. It is believed that the users of this type of proxy service were conducting large scale attacks against authentication services, also known as credential stuffing, and anonymizing themselves when accessing compromised social media accounts, or sending malicious email, such as phishing messages.

As alleged in the unsealed warrant, FBI investigators used undercover purchases to obtain access to the RSOCKS botnet in order to identify its backend infrastructure and its victims. The initial undercover purchase in early 2017 identified approximately 325,000 compromised victim devices throughout the world with numerous devices located within San Diego County. Through analysis of the victim devices, investigators determined that the RSOCKS botnet compromised the victim device by conducting brute force attacks. The RSOCKS backend servers maintained a persistent connection to the compromised device. Several large public and private entities have been victims of the RSOCKS botnet, including a university, a hotel, a television studio, and an electronics manufacturer, as well as home businesses and individuals. At three of the victim locations, with consent, investigators replaced the compromised devices with government-controlled computers (i.e., honeypots), and all three were subsequently compromised by RSOCKS. The FBI identified at least six victims in San Diego.

This case was investigated by the FBI and is being prosecuted by Assistant U.S. Attorney Jonathan I. Shapiro of the Southern District of California and Ryan K.J. Dickey, Senior Counsel for the Department of Justice Criminal Division's Computer Crimes and Intellectual Property Section. The Department of Justice extends its appreciation to the authorities of Germany, the Netherlands, and the United Kingdom, the Justice Department's Office of International Affairs and private sector cybersecurity company Black Echo, LLC for their assistance provided throughout the investigation.

In September 2020, FBI Director Christopher Wray announced the FBI's new strategy for countering cyber threats. The strategy focuses on imposing risk and consequences on cyber adversaries through the FBI's unique authorities, world-class capabilities, and enduring partnerships. Victims are encouraged to report the incident online with the Internet Crime Complaint Center (IC3) www.ic3.gov.
