Feds seize 13 more DDoS-for-hire platforms in ongoing international crackdown



Enlarge / A domain seizure notice from the Justice Department, showing the national seals of several other governments.

reader comments

21 with

The US Justice Department has sized the domains of 13 DDoS-for-hire services as part of an ongoing initiative for combatting the Internet menace.

The providers of these illicit services platforms describe them as “booter” or “stressor” services that allow site admins to test the robustness and stability of their infrastructure. Almost, if not all, are patronized by people out to exact revenge on sites they don’t like or to further extortion, bribes, or other forms of graft.

The international law enforcement initiative is known as Operation PowerOFF. In December, federal authorities seized another 48 domains. Ten of them returned with new domains, many that closely resembled their previous names.

“Ten of the 13 domains seized today are reincarnations of services that were seized during a prior sweep in December, which targeted 48 top booter services,” the Justice Department said. “For example, one of the domains seized this week—cyberstress.org—appears to be the same service operated under the domain cyberstress.us, which was seized in December. While many of the previously disrupted booter services have not returned, today’s action reflects law enforcement’s commitment to targeting those operators who have chosen to continue their criminal activities.”

According to a seizure warrant filed in federal court, the FBI used live accounts available through the services to take down sites with high-capacity bandwidth that were under FBI control.

Advertisement

“The FBI tested each of the services associated with the SUBJECT DOMAINS, meaning that agents or other personnel visited each of the websites and either used previous login information or registered a new account on the service to conduct attacks,” FBI Special Agent Elliott Peterson wrote in the affidavit. “I believe that each of the SUBJECT DOMAINS is being used to facilitate the commission of attacks against unwitting victims to prevent the victims from accessing the Internet, to disconnect the victim from or degrade communication with established Internet connections, or to cause other similar damage.”

The Justice Department also said in Monday’s announcement that four of the defendants charged in December pleaded guilty earlier this year. Those defendants and their pleas are:

- Jeremiah Sam Evans Miller, aka “John The Dev,” 23, of San Antonio, Texas, pleaded guilty on April 6 to conspiracy and violating the computer fraud and abuse act related to the operation of a booter service named RoyalStresser.com (formerly known as Supremesecurityteam.com);
- Angel Manuel Colon Jr., aka “Anonghost720” and “Anonghost1337,” 37, of Belleview, Florida, pleaded guilty on February 13 to conspiracy and violating the computer fraud and abuse act related to the operation of a booter service named SecurityTeam.io;
- Shamar Shattock, 19, of Margate, Florida, pleaded guilty on March 22 to conspiracy to violate the computer fraud and abuse act related to the operation of a booter service known as Astrostress.com; and
- Cory Anthony Palmer, 23, of Lauderhill, Florida, pleaded guilty on February 16 to conspiracy to violate the computer fraud and abuse act related to the operation of a booter service known as Booter.sx.

DDoS refers to distributed denial-of-service attacks, in which hundreds of thousands of sites simultaneously direct torrents of junk traffic at a given site to cause it to “deny service” to normal users.

https://arstechnica.com/?p=1937636