

Two Individuals Sentenced for Providing “Bulletproof Hosting” for Cybercriminals

 justice.gov/opa/pr/two-individuals-sentenced-providing-bulletproof-hosting-cybercriminals

October 20, 2021



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, October 20, 2021

Two Eastern European men were sentenced for providing “bulletproof hosting” services, which were used by cybercriminals between 2009 to 2015 to distribute malware and attack financial institutions and victims throughout the United States.

On June 28 and Oct. 20, Chief Judge Denise Page Hood of the U.S. District Court for the Eastern District of Michigan sentenced Pavel Stassi, 30, of Estonia, to 24 months in prison; and Aleksandr Skorodumov, 33, of Lithuania, to 48 months in prison, for their roles in the scheme.

According to court documents, Stassi and Skorodumov were members of a bulletproof hosting organization founded and led by two co-defendants, Aleksandr Grichishkin and Andrei Skvortsov, both 34 and of Russia. The group rented IP addresses, servers, and domains to cybercriminal clients who employed this technical infrastructure to disseminate malware used to gain access to victims’ computers, form botnets, and steal banking credentials for use in frauds. Malware hosted by the organization included Zeus, SpyEye, Citadel, and the Blackhole Exploit Kit, which attacked U.S. companies and financial institutions between 2009 and 2015 and caused or attempted to cause millions of dollars in losses to U.S. victims. The defendants also helped their clients evade detection by law

enforcement and continue their crimes uninterrupted by monitoring sites used to blocklist technical infrastructure used for crime, moving “flagged” content to new infrastructure, and registering all such infrastructure under false or stolen identities.

“Cybercrime presents a serious and persistent threat to the United States, and these prosecutions send a clear message that ‘bulletproof hosters’ who purposely aid other cybercriminals are responsible, and will be held accountable, for the harms their criminal clients cause within our borders,” said Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department’s Criminal Division.

“Given their international nature, and the anonymity of the internet, cybercrime investigations often take years,” said Acting U.S. Attorney Saima Mohsin for the Eastern District of Michigan. “They can require the resources of multiple law enforcement agencies, the cooperation of multiple governments, skilled interpreters, and time-consuming extradition procedures. The persistence and hard work of our law enforcement partners has led to these successful prosecutions and sends a message to cybercriminals that they will be brought to justice.”

“Over the course of many years, the defendants facilitated the transnational criminal activity of a vast network of cybercriminals throughout the world by providing them a safe-haven to anonymize their criminal activity,” said Special Agent in Charge Timothy Waters of the FBI’s Detroit Field Office. “This resulted in millions of dollars of losses to U.S. victims. Cybercriminals may believe they are beyond the reach of the FBI and our international partners, but today’s proceeding proves that anyone who facilitates or profits from criminal cyber activity will be brought to justice.”

According to court filings and statements made in connection with the defendants’ guilty pleas, Skorodumov was one of the organization’s lead systems administrators and, at some points, its only systems administrator. In this role, he configured and managed the clients’ domains and IP addresses, provided technical assistance to help clients optimize their malware and botnets, and monitored and responded to abuse notices. Stassi undertook various administrative tasks for the organization, including conducting and tracking online marketing to the organization’s criminal clientele and using stolen and/or false personal information to register webhosting and financial accounts used by the organization.

Stassi, Skorodumov, Grichishkin and Skvortsov each pleaded guilty to one count of Racketeer Influenced and Corrupt Organizations (RICO) conspiracy. Grichishkin and Skvortsov are pending sentencing and face a maximum penalty of 20 years in prison. A federal district court judge will determine each sentence after considering the U.S. Sentencing Guidelines and other statutory factors.

The FBI investigated the case with critical assistance from law enforcement partners in Germany, Estonia and the United Kingdom.

Senior Counsel Louisa K. Marion of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Patrick E. Corbett of the Eastern District of Michigan prosecuted the case. The Justice Department's Office of International Affairs provided substantial assistance.