


Four Individuals Plead Guilty to RICO Conspiracy Involving “Bulletproof Hosting” for Cybercriminals

 [justice.gov/opa/pr/four-individuals-plead-guilty-rico-conspiracy-involving-bulletproof-hosting-cybercriminals](https://www.justice.gov/opa/pr/four-individuals-plead-guilty-rico-conspiracy-involving-bulletproof-hosting-cybercriminals)

May 7, 2021



Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Friday, May 7, 2021

Four Eastern European nationals have pleaded guilty to conspiring to engage in a Racketeer Influenced Corrupt Organization (RICO) arising from their providing “bulletproof hosting” services between 2008 and 2015, which were used by cybercriminals to distribute malware and attack financial institutions and victims throughout the United States.

According to court documents, Aleksandr Grichishkin, 34, and Andrei Skvortsov, 34, of Russia; Aleksandr Skorodumov, 33, of Lithuania; and Pavel Stassi, 30, of Estonia, were founders and/or members of a bulletproof hosting organization. The group rented Internet Protocol (IP) addresses, servers, and domains to cybercriminal clients, who used 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 rampantly 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. A key service provided by the defendants was helping their clients to evade detection by law enforcement and continue their crimes uninterrupted; the defendants did so by monitoring sites used to blacklist technical infrastructure used for crime, moving “flagged” content to new infrastructure, and registering all such infrastructure under false or stolen identities.

“Every day, transnational organized cybercriminals deploy malware that ravages our economy and victimizes our citizens and businesses,” said Acting Assistant Attorney General Nicholas L. McQuaid of the Justice Department’s Criminal Division. “The criminal organizations that purposefully aid these actors — the so-called bulletproof hosters, money launderers, purveyors of stolen identity information, and the like — are no less responsible for the harms these malware campaigns cause, and we are committed to holding them accountable. Prosecutions like this one increase the costs and risks to cybercriminals and ensure that they cannot evade responsibility for the enormous injuries they cause to victims.”

“Fraud over the internet has had a major economic impact on our community, and all over our nation and the world,” stated Acting U.S. Attorney Saima S. Mohsin of the Eastern District of Michigan. “An essential part of reducing the fraud involves vigorously investigating and prosecuting individuals such as these ‘bulletproof hosters’ who enable the fraudsters in victimizing people over the internet.”

“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. Today’s guilty plea sends a message to cybercriminals across the globe that they are not beyond the reach of the FBI and its international partners, and 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 their guilty pleas, Grichishkin and Skvortsov were founding members of the organization and its proprietors. Skvortsov was responsible for marketing the organization’s criminal business and served as a point of contact for important and/or disgruntled clients, and Grichishkin was the organization’s day-to-day leader and oversaw its personnel. 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, and Grichishkin pleaded guilty in February and March 2021 to one count of RICO conspiracy. Skvortsov pleaded guilty today to the same charge. All four guilty pleas took place before Chief U.S. District Judge Denise Page Hood in the Eastern District of Michigan. Sentencing of Stassi, Skorodumov, Grichishkin, and Skvortsov has been set for June 3, June 29, July 8, and Sept. 16, respectively. Each defendant faces 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.