## United States v. Aleksandr Andreevich Panin, a/k/a Harderman, a/k/a Gribodemon, and Hamza Bendelladj, a/k/a Bx1

## Court Docket Number: 1:11-CR-0557-AT-AJB

This case is assigned to United States District Judge Amy Totenberg and United States Magistrate Judge Alan J. Baverman, United States District Court for the North District of Georgia, Richard B. Russell Federal Building and Courthouse, 75 Spring Street, SW, 2211 U.S. Courthouse, Atlanta, GA 30303-3361.

On December 20, 2011, a Northern District of Georgia grand jury returned a 23-count indictment against defendants Panin, who had yet to be fully identified, and Bendelladj. The indictment charged one count of conspiracy to commit wire and bank fraud (18 U.S.C. §§ 1343 and 1349); ten counts of wire fraud (18 U.S.C. §§ 1343 and 2); one count of conspiracy to commit computer fraud (18 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B)(i), 1030(a)(4), 1030(c)(3)(A), 1030(a)(5)(A), 1030(c)(4)(B), and 371); and 11 counts of computer fraud (18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B), 1030(a)(2)(C), 1030(c)(2)(B)(i), and 2). A superseding indictment was subsequently returned identifying Panin by his true name.

According to court documents, charges, and other information presented in Court, SpyEye is a sophisticated malicious computer code designed to automate the theft of confidential personal and financial information, such as online banking credentials, credit card information, usernames, passwords, PINs, and other personally identifying information. SpyEye facilitates this theft of information by secretly infecting victims' computers, enabling cyber criminals to remotely control the infected computers (or bots) through command and control (C2) servers. Once the victims computers are infected and under control, cybercriminals remotely access the infected computers, without authorization, and steal the victims' personal and financial information through a variety of techniques, including web injects, keystroke loggers, and credit card grabbers. The victims' stolen personal and financial data is then surreptitiously transmitted to C2 servers, where it is used to steal money from the victims' financial accounts. Until dismantled, SpyEye was the preeminent malware banking Trojan from 2010-2012. Used by a global syndicate of cybercriminals, SpyEye infected over 1.4 million computers worldwide; compromised over 100,000 bank accounts; and is believed to have caused an estimated $500,000,000 in losses.

Defendant Panin was the primary developer and distributor of SpyEye. Operating from Russia from 2009 to 2011, Panin conspired with others, including allegedly defendant Bendelladj, to develop, market, and sell various versions of SpyEye and component parts on the Internet. Bendelladj is alleged to have purchased, operated, modified, developed add-ons for, and advertised the sale of SpyEye.

The public is reminded that the indictment contains only allegations, and defendants are presumed innocent unless and until proven guilty.