**SpyEye Developer Pleads Guilty**

**Malware Has Infected 1.4 Million Computers**

By [Jeffrey Roman](https://plus.google.com/108994419603328824318), January 28, 2014. Follow Jeffrey [@](https://twitter.com/gen_sec)



The primary developer and distributor of SpyEye [**malware**](http://www.bankinfosecurity.com/anti-malware-c-309?webSyncID=3ed490a6-b97e-b058-6704-1a0d58c7b40d&sessionGUID=eab88584-24bd-dd2a-26bc-66853cb91540&spMailingID=6063990&spUserID=NTQ5MzM0MzE0MDES1&spJobID=363206412&spReportId=MzYzMjA2NDEyS0), designed to steal online banking credentials and credit card information, has pleaded guilty to conspiracy to commit wire and bank [**fraud**](http://www.bankinfosecurity.com/fraud-c-148?webSyncID=3ed490a6-b97e-b058-6704-1a0d58c7b40d&sessionGUID=eab88584-24bd-dd2a-26bc-66853cb91540&spMailingID=6063990&spUserID=NTQ5MzM0MzE0MDES1&spJobID=363206412&spReportId=MzYzMjA2NDEyS0), federal prosecutors say.

[**Aleksandr Andreevich Panin**](http://www.justice.gov/usao/gan/press/2014/01-28-14.html), a Russian national also known as "Gribodemon" and "Harderman," pleaded guilty Jan. 28. Sentencing is scheduled for April 29.

**SpyEye has infected more than 1.4 million computers in the United States, according to the U.S. Justice Department.** It was the dominant malware toolkit used from 2009 to 2011. **Still, the financial services industry says more than 10,000 bank accounts were compromised by SpyEye infections in 2013**. Although some cybercriminals continue to use the malware, its effectiveness is now limited because software makers have added detection for SpyEye to their malware removal programs, prosecutors add.

### Malware's History

From 2009 to 2011, Panin developed, marketed and sold various versions of the SpyEye virus, along with co-defendant Hamza Bendelladj, according to the U.S. Attorney's Office for the Northern District of Georgia.

[**SpyEye**](http://www.bankinfosecurity.com/interviews/top-malware-threats-2013-i-1770?webSyncID=3ed490a6-b97e-b058-6704-1a0d58c7b40d&sessionGUID=eab88584-24bd-dd2a-26bc-66853cb91540&spMailingID=6063990&spUserID=NTQ5MzM0MzE0MDES1&spJobID=363206412&spReportId=MzYzMjA2NDEyS0) was sold for prices ranging from **$1,000 to $8,500**, prosecutors say. Panin allegedly sold the virus to at least 150 customers, advertising the malware on online, invite-only criminal forums.

The SpyEye malware is designed to automate the theft of confidential personal and financial information, including online banking credentials, credit card information, usernames, passwords, PINs and other personally identifying information.

**The malware secretly infects victims' computers, enabling cybercriminals to remotely control the infected computers through command-and-control servers,** the **U.S. attorney's office says. Once infected, cybercriminals remotely access the computers and steal personal and financial information through a variety of techniques.**

### Takedown

**In February 2011, the Federal Bureau of Investigation seized a SpyEye command-and-control server allegedly operated by Bendelladj in the U.S., which controlled more than 200 computers infected with SpyEye and contained information from numerous financial institutions, prosecutors say.**

**FBI sources in June and July 2011 communicated directly with Panin about the SpyEye virus.**

**The FBI purchased a version of the virus from Panin that contained features designed to steal confidential financial information, initiate fraudulent online banking transactions, install keystroke loggers and initiate distributed-denial-of-service attacks from computers infected with the SpyEye malware, federal authorities say.**

A Northern District of Georgia grand jury returned a 23-count indictment against Panin on Dec. 20, 2011, charging him and Bendelladj with one count of conspiracy to commit wire and bank fraud, ten counts of wire fraud, one count of conspiracy to commit computer fraud and 11 counts of computer fraud.

Bendelladj was apprehended in **Bangkok on Jan. 5, 2013, while in transit to Algeria. He was extradited from Thailand to the U.S. on May 2, 2013**, the U.S. attorney's office says. His charges are currently pending in the Northern District of Georgia.

Panin was arrested by U.S. authorities on July 1, 2013, when he flew through Hartsfield-Jackson Atlanta International Airport, the U.S. attorney's office says.

"As several recent and widely reported [**data breaches**](http://www.databreachtoday.com/breaches-c-318?webSyncID=3ed490a6-b97e-b058-6704-1a0d58c7b40d&sessionGUID=eab88584-24bd-dd2a-26bc-66853cb91540&spMailingID=6063990&spUserID=NTQ5MzM0MzE0MDES1&spJobID=363206412&spReportId=MzYzMjA2NDEyS0) have shown, cyber-attacks pose a critical threat to our nation's economic security," said United States Attorney Sally Quillian Yates. "Today's plea is a great leap forward in our campaign against those attacks. Panin was the architect of a pernicious malware known as 'SpyEye' that infected computers worldwide. He commercialized the wholesale theft of financial and personal information. And now he is being held to account for his actions."

Follow Jeffrey Roman on Twitter: [@gen\_sec](https://twitter.com/gen_sec)