Russian man who created SpyEye pleads guilty (Update)

January 28 2014, by Kate Brumback

A US Department of Justice seal on December 11, 2012

A Russian man pleaded guilty to a conspiracy charge Tuesday after federal authorities say he created a computer program that has been used to drain bank accounts.

Aleksandr Andreevich Panin, who's also known as "Gribodemon" and "Harderman," pleaded guilty to a single count of conspiracy to commit

bank fraud and wire fraud. He appeared in federal court wearing an orange jail uniform with his legs chained together as he entered a guilty plea after reaching a plea agreement with prosecutors.

Another man, Hamza Bendelladj, was also indicted in the case and pleaded not guilty in May after being extradited from Thailand, where he was arrested a year ago. The case against him is still pending.

Authorities say the 24-year-old Panin is the main author of SpyEye. The program is a type known as a banking Trojan, which was implanted onto computers to harvest financial information so its users could drain bank accounts. Authorities said the malware has infected more than 1.4 million computers in the United States and abroad and is responsible for untold amounts of financial theft.

Federal prosecutor John Horn called Panin "one of the pre-eminent cybercriminals that we've been able to apprehend and prosecute so far." Operating from Russia, Panin "wrote and polished the code for SpyEye until he had a product that experts described as professional grade," Horn said.

Trojans such as SpyEye can be profitable for cybercriminals. A small group of hackers in Eastern Europe arrested in 2010 was able to steal about $70 million from companies, municipalities and churches in Europe and the U.S.

SpyEye was designed to automatically steal sensitive information—such as bank account credentials, credit card information, passwords and PIN numbers—after being implanted in victims' computers. After the program took control of a computer, it allowed hackers to use a number of covert techniques to trick victims into giving up their personal information—including data grabbing and presenting victims with a fake bank account page. The information was then relayed to a command and

control server, which was used to access bank accounts.

Panin conspired with others, including Bendelladj, to advertise the SpyEye virus in online forums focused on cybercrime and other criminal activity and sold versions of the software for prices ranging from $1,000 to $8,500, prosecutors said. Cybercriminals were able to customize their purchases to choose specific methods of gathering personal information from victims. He is believed to have sold it to at least 150 clients. A single client of his, known by his online name "Soldier," reportedly used the program to make more than $3.2 million in a six-month period, Horn said.

Between 2009 and 2011, SpyEye was the pre-eminent malware toolkit used by cybercriminals, and it is still being used today, Horn said. Information from the financial services industry indicates that more than 10,000 bank accounts were compromised by the program in 2013 alone.

Agents with the FBI in February 2011 searched and seized a SpyEye server they said was operated by Bendelladj in Georgia. That server controlled more than 200 computers infected with the virus and contained information from many financial institutions, authorities said.

In June and July 2011, covert FBI sources communicated directly with Panin, who was using his online nicknames. The FBI sources were able to buy a version of SpyEye from Panin that included features designed to steal financial information, initiate fraudulent online banking transactions, among other operations.

Panin, whose real name wasn't yet known at the time, and Bendelladj were indicted in December 2011.

Bendelladj was on a trip from Malaysia to Egypt when he was arrested during a layover at an airport in Bangkok on Jan. 5, 2013. Police seized

two laptops, a tablet computer, a satellite phone and external hard drives.

Panin was arrested July 1 when he flew through Atlanta's airport. Horn, the prosecutor, declined to comment on the circumstances surrounding Panin's arrest. He is set to be sentenced April 29.

Federal agents continue to investigate the case, and Horn said investigators have been able to provide information to authorities in Bulgaria and the United Kingdom that have allowed them to make arrests.

© 2014 The Associated Press. All rights reserved.

Citation: Russian man who created SpyEye pleads guilty (Update) (2014, January 28) retrieved 25 March 2023 from https://phys.org/news/2014-01-russian-spyeye-guilty.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.