Creator of malware used to drain bank accounts gets 9 years

April 20 2016, by By Kate Brumback

The Russian creator of a computer program that enabled cybercriminals to infect millions of computers and drain bank accounts in multiple countries was sentenced Wednesday to serve 9 ½ years in federal prison.

Aleksandr Andreevich Panin, 27, who went by aliases "Gribodemon" and "Harderman" online, pleaded guilty to a count of conspiracy to commit bank and wire fraud in January 2014 after reaching a deal with prosecutors. He created SpyEye, which prosecutor Steven Grimberg said was a pre-eminent malware from 2010 to 2012 and was used to infect more than 50 million computers and cause nearly $1 billion in damage to individuals and financial institutions around the world.

A second man, Hamza Bendelladj, a 27-year-old Algerian known online as "Bx1," was sentenced to 15 years Wednesday afternoon. Prosecutors said he sold versions of SpyEye online and used the malware to steal financial information.

SpyEye was a type of Trojan virus that secretly implanted itself on victims' computers to steal sensitive information, including bank account credentials, credit card information, passwords and PIN numbers. Once it took over a computer, it allowed hackers to trick victims into surrendering personal information—including data grabbing and fake bank account pages. The information was relayed to a command and control server to be used to access victim accounts.

Panin conspired with others to advertise SpyEye in online cybercrime forums and sold versions of the software for prices ranging from $500 to $10,000, FBI Special Agent Mark Ray testified.

SpyEye was more user-friendly than its predecessors, functioning like "a Swiss army knife of hacking" and allowing users to customize it to choose specific methods of gathering personal information, Ray said. Panin is believed to have sold it to at least 150 clients.

Jon Clay with IT security firm Trend Micro, which helped the FBI investigate SpyEye, said the program wasn't the most sophisticated but had good code and was reasonably priced.

"He had definitely created some capabilities that were not available in some of the other banking Trojans at the time," Clay said. "That's why he was pretty popular among the cybercriminal underground."

FBI agents in February 2011 searched and seized a SpyEye server they said Bendelladj operated in the Atlanta area. That server controlled more than 200 infected computers and contained information from many financial institutions, authorities said.

In June and July 2011, covert FBI sources communicated directly with Panin, who used his online nicknames, and bought a version of SpyEye.

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

Bendelladj was traveling from Malaysia to Egypt when he was arrested Jan. 5, 2013 during a layover at Bangkok's airport. Police seized laptops and external hard drives.

Panin was arrested the following July, when he flew through Atlanta's airport.

Ray's testimony offered a glimpse into the world of online marketplaces where cybercriminals advertise, buy and sell malicious software, using aliases to avoid arrest.

Panin advertised SpyEye as early as June 2010 on Darkode.com, a cybercrime forum dismantled by the FBI last July. Before it was taken down, Darkode.com was the most sophisticated of the cybercrime forums, frequented by the cybercrime elite with access limited to those with a trusted connection, Ray said.

With the cover of anonymity and payments made through online currency servers, reputation is extremely important on cybercrime forums, Ray said. After Panin's June 2010 posting as Gribodemon, Bendelladj—posting as Bx1—wrote a comment saying he'd worked with him before and vouched for him.

The use of aliases can be frustrating to those who track them, said Willis McDonald, a senior threat researcher at security firm Damballa. Frequently, a cybercriminal "will disappear into the background and come up with a new alias and a new piece of malware so that trail you've been trying to follow to track them down vanishes and they pop up under a new name and you have to start all over again trying to figure out who they are," he said.

That's why disabling the infrastructure for a cybercrime network isn't nearly as effective for stopping the spread of a particular malware as catching the creator, McDonald and Clay said. Both said SpyEye infections had dwindled to negligible numbers within about a year after Panin's arrest.

© 2016 The Associated Press. All rights reserved.

Citation: Creator of malware used to drain bank accounts gets 9 years (2016, April 20) retrieved

6 May 2024 from https://phys.org/news/2016-04-creator-malware-bank-accounts-years.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.