

US: 3 charged over 'Gozi' global computer virus (Update)

January 23 2013, by Larry Neumeister

Three men from Russia, Romania and Latvia were in custody Wednesday in the U.S. on charges that they spread a computer virus to more than a million computers worldwide, including almost 200 of the U.S. space agency, siphoning off passwords and online banking information that allowed hackers to steal tens of millions of dollars.

Their arrests were announced as federal authorities unsealed court documents accusing the men of participating in a conspiracy that began in 2005. NASA computers were among those infected by what was called the Gozi virus.

The NASA breach occurred from Dec. 14, 2007, to Aug. 9, 2012, when about 190 agency computers were infected, according to court documents. Between May and August last year, they said, the infected computers sent data without the user's authorization, including the contents of Google chat messages.

The Gozi virus was designed in 2005 and distributed beginning in 2007, when it was secretly installed onto each victim's computer in a manner that left it virtually undetectable by antivirus software, the complaint said.

According to court papers, Romanian national Mihai Ionut Paunescu set up online infrastructure that allowed others to distribute the damaging programs, causing tens of millions of dollars in losses and affecting well over a million computers worldwide.

Paunescu was arrested in Romania. Deniss Calovskis was arrested in Latvia, where he is a citizen and resident, on charges including bank fraud conspiracy. Nikita Kuzmin, a Russian national, was arrested in New York on various charges, including bank fraud and bank fraud conspiracy.

It was not immediately clear who would represent the defendants in court.

A charging document against Kuzmin accused him of designing the Gozi virus as a way to steal the personal bank account information of individuals and businesses in a widespread way.

It said he hired a programmer to write it and began in 2006 to rent the virus to others for a weekly fee, advertising it on Internet forums devoted to cybercrime and other criminal activities. In 2009, according to the document, Kuzmin was approached by others who wanted to acquire the source code so they could attack computers and steal money from bank accounts in the United States and, in particular, European countries. The document said Kuzmin offered the code to other groups of people for \$50,000 plus a guaranteed share of future profits.

According to court documents, Calovskis had training and expertise in computer programming when he was hired by a co-conspirator to upgrade the virus with new code that would deceive victims into divulging additional personal information, such as mother's maiden names. Federal authorities sought at least \$50 million from Calovskis, an amount of money they said was obtained through the conspiracy.

Copyright 2013 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: US: 3 charged over 'Gozi' global computer virus (Update) (2013, January 23) retrieved

10 April 2024 from <https://phys.org/news/2013-01-gozi-virus.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.