United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT of NEW YORK

Department of Justice

U.S. Attorney's Office

Southern District of New York

FOR IMMEDIATE RELEASE Monday, May 2, 2016

Nikita Kuzmin, Creator Of The Gozi Virus, Sentenced In Manhattan Federal Court

Gozi Was Used to Empty Bank Accounts Across the United States and Europe

Preet Bharara, the United States Attorney for the Southern District of New York, announced today that NIKITA KUZMIN, the creator of "Gozi" malware, was sentenced in Manhattan federal court to time served (37 months). Gozi, which was used to steal money from bank accounts across the United States and Europe, infected over one million computers globally and caused tens of millions of dollars in losses. KUZMIN pled guilty, pursuant to a cooperation agreement, to various computer intrusion and fraud charges in May 2011. He was sentenced today by the Honorable Kimba M. Wood.

According to the charging and sentencing documents, and statements made in Manhattan federal court:

In approximately 2007, computer network security experts identified, for the first time, a form of malicious software, or malware, that was stealing victims' personal bank account information on a widespread basis. The malware, which the experts named "Gozi" (and which is sometimes called the "Gozi Virus") infected the victim's computer, among other ways, when the victim received and opened a .pdf document that was designed to appear innocuous and relevant to the victim. Opening the .pdf caused Gozi to be downloaded onto the victim's computer secretly, where it generally remained undetectable by anti-virus software. Once downloaded, the malware collected bank account-related data from the victim's computer, including the username and password, to access the victim's bank account online. The malware transmitted that data to the individuals who controlled the malware, which they used fraudulently to transfer money out of victims' bank accounts. The network security experts subsequently identified a server that contained certain data stolen by Gozi, including 10,000 account records belonging to over 5,200 personal computer users. The records included login information for accounts at over 300 companies, including leading global banks and financial services firms.

Coordinated efforts between U.S. and foreign law enforcement ultimately led to the identification of KUZMIN, a Russian national, as the individual who controlled the malware. KUZMIN previously had significant computer science training, attending two major engineering universities in Russia and graduating with a computer science degree.

In addition to creating Gozi, KUZMIN developed an innovative means of distributing and profiting from it. Unlike many cybercriminals at the time, who profited from malware solely by using it to steal money,

KUZMIN rented out Gozi to other criminals, pioneering the model of cybercriminals as service providers for other criminals. For a fee of $500 a week paid in WebMoney, a digital currency widely used by cybercriminals, KUZMIN rented the Gozi "executable," the file that could be used to infect victims with Gozi malware, to other criminals. KUZMIN designed Gozi to work with customized "web injects" created by other criminals that could be used to enable the malware to target information from specific banks; for example, criminals who sought to target customers of particular American banks could purchase web injects that caused the malware to search for and steal information associated with those banks. Once KUZMIN's customers succeeded in infecting victims' computers with Gozi, the malware caused victims' bank account information to be sent to a server that KUZMIN controlled where, as long as the criminals had paid their weekly rental fee, KUZMIN gave them access to it. KUZMIN, who used the online identity "76," advertised this cybercriminal business, which he called "76 Service," on underground cybercriminal forums. KUZMIN made at least a quarter of a million dollars renting and selling Gozi to other criminals.

In the course of the investigation, Gozi was found to have infected over one million computers across the United States, Germany, Great Britain, Poland, France, Finland, Italy, Turkey, and other countries. U.S. victims include individuals, companies, and others, including the National Aeronautics and Space Administration ("NASA"). Gozi caused at least tens of millions of dollars in losses to victims.

* * *

In addition to the sentence, KUZMIN, 28, a citizen of Russia, was ordered to pay forfeiture and restitution in the amount of $6,934,979.

On January 5, 2016, Deniss Calovskis, a/k/a "Miami," a Latvian national who wrote the computer code for certain "web injects" that enabled Gozi to target information from particular banks, was sentenced to time served (21 months) for his role in the offense. Mihai Ionut Paunescu, a/k/a "Virus," a Romanian national who allegedly ran a "bulletproof hosting" service that enabled cybercriminals to distribute Gozi and other notorious malware, was arrested in Romania in December 2012 and currently awaits extradition to the United States.

Mr. Bharara praised the Federal Bureau of Investigation for its outstanding work in the investigation. He also specially thanked the NASA Office of Inspector General.

The case is being handled by the Office's Complex Frauds and Cybercrime Unit. Assistant United States Attorneys Nicole Friedlander and Sarah Lai are in charge of the prosecution.

Topic(s):
Cyber Crime

Component(s):
USAO - New York, Southern

Press Release Number:
16-105

Updated May 2, 2016