The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

U.S. Charges Russian Citizen in Cyber Conspiracy

By The Moscow Times

June 02, 2014

U.S. Assistant Attorney General Leslie Caldwell (at podium) of the Justice Department's Criminal Division announces criminal charges and two global cyber fraud disruptions.

A Russian man has been charged by U.S. authorities with controlling a hacking gang that infected hundreds of thousands of PCs around the globe with malicious software used for stealing banking credentials.

A criminal complaint unsealed Monday in Nebraska accused Yevgeny Mikhaylovich Bogachev and others of participating in the conspiracy, with court documents suggesting officials suspect that Bogachev wrote Zeus— one of the most effective pieces of theft software ever found.

Authorities in nearly a dozen countries worked with private security companies to wrest control of the network of infected machines, known by the name of its master software, Gameover Zeus.

Court documents said that between 500,000 and 1 million machines worldwide were infected with the malicious software, which was derived from the original "Zeus" trojan for stealing financial passwords that emerged in 2006.

In addition to stealing from the online accounts of businesses and consumers, the Gameover Zeus crew installed other malicious programs, including one called Cryptolocker that encrypted files and demanded payments for their release. Cryptolocker alone infected more than 234,000 machines and won $27 million in ransom payments in just its first two months, the Justice Department said.

The two programs together brought the gang more than $100 million, prosecutors said in court documents, including $198,000 in an unauthorized wire transfer from an unnamed Pennsylvania materials company and $750 in ransom from a police department in Massachusetts that had its investigative files encrypted. Other victims included PNC Bank and Capital One Bank, according to court documents.

Accused Mastermind in Russia

U.S. officials said Bogachev was last known to be living in the Black Sea resort town of Anapa. In an FBI affidavit filed in the Nebraska case, an agent cited online chats in which aliases associated with Bogachev claimed authorship of the original Zeus trojan, which has infected more than 13 million computers and is blamed for hundreds of millions of dollars in losses.

"That's what he claimed. There were probably a number of people involved," said Dmitri Alperovitch, co-founder of security firm CrowdStrike, which also worked with the FBI. A person familiar with the case said that Bogachev's ICQ number, which is an assigned Internet chat query identifier, matched that of the known Zeus author.

Attempts to reach Bogachev were unsuccessful. The FBI declined to comment on Zeus' authorship, citing the ongoing investigation, and Justice Department officials did not respond to questions on the issue.

Zeus's code has since been publicly released, and many variants are still being used by gangs large and small.

"Zeus is probably the most prolific and effective piece of malware discovered since 2006," said Lance James, head of cyber-intelligence at consultancy Deloitte & Touche, which also helped authorities.

Russia does not extradite accused criminals to other countries, so Bogachev may never be arrested. He was named as part of a new policy on aggressively exposing even those the U.S. has little hope of catching.

When asked whether Russian authorities would turn Bogachev over to the U.S., Deputy Attorney General James Cole said "as far as Russia, we are in contact with them and we've been having discussions with them about moving forward and about trying to get custody of Mr. Bogachev," but declined to provide further detail of those talks.

See also:

[Ex-Soviet Hackers Dominate Cyber Crime World]

Original url:
https://www.themoscowtimes.com/2014/06/02/us-charges-russian-citizen-in-cyber-conspiracy-a36077