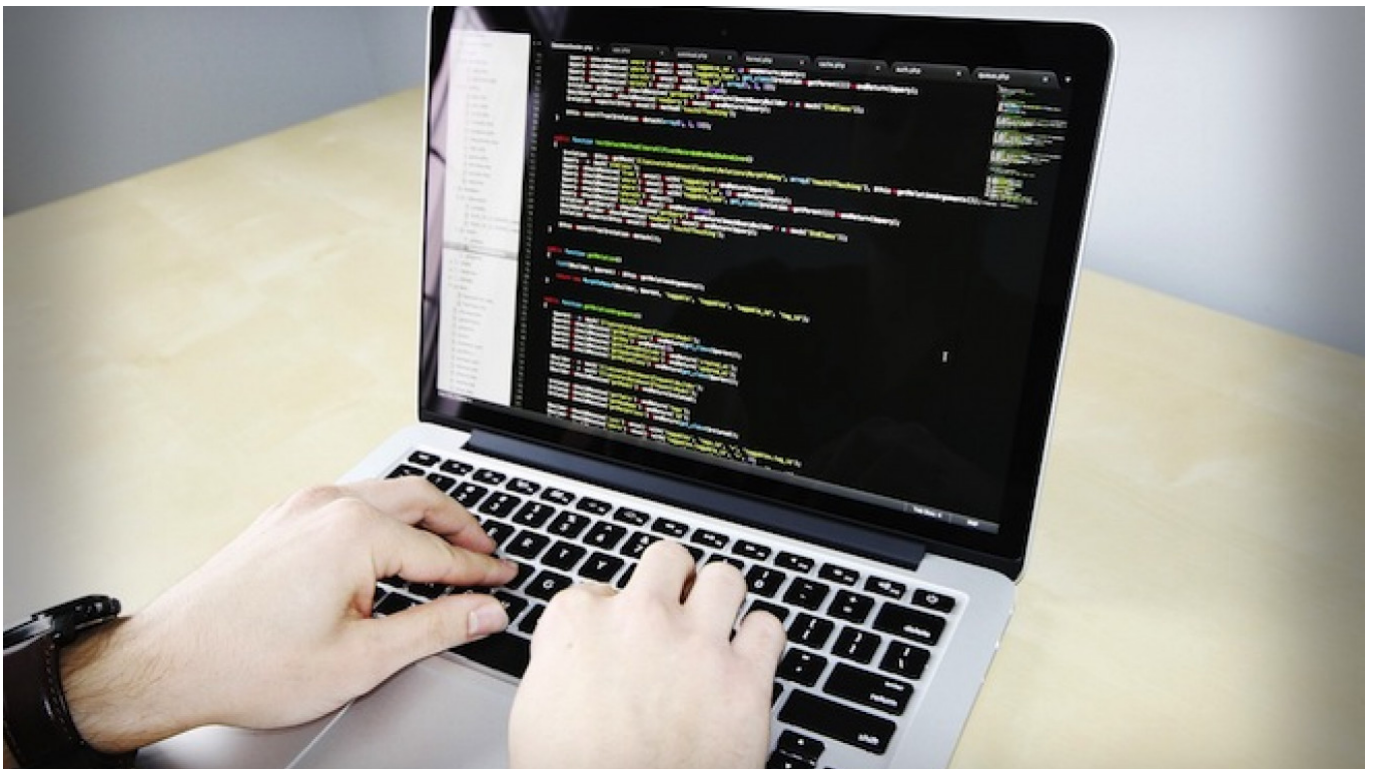


Russian Sentenced to 4 1/2 Years in U.S. Prison for 'Citadel' Malware

September 30, 2015



Citadel, which first appeared in 2011, was designed to capture banking and credit card information from computers and had the ability to block antivirus software.

A Russian national was sentenced on Tuesday to 4 1/2 years in U.S. prison for using sophisticated malware known as "Citadel" to try to steal banking information from thousands of computers, authorities said.

Dmitry Belorossoff, 22, of St. Petersburg, had pleaded guilty in July 2014 to one count of conspiring to commit computer fraud for his role in a \$500 million global cyber crime scheme that infected more than 11 million computers worldwide.

U.S. District Judge Thomas Thrash in Atlanta imposed the sentence, which also requires Belorossoff to pay more than \$320,000 in restitution.

Belorossoff's defense lawyer did not immediately respond to a request for comment.

Citadel, which first appeared in 2011, was designed to capture banking and credit card

information from computers and had the ability to block antivirus software.

Criminals installed the malware through malicious attachments contained in spam emails and other means. Belorossoff, who used the online alias "Rainerfox," downloaded one version of Citadel in 2012 and eventually gained access to more than 7,000 computer systems, U.S. authorities said.

Microsoft Corp and the Federal Bureau of Investigation, working with authorities in dozens of countries, launched an assault in 2013 on the malicious computer networks that were used by the Citadel gang. The company said the attack had freed as many as 5 million personal computers from the malware.

The global crime ring was believed to have stolen more than \$500 million from dozens of financial institutions, including American Express Co, Bank of America Corp, Citigroup Inc, Credit Suisse AG, PayPal Holdings Inc, HSBC Holdings PLC, JPMorgan Chase & Co, Royal Bank of Canada and Wells Fargo & Co, Microsoft said in 2013.

Belorossoff was extradited from Spain in 2014.

Original url:

<https://www.themoscowtimes.com/2015/09/30/russian-sentenced-to-4-12-years-in-us-prison-for-citadel-malware-a49940>