Russian pleads guilty to charge related to Citadel malware

March 20 2017, by Kate Brumback

A Russian man accused of helping develop and distribute malicious software designed to steal personal financial information pleaded guilty Monday to a charge of computer fraud.

Mark Vartanyan, 29, who's known to have used the online alias "Kolypto," was arrested in Norway in October 2014 and was extradited to the U.S. in December. He entered a guilty plea in federal court in Atlanta after reaching a deal to cooperate with federal prosecutors, who have agreed not to seek more than five years in prison.

He's scheduled to be sentenced June 21.

Vartanyan, a native of Moscow, was involved in the development, improvement, maintenance and distribution of Citadel, which infects computer systems and steals financial account credentials and personally identifiable information, prosecutor Greg D'Agincourt said in court.

Starting in 2011, Citadel was marketed on invite-only, Russian-language internet forums used by cybercriminals, and users targeted the computer networks of major financial and government institutions around the world, prosecutors have said. Industry estimates indicate it infected about 11 million computers worldwide and caused more than $500 million in losses.

Vartanyan was involved in the development, improvement, maintenance and distribution of Citadel from August 2012 to January 2013 while

living in Ukraine and again from April 2014 to June 2014 while living in Norway, prosecutors have said.

Citadel was a top-tier malware at its height but had a relatively short run compared to some similar programs because its source code was leaked early on, making it easier for antivirus companies to spot it and block it, Mark Ray, a former FBI special agent who is now director of cyber investigations at PricewaterhouseCoopers in Atlanta, told The Associated Press in a phone interview.

"What made Citadel so unique is that it was the first one that really incorporated this concept of a customer relationship development module, where the developers wanted feedback from the users on improvements and additions and new features," said Ray, who was still working for the FBI in 2014 and traveled to Norway to interview Vartanyan following his arrest.

Vartanyan was one of many people who helped develop Citadel, Ray said, adding that just like with the development of legitimate software programs, developers of malware rely on different programmers with different tools and skills to build and improve their programs.

Another Russian, Dimitry Belorossov of St. Petersburg, known as Rainerfox, was sentenced in September 2015 to serve 4 1/2 years in prison after pleading guilty in Atlanta to conspiring to commit computer fraud for distributing and installing Citadel onto computers using a variety of methods, prosecutors said.

The Department of Justice investigation into the creator of Citadel is ongoing.