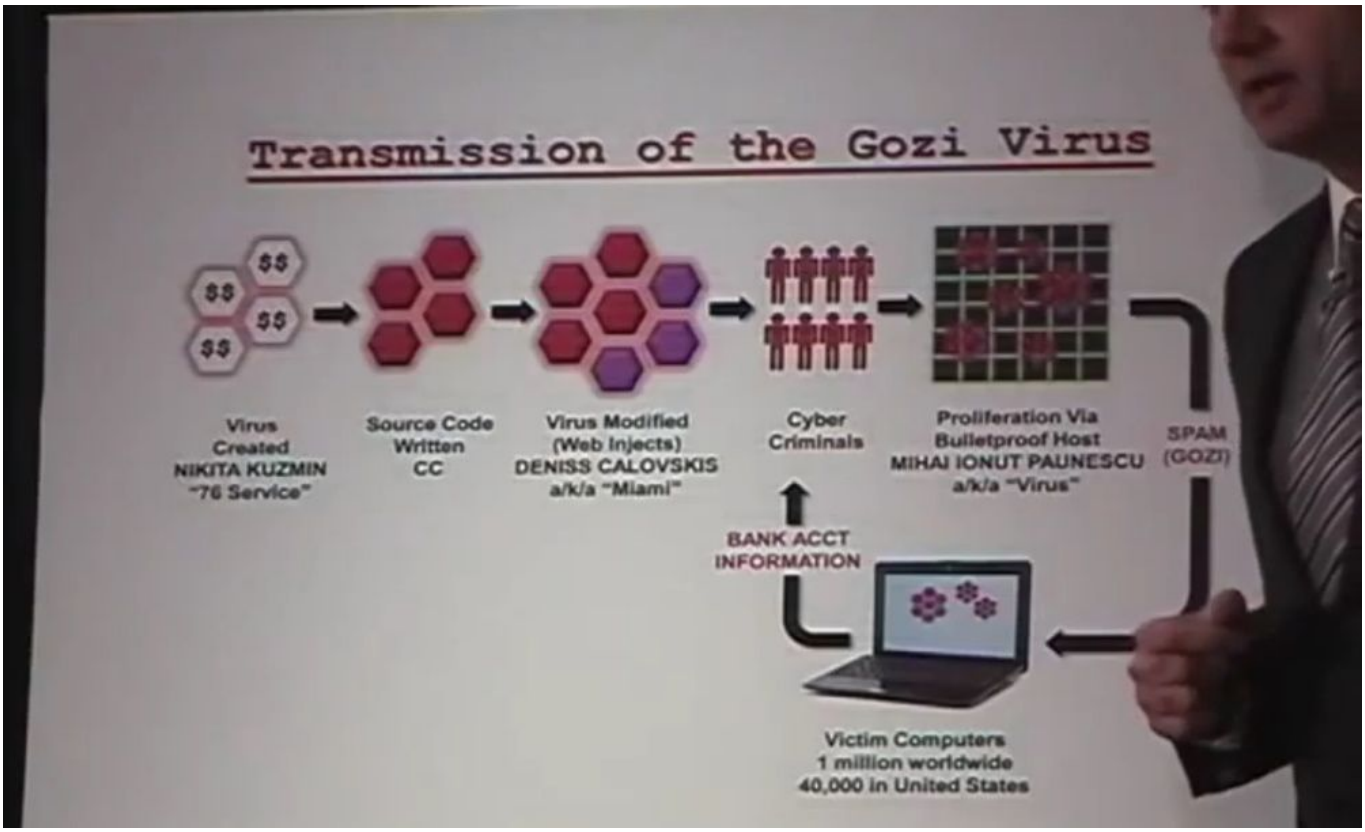


GOZI-SCHEME|PAUNESCU 2012 ARREST|GOZI-VARIANTS

Catalin Cimpanu

June 30th, 2021

Malware | News | Cybercrime

Gozi malware gang member arrested in Colombia

Authorities in Colombia have arrested this week a Romanian national named Mihai Ionut Paunescu, one of the three suspects charged in 2013 for creating and operating the

infamous Gozi banking trojan.

Paunescu was detained this week at the El Dorado airport in Bogotá, Colombia's capital, the country's attorney general office announced on Thursday.

Paunescu was first arrested in Bucharest, Romania, in December 2012 and was officially charged in the US in January 2013 for having a crucial role in the distribution of Gozi, a type of malware that collected e-banking credentials and allowed crooks to steal funds from victims' accounts.

US prosecutors claimed that Paunescu, who went online under the moniker of "**Virus**," operated ***PowerHost[.]ro***, a company that provided "bulletproof hosting" services to malware authors by refusing to cooperate with authorities and helping cybercriminals protect their command and control infrastructure against law enforcement inquiries and takedowns.

While Paunescu provided protected hosting to multiple gangs, such as those operating the Zeus and SpyEye trojans, authorities said he worked very closely with the Gozi gang.

US officials said Paunescu was one of the three core members responsible for the malware's botnet huge growth, which eventually infected more than one million computers between 2007 and 2013 -- with Paunescu coming on board in 2010 when the Gozi 2.0 variant was first released.

However, despite the solid case US authorities had against Paunescu, US prosecutors failed to obtain the suspect's extradition from Romania.

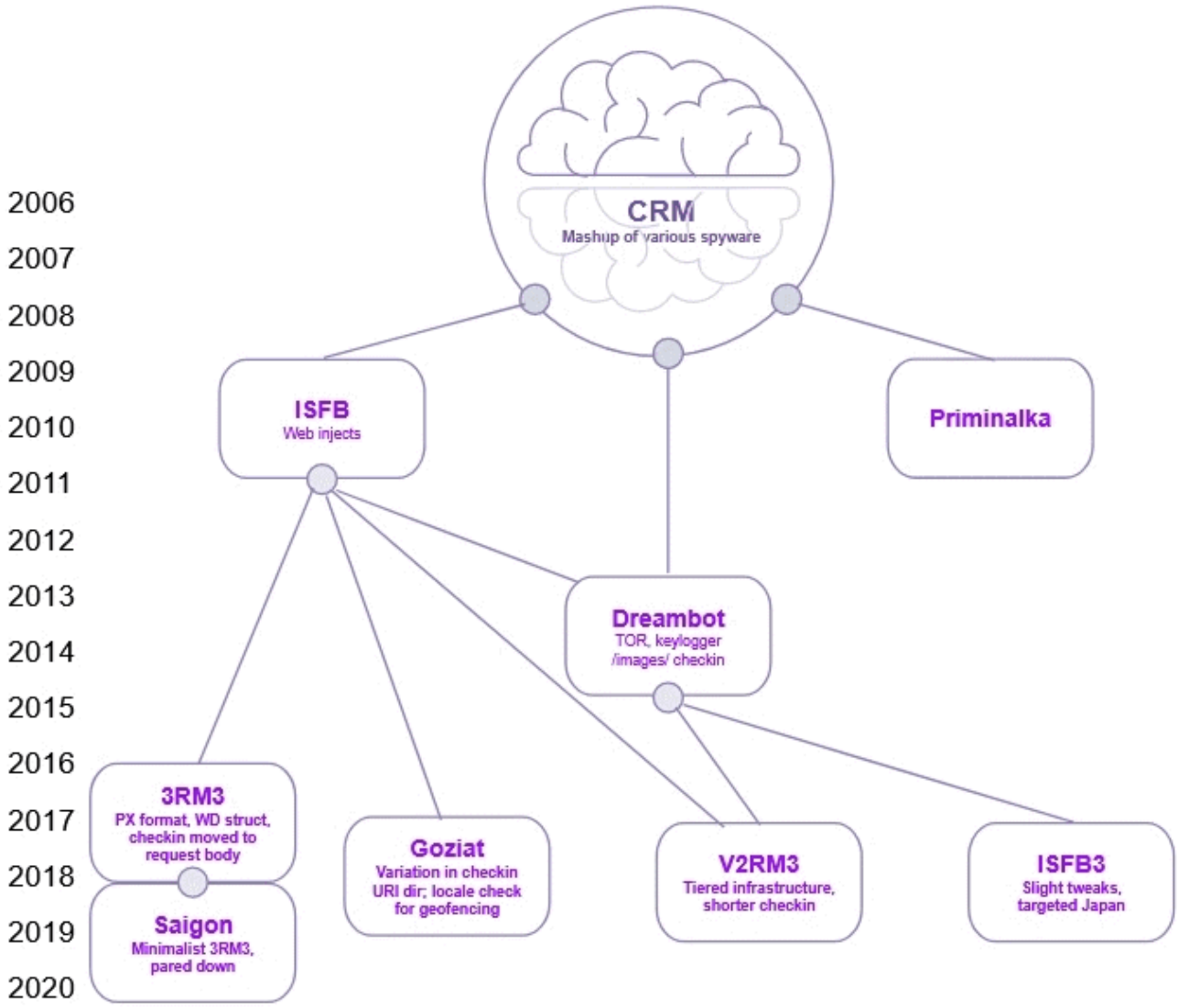
In light of the recent arrest, US officials said they plan to begin new extradition procedures in Colombia.

If extradited and found guilty in the US, Paunescu, now 36, faces up to 65 years in prison.

Of the two other Gozi suspects, Nikita Kuzmin, a Russian national accused of first creating the Gozi trojan, was arrested in California in 2013 and sentenced to 37 months in prison, time served, in May 2016. He was also fined $6,934,979.

Deniss Calovskis, who created Gozi's "web injects" (fake e-banking login pages), was arrested in Latvia, but authorities refused to extradite him to the US due to a too harsh prison sentence that could have reached up to 67 years in prison.

After the Gozi malware gang was charged in January 2013, the malware's source code also leaked online and is now at the heart of many banking trojan strains, such as Gozi Prinimalka, Gozi ISFB, Gozi CRM, Schnitzel Gozi, Goziv3, Neverquest, Rovnix, Vawtrack, Tepfer, Dapato, Ursnif, and many others.



Tags

malware Arrest Banking trojan Cybercrime

Previous article

Next article

CATALIN CIMPANU