FastPOS Malware Creator Pleads Guilty

By Akshaya Asokan

Archived: 2026-04-05 13:59:12 UTC

Card Not Present Fraud , Cybercrime , Cybercrime as-a-service

Prosecutors Say He Provided Help to Cybercriminals Via Infraud Site (asokan_akshaya) • August 1, 2020

The Infraud Organization website was shuttered by law enforcement in 2018. (Source: U.S. Justice Department)

A one-time member of the infamous Infraud Organization who was the creator of a malware strain called FastPOS has pleaded guilty to a federal conspiracy charge, according to the U.S. Justice Department.

See Also: OnDemand | Transform API Security with Unmatched Discovery and Defense

On Friday, Valerian Chiochiu, 30, pleaded guilty to a single charge of conspiracy under the Racketeer Influenced and Corrupt Organizations Act, commonly known as RICO, according to the Justice Department. Chiochiu, a native of Moldova who is living in the U.S., could face up to 10 years in prison when he is sentenced on Dec. 11.

After the Infraud website was seized and shuttered by international law enforcement in 2018, Chiochiu was among 36 individuals indicted for running the website, which authorities say caused $530 million in confirmed fraud losses and attempted to steal more than $2.2 billion (see: *Feds Dismantle Ukrainian's $530 Million Carding Empire*).

Chiochiu, who is currently free on bond, is the second member of the Infraud Organization to plead guilty. In June, Sergey Medvedev, a co-founder of Infraud, entered a guilty plea and now faces up to 10 years in federal prison (see: *Co-Creator of Site That Sold Payment Card Data Pleads Guilty*).

The organization's other co-founder, Svyatoslav Bondarenko, remains at large, according to the Justice Department.

Chiochiu's Role

Chiochiu, who also went by the online names of "Onassis," "Flagler," "Socrate" and "Eclessiastes," joined Infraud Organization in 2012, according to the Justice Department. Although a resident of Moldova, federal prosecutors alleged that Chiochiu was residing in the U.S. during the time of conspiracy.

While other members of the group worked to promote the Infraud Organization website, prosecutors charged that Chiochiu helped provide "guidance to other members on the development, deployment and use of random access memory point-of-sale malware as a means of harvesting stolen data," according to federal court documents.

In addition to his role in the Infraud Organization, Chiochiu acknowledged during his plea agreement that he created a malware strain called FastPOS, which was designed to target point-of-sale devices in to steal payment card data, prosecutors say.

FastPOS was first discovered by researchers from security firm TrendMicro in 2016. The malware was designed to immediately exfiltrate any payment card data from a POS device, instead of storing it locally in a file and periodically sending it to its creators.

At the time, Trend Micro found that FastPOS had infected devices all over the world, including in the U.S. The researchers also noted the creators of the malware were using the same command-and-control server to harvest and then sell the stolen credentials and payment card data.

Infraud Organization

The Infraud Organization ran an online forum dedicated to criminal activity that federal prosecutors claim had more than 10,000 members in March 2017. The site used the slogan "In Fraud We Trust," according to the Justice Department.

The gang that operated Infraud engaged in a variety of identity theft and financial fraud from October 2010 to February 2018, prosecutors say. It's believed to be responsible for the sale or purchase of over 4 million compromised payment card numbers during that time, according to the court filing. The aim of the organization was to develop the "premier online destination for the purchase and sale of stolen property and other contraband" that also serves as the source of other contraband vendors, prosecutors say.

The gang used advertising to direct traffic from its website to other automated sites that were owned or operated by its members, helping other cybercriminals traffic in point-of-sale malware, banking Trojans, stolen payment card details and counterfeit identification, according to court documents.