

Admin of carding portal behind \$568M in losses pleads guilty

bleepingcomputer.com/news/security/admin-of-carding-portal-behind-568m-in-losses-pleads-guilty/

Sergiu Gatlan

By

[Sergiu Gatlan](#)

- June 26, 2020
- 07:36 PM
- [0](#)



Russian national Sergey Medvedev, one of the co-founders of Internet-based cybercriminal enterprise Infraud Organization and an admin on the organization's carding portal, today pleaded guilty to RICO conspiracy.

In February 2018, US authorities indicted 36 individuals for alleged roles in the transnational Infraud cybercrime group, out of 10,901 registered members in March 2017, and apprehended 13 defendants from the United States and six countries: Australia, the United Kingdom, France, Italy, Kosovo and Serbia.

"During the course of its seven-year history, the Infraud Organization inflicted approximately \$2.2 billion in intended losses, and more than \$568 million in actual losses, on a wide swath of financial institutions, merchants, and private individuals, and would have continued to do so for the foreseeable future if left unchecked," a DoJ release says.

Underground forum for selling financial info, PII, more

Infraud facilitated the large-scale acquisition, sale, and distribution of stolen identity information and payment cards, personally identifiable data, financial and banking info, computer malware, and various other contraband.

The Infracred organization also "directed traffic and potential purchasers to the automated vending sites of its members, which served as online conduits to traffic in stolen means of identification, stolen financial and banking information, malware, and other illicit goods."

The operation and its website were active between October 2010 when it was created by Svyatoslav Bondarenko (at infracred[.]cc and infracred[.]ws, later moved to other locations) and until February 2018 when Infracred and its site were taken down following a joint operation between law enforcement agencies from seven countries.



Infracred takedown

notice (DoJ)

All members needed admin approval to join

Infracred's forum hierarchy included administrators (4DMini57r470rz), super-moderators (Super MODER470R5), and moderators (M0d3r470r2) who oversaw the activity of users known as vendors (Doctors or Professors), VIP members (Fratello Masons or Advanced Members), and regular members (Phr4Ud573r).

To join Infracred's online forum, all users needed approval from one of the Infracred administrators and they also faced removal if the products they sold on the forum were considered subpar by the admins.

Medvedev, as one of Infracred's co-founder, operated an 'escrow' / currency exchanging service that ensured the transaction integrity between organization members. Medvedev took the role of owner and admin of the Infracred Organization after Bondarenko went missing in 2015.

The roles of each of the defendants indicted two years ago are explained in detail in this second superseding criminal indictment filed on February 7, 2018.



Infraud hierarchy (DoJ)

Today, another Russian national, Aleksey Yurievich Burkov, was sentenced to 9 years in prison for operating Cardplanet and Direct Connection, two sites that facilitated payment card fraud, computer hacking, and other cybercrimes according to another release published today by DoJ officials.

The Cardplanet site was a card shop (also known as a CVV shop and carding site) where Burkov oversaw the selling of payment card (debit and credit card) numbers stolen from hundreds of thousands of individuals, many of them U.S. Citizens, between at least early 2009 through at least August 2013.

The carding shop was also used to sell data from over 150,000 stolen payment cards which resulted in estimated fraud losses and fraudulent purchases of over \$20,000,000.

Related Articles:

[US charges hacker for breaching brokerage accounts, securities fraud](#)

[REvil ransomware returns: New malware sample confirms gang is back](#)

[Russian hackers are seeking alternative money-laundering options](#)

[US and allies warn of Russian hacking threat to critical infrastructure](#)

[US, UK link new Cyclops Blink malware to Russian state hackers](#)

- [Carding](#)
- [Cybercrime](#)
- [Fraud](#)
- [Identity Theft](#)
- [Russia](#)
- [USA](#)

[Sergiu Gatlan](#)

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- [Previous Article](#)
- [Next Article](#)

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
