Another Alleged FIN7 Cybercrime Gang Member Arrested

By Ishita Chigilli Palli

Account Takeover Fraud , Cybercrime , Fraud Management & Cybercrime

Faces 13 Charges, Including Computer Hacking (Ishita_CP) • May 27, 2020

The FBI has arrested another alleged member of the FIN7 cybercrime gang, which has been stealing millions of payment cards and other financial data since at least September 2015, according to federal court documents.

Ukrainian national Denys Iarmak was extradited from Thailand and arrested in Seattle on Friday, according to documents unsealed by the U.S. District Court for the Western District of Washington in Seattle. He's the fourth alleged member of the group to be arrested and charged in the last two years.

Iarmak, who remains in federal custody, has been charged with multiple criminal counts, including wire fraud; conspiracy to commit computer hacking; conspiracy to commit wire and bank fraud; three counts of aggravated identity theft; three counts of accessing a protected computer in furtherance of fraud; three counts of intentional damage to a protected computer; and access device fraud and forfeiture allegations, the federal court documents show.

FIN7, also known as Carbanak or Navigator, is a financially motivated cybercrime group known to use spear-phishing mails containing malicious Word and Google document attachments that load malware on targeted

devices to steal payment card information, according to federal prosecutors.

Over the years, authorities allege, FIN7 has targeted restaurant chains, casinos and hospitality businesses, including Chipotle Mexican Grill, Arby's, Chili's, Red Robin Gourmet Burgers, Taco John's, Sonic Drive-in and Emerald Queen Hotel and Casino (see: *Credit Card Theft Ringleader Pleads Guilty*).

The group allegedly stole more than 15 million payment card records from over 6,500 point-of-sale terminals across more than 3,600 business locations, according to the Justice Department.

Iarmark's Role

To carry out its activities, FIN7 created a front company called Combi Security that purported to be a cybersecurity pen-testing firm based in Russia and Israel, prosecutors allege in court documents.

The front company then "hired" computer programmers under the pretense of having them work on pen-testing for clients, prosectutors allege. Iarmak was allegedly one such "pen-tester" whose job was breaching the security of victims' networks, according to the indictment.

"In truth and in fact, the defendant and his FIN7 co-conspirators well knew Combi Security was a front company used to hire and deploy hackers who were given tasks in furtherance of the FIN7 conspiracy," the indictment states.

Law enforcement officials allege that Iarmak sent internal system information stolen from a victim company to FIN7 manager Fedir Hladyr in a Jabber communication. Numerous other Jabber communications between Iarmark and other FIN7 members discussing phishing emails, malware tools, victim information and other illegal activities were also found, according to the indictment.

Hladyr, who is also from Ukraine, pleaded guilty to multiple charges in federal court September 2019 and is awaiting sentencing, federal prosecutors say.

FIN7's Illegal Activities

The spear-phishing emails lured victims by faking an interest in their organization or by falsely claiming to be from organizations such as the U.S. Securities and Exchange Commission, according to the indictment. While targeting one restaurant chain, the hackers inquired about placing a catering order, the details of which they said were in a malicious attachment, according to court documents.

The FIN7 hackers went one step further, calling the victims to convince them to open the attached documents, the indictment alleges.

Once a victim's computer was infected, FIN7 allegedly would install additional malware, such as the backdoor Carbanak, to remotely control the device and then add it to the gang's botnet, according to the court documents. The group operated a global network of servers and used Jira project management software to collaborate with other members of the group and share attack details, the document adds.

Other Arrests

In 2018, the Justice Department unsealed indictments against three alleged high-level members of the gang: Hladyr, Dmytro Fedorov and Andrii Kolpakov.

Fedorov was arrested in Bielsko-Biala, Poland, and Kolpakov was arrested in Lepe, Spain, in 2018. Both were later extradited to the U.S. and pleaded not guilty. Their trial began in August 2019 and is set to continue in October 2020.

According to an FBI alert, the FIN7 group is still active. In March, the bureau warned businesses that FIN7 was mailing malicious USB storage devices to victims, along with a teddy bear and supposed $50 gift card to Best Buy (see: FBI: Cybercrime Gang Mailing 'BadUSB' Devices to Targets).
