High-Level Organizer of Notorious Hacking Group Sentenced to Prison for Scheme that Compromised Tens of Millions of Debit and Credit Cards

Press Release

Friday, April 16, 2021

For Immediate Release
Office of Public Affairs

Overall Damage to Banks, Merchants, Card Companies, and Consumers Estimated at more than $1 Billion

A Ukrainian national was sentenced today in the Western District of Washington to 10 years in prison for his high-level role in the criminal work of the hacking group FIN7.

Fedir Hladyr, 35, served as a manager and systems administrator for FIN7. He was arrested in Dresden, Germany, in 2018, at the request of U.S. law enforcement and was extradited to Seattle, Washington. In September 2019, he pleaded guilty to one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer hacking.

“The defendant and his conspirators compromised millions of financial accounts and caused over a billion dollars in losses to Americans and costs to the U.S. economy,” said Acting Assistant Attorney General Nicholas L. McQuaid of the Justice Department’s Criminal Division. “Protecting businesses – both large and small – online is a top priority for the Department of Justice. The department is committed to working with our international partners to hold such cyber criminals accountable, no matter where they reside or how anonymous they think they are.”

“This criminal organization had more than 70 people organized into business units and teams. Some were hackers, others developed the malware installed on computers, and still others crafted the malicious emails that duped victims into infecting their company systems,” said Acting U.S. Attorney Tessa M. Gorman of the Western District of Washington. “This defendant worked at the intersection of all these activities and thus bears heavy responsibility for billions in damage caused to companies and individual consumers.”

“These cyber thieves orchestrated an elaborate network of hackers and systems to infiltrate businesses and exploit consumers’ personal information,” said Special Agent in Charge Donald M. Voiret of the FBI’s Seattle Field Office. “Their specialized skills to target certain industries amplified the damage exponentially. Thanks to the hard work of law enforcement partners both in the U.S. and overseas, these fraudsters are not beyond our reach and cannot hide from the law.”

According to documents filed in the case, since at least 2015, members of FIN7 (also referred to as Carbanak Group and the Navigator Group, among other names) engaged in a highly sophisticated malware campaign to attack hundreds of U.S. companies, predominantly in the restaurant, gambling, and hospitality industries. FIN7 hacked into thousands of computer systems and stole millions of customer credit and debit card numbers that were then used or sold for profit. FIN7, through its dozens of members, launched waves of malicious cyberattacks on numerous businesses operating in the United States and abroad. To execute its scheme, FIN7 carefully crafted email messages that would appear legitimate to a business’ employees, and accompanied emails with telephone calls intended to further legitimize the emails. Once a file attached to a fraudulent email was opened and activated, FIN7 would use an adapted version of the Carbanak malware, in addition to an arsenal of other tools, to access and steal payment card data for the business’s customers. Since 2015, many of the stolen payment card numbers have been offered for sale through online underground marketplaces.

In the United States alone, FIN7 successfully breached the computer networks of businesses in all 50 states and the District of Columbia, stealing more than 20 million customer card records from over 6,500 individual point-of-sale terminals at more than 3,600 separate business locations. According to court documents, victims incurred enormous costs that, according to some estimates, totaled billions of dollars. Additional intrusions occurred abroad, including in the United Kingdom, Australia, and France. Companies that have publicly disclosed hacks attributable to FIN7 include such chains as Chipotle Mexican Grill, Chili’s, Arby’s, Red Robin, and Jason’s Deli.

Hladyr originally joined FIN7 via a front company called Combi Security – a fake cyber security company that had a phony website and no legitimate customers. Hladyr admitted in his plea agreement that he soon realized that, rather than a legitimate company, Combi was part of a criminal enterprise. Hladyr served as FIN7’s systems administrator who, among other things, played a central role in aggregating stolen payment card information, supervising FIN7’s hackers, and maintaining the elaborate network of servers that FIN7 used to attack and control victims’ computers. Hladyr also controlled the organization’s encrypted channels of communication.

This case is the result of an investigation conducted by the Seattle Cyber Task Force of the FBI and the U.S. Department of Justice. The Justice Department's Office of International Affairs, the National Cyber-Forensics and Training Alliance, numerous computer security firms and financial institutions, FBI offices across the nation and globe, as well as a number of international agencies provided significant assistance. German law enforcement authorities provided significant assistance by arresting Hladyr.

This case was prosecuted by Trial Attorney Anthony Teelucksingh of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorneys Francis Franze-Nakamura and Steven Masada of the Western District of Washington.

Updated April 16, 2021

Topic

Cybercrime

Press Release Number: 21-338