High-level organizer of notorious hacking group FIN7 sentenced to ten years in prison for scheme that compromised tens of millions of debit and credit cards

justice.gov/usao-wdwa/pr/high-level-organizer-notorious-hacking-group-fin7-sentenced-ten-years-prison-scheme

April 16, 2021

THE UNITED STATES
DEPARTMENT
of JUSTICE

Department of Justice

U.S. Attorney's Office

Western District of Washington

FOR IMMEDIATE RELEASE

Friday, April 16, 2021

Overall damage to banks, merchants, card companies, and consumers estimated at more than $3 billion

Seattle – The first high-level manager of the notorious hacking group FIN7 was sentenced today in U.S. District Court in Seattle to ten years in prison, announced Acting U.S. Attorney Tessa A. Gorman. Fedir Hladyr, 35, a Ukranian national, served as a high-level 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. In September 2019, he pleaded guilty to conspiracy to commit wire fraud and one count of conspiracy to commit computer hacking. At today's sentencing hearing, Chief U.S. District Judge Ricardo S. Martinez said, "Cybercrime has become the greatest threat to American's financial health, and to citizens around the globe."

“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 Gorman. “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.”

According to records filed in the case, since at least 2015, FIN7 members (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, gaming, and hospitality industries. FIN7 hacked into thousands of computer systems and stole millions of customer credit and debit card numbers which were used or sold for profit.

FIN7, through its dozens of members, launched numerous waves of malicious cyberattacks on numerous businesses operating in the United States and abroad. FIN7 carefully crafted email messages that would appear legitimate to a business’s employees and accompanied emails with telephone calls intended to further legitimize the email. Once an attached file was opened and activated, FIN7 would use an adapted version of the notorious Carbanak malware in addition to an arsenal of other tools ultimately 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. Additional intrusions occurred abroad, including in the United Kingdom, Australia, and France. Companies that have publicly disclosed hacks attributable to FIN7 include such familiar chains as Chipotle Mexican Grill, Chili’s, Arby’s, Red Robin, and Jason’s Deli.

“These cyber thieves orchestrated an elaborate network of hackers and systems to infiltrate businesses and exploit consumers’ personal information,” said Donald M. Voiret, FBI Special Agent in Charge of the 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.”

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 quickly realized that, far from being 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.

Speaking to the court, Hladyr said he had "ruined years of my life and put [his] family through great risk and struggle."

Noting that cyber criminals must be deterred by significant sentences, Chief Judge Martinez said he was cognizant of the "ease of sitting at a keyboard and stealing money from people around the globe" and emphasized that would-be cybercriminals "must understand that, once caught, the punishment will be significant." The judge also ordered Hladyr to pay $2.5 million in restitution.

This case is the result of an investigation conducted by the Seattle Cyber Task Force of the FBI and the U.S. Attorney's Office for the Western District of Washington, with the assistance of the Justice Department's Computer Crime and Intellectual Property Section and 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 numerous international agencies. German law enforcement authorities provided significant assistance by arresting Hladyr.

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

Topic(s):

Cybercrime

Component(s):

USAO - Washington, Western
Contact:

Press contact for the U.S. Attorney's Office is Communications Director Emily Langlie at (206) 553-4110 or Emily.Langlie@usdoj.gov.