


Member of hacking group sentenced for scheme that compromised tens of millions of debit and credit cards

 [justice.gov/usao-wdwa/pr/member-hacking-group-sentenced-scheme-compromised-tens-millions-debit-and-credit-cards](https://www.justice.gov/usao-wdwa/pr/member-hacking-group-sentenced-scheme-compromised-tens-millions-debit-and-credit-cards)

April 7, 2022



Department of Justice

U.S. Attorney's Office

Western District of Washington

FOR IMMEDIATE RELEASE

Thursday, April 7, 2022

Damage to banks, merchants, card companies and consumers estimated at more than \$1 billion

Seattle – A Ukrainian man was sentenced today in the Western District of Washington to 5 years in prison for his criminal work in the hacking group FIN7. Denys Iarmak, 32, served as a high-level hacker, whom the group referred to as a “pen tester,” for FIN7. He was arrested in Bangkok, Thailand in November 2019 at the request of U.S. law enforcement. At the sentencing hearing Chief U.S. District Judge Ricardo S. Martinez noted that Iarmak had been in custody during both the COVID pandemic and now the war in Ukraine. “There is some irony, that the nation you were plundering is now leading an international effort to protect your country, your people, your family.”

Iarmak is the third FIN7 member of the group to be sentenced in the United States. On April 16, 2021, FIN7 member Fedir Hladyr was sentenced to 10 years in prison. On June 24, 2021, FIN7 member Andrii Kolpakov was sentenced to seven years in custody.

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, exceeded \$1 billion 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.

"Iarmak and his conspirators compromised millions of financial accounts, causing over a billion dollars in losses to Americans and costs to America's economy," said Assistant Attorney General Kenneth A. Polite, Jr. of the Justice Department's Criminal Division. "Protecting businesses – both large and small – online is a top priority for the Department of Justice. We are committed to working with our international partners to hold such cyber criminals accountable, no matter where they live or how anonymous they think they are."

"Mr. Iarmak was directly involved in designing phishing emails embedded with malware, intruding on victim networks, and extracting data such as payment card information," said U.S. Attorney Nicholas W. Brown of the Western District of Washington. "To make matters worse, he continued his work with the FIN7 criminal enterprise even after the arrests and prosecution of co-conspirators. He and others in this cybercrime group used hacking techniques to essentially rob thousands of locations of multiple restaurant chains at once, from the comfort and safety of their keyboards in distant countries."

"This cyber-criminal probed and mapped victims' networks searching for data to exploit," said Special Agent in Charge Donald M. Voiret of the FBI's Seattle Field Office. "Masquerading as a legitimate business, the hacking group he belonged to recruited other members to assist with their criminal activities. Thanks to the hard work of law enforcement, this defendant, who is responsible for an enormous loss amount, will be spending the next few years in prison."

According to court documents, 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.

larmak was involved with FIN7 from approximately November 2016 through November 2018. larmak frequently used project management software such as JIRA, hosted on private virtual servers in various countries, to coordinate FIN7 malicious activity and to manage the assorted network intrusions. JIRA is a project management and issue-tracking program used by software development teams. JIRA allows team members to create “projects” containing posted “issues” under which other team members can make comments and share data. Under each issue, FIN7 members tracked their progress breaching a victim’s security, uploaded data stolen from the victim, and provided guidance to each other. As one example, larmak created a JIRA issue, to which he and other members of the cybergroup had access, for a specific victim company, and, on or about March 3, 2017, larmak updated that JIRA and uploaded data he had stolen from that company. During the course of the scheme, larmak received compensation for his participation in FIN7, which far exceeded comparable legitimate employment in Ukraine. Moreover, FIN7 members, including larmak, were aware of reported arrests of other FIN7 members, but nevertheless continued to attack U.S. businesses.

larmak initially fought extradition but in February 2020 he consented to extradition in a Thai court. In May 2020 he was transferred to U.S. custody. In November 2021, larmak pleaded guilty to one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer hacking.

This case is the result of an investigation conducted by the FBI’s Seattle Cyber Task Force. 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. Thailand law enforcement authorities provided significant assistance by arresting larmak.

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

Topic(s):

Consumer Protection

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.