FIN7 manager sentenced to 7 years for role in global hacking scheme

By Adam Janofsky

Published: 2022-12-17 · Archived: 2026-04-05 16:08:04 UTC

A key member of the international cybercrime group FIN7 was sentenced to 84 months in prison and ordered to pay $2.5 million in restitution on Thursday for his role in breaching a wide range of American businesses.

Andrii Kolpakov, a Ukranian national, pleaded guilty in November to conspiracy to commit wire fraud and computer hacking. Kolpakov worked as a manager and recruiter for the gang, hiring and supervising hackers who stole payment card information from dozens of companies primarily in the restaurant, gaming, and hospitality industries, including Chipotle, Chili's, Arby's, and Red Robin.

Prosecutors said FIN7 attacked hundreds of U.S. businesses to steal tens of millions of payment cards, causing over $1 billion in damages according to some estimates. The group monetized the stolen information in various ways, including selling large dumps of credit cards on underground marketplaces such as Joker's Stash. Kolpakov's offenses carried a penalty of up to 25 years in prison and fines of up to half a million dollars, which were waived by the judge.

In the sentencing hearing held in a Seattle court on Thursday, Kolpakov's lawyer said that he was not a criminal mastermind, but a person who was "backed into a corner" after unwittingly joining the group. Kolpakov maintained that he did not seek to join FIN7—he applied to a classified advertisement for what he thought was a legitimate cybersecurity job at a company called Combi Security. Additionally, Kolpakov made about $75,000 for his work—an amount that provided his family security and stability, but a modest sum for a cybercriminal.

d. FIN7 used a front company called Combi Security to recruit hackers and to provide a veil of legitimacy to the illegal enterprise. Combi Security portrayed itself as a legitimate computer security company that provided penetration-testing services to a variety of companies around the world. On its public website, Combi Security presented itself as "one of the leading international companies in the field of information security." In truth and fact, Combi Security carried out no legitimate work, and was not hired by any company to provide security-related services.

Kolpakov's lawyer claimed that he was unaware of FIN7's illegal activity, and joined the group after applying for a job at Combi Security, which he believed to be legitimate.

Kolpakov spoke during the sentencing hearing, apologizing for his work with the group and asking for forgiveness from his victims, saying that he suffered greatly while in custody during a pandemic in a foreign country.

According to prosecutors, FIN7 masqueraded as Combi in order to recruit hackers and give its workers plausible deniability that they were involved in a global hacking scheme. They also claimed it would be obvious to a key

employee like Kolpakov that the organization was engaging in illegal activity.

From at least april 2016 to June 2018, prosecutors alleged that Kolpakov served as a “high-level hacker” in the organization, probing and mapping victims’ networks in search of point-of-sale systems and customer payment card data. They specifically tied him to the hack of Jason’s Deli, a restaurant chain with hundreds of locations across the U.S. that had millions of customer records breached and sold on the dark web.

“He was elevated to a managerial role in which he also managed and supervised a small team of hackers tasked with breaching the security of victims’ computer systems,” prosecutors wrote in a memorandum submitted days before the sentencing. “He was assigned to supervise and train new recruits and appraised his team members of new tools and developments in the FIN7’s phishing campaigns and malware arsenal.”

FIN7 typically launched tailored phishing campaigns against employees of target companies, especially targeting customer service representatives and managers. In one email sent to a restaurant manager, a group member complained about food poisoning to pressure the victim into clicking on a malicious attachment. “Yesterday my colleagues ate your food. In a few hours we felt discomfort in the stomach… I would like to understand what had happened and solve the issue. Enclosed file contains all the necessary information.”

Spanish police arrested Kolpakov in 2018 while he was on vacation in the town of Lepe. He was in possession of electronic devices, including a laptop, phone, and storage devices that were used in the scheme, and he was extradited to the U.S. the following year.

Adam Janofsky

is the founding editor-in-chief of The Record from Recorded Future News. He previously was the cybersecurity and privacy reporter for Protocol, and prior to that covered cybersecurity, AI, and other emerging technology for The Wall Street Journal.
