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

justice.gov/opa/pr/high-level-member-hacking-group-sentenced-prison-scheme-compromised-tens-millions-debit-and

June 24, 2021

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, June 24, 2021

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 seven years in prison for his role in the criminal work of the hacking group FIN7. The defendant was also ordered by the court to pay restitution in the amount of $2,500,000.

According to documents filed in the case, statements made at the sentencing, and public documents, Andrii Kolpakov, 33, who has used a number of different names, served as a high-level hacker, whom the group referred to as a "pen tester," for FIN7. He was arrested in Lepe, Spain, on June 28, 2018, at the request of U.S. law enforcement and was extradited to the United States on June 1, 2019. In June 2020, he pleaded guilty to one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer hacking.

According to public 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. 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 emails. Once an attached file 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, exceeded $1 billion. Additional intrusions occurred abroad, including in the United Kingdom, Australia and France. Companies that have publicly disclosed hacks attributable to FIN7 include Chipotle Mexican Grill, Chili's, Arby's, Red Robin and Jason's Deli.

Kolpakov was involved with FIN7 from at least April 2016 until his arrest in June 2018. He also managed other hackers tasked with breaching the security of victims' computer systems. During the course of the scheme, Kolpakov received compensation for his participation in FIN7, which far exceeded comparable legitimate employment in Ukraine. Moreover, FIN7 members, including Kolpakov, were aware of reported arrests of other FIN7 members, but nevertheless continued to attack U.S. businesses.

Acting Assistant Attorney General Nicholas L. McQuaid of the Justice Department's Criminal Division; Acting U.S. Attorney Tessa M. Gorman for the Western District of Washington; and Special Agent in Charge Donald M. Voiret of the FBI's Seattle Field Office made the announcement.

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. Spanish law enforcement authorities provided significant assistance by arresting Kolpakov.

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.