Three Members of Notorious International Cybercrime Group “Fin7” In Custody for Role in Attacking Over 100 U.S. companies

Published: 2018-08-01 · Archived: 2026-04-02 11:32:10 UTC

Three high-ranking members of a sophisticated international cybercrime group operating out of Eastern Europe have been arrested and are currently in custody facing charges filed in U.S. District Court in Seattle, announced Assistant Attorney General Brian A. Benczkowski of the Justice Department’s Criminal Division, U.S. Attorney Annette L. Hayes for the Western District of Washington and Special Agent in Charge Jay S. Tabb Jr. of the FBI Seattle Field Office.

According to three federal indictments unsealed today, Ukrainian nationals Dmytro Fedorov, 44, Fedir Hladyr, 33, and Andrii Kolpakov, 30, are members of a prolific hacking group widely known as FIN7 (also referred to as the Carbanak Group and the Navigator Group, among other names). Since at least 2015, FIN7 members engaged in a highly sophisticated malware campaign targeting more than 100 U.S. companies, predominantly in the restaurant, gaming, and hospitality industries. As set forth in indictments, FIN7 hacked into thousands of computer systems and stole millions of customer credit and debit card numbers, which the group used or sold for profit.

In the United States alone, FIN7 successfully breached the computer networks of companies in 47 states and the District of Columbia, stealing more than 15 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. Additionally in Western Washington, FIN7 targeted other local businesses.

“The three Ukrainian nationals indicted today allegedly were part of a prolific hacking group that targeted American companies and citizens by stealing valuable consumer data, including personal credit card information, that they then sold on the Darknet,” said Assistant Attorney General Benczkowski. “Because hackers are committed to finding new ways to harm the American public and our economy, the Department of Justice remains steadfast in its commitment to working with our law enforcement partners to identify, interdict, and prosecute those responsible for these threats.”

“Protecting consumers and companies who use the internet to conduct business – both large chains and small ‘mom and pop’ stores -- is a top priority for all of us in the Department of Justice,” said U.S. Attorney Hayes. “Cyber criminals who believe that they can hide in faraway countries and operate from behind keyboards without getting caught are just plain wrong. We will continue our longstanding work with partners around the world to ensure cyber criminals are identified and held to account for the harm that they do – both to our pocketbooks and our ability to rely on the cyber networks we use.”

“The naming of these FIN7 leaders marks a major step towards dismantling this sophisticated criminal enterprise,” said Special Agent in Charge Tabb. “As the lead federal agency for cyber-attack investigations, the

FBI will continue to work with its law enforcement partners worldwide to pursue the members of this devious group, and hold them accountable for stealing from American businesses and individuals."

Each of the three FIN7 conspirators is charged with 26 felony counts alleging conspiracy, wire fraud, computer hacking, access device fraud, and aggravated identity theft.

In January 2018, at the request of U.S. officials, foreign authorities separately arrested Ukrainian Fedir Hladyr and a second FIN7 member, Dmytro Fedorov. Hladyr was arrested in Dresden, Germany, and is currently detained in Seattle pending trial. Hladyr allegedly served as FIN7's systems administrator who, among other things, maintained servers and communication channels used by the organization and held a managerial role by delegating tasks and by providing instruction to other members of the scheme. Hladyr's trial is currently scheduled for Oct. 22.

Fedorov, a high-level hacker and manager who allegedly supervised other hackers tasked with breaching the security of victims' computer systems, was arrested in Bielsko-Biala, Poland. Fedorov remains detained in Poland pending his extradition to the United States.

In late June 2018, foreign authorities arrested a third FIN7 member, Ukrainian Andrii Kolpakov in Lepe, Spain. Kolpakov, also alleged to be a supervisor of a group of hackers, remains detained in Spain pending the United States' request for extradition.

According to the indictments, 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' employee, 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 to ultimately access and steal payment card data for the business' customers. Since 2015, FIN7 sold the data in online underground marketplaces. (Supplemental document "How FIN7 Attacked and Stole Data" explains the scheme in greater detail.)

FIN7 used a front company, Combi Security, purportedly headquartered in Russia and Israel, to provide a guise of legitimacy and to recruit hackers to join the criminal enterprise. Combi Security's website indicated that it provided a number of security services such as penetration testing. Ironically, the sham company's website listed multiple U.S. victims among its purported clients.

The charges in the indictments are merely allegations, and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

The indictments are 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. Arrests overseas were executed in Poland by the "Shadow Hunters" from CBŚP (Polish Central Bureau of Investigation); in Germany by the LKA Sachsen - Dezernat 33, (German State Criminal Police Office) and the Polizeidirektion Dresden (Dresden Police); and in

Spain the Grupo de Seguridad Logica within the Unidad de Investigación Technologica of the Cuerpo Nacional de Policía (Spanish National Police)..

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