Related news

cyberscoop.com/fin7-recruiter-andrii-kolpakov-pleads-guilty-role-global-hacking-scheme/

November 17, 2020

financial

FIN7 recruiter Andrii Kolpakov pleads guilty to role in global hacking scheme

(Getty Images)
Written by Jeff Stone
Nov 17, 2020 | CYBERSCOOP
One of the ringleaders of FIN7, a global hacking crew accused of stealing more than $1 billion by posing as a cybersecurity vendor, has admitted his role in the scheme.

Andrii Kolpakov pleaded guilty on Monday to conspiracy to commit wire and bank fraud and conspiracy to commit computer hacking as part of his involvement with FIN7. U.S. prosecutors had accused Kolpakov, a Ukrainian national, of working as a manager and recruiter for the crew, a role in which he hired and supervised computer specialists who spent their days stealing payment card information from dozens of companies, including Chipotle, Red Robin and Sonic Drive-In.

“During the course of the scheme, [Kolpakov] received compensation for his participation in FIN7, which far exceeds comparable legitimate employment in Ukraine,” the plea deal notes. “For the purposes of this plea agreement, the parties agree that — during [Kolpakov’s] participation in the malware scheme — FIN7 illegal activity resulted in over $100 million in losses to financial institutions, merchant processors, insurance companies, retail companies and individual cardholders.”

FIN7 is a notorious cybercrime group that’s attracted from international law enforcement agencies and an array of private security firms. Dozens of hackers worked as part of the scheme, according to the U.S. Justice Department, masquerading as a legitimate vendor called “Combi Security,” which presented itself as a penetration testing company. Rather than conducting security assessments, though, FIN7, would breach protected systems to steal credit data and other personal information.

Researchers have blamed the group for stealing more than $1 billion. The target list also included Whole Foods, Saks Fifth Avenue, Trump Hotels and other organizations with a wealth of customer payment data. Scammers still were using FIN7 malware into 2020, researchers have found.

Spanish police arrested Kolpakov in June 2018, ultimately extraditing him to the U.S. in 2019. Kolpakov was in possession of a laptop computer, multiple hard drives and a mobile phone containing “multiple thousands of payment card numbers” and usernames and passwords stolen from American companies, according to the plea deal.

Kolpakov now faces up to 25 years in prison under the terms of the plea deal.

Fedir Hladyr, another FIN7 member, pleaded guilty in September 2019. Hladyr’s sentencing is scheduled for Dec. 11.

Kolpakov’s plea agreement is available in full below.