Feds indict ‘fxmsp’ in connection with million-dollar hacking operation

By Jeff Stone

Published: 2020-07-07 · Archived: 2026-04-05 16:06:00 UTC

The U.S. Department of Justice has charged a man with hacking-related crimes as part of an investigation into a group of foreign scammers accused of targeting more than 300 organizations throughout the world.

Prosecutors in the Western District of Washington charged Andrey Turchin, who resides in Kazakhstan, with five felony counts in connection with a year-long fraud effort. Last known to be in Kazakhstan, Turchin allegedly sold remote access hacking tools on cybercriminal forums, typically charging tens of thousands of dollars for access to data that would cost victims tens of millions of dollars.

Turchin went by a series of aliases, including “fxmsp,” according to the Justice Department. He was initially charged in December 2018, though the indictment was kept under seal until Tuesday, one month after security vendor Group-IB released its own research documenting the work of a hacker known by the “fxmsp” alias.

“U.S. authorities have reason to believe that Turchin is aware of the existence of pending criminal charges in the United States,” the indictment states without elaboration.

Between October 2017 and December 2018, the indictment says, Turchin and his gang used hacking techniques — including phishing emails, malicious software, and brute-force password guessing— to access protected computers and steal data. Victims included a financial company in New York, a hotel chain with locations in Washington, an olive oil manufacturing company in California and dozens of others, according to court documents.

The group then would sell that stolen information on forums including Exploit.in, Omerta, Club2Card, Blackhacker and others.

“Following a sale, the conspirators typically provided the buyer with ongoing technical assistance with respect to purchased network access for a negotiated period of time,” the indictment says.

A separate Group-IB report detailing fxmsp’s known activities suggests the operation earned $1.5 million, though the company suggested the figures could be much higher. Fxsmp appeared on cybercriminal scene in September 2016, researchers noted, by asking other users about their experience with various strains of malware, and accidentally exposing his contact information.

By 2017, Group-IB went on, Fxmsp had advertised access to information stolen from a bank in Nigeria, and had publicly discussed launching attacks against IBM and Microsoft. The number of victims had reached 18 in early 2018, researchers found, and Fxmsp had begun working with other forum users with names like Lampeduza, who is named in the indictment, to sell access to dozens of companies.

“Fxmsp is one of the most prolific sellers of access to corporate networks in the history of [the] Russian-speaking cybercriminal underground who publicly advertised the access to 135 companies[,]” Group-IB chief technology officer Dmitry Volkv said in the report.

Often, when the U.S. Justice Department unseals an indictment against alleged hackers outside American jurisdiction, it’s an implicit acknowledgment that the suspect will be apprehended soon. John Demers, assistant attorney general for national security, told CyberScoop in February that, if prosecutors believe an arrest is likely to occur “within a reasonable time frame,” the government will keep charges sealed.

Seamus Hughes, the deputy director of the Program on Extremism at George Washington University and a specialist on court filings, first noticed the court documents had been made public.

The indictment is available in full below.

[documentcloud url=”http://www.documentcloud.org/documents/6982480-Andrey-Turchin.html” responsive=true]
