U.S.

Overseas Traders Face Charges for Hacking SEC's Public Filings Site

Network accused of making $4.1 million off 157 earnings announcements

The Securities and Exchange Commission building in Washington. PHOTO: ZACH GIBSON/BLOOMBERG NEWS

By Dave Michaels and Gabriel T. Rubin
Updated Jan. 15, 2019 2:00 p.m. ET

WASHINGTON—U.S. authorities charged traders with breaking into a government computer system that stores market-moving corporate data, moving on a breach that raised questions about the government's ability to protect sensitive data in a relentless era of computer hacking.

The Securities and Exchange Commission on Tuesday said a network of overseas traders made $4.1 million off 157 earnings announcements. It alleged a 27-year-old Ukrainian hacker, Oleksandr Ieremenko, spearheaded the intrusion of its trove of corporate filings and transmitted the information to other people who made the trades based upon an early view of filings, according to a civil lawsuit filed in the U.S. District Court for the District of New Jersey.

U.S. prosecutors are expected to file separate criminal charges against the individuals involved in the scheme, officials said.

None of the named defendants could immediately be reached for comment. Mr. Ieremenko remains in Ukraine, according to the complaint.

The SEC disclosed the hack in September 2017. Some SEC officials were aware of the breach in 2016 but initially failed to connect it to possible illicit trading. After the incident, the SEC stopped taking in some types of vulnerable data, including personally identifying information of corporate officers.

The scheme benefited from malware that Mr. Ieremenko planted on SEC computers by sending phishing emails to SEC employees posing as SEC security personnel. It was the second part of a long-term effort to hack repositories of lucrative data, following an earlier phase that targeted newswire services that disseminate corporate earnings releases, the SEC lawsuit said.

The information allegedly stolen by the hackers included filings that public companies use to test their access to the SEC's Electronic Data Gathering, Analysis and Retrieval system, known as Edgar. The test filings sometimes contained data that was to be released to investors later as part of the company's quarterly earnings announcement. Once inside Edgar, Mr. Ieremenko and his accomplices were able to download thousands of copies of the unpublished filings.

Before the test filings were made public, Mr. Ieremenko passed along the illegally obtained information to traders, who were able to profit by either buying securities or selling them short depending on how the market was expected to respond to the earnings reports. The traders used multiple brokerage accounts and entities to conceal their use of hacked information.

Mr. Ieremenko's scheme relied on speed. An unnamed public company whose stock trades on Nasdaq posted a test filing to Edgar at 2:19 p.m. on August 4, 2016, in anticipation of a negative public announcement after the market closed that day. Within eight minutes, Mr. Ieremenko's automated program dubbed "The Exfiltration Machine" had a copy of the filing. By 3:19 p.m., the trader network had started to short the stock in advance of the 4:01 p.m. announcement.

The following day, the stock closed down 12%, and the trader network had netted around $307,000.

The hackers went undetected in the SEC's corporate filing system for more than five months, when IT staffers detected an attack on Edgar and patched a defect in the system's software. The SEC's complaint said the patch blocked Mr. Ieremenko's access to company test filings.

The traders continued to trade on the remaining nonpublic information they had left, but their activity came to a halt once that material had been used up and their access to new information was cut off.

The Edgar heist and the prior newswires infiltration were notches in the belt of the at-large hacker. In the summer of 2018, using an alias for online communications, Mr. Ieremenko bragged about his successes and posted links to English and Russian-language news coverage of the hacks.

Two traders in Los Angeles were part of the network that paid Mr. Ieremenko for access to the information, the SEC said. Sungjin Cho, 38, and David Kwon, 44, were charged as defendants in the SEC lawsuit.

Several traders based in Russia were also part of the scheme, the SEC lawsuit alleged. One of the Russian traders, Andrey Sarafanov, also participated in the hack of the newswire systems that began in 2010, the SEC complaint says.

In the newswires infiltration, which took place between 2010 and 2015, hackers led by Mr. Ieremenko infiltrated newswire services' computer systems to access over 100,000 draft press releases from companies which contained nonpublic information. The targeted services included Marketwired LP, now owned by West Corporation; UBM PLC's PR Newswire, now owned by Cision Ltd.; and Berkshire Hathaway Inc.'s Business Wire.

The hackers then gave the as-yet-unpublished information to a network of traders who placed trades based on the hacked press releases before they were made public. That scheme was disrupted in 2015, and charges against Mr. Ieremenko and his accomplices remain pending.

"This action illustrates that the SEC faces many of the same cybersecurity threats that confront exchange-listed companies, other SEC-registered entities and market participants," SEC Chairman Jay Clayton said in a written statement. "These threats to our marketplace are significant and ongoing."

Mr. Clayton added that the SEC has worked to enhance its cybersecurity defenses in the wake of the hack, turning to other government agencies and outside consultants to "bolster our cybersecurity defenses and reduce our cyber risk profile."

The fallout from the hack has changed the SEC's approach to cybersecurity both for the SEC itself and for the companies it regulates, said John Reed Stark, a cybersecurity consultant and former SEC enforcement attorney. He said the agency has shifted from blaming breaches on the affected firms, and instead is emphasizing the importance of internal controls, training for employees and getting senior management involved as soon as possible after an attack is detected—a focus he attributes to the SEC's own top-down reorganization following the Edgar hack.

"They are a little more sympathetic to the entities they examine—they're not looking for perfection, they're looking for good governance," he said. "It's a case of, 'There but for the grace of God go I.'"

Write to Dave Michaels at dave.michaels@wsj.com and Gabriel T. Rubin at gabriel.rubin@wsj.com