MarketWatch

SEC’s case against Edgar hackers highlights regulator’s own cyber weaknesses

By Francine McKenna
Published: Jan 15, 2019 3:24 p.m. ET

The trading network allegedly used the stolen information to make more than $4.1 million in trading profits after making $100 million for the 2015 newswire scheme.

Chip Somodevilla/Getty Images
SEC Chairman Jay Clayton

The charges brought by the Securities and Exchange Commission against a hacker and a network of traders highlight the agency’s own vulnerabilities to cyberattacks.

The SEC on Tuesday filed charges on Tuesday in federal court for the 2016 illegal hack and trading on information stolen from the Edgar system against the same hacker and some of the same traders indicted in 2015 for the alleged cybertheft and trading on non-public company information from newswire services.

The U.S. Attorney’s Office for the District of New Jersey also announced related criminal charges in the case on Tuesday.

The defendants allegedly used the information stolen from the SEC to make more than $4.1 million in trading profits. These illicit gains are in addition to more than $100 million in profits generated during the earlier phase of the scheme when Oleksandr Ieremenko and others allegedly hacked material nonpublic information from at least three newswire services.

The SEC alleges that after hacking into the newswire services in 2015, Ieremenko, a Ukrainian hacker, bypassed Edgar’s user security to obtain nonpublic “test files,” which companies can submit to make sure the agency would process the actual filings correctly.

Some issuers had included nonpublic information in these optional test filings, such as actual quarterly earnings results not yet released to the public, the SEC said. Ieremenko passed the material non-public information to six traders in

California, the Ukraine, and Russia, and two related companies who then kicked-back a percentage of their profits to him.

“Why is the SEC allowing companies to include material non-public information in test filings given the substantial risks of cyber theft?” asked David Chase, a former attorney with the SEC’s division of enforcement, when contacted by MarketWatch. “It seems the test process is for confirming the filing mechanics and not to check content and thus why would the companies willingly submit, and the SEC permit, the inclusion of such sensitive and potentially valuable data?”

After making sure his manually executed plan worked, Ieremenko deployed a computer server to automate the theft of the material nonpublic information from test files stored in SEC servers in Middlesex County, New Jersey. Many of the illegal trades were also conducted by the trading network on various national securities exchanges, many of which process orders with servers also located in Middlesex County, New Jersey.

Ieremenko paid for the server using a cryptocurrency account of an unnamed individual.

SEC Chairman Jay Clayton said in a statement issued on Tuesday, “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 of all types. No system can be entirely safe from a cyber intrusion.”

The SEC voted in February unanimously to approve a statement and interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents. The guidance “addresses the importance of cybersecurity policies and procedures and the application of disclosure controls and procedures, insider trading prohibitions, and Regulation FD and selective disclosure prohibitions in the cybersecurity context.”

Chase says Clayton just gave companies a great excuse when the SEC comes after them for letting in criminal hackers. “The bar should be higher for the SEC. If I’m defending a company that the SEC prosecutes for weak cybersecurity controls, I can use Clayton’s own words to say it’s impossible to prevent these cyberhacks,” Chase told MarketWatch.

U.S. law enforcement charged 32 people in August 2015 with stealing non-public information about corporate earnings from the newswires to make more than $100 million over five years. The Department of Justice’s indictment of the newswire hackers said that Business Wire’s networks had been broken into more than 39 times. The Ukrainian hackers stole more than 100,000 publicly-traded company press releases which included earnings data from U.S. newswire services including Business Wire and PRNewswire before their official release. Those documents were used by a network of traders to buy or sell securities based on how they anticipated the market would react to the announcements, according to the SEC complaint.

See also: Traders busted after enlisting hackers to play stock market to net $100 million

Clayton found out about the original 2016 breach of Edgar when the agency’s lawyers realized while investigating an insider-trading case in August 2017 that their case was based on the non-public information stolen from the SEC’s own systems. Despite immediately patching the hole that hackers went through, the material non-public information had been distributed so widely to the criminal network that they were still running into instances where it had been potentially used for illegal trading.

Clayton revealed the previously unknown 2016 hack half-way through a 4,000-word statement on general cybersecurity issues that came out of nowhere on Sept. 20, 2017.

See also: SEC staff forced to tell chairman about hack when stolen data used by inside trader

The two connected cases follow a crime template established by another Ukrainian, Oleksandr Dorozhko, who in Oct. 2007 illegally hacked into Thomson Financial’s servers and stole confidential quarterly earnings information for IMS Health. Dorozhko gained access to the data while the markets were still open and purchased about $42,000 worth of IMS “put” options. IMS announced earnings that were significantly below Wall Street analyst expectations after the market closed and its stock sank almost immediately. Dorozhko made an overnight profit of nearly $287,000. His brokerage house reported the activity to the SEC.