Hacker group targets company financial info (Update)

December 1 2014

A hacker group has tapped into email accounts of executives in more than 100 companies that could give them lucrative access to market-moving information, a US security firm said Monday.

San Francisco-based FireEye said the mysterious group, dubbed FIN4, showed deep familiarity with the way businesses work and appeared to target the accounts of officials with knowledge of merger and acquisitions and other valuable corporate secrets.

Based on information from its corporate security clients, FireEye said FIN4 has gone after access to email accounts of companies' top executives, legal counsel, outside consultants and researchers.

Some two-thirds of the companies FIN4 has targeted since mid-2013 are in the pharmaceutical and healthcare industries, where there has been a surge of large deals in the past year, FireEye said.

FireEye said that of the companies it knows were targeted by the group, all but three were listed on the New York Stock Exchange or the Nasdaq Stock Market.

But it would not divulge their names, citing client confidentiality.

"FIN4 knows their targets," the FireEye report said.

"We can only surmise how they may be using and potentially benefiting

from the valuable information they are able to obtain.

"However one fact remains clear: access to insider information that could make or break stock prices for dozens of publicly traded companies could surely put FIN4 at a considerable trading advantage."

FIN4's techniques for obtaining access to executives' communications involves "spearphishing" schemes.

Those involve ostensibly real emails that trick the targeted individual into an action—like linking to a website—that can divulge to the hackers crucial login information.

In the FIN4 case, the bait emails often play on executives' concerns over the security of corporate information and adhering to securities regulations, according to FireEye.

Some of the lures are previously stolen company documents, and the hacker emails often "would be incredibly difficult to distinguish from a legitimate email" in the victim's email account.

The bait emails insert themselves into group email threads, helping them to access multiple accounts at a high level in corporate activities.

The tactics are not particularly new. What is different is the large scale and intense push of FIN4's operations. FireEye said.

FireEye did not say where the hacker group might be operating from, but it suggested FIN4 was more sophisticated than some Russian or Chinese groups.

"Their spearphishing themes appear to be written by native English speakers familiar with both investment terminology and the inner

workings of public companies."