FIN4 May Have Embarked on a Risky Hacking/Insider Trading Strategy

David Smyth
July 1, 2015

Topics: Data Security

I haven't yet turned to a life of crime, so far be it from me to criticize actual criminals' profit-maximizing strategies. It's easy for me to nitpick, but I'm not the one strapping on my mask and trying to earn a (dis)honest dollar every day. But have a look at this Reuters story from Tuesday.

In it, we learn that the SEC and the Secret Service are investigating a sophisticated computer hacking group known as "FIN4" that allegedly "has tried to hack into email accounts at more than 100 companies, looking for confidential information on mergers and other market-

BLOG ARCHIVE

TOPICS

About This Blog
Access to Court Dockets
Access to Courtrooms
Access to Search Warrants
Anti-SLAPP Statutes
Contact
Cyberattack
Data Breach
Data Security
Defamation
Digital Media and Data Privacy Law
Disclaimer
Drone Law
Fair Report Privilege
FCC Matters
First Amendment
First Amendment Retaliation
FOIA
HIPAA
Indecency
Internet
Intrusion
Miscellaneous
Mobile Privacy
Newsroom Search Warrants
Newsroom Subpoenas
Political Advertising
Prior Restraints
Privacy
Privacy Policies
Public Records

moving events. The targets include more than 60 listed companies in biotechnology and other healthcare-related fields, such as medical instruments, hospital equipment and drugs." Apparently their plan is to harvest this information and then trade on it. Nobody knows where FIN4 is from. They could be overseas, but supposedly their English is flawless and they have a deep knowledge of how financial markets work, so maybe they're in the United States. At one level, a little terrifying!

But this group hasn't devised a complex, superpowered algorithm to steal information. Instead, it's allegedly stealing information the (sort of) old fashioned way: through social engineering. The Reuters story explains that FIN4 "used fake Microsoft Outlook login pages to trick attorneys, executives and consultants into surrendering their user names and passwords." In at least one case, "the hackers used a confidential document, containing significant information that they had already procured, to entice people discussing that matter into giving their email credentials."

I have two main thoughts. First, sound information handling practices, and appropriate wariness among professionals using email, still go a long way toward securing confidential data within organizations. It's often not the most technologically advanced tactics that yield the worst data breaches. Second, FIN4 has embarked on a complex money-making plan. There may be many uses of this information, but one of them seems to be trading securities in the public markets. That's not as simple as it seems. If you're doing that, you're on the grid and can't really hide. FINRA sees all of those trades and it isn't that hard for regulators to find out who is making them. When the Consolidated Audit Trail comes online,* it will be substantially easier and faster. In the meantime, broker-dealers are

Reporters Privilege
Services
Shield Laws
Wiretapping

LINKS

International Association of Privacy Professionals
National Association of Broadcasters
North Carolina Cable Telecommunications Association
North Carolina Press Association
North Carolina Association of Broadcasters
Radio-Television News Directors Association of the Carolinas
Media Law Resource Center
The Reporters Committee for Freedom of the Press
Society of Professional Journalists
The Journalist's Toolbox - American Press Institute
Law Blog - WSJ.com
Legal Blog Watch
North Carolina Business Litigation Report

obligated to identify who their customers are. If those people have electronic connections to the ones involved in the hacking, those links could be enough for the SEC to get an asset freeze before profits are siphoned overseas.

What FIN4 is allegedly doing is scary, but they haven't yet built a criminal ATM.