Threat Research

FIN4: Stealing Insider Information for an Advantage in Stock Trading?

December 01, 2014 | by Kristen Dennesen, Jordan Berry, Barry Vengerik, Jonathan Wrolstad | Threat Intelligence

CYBER CRIME | THREAT INTELLIGENCE | CYBERSECURITY | IT SECURITY | INFOSECURITY | DATA BREACH | EMAIL SECURITY | THREAT RESEARCH

At FireEye, we investigate cyber threat activity that typically aligns with one of two goals: the pursuit of sensitive information to fulfill a government's goals, or the theft of data for financial gain. The media echoes these two objectives daily in news stories about Eastern European cybercriminals stealing payment card data from retailers, or China-based threat groups targeting high tech firms' latest innovations. A reader skimming the headline, "Hackers Steal Data from Pharmaceutical Firms" could be forgiven for assuming that the article tells the story of a government-backed group in pursuit of new drug innovations. However, in a campaign FireEye is uncovering today, this headline tells another story.

FireEye tracks a threat group that we call "FIN4," whose intrusions seem to have a different objective: to obtain an edge in stock trading. FIN4 appears to conduct intrusions that are focused on a single objective: obtaining access to insider information capable of making or breaking the stock prices of public companies. The group specifically targets the emails of C-level executives, legal counsel, regulatory, risk, and compliance personnel, and other individuals who would regularly discuss confidential, market-moving information.

FIN4 has targeted over 100 companies since at least mid-2013. All of the targeted organizations are either public companies or advisory firms that provide services to public companies (such as investor relations, legal, and investment banking firms). Over two-thirds of the targeted organizations are healthcare and pharmaceutical companies. FIN4 probably focuses on these types of organizations because their stocks can move dramatically in response to news of clinical trial results, regulatory decisions, or safety and legal issues.

We've been able to characterize FIN4's activity via our incident response engagements, FIN4's attempts to compromise our managed service clients, our product detection data, and further independent research. Our visibility into FIN4's activities is limited to its network operations; we can only surmise how they may be using and potentially benefitting from the valuable information they are able to obtain. However, one fact remains clear: access to insider information that could significantly impact stock prices for dozens of publicly traded companies surely puts FIN4 at a considerable trading advantage.

FireEye is releasing indicators to help organizations detect FIN4 activity. Those indicators can be downloaded here.

The complete report can be downloaded.

PREVIOUS POST NEXT POST

Recent Posts

23 Mar 2020
Monitoring ICS Cyber Operation Tools and Software Exploit Modules To Anticipate Future Threats >

17 Mar 2020
Six Facts about Address Space Layout Randomization on Windows >

16 Mar 2020
They Come in the Night: Ransomware Deployment Trends >

RSS FEED: STAY CONNECTED