SEC Pushes New Limits on Cyber-Security, Securities Fraud

John Reed Stark (http://www.complianceweek.com/authors/john-reed-stark) | August 11, 2015


GUEST COLUMNIST
John Reed Stark
Independent Consultant

Suppose an employee sneaks into his CFO's office, reads secret files about an upcoming positive earnings announcement, and then buys the company's stock before that announcement. Is the employee guilty of unlawful insider trading? Of course.

But suppose instead that a thief, who does not work at the company, breaks into its headquarters via a basement window at midnight, and orchestrates the same scheme. Is the thief guilty of insider trading? Historically, no—because a thief is just a thief, not a securities swindler.

In a recent dramatic turn, however, the Securities and Exchange Commission has begun targeting the thief, because the break-in is no longer through a *basement* window; instead, the break-in is through a *virtual* window, in cyber-space.

Early in 2015, the SEC began issuing new (and novel) requests and subpoenas (http://news.yahoo.com/exclusive-sec-hunts-hackers-stole-corporate-emails-trade-141938154--finance.html) to public companies about data breaches they have experienced. The SEC apparently selected public companies that, per cyber-security firm FireEye, had experienced recent data breaches targeting inside information. FireEye had previously released a December 2014 report (https://www2.fireeye.com/fin4.html) about a group of hackers called "FIN4," who target the e-mail accounts of top executives, lawyers, and others to access non-public information about public companies.

This SEC dragnet is not about insider trading, but is rather "outsider trading," and it is yet another example of the SEC's ambitious cyber-security swagger. Because to prevail in an outsider-trading enforcement action, the SEC will not only have to catch the hacker and prove the traditional elements of insider trading (typically done circumstantially), it will also have to develop "malware reverse-engineering" expertise.

Understanding the newfangled SEC jurisprudence of outsider trading and its malware-reverse engineering requirement begins with a brief discussion of insider trading.

For starters, most insider trading is perfectly legal, such as when corporate executives buy stock in their own companies as an investment. *Unlawful* insider trading occurs when, for instance, executives buy stock in their own company based on material, non-public information learned at the office. The executives have a duty not to trade on material, non-public corporate information, described in the law as a "fiduciary duty or other duty of trust and confidence."

The rationale for policing unlawful insider trading is that for the markets to work efficiently and fairly, everyone needs to be working with the same basic information, or at least that someone with access to non-public information should be prevented from taking advantage of it before other investors. The prohibition on unlawful insider trading levels the playing field and protects the integrity of financial markets.

But U.S. statutes, rules, and regulations make no explicit mention of insider trading; the prohibition is purely a judicial creation, and its outer edges are murky at best. And with cyber-thieves who trade on information stolen during a data breach, the SEC is pushing these outer edges and extending unlawful insider trading to a third and new category of securities miscreant: "outsiders," who do not work for (or with) the company, and who do not owe any duty to anyone.

> Outsider trading is the next wave for both hackers and securities swindlers. If allowed to swell, it could dramatically affect the integrity of the global financial marketplace.

SEC v. Dorozhko

Only one federal matter, *SEC v. Oleksander Dorozhko*, (https://www.sec.gov/litigation/complaints/2007/comp20349.pdf) has actually adjudicated the SEC's outsider trading theory. *Dorozhko* involved a Ukrainian engineer who bet nearly a year's worth of his income that the stock price of publicly traded company IMS Health would drop in two days, realizing profits of $280,000 (more than five times his yearly income). The SEC alleged that Dorozhko gained access to material non-public information from a data breach into Thomson Financial, a third-party online information service, and traded based on that unlawfully accessed information.

After the SEC filed an enforcement case against Dorozhko, the district court dismissed the SEC action, (http://online.wsj.com/public/resources/documents/dismiss.pdf)noting that because Dorozhko was not an officer, director, representative, or agent of IMS Health or Thomson Financial, Dorozhko owed no fiduciary duty to anyone and

Related articles

The Workflows You Need to Use After a Data Breach (http://www.complianceweek.com/news/news-article/the-workflows-you-need-to-use-after-a-data-breach)

Preparing Your Board for Cyber-Security Oversight (http://www.complianceweek.com/news/news-article/preparing-your-board-for-cyber-security-oversight)

that his trading was not "deceptive." In other words, the district court found that Dorozhko was not an insider, he was instead an *outsider*, who might be criminally liable for theft and computer crime, but it was too much of a stretch to charge him with securities fraud.

The SEC appealed, and the 2nd Circuit Court of Appeals (http://media.mofo.com/docs/pdf/090722SECvDorozhko.pdf) overturned the district court. The 2nd Circuit held that the SEC did not need to prove the existence of a fiduciary duty, because Dorozhko affirmatively misrepresented himself by his hacking. That decision recognized for the first time that when a cyber-attacker trades on stolen, exfiltrated confidential information, the SEC can charge the cyber-attacker with outsider trading.

Though Dorozhko seemed a clear victory for the SEC's outsider trading theory, a careful reading of the decision actually presents a snag for the SEC. The 2nd Circuit remanded the case back to the district court to determine the *nature of Dorozhko's hacking process*—noting that hacking might not be a securities fraud if, for instance, it was based on discovering weaknesses in software, rather than based upon a deception, such as a hacker using hijacked employee credentials.

Therein lies the rub: For the SEC staff to charge a violation of outsider trading, the SEC will have to "reverse-engineer" the malware involved in the cyber-attack and confirm that it involved a deception. This is not easy to do.

Whether the perpetrator of an insider-trader scheme is orchestrating SQL injections, cold fusion exploits, advanced persistent threat (APT) assaults, or any other online cyber-attack to access material, non-public information, the SEC staff will for the first time in its history have to offer evidence of the precise technical nature of the data breach.

For example, if a data breach occurred because a company failed to install a critical software patch, leaving a virtual door open for an online intruder, a court may find that the attack was merely breaking and entering, not a securities fraud. On the other hand, if the data breach involved the use of a rootkit (a stealthy type of malicious software, designed to hide the existence of certain processes or programs from normal methods of detection) and the kit allowed continued unauthorized access to a network, the cyber-attack may arguably involve a deception, triggering SEC jurisdiction.

Malware-Reverse Engineering

The term "malware" is misunderstood. It is often defined as software designed to interfere with a computer's normal functioning, such as viruses (which can wreak havoc on a system by deleting files or directory information); spyware (which can gather data from a user's system without the user knowing it.); worms (which can replicate themselves independently to spread to other computers); or Trojan horses (which are non-self-replicating programs containing malicious code that, when executed, can carry out an attacker's actions).

The definition of malware is actually far broader. In the context of a cyber-attack, malware means any program or file used by attackers to infiltrate a computer system. Like the screwdriver a burglar uses to gain unlawful entry into a company's headquarters, legitimate software can actually be malware. For example, during an APT attack, attackers might use "RAR" files as containers for transporting exfiltrated information, yet RAR files have a wide range of legitimate uses.

Malware can therefore be hiding in plain sight, making its reverse-engineering both an art and a science. Thus, the SEC will need forensic investigators, incident responders, security engineers, and IT administrators to employ a broad range of skills to analyze the many varieties of malware used in outsider-trading schemes.

A New Era for the SEC

Outsider trading is the next wave for both hackers and securities swindlers. If allowed to swell, it could dramatically affect the integrity of the global financial marketplace. Of all the regulators and law enforcement agencies who mark securities fraud as their territory, the SEC stands alone in its expertise, experience, and wherewithal, so it is not surprising that the 2nd Circuit validated the SEC's outsider-trading theory (albeit with a malware reverse-engineering glitch).

Whether the SEC builds its own malware reverse-engineering team in-house or engages experts from the private sector, the SEC's foray into malware reverse engineering will not only be complicated; it will be costly. Malware reverse engineers charge hourly rates akin to a law firm partner's, and even finding specialists with malware reverse-engineering skills is a challenge. Many malware specialists are self-taught or are "home-grown" within digital forensic firms, and educational institutions are only just beginning to turn out graduates with malware skills.

Only time will tell whether the SEC's outsider-trading dragnet will go down in history as the right move to protect investors or will instead be labeled yet another gratuitous jurisdictional expansion borne more from cyber-security bluster than common sense. But under any circumstance, the SEC's outsider-trading dragnet is a bold one. Whether anticipated or not, thanks to *Dorozhko*, malware reverse engineering know-how is clearly the SEC dragnet's prerequisite.