Law firm hacks traced back to Bay Area transactions

San Francisco Chronicle

By Dominic Fracassa
Tuesday, December 27, 2016

A trio of Chinese stock traders are facing federal insider-trading charges for allegedly hacking into the computer networks of two prominent law firms to steal confidential emails and other information related to active mergers and acquisitions.

The Securities and Exchange Commission and the U.S. Attorney’s Office for the Southern District of New York unveiled parallel charges Tuesday accusing Iat Hong, Bo Zheng and Hung Chin of netting about $4 million in illegal profits from stock trades based on nonpublic information from April 2014 to late 2015.

The traders were also charged with attempting to breach five other law firms for the same purpose.

Lawyers have become increasingly attractive targets to hackers in recent years given the amount of sensitive data that they inherently traffic in.

“This case of cyber meets securities fraud should serve as a wake-up call for law firms around the world: you are and will be targets of cyber hacking, because you have information valuable to would-be criminals,” said Manhattan U.S. Attorney Preet Bharara in a statement announcing his office’s 13-count indictment against the stock traders.

The names of the hacked law firms weren’t revealed Tuesday, but the charges indicate that one of the firms was breached during its involvement in two separate transactions tied to Bay Area companies.

According to the indictment, one firm was tapped to represent Intel in its $16.7 billion acquisition of integrated circuit maker Altera. After breaching the firm’s network, the hackers allegedly extracted 2.8 gigabytes of emails between January and February of 2015 and used them to buy 210,000 Altera shares. Intel publicly announced its intent to acquire Altera on June 1, 2015, netting the traders $1.4 million in profits.

An Intel spokesman said the company had no comment on the matter. In a press release announcing the Altera deal, Intel named the law firms Gibson Dunn & Crutcher and Weil Gotshal & Manges as its legal counsel. This past March, the Wall Street Journal reported that federal investigators were looking into reports of hacks suffered by Weil Gotshal and another law firm, Cravath Swain & Moore.

The firm targeted in the Intel-Altera deal was also retained by an unnamed company that was considering acquiring the Brisbane-based pharmaceutical maker InterMune in June 2014. Over
the course of about 20 days, the traders downloaded some 50 gigabytes of information from the law firm’s servers and purchased 18,000 Intermune shares.

The firm’s client ended up dropping its bid for InterMune. The company was eventually purchased by the Swiss drug giant Roche for $8.3 billion in August 2014, a deal that federal officials say netted the traders about $380,000. Roche did not respond to requests for comment.

The second law firm was hacked in April 2015 while providing counsel to the business services company Pitney Bowes, which was working to buy the e-commerce company Borderfree. The traders allegedly made $841,000 after sifting through seven gigabytes of confidential information lifted from the law firm. Cravath Swain & Moore represented Pitney Bowes in the Borderfree deal.

The traders are accused of initiating their hacks using “unlawfully obtained credentials” stolen from employees of the respective firms, according to the indictment. The traders then allegedly installed malware that gave them access to the firms’ email servers, and targeted attorneys who were working on mergers and acquisitions.

Using those emails, the traders bought shares of companies who appeared to be up for sale, but before any sale was announced. Stock prices of target companies usually spike after an acquisition is announced, giving traders with nonpublic information an unfair advantage to profit.

The indictments Tuesday in some ways echo the insider trading charges levied against an information-technology employee at the prominent Silicon Valley law firm Wilson Sonsini Goodrich & Rosati. In June 2015, Dmitry Braverman was sentenced to two years in prison after admitting to using confidential information to trade shares in companies the firm was advising in deals.

Last year, the American Bar Association reported that 15 percent of law firms have experienced a cybersecurity breach due to a hack, physical break-in or stolen smartphone. Larger firms may be more attractive targets: One in four law firms with at least 100 attorneys saw breaches.

In 2012, the association reported that just 10 percent of law firms had experienced a breach. Notably, its research also indicated that 47 percent of the 90,000 lawyers it surveyed had no response plan in place to address a security breach.