THE LATEST CHINESE HACKING STORY: BOTS WITHIN BOTS

Because the press tends to report what the government wants it to on indictments of Chinese hackers, rather than what they've really indicted, I wanted to look closely at the case against three Chinese nationals accused — per the news reports — of engaging in insider trading. Here's how Reuters describes the case against Iat Hong, Bo Zheng, and Chin Hung.

> Three Chinese citizens have been criminally charged in the United States with trading on confidential corporate information obtained by hacking into networks and servers of law firms working on mergers, U.S. prosecutors said on Tuesday.
>
> Iat Hong of Macau, Bo Zheng of Changsha, China, and Chin Hung of Macau were charged in an indictment filed in Manhattan federal court with conspiracy, insider trading, wire fraud and computer intrusion.
>
> Prosecutors said the men made more than $4 million by placing trades in at least five company stocks based on inside information from unnamed law firms, including about deals involving Intel Corp and Pitney Bowes Inc.

The indictment does, indeed, accuse the three men of hacking (probably by phishing) into a number of law firms — definitely Cravath Swain & Moore and probably Weil Gotshal to steal information on upcoming mergers and acquisitions. The indictment focuses on the contemplated acquisition of Intermune, by Intel of Altera, and by Pitney Bowes of Borderfree.

Note the indictment never says *who* was trying to

buy Intermune (that is, who the M&A customer of the law firm was). Indeed, in actuality *that* customer never bought Intermune; Roche did.

> 23. The Contemplated Intermune Transaction was never consummated or announced. Instead, before the market opened on Monday, August 25, 2014, Intermune announced that it had reached an agreement to be acquired by Roche AG, a German company. On that day, Intermune's share price increased by approximately $19 per share, or approximately 40 percent from the closing price on Friday, August 22, 2014, the last prior trading day. That same day, August 25, 2014, IAT HONG and BO ZHENG, the defendants, sold the 18,000 shares that they had begun acquiring twelve days earlier for profits of approximately $380,000.

That is, for this one transaction, the insider information didn't necessarily help, because the best information would have involved hacking Roche's firm.

Other potential buyers of Intermune listed in what may be an article cited in the indictment were Sanofi, Actelion, and GlaxoSmithKline.

That's not all that big a deal. The indictment at least alleges insider trading accomplished after hacking the lawyers advising on the deals.

Though note that M&A information may not be the only thing to find at the target firms. Christine Varney is the Cravath partner overseeing AT&T's purchase of Time Warner. That deal was first announced on October 22. This indictment was actually dated October 13 and the first item in the docket dates to June. There would be far more interesting information to some entities, including the Chinese state, about merger involving AT&T that would reside on Cravath's servers than offering prices, especially given Varney's close ties to government. That merger necessarily deals with communications policy, up to and including certain surveillance agreements. One would assume the FBI wouldn't let Cravath to continue to be hacked after the first discovery of this (though John Podesta would argue differently); but if someone like Varney were targeted, there

would be far more interesting information than just deal terms.

That said, the detail I found particularly interesting is the way the indictment alleges intellectual property theft. On top of being traders hacking for insider trading information, the indictment claims, the defendants also ran a robotics start-up.

> 3. At certain times relevant to this Indictment, the Robotics Company was a start-up robotics design company based in China, started by BO ZHENG, the defendant, which was engaged in the business of developing robot controller chips and providing control system solutions. IAT HONG and CHIN HUNG, the defendants, were both involved in running the Robotics Company.

And in addition to stealing information from M&E law firms, the indictment claims the defendants also stole information from a US and a Taiwanese firm involved in robotics.

> 7. At all times relevant to this Indictment, Robotics Company Victim-1 was a U.S.-based company engaged in the business of designing and building robots, including through the development of consumer robotics.
>
> 8. At all times relevant to this Indictment, Robotics Company Victim-2 (together with Robotics Company Victim-1, the "Robotics Company Victims") was a Taiwan-based company engaged in the design, testing, manufacture and distribution of analog integrated circuits for use in consumer electronics, computers, and communications equipment.

Indeed, the indictment claims that the defendants were stealing key intellectual property from competitors, from the very beginning of the charged period.

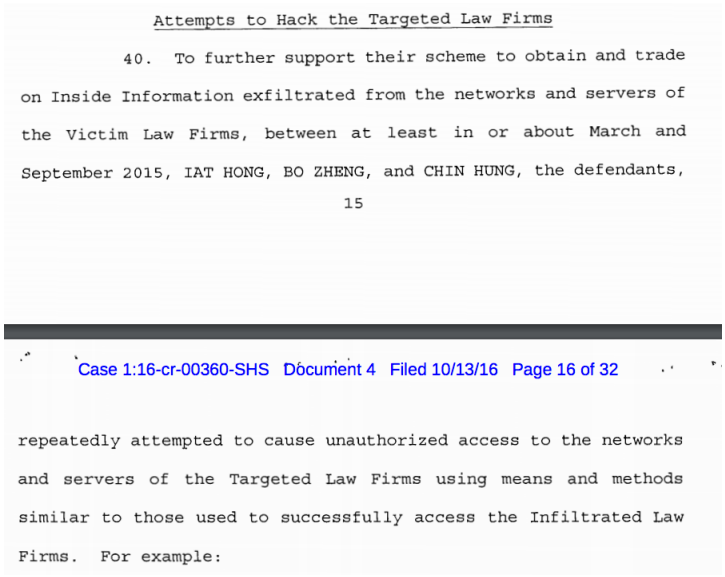
41. Also between at least April 2014 and late 2015, in addition to their efforts to hack the Victim Law Firms' networks and servers, IAT HONG, BO ZHENG, and CHIN HUNG, the defendants, also caused confidential information to be exfiltrated from the networks and servers of the Robotics Company Victims, using substantially similar means and methods of exfiltration as were used to access and attempt to access and exfiltrate information from the Victim Law Firms. Specifically, certain of the same servers that were used to carry out the hacks of the Robotics Company Victims also were used to carry out the hacks and attempted hacks of the Victim Law Firms. Among other confidential information, HONG, ZHENG and HUNG obtained confidential and proprietary information concerning the technology and design of consumer robotic products, including detailed and confidential design schematics (the "Proprietary Schematics"). Following these exfiltrations from the Robotics Company Victims, HONG, ZHENG and HUNG exchanged emails containing certain of the confidential information they had caused to be exfiltrated from the Robotics Company Victims, including the Proprietary Schematics.

This is interesting to me for several reasons. First, as I have noted, the government likes to claim a Pittsburgh indictment involves IP theft, but in reality, the indictment mostly charges the theft of information pertaining to negotiations, something the US does as well. The sole exception is the theft of nuclear reactor information between companies that already had an information sharing deal.

But also note the timing laid out in the indictment gets awfully vague when it describes the end of the theft of IP. "Late 2015" might or might not be sometime after Obama got Xi Jinpeng to agree to cut down on the hacking of the US in September 2015.

The US has generally played up any possible instance of IP theft involving Chinese nationals. That's not what happened here. Instead, this is a story about insider trading theft.

Which brings me to one other interesting passage from the indictment, which explains how the defendants tried to hack a bunch of other law firms.



Attempts to Hack the Targeted Law Firms

40. To further support their scheme to obtain and trade on Inside Information exfiltrated from the networks and servers of the Victim Law Firms, between at least in or about March and September 2015, IAT HONG, BO ZHENG, and CHIN HUNG, the defendants,

15

Case 1:16-cr-00360-SHS Document 4 Filed 10/13/16 Page 16 of 32

repeatedly attempted to cause unauthorized access to the networks and servers of the Targeted Law Firms using means and methods similar to those used to successfully access the Infiltrated Law Firms. For example:

Here, the indictment does list an end date: September 2015, the same month Obama and Xi reached their agreement.

What follows that accusation is a list of five more victim law firms the defendants allegedly tried to hack. All the attempted hacks listed took place on either March 31, or April 3, or April 6, 2015 (so nowhere close to September). Because the information is attempt focused, it might not derive from the targeted law firms (though it could come from a contractor who worked with multiple law firms), but from an attack point.

In any case, thus far this indictment has been spun as another of Preet Bharara's insider trading indictments. But there may be more here.