Client Update

Cyber Crime Gets Back to Basics: How Cyber Criminals Are Monetizing Stolen Information Through Well-Worn Criminal Strategies

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

David A. O'Neil
daoneil@debevoise.com

James J. Pastore
jjpastore@debevoise.com

David Sarratt
dsarratt@debevoise.com

BACKGROUND

News of how cyber criminals have been able to monetize the information they steal typically has been harder to come by, and less scary, than news of data breaches themselves. Last week brought two counter-examples in which cyber criminals were able to grab over $75 million in ill-gotten gains.

THE SCHEMES AND HOW THEY WORKED

Insider Trading

On August 11, 2015, the Department of Justice and the SEC jointly announced charges against a criminal group who combined hacking and insider trading in a remarkably simple way: by gaining access to earnings announcements on wire services' computer systems before they were released to the market.

News releases announcing earnings reports are typically released simultaneously by various wire services shortly after the market close. But for practical reasons, the information is uploaded to the wire services' computers earlier in the day. The criminals here used SQL injection, credential theft and other familiar hacking techniques to get access to the earnings reports before they were released publicly. Then they traded on the information, often shorting a stock just before negative news hit the street. Authorities estimated that this scheme netted the attackers more than $30 million over several years.

Impersonating the Boss

Separately, a California maker of network equipment, Ubiquiti, reported in its securities filings that it was the victim of an even more damaging cyber heist, through an even simpler means. The attackers spoofed emails that appeared to be from company executives, directing lower level employees to make funds transfers to overseas accounts, purportedly as payments to suppliers, something the company often does in the ordinary course. But these transfers were, of course, to accounts controlled by the hackers. The company reported that as a result of the spoofed emails, it transferred approximately **$46.7 million** to the thieves' accounts. The company reported that, working with law enforcement and counsel, it has recovered approximately $8.1 million of the transferred funds, and believes it will recover more from funds that have been frozen in foreign accounts.

LESSONS FOR OTHER COMPANIES

First, encourage your IT security team to spend some time thinking like a common criminal. How would you attack your business, and what would be the weak links in your human defenses, business processes and controls against scams or frauds that come through your computer systems? Perhaps your existing program of penetration testing includes questions like this; if not, consider expanding the program.

Like the two examples discussed above, many of the most damaging cyber attacks are not necessarily innovative or novel, and exploit human relationship dynamics rather than technological security gaps. Where you find potential weak points, build in redundancy to your systems and controls. Companies should also consider enhancing their processes around funds transfers—particularly for international transfers or those in excess of certain amounts—to include additional verifications before money is moved.

Second, if you are the victim of an attack, think seriously about reaching out to and cooperating with law enforcement. Corporate America has, with good reason, been concerned that civil regulators like the U.S. Federal Trade Commission will come after the victims of a data breach on the theory that their security was so inadequate as to be unlawful. But notably, in announcing the insider trading charges, the government did not make any suggestion that the newswires had inadequate security defenses. Quite the contrary, the government focused on the "sophisticated" nature of the cyber intrusions and expressly thanked the newswires, which "cooperated with law enforcement over the course of the investigation."

This statement dovetails with a recent announcement by the FTC that, in assessing the reasonableness of a company's cyber defenses, it will consider "whether [a victim] cooperated with criminal and other law enforcement agencies in their efforts to apprehend the people responsible for the intrusion."[1] Indeed, the FTC noted that "a company that has reported a breach to the appropriate law enforcers and cooperated with them has taken an important step to reduce the harm from the breach," and one that will cause the FTC to "view that company more favorably than a company that hasn't cooperated."

Both of these statements—from law enforcement and the FTC—reflect an effort to assure wary victims that regulators will not follow a "no good deed goes unpunished" policy, and that, as in other areas of enforcement actions, genuine cooperation will be rewarded. It remains to be seen how much credit cooperation will earn companies, particularly where the breach was a result of obvious security failures, but the potential benefits of cooperation bear serious consideration in every case.

* * *

Please do not hesitate to contact us with any questions.

[1] *See* "If the FTC Comes to Call," FTC Business Blog, available at https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call (last visited August 14, 2015).