BOARDMEMBER.com

Click to Print

May 14, 2013

Becoming a Victim: How Executives and Board Members Unknowingly Fall Victim to Cyber-Attacks

by Nicholas J. Percoco, Trustwave

It's 7:36 AM on a Monday morning. You just arrived at the office. As you sip your morning coffee, you notice a new email from your CFO. She is passing along the resume of a potential candidate for the head of marketing position – a position your company has been looking to fill for the past three months. Attached to the email is a document with a name that indicates it is the candidate's resume. You have a few minutes before you need to head down to the boardroom so you open it for a quick review. Oddly enough, the document is blank, so you move on to other items of interest in your inbox planning to come back to the resume after your Monday morning management team meeting.

Little do you know, you are now the victim of a targeted cyber-attack. Although the above scenario seemed completely normal to you, it was not. The end result? Every document, spreadsheet and presentation on your computer is now being sent to the attacker's computer, and it's happening in a matter of seconds.

Let's dissect this attack starting from before you received the email early this morning. One of your competitors hired a hacker to obtain business plans, financial statements, price lists, etc. from your company. This activity is known as corporate espionage and has been going on since businesses started competing, just not in the same way it is happening today – through the click of a mouse.

The hacker started by profiling your company. He read your company's SEC filings, recent press releases, company website, and even job postings.

From the SEC filings, the hacker identified the main members of your management team and board. One by one, he studied all of you, examining your public profile and anything you had published online including social media accounts, blogs, and letters to your shareholders and customers.

He also found that your company had been posting job openings for a new head of marketing on various job boards. By studying the people and a particular area of interest or need your management team had, the hacker was able to build a plan of attack.

Your competitor paid this hacker $500,000 to perform this attack. With a portion of that money, he located a vulnerability broker. The broker found a method to attack your company's computers that was unknown to your IT vendors. It was a new attack method that had been discovered but wasn't widely known. In the hacker world, this is called a Zero Day vulnerability.

Now that the hacker had this Zero Day in hand, he was able to fully craft the sequence of events and launch the attack. First, he drafted an email that was written in the same prose your CFO would use. He then created a fake resume and embedded the Zero Day within it. Finally, he spoofed your CFO's

email address and sent the email specifically at 7:36 AM because he knew that there was a good chance of catching you off guard at that time.

Once the emails were sent, the hacker sat back and watched the files flow in from your computer.

When you opened that resume, the Zero Day exploited a problem in your document reader. It installed a custom piece of malware written by the hacker that scoured your computer for the types of documents he was being paid to steal. Once the malware gathered those files, it then sent them over the Internet to the hacker's system.

This scenario may be scary, but it is important to understand that this is very real. You can find examples of these types of attack in the media every week, so it is important to understand how you and your company can protect itself from these types of attacks.

To protect yourself and your company, you should follow these steps:
1. Implement a cyber-security strategy that includes attack protection technology to help filter out emails that can contain malicious links and attachments. The technology prevents the malicious email from ending up in your inbox.

2. You also need technology and processes to monitor for unusual activity such as a large number of documents being sent from one computer to a computer or system not owned by your company.

3. Have a heightened sense of security around major company events, especially when executives are in the media or significant corporate achievements are made public.

4. Ensure that your IT department keeps executives computers, software and mobile devices updated with the latest software and patches.

5. Finally, be aware that an "attack" could come from someone you know after their account has been compromised, so be extremely cautious when prompted to take action towards an out of the ordinary request.
There is a new breed of attacks being used by hackers today and it is important that all companies are aware of the risks so they can better plan their defenses.

Nicholas J. Percoco is Senior Vice President at Trustwave. He has more than 16 years of information security experience. In his role at Trustwave, he leads the team that has performed more than 1500 computer incident response and forensic investigations globally, as well as thousands of penetration and application security tests for clients ranging from the largest companies in the world to startups.

Topic tags: board of directors, corporate governance, cyber attacks, technology risk