Law firm's trust account hacked, 'large six figure' taken

Monday, 07 January 2013 08:00 | Written By Yamri Taddese

While law firms were busy wrapping up the year and planning holiday parties, marauding fraudsters were cooking up a "scary" scam LawPRO is warning lawyers about.

"The other fraud reported to us is a scary one," LawPRO said in a Dec. 21 alert.

In a scam never seen before in Ontario, a Toronto-area law firm lost "a large six figure" over the holidays after a virus gave hackers backdoor access to its bookkeeper's computer. The virus copied bank account passwords as she typed them.

"The level of sophistication of this one was unbelievable," says Dan Pinnington, LawPRO's vice president of claims prevention and stakeholder relations.

The virus "tricked the [bookkeeper] into giving the trust account's password to the fraudsters, allowing them essentially full access to the trust account, including the ability to go in, monitor it, and wire money to foreign countries shortly after deposits were made," Pinnington adds.

Pinnington believes the hacking took place after the bookkeeper clicked on a link, opened an e-mail attachment or downloaded something as mundane as a screen saver from the Internet.

"It could be a Word document or something else, but there is a little program built or hidden inside," Pinnington says.

The built-in program, in this case, was the Trojan banker virus. It has an ability to mimic a bank's web site and when a user types in a password, the program logs the keys and sends a transcript to the hackers in real time.
An e-mail pretending to be from the bank may have provided the bookkeeper a link that launched into a spoof web site prompting her to log in, says Pinnington. But she couldn't successfully gain access using her primary password. Another window, also designed to look like the bank's web site, then asked her for her name and telephone number.

She later received a phone call, presumably from the bank.

"I see you're having problems trying to log in," a convincing fraudster reportedly told her. "We were having maintenance issues but we think we're fixed. Can you try logging in again?"

The bookkeeper did so. This time, she entered both the primary password and a second more secure password generated to last only a few minutes.

"So I guess what was happening in the background was the hackers were able to see and get what she was typing in password-wise and they immediately logged in to the firm's trust account," says Pinnington.

"They were watching. When money went in, they transferred out slightly less than the amount that went in."

Three days later, the firm noticed it was missing a six-figure amount.

The Trojan virus is known to realistically mimic U.S. bank web sites, but this time it was "a major Canadian bank," says Pinnington.

It appears the swindlers also knew the firm had done banking with another Canadian bank, he adds, noting there was evidence they sought information on another bank account as well.

Lawyers, known to have large amounts of money in their trust accounts, are often targets of such scams.

In fact, another Toronto-area lawyer was a victim of another well-known scam over the holidays. An otherwise legitimate-sounding client sent a cheque to the lawyer who deposited it into a trust account. The lawyer then wired back money owed to the client in a foreign country.

It turned out the cheque was fake and the lawyer had sent money that never went into his account.

Such scams are so frequent that LawPRO had this specific fake client's name already registered on its fraud list. If the lawyer had checked the name of the client against the list, the scam likely wouldn't have happened, LawPRO said in a recent fraud alert.

"There's been, over the last two years or so, more than 3,000 attempts at this reported to us," Pinnington says.

"Ontario lawyers are aware of them thanks to our efforts, but once in a while they are really good, they are really sophisticated, they present themselves very nicely, got real-looking documents. So every once in a while, still they're able to trick an Ontario lawyer."

A red flag in a scam like this is the fact that the client decides to pay up very fast, Pinnington adds.

Holiday distractions and bank closures make certain times of the year more convenient for scammers. But there are ways firms and lawyers can protect themselves. LawPRO, for example, has a few tips for lawyers:

- Monitor activities in all bank accounts closely and regularly.
- If a person from a bank calls, be very suspicious.
- Lawyers should immediately contact their bank through verified numbers or in person to investigate any problems with accessing bank accounts online.
- Be wary of e-mails from banks. Lawyers should contact their bank to confirm the validity of messages prompting them to take action.
- Lawyers should eliminate features on their online banking access that they don't use, such as the ability to initiate wires.
- Educate firm employees, particularly bookkeeping staff, on fraud prevention.
- Install anti-virus and anti-malware software on all computers at the office. Be sure such software will automatically update itself and that real-time scanning is on.
- Install a firewall that will block unnecessary connections between networks.
- Allow low levels of privilege to computer users that will limit the ability to download software without an administrator's permission.
- Train staff not to open e-mails or download attachments from unknown senders.
- Encourage using strong passwords that change. Using the same password for different accounts isn't a good idea.

Besides those recommendations, running regular security patches is crucial to plugging security holes that allow the majority of virus entries, says Karim Jinnah of Animate Inc., a legal information technology company.

Law firms should have a plan in place to take advantage of security updates Microsoft releases once a month, says Jinnah.

"On a regular basis, the bad guys identify vulnerabilities in the Microsoft operating systems and they write programs, malware or viruses, that exploit those vulnerabilities that they have identified."