Stolen-data trove offers look inside a botnet

March 15 2009, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- Getting hacked is like having your computer turn traitor on you, spying on everything you do and shipping your secrets to identity thieves.

Victims don't see where their stolen data end up. But sometimes security researchers do, stumbling across stolen-data troves that offer a glimpse of what identity theft looks like from criminals' perspective.

Researchers from U.K.-based security firm Prevx found one such trove, a Web site used as a stash house for data from 160,000 infected computers before it was shut down this month.

The find offers a case study on just how much data criminals are stealing every day, from the utterly inconsequential to the alarmingly private.

It also shows the difficulty in shuttering criminals' ID-theft beachheads: The Web site that Prevx found, which was operating on a server in Ukraine, was still online for nearly a month after security researchers alerted the Internet service provider and law-enforcement authorities. The site was sucking up data from 5,000 newly infected computers each day.

The victims in the Prevx find are mostly everyday people handing over their passwords for Facebook and banking sites, along with their love notes and other e-mails. But more dangerous personal information is there, too, including Social Security numbers and other account information from one bank's infected computer.

Caches of stolen data like these are hidden throughout the Internet, usually locked away inside password-protected Web sites or heavily fortified servers. Prevx's researchers were able to infiltrate this site because it was protected with poor encryption.

In that sense, the find illustrates how even sloppy crooks can vacuum up enormous amounts of information through massive "botnets" - armies of infected computers formed by spreading a computer virus that orders compromised machines to phone home for further instructions, such as sending out spam or relaying passwords.

The botnet Prevx found was only harvesting data, though Prevx said it could have been upgraded to do other things.

Ordinary Internet sessions are logged in great detail. One Southern California 22-year-old could be seen registering a domain name with GoDaddy.com, changing his Yahoo e-mail password and ordering a meal online from Pizza Hut. His credit card number, birth date, telephone number, address and passwords are now all in criminals' hands, though it's unclear what, if anything, criminals have done with the information yet.

Some victims are gold mines for sensitive data. An infected computer at a Georgia bank exposed customer details and credentials for the bank's wire-transfer system. Bank employees were checking e-mail, looking up BMWs and Infinitis and working with customers' accounts on the same infected machine.

Government computers were also hit, including one in Texas that coughed up Web site logins for one of the government's health care providers, and another in North Carolina that revealed access to an agency's human resources system.

"This is giving criminals the keys to the castle," said Prevx's director of malware research, Jacques Erasmus. "Once they're into this system, it might not seem at this point like it's the biggest data heist ever, but this is how they get into a network. This is their game - they do this every day."

In other words, criminals start small, then use their first point of attack as a way to jump onto more sensitive computers.

Researchers who discover these stolen-data caches then have to figure out what to do with them. Notifying victims is time-consuming and difficult, and researchers tend to focus on trying to get service providers to deactivate the servers before criminals get to the data on them.

Prevx said it alerted the site's Internet provider, the FBI and U.K. authorities about the breach it discovered. The company also talked to the affected bank, Doraville, Ga.-based Metro City Bank, a community bank whose Web site lists four locations, and Prevx said the bank has removed the infected computer.

One customer - Yoon-Kee Hong, a 22-year-old college student from Suwanee, Ga. - had signed up for an account with Metro City Bank just a month before learning about the breach. He said he had not been alerted by the bank that his Social Security number and other personal details were stolen.

After being told about the breach by The Associated Press, which picked his name from the files provided by Prevx, the student said he planned to cancel his account.

"I cannot trust them any more," he said. "They're not doing what they're supposed to do. They didn't even notify me. It's like they're trying to hide it from their customers."

He later relented and decided to stay with the bank after he was offered a new account and promises of fraud alerts.

The bank said in a statement that it is notifying customers and is investigating the breach, refusing to comment further. State officials in North Carolina and Texas didn't return calls on the breaches there. The FBI didn't return a call about the breaches.

Such finds are becoming more common as the barrier lowers for crooks to jump into the online identity-theft racket. Top-of-the-line viruses, also known as Trojans, can be had for under $1,000.

Joe Stewart, a SecureWorks Inc. botnet expert who was not involved in Prevx's research, said that last year, he helped shut down a command-and-control server for a huge botnet that had infected more than 378,000 machines and had stolen more than 460,000 usernames and passwords.

There are countless other smaller botnets, set up by less sophisticated criminals who steal as much data as they can and simply pull up stakes, and do it all over again, once their operation has been detected.

"The level of amateurness speaks to how widespread it is," Stewart said. "Literally anybody with a little bit of computer knowledge at all, if they have the criminal bent, can get access to one of these Trojans and get it out there and start stealing people's data."

How to tell, what to do if computer is infected

Computer-virus infections don't cause your machine to crash anymore.

Nowadays, the criminals behind the infections usually want your computer operating in top form so you don't know something's wrong. That way, they can log your keystrokes and steal any passwords or credit-

card numbers you enter at Web sites, or they can link your infected computer with others to send out spam.

Here are some signs your computer is infected, tapped to serve as part of "botnet" armies run by criminals:

- You experience new, prolonged slowdowns. This can be a sign that a malicious program is running in the background.

- You continually get pop-up ads that you can't make go away. This is a sure sign you have "adware," and possibly more, on your machine.

- You're being directed to sites you didn't intend to visit, or your search results are coming back funky. This is another sign that hackers have gotten to your machine.

So what do you do?

- Having anti-virus software here is hugely helpful. For one, it can identify known malicious programs and disable them. If the virus that has infected your machine isn't detected, many anti-virus vendors offer a service in which they can remotely take over your computer and delete the malware for a fee.

- Some anti-virus vendors also offer free, online virus-scanning services.

- You may have to reinstall your operating system if your computer is still experiencing problems. It's a good idea even if you believe you've cleaned up the mess because malware can still be hidden on your machine. You will need to back up your files before you do this.

How do I know what information has been taken?

- It's very hard to tell what's been taken. Not every infection steals your data. Some just serve unwanted ads. Others poison your search result or steer you to Web sites you don't want to see. Others log your every keystroke. The anti-virus vendors have extensive databases about what the known infections do and don't do. Comparing the results from your virus scans to those entries will give you a good idea about what criminals may have snatched up.

On the Net:

http://www.prevx.com/blog.asp