Cyber Theft Ring is Caught

Wall Street Journal 10-12-10 Technology Section

By M.P. MCQUEEN

When a giant international cyber-theft ring was broken up last week, details emerged about a new tactic hackers are using: bombarding individual and business phones with incessant calls using automated dialing programs and, while the phones are tied up, raiding bank and brokerage accounts.

View Full Image

Alex Nabaum

If the financial institutions can't reach the victims to ask about the suspicious activity, the transactions often go through, law-enforcement officials say. It is a new twist on so-called denial-of-service attacks, in which hackers overload financial-services websites with information in order to crash them.

The cyber-theft ring—in which dozens of arrests were made in the U.S., the U.K., the Netherlands and Ukraine, according to court documents and federal officials—allegedly used the tactic, among others.

The ring was responsible for losses of $70 million from accounts at various banks and brokerage firms, including J.P. Morgan Chase& Co., E*Trade Financial Corp. and TD Ameritrade Holding Corp.'s TD Ameritrade, according to the Federal Bureau of Investigation.

TD Ameritrade confirms that it has been working with the FBI in its investigation of the ring since last December. Chase says it is working closely with national and local law enforcement and cyber-security experts. An E*Trade spokeswoman says the company is cooperating with the investigation.

The ring allegedly used a "malware" program called "Zeus Trojan" to hijack accounts, embedding it in email messages and attachments. Once installed, it grabbed user names and passwords from banking and brokerage accounts, enabling the alleged thieves to drain the accounts.

At the same time, victims' phones were tied up with a barrage of phone calls, according to the federal complaints, preventing them from contacting their bank or brokerage. Busy signals also prevented fraud monitors at the institutions from contacting victims, according to FBI officials who were interviewed before the announcement of the arrests.

The ring then allegedly took over the accounts, transferring funds to new ones set up by "mules," or accomplices, who collected funds and transferred them elsewhere.

The telephone bombardments lasted as long as a week, sometimes forcing victims to disconnect their lines or switch phone numbers, which bought the suspects time to raid their accounts.

"They overwhelm a victim's phones so that the bank can't call the victim and the victim can't call them," says Timothy Ryan, supervisor for the cyber-investigations unit of the FBI's Newark, N.J., office. The FBI issued an alert for consumers about the telephone denial-of-service attacks in June.

Investigators say the computer attacks on financial institutions originated from Eastern Europe, and many but not all of the mules were students visiting the U.S. from Russia.

Victims across the U.S. have had anywhere from a few thousand to several hundred thousand dollars stolen from their accounts, officials say. Bryan Sartin, a security expert at Verizon Communications Inc., says he knows of at least a dozen institutions that have been targeted since February 2010, and at each one, up to hundreds of customers were affected.

One victim, a dentist in Florida, had nearly $400,000 siphoned from a TD Ameritrade account last December. The victim was reimbursed by the brokerage, a spokeswoman says.

Avivah Litan, a security analyst at Gartner Inc., a technology consultancy, says this type of denial-of-service attack is increasing as financial institutions' attempts at telephone verification become more common. Similar tactics already have been used in the U.K., Scandinavia and South Africa, and are part of an upsurge in wire and electronic-funds transfer thefts at financial institutions that have drastically escalated in the past year, affecting mostly small businesses and nonprofit groups.

"It's the fastest-growing crime, along with ATM skimming," Ms. Litan says.

Federal laws protect consumers' deposit accounts and bank-issued credit cards from liability for unauthorized electronic funds transfers, as long as they are reported in a timely fashion, according to the Federal Reserve. But these laws don't always protect small businesses and other organizations.

Online investors are generally protected by federal and state laws requiring broker-dealers to safeguard financial assets and information. Some brokerages, including TD Ameritrade and E*Trade, have policies that state they will reimburse victims for thefts of funds if they are reported in a timely fashion and if the investor can demonstrate the thefts weren't their fault.

FBI officials and security experts say the best way to protect against computer-assisted fraud is to use a dedicated computer for online banking and brokerage transactions. Web surfing increases your risk of having malware installed on your computer.

Use secure passwords and change them often. Update antivirus and firewall software regularly and be wary of suspicious or unsolicited emails, attachments and links. Check financial statements often and promptly notify financial institutions of suspicious transactions.

Contact your telephone-service provider immediately if you are a victim, as well as your financial institution. You also should notify the FBI at the Internet Crime Complaint Center website (www.ic3.gov).

Questions for GVSU students to answer prior to Class:

1. **Summarize the Cyber Attacks described in this article.**
2. **What is a Zeus Trojan and how does it work?**
3. **What are the fastest growing net crimes?**
4. **What does the article suggest that companies and individuals do to prevent these cyber attacks?**
5. **How much of an impact do you think these cyber attacks have on the global economy?**

6. **Take a look at the FBI net complaint web site listed above.**