Cyberthieves still rely on human foot soldiers

November 22 2010, By ALICIA A. CALDWELL and PETE YOST , Associated Press

This poster released by the FBI shows photos of individuals wanted by the FBI and shows Eastern European Cyber Criminals, wanted on a variety of federal charges stemming from criminal activities including money laundering, bank fraud, passport fraud, and identity theft in New York. Complaints were issued by the United States District Court, Southern District of New York, in September of 2010. The court records of Operation Trident Breach reveal a surprise: For all the high-tech tools and tactics employed in these computer crimes, platoons of low-level human foot soldiers, known as "money mules," are the indispensable cogs in the cybercriminals' money machine. (AP Photo/FBI)

(AP) -- Sitting at a computer somewhere overseas in January 2009, computer hackers went phishing.

Within minutes of casting their electronic bait they caught what they were looking for: A small Michigan company where an employee

unwittingly clicked on an official-looking e-mail that secretly gave cyberthieves the keys to the firm's bank account.

Before company executives knew what was happening, Experi-Metal Inc., a suburban Detroit manufacturing company, was broke. Its $560,000 bank balance had been electronically scattered into bank accounts in Russia, Estonia, Scotland, Finland and around the U.S.

In August, the Catholic Diocese in Des Moines, Iowa, lost about $680,000 over two days. Officials there aren't sure how hackers got into their accounts, but "they took all they could" before the bank noticed what was going on, according to Jason Kurth, diocese vice chancellor.

The diocese and the Detroit company were among dozens of individuals, businesses and municipalities around the country victimized by one of the largest cybertheft rings the FBI has uncovered.

In September, the bureau and its counterparts in Ukraine, the Netherlands and Britain took down the ring they first got wind of in May 2009 when a financial services firm tipped the bureau's Omaha, Neb., office to suspicious transactions. Since then, the FBI's Operation Trident Breach has uncovered losses of $14 million and counting.

Overall in the last two years, the FBI has opened 390 cases against schemes that prey on businesses that process payments electronically through the Automated Clearinghouse, which handles 3,000 transactions every five seconds. In these cases, bureau agents have uncovered attempted thefts totaling $220 million and actual losses of $70 million.

But the court records of Operation Trident Breach reveal a surprise: For all the high-tech tools and tactics employed in these computer crimes, platoons of low-level human foot soldiers, known as "money mules," are the indispensable cogs in the cybercriminals' money machine.

A dozen FBI criminal complaints filed in New York provide an inside look at how this cybertheft ring worked:

Operating from Eastern Europe and other overseas locations, the thieves used malicious software, known as malware, to infect the computers of unsuspecting users in the United States by e-mail. The malware-infected e-mails were written to look like they came from a company manager or colleague who might send an e-mail message to everyone in a company, such as the head of human resources.

When the e-mail recipient clicked on an embedded link to a website or opened an attachment, a Trojan horse virus called Zeus installed itself and gathered usernames, passwords and financial account numbers typed by the victims on their own computers. The hackers then used this information to move the victims' money electronically into bank accounts set up in the United States by the money mules.

The money mules set up shell bank accounts to receive the money. Then they withdrew the funds from the shell accounts in amounts they thought were small enough to elude detection by banks and law enforcement. In some cases, the cyberthieves bombarded telephone numbers attached to the targeted accounts with calls to block the company from calling to verify the transactions.

The mules sent most of the stolen funds overseas electronically to accounts controlled by the ring leaders; the mules usually kept 8 to 10 percent as their cut.

For instance, the FBI said money belonging to one TD Ameritrade customer landed in the bank account of a fake company, the Venetian Development Construction Service Corp., which was registered at an unmarked, two-story brick building in Brooklyn. The sole name on the construction company's account was that of one of the money mules.

Eventually some of the money wound up in accounts in Singapore and Cyprus and some walked out the bank's door in the pockets of mules. TD Ameritrade spokeswoman Kim Hillyer said the company has reimbursed customers who lost money

Just like in the illegal drug trade, the ring leaders overseas reaped the big profits but relied on the mules to do the risky, dirty work.

For each shell account, a mule had to walk into a bank, in full view of surveillance cameras and leave copies of personal identification documents. The ring leaders hid behind computer screens overseas.

Operation Trident Breach found many mules are Eastern Europeans who came to the U.S. on student visas.

Among the allegations in the FBI's criminal complaints:

One mule was an immigrant from Moldova who within a few months of her arrival in New York this year had opened at least six bank accounts using a trio of names. Another mule, a Russian national, opened eight accounts at three different banks using five different aliases.

The criminal networks used so many money mules that full-time recruiters were needed. One recruiter placed advertisements on Russian language websites seeking students with U.S. visas.

A pair of Russian roommates living in Brooklyn worked together. One smuggled at least $150,000 in cash to hackers in Russia, arranged for fake passports to be smuggled into the U.S., and acted as a middleman picking up and delivering stolen money from other mules. The other roommate opened accounts with fake names and false passports in New York and New Jersey this summer.

This cybertheft ring zeroed in on individuals and small- and medium-sized businesses because they usually have fewer computer security safeguards than huge companies. Among its targets: municipalities in Massachusetts and New Jersey, the account held by a hospital at a California bank and the computers of at least 30 customers of E Trade Financial Corp.

Like a number of victims, Experi-Metal has sued its bank over the thefts.

A lawyer for Experi-Metal, Richard Tomlinson, said the thieves emptied the company's account and then tried to siphon another $5 million out through an empty savings account of an Experi-Metal employee. They actually transferred another $1.34 million before the bank shut down the mystery wire transfers, Tomlinson said.

According to court records, the company's bank, Dallas-based Comerica Inc., has recovered all but the company's original balance of $560,000. Tomlinson said the bank should be liable for the company's losses because the wire transfers were obviously dubious - the company hadn't made any transfers in more than two years and never to Eastern Europe.

"Canada was maybe as exotic as we got and it was maybe three or four years before this," Tomlinson said.

Comerica says it wasn't part of the problem.

"This was caused solely by the actions of that (Experi-Metal Inc.) employee," a lawyer for the bank wrote in a court filing. "The criminal that accessed Experi-Metal's accounts was able to do so only because Experi-Metal gave him its key."

More information:

FBI background: http://tinyurl.com/27ae5bc

E Trade security: http://tinyurl.com/34g9zya

E Trade losses: http://tinyurl.com/2v3oga7

TD Ameritrade: http://www.tdameritrade.com/security/index.html

Comerica security: http://tinyurl.com/2u9akou