For banks, cyberattacks lurk as constant threat

November 16 2012, by Jennifer Bjorhus

When denial-of-service cyberattacks were jamming up major bank websites in September, the public disruption made headlines.

But in the sketchy recesses of the underground Web, something potentially much more damaging was apparently brewing. IT security company RSA noted in an Oct. 4 blog post that a cybergang linked to Eastern Europe was recruiting about 100 botmasters for a planned "blitzkrieg-like series of Trojan attacks" on 30 U.S. financial institutions. The weapon was dubbed Gozi Prinimalka, a mutation of the Gozi financial malware that has bedeviled banks for several years now.

RSA analyst Mor Ahuvia, in Israel, blogged that if the project materialized it would be "the largest coordinated attack on American financial institutions to date."

The Gozi rumblings illustrate the significant challenge banks face defending against myriad shifting cyberthreats. The denial-of-service attacks inconvenienced customers and made a statement. But Gozi, like its older cousin Zeus and other financial malware, is about draining money right out of accounts. It's a subject banks have been loath to discuss.

RSA, the security division of tech giant EMC Corp. in Massachusetts, wouldn't release the list of targets. But Internet security firm Trend Micro Inc. in Cupertino, Calif., provided a list that includes 26 companies including Charles Schwab and Scottrade as well as several of the country's top banks.

Wells Fargo & Co. and U.S. Bank declined to comment for this story.

The Gozi cyberheist isn't targeting bank networks. It goes after customers banking online, and siphons money from accounts by essentially taking them over without victims knowing it. Gozi allows cyberthieves to steal a company's online banking credentials to gain access to their business accounts, impersonating both the victim and the financial institution. Detection is very difficult.

"It's the scariest way that they commit fraud," said Ryan Elmer, an account executive at Total Networx Inc., an IT security company in Burnsville, Minn., that's focused on banks.

The malware can lurk in email attachments, for instance, or be embedded in poisonous websites that victims unwittingly browse.

Cyberthieves looting company bank accounts by taking them over - dubbed corporate account takeover - is a top fraud concern of banks. Gozi is the latest tactic in corporate account takeover, according to Total Networx. Increasingly, attacks target small-business bank customers.

They're an attractive target. Small companies typically lack the IT resources and controls of large ones. And unlike individual bank customers with a checking account, businesses wire large sums of money around and use the electronic Automated Clearing House to handle such transactions as payroll.

Corporate account takeovers caused losses of at least $45 million last year, according to the Federal Deposit Insurance Corp. The FBI says it's investigating about 230 reported cases of such fraud, involving the attempted theft of more than $255 million, with actual losses around $85 million.

Last month, hackers stole more than $400,000 from a Bank of America account held by the town of Burlington, Wash., near Seattle.

Ahuvia, at RSA, said the thieves behind the purported Gozi campaign are targeting U.S. financial institutions partly because they don't use a second layer of authentication - an added security measure beyond a login and password - for private banking customers to the extent banks in Europe do. Federal bank regulators last year recommended banks use multiple layers of authentication, but it's not a mandate.

What's notable about the latest Gozi version, she said, is the degree to which it can impersonate an account holder, duplicating the victim's complete PC settings in an attempt to deceive the bank's back-end security systems. The scheme involves phone-flooding software to block victims from getting a call or text message from the financial institution that would verify online account activity.

Cyber security expert Brian Krebs blogged that he thinks RSA's findings are linked to a Russian hacker nicknamed "vorVzakone" who communicated on underground forums in September that he was planning Project Blitzkrieg. Curiously, a man claiming to be vorVzakone posted a gloomy video of himself on YouTube driving a Toyota Land Cruiser and giving a tour of a two-level suburban-style house he said was his home.

Krebs aptly described him as a "stocky bald guy in sunglasses."

Tech security circles have buzzed about the timing of the potential Gozi spree, which was expected to hit as early as this month. There are plenty of skeptics. In a recent interview, Daniel Cohen, RSA's head of business development for Online Threats Managed Services, said the Gozi blitzkrieg may be off altogether.

"The leader of this attack campaign has since posted within the underground forums that he has canceled his plans, though we suspect he has probably gone deeper underground," Cohen said via email. "They may very well attempt to regroup and launch the same campaign but with more secrecy. We are continuing to monitor the forums for any developments."

Doug Johnson, vice president of risk management policy at the American Bankers Association, said he couldn't help but laugh at the vorVzakone video. But whether or not you think the big Gozi heist is real, it must be taken seriously, he said.

"We're aware clearly that the overall cyberthreat environment is escalating," Johnson said. "We are practicing an extra level of diligence."

Whether the blitzkrieg is a go, Elmer said he's staying on high alert. Threat levels change, but the threats never permanently vaporize, he said.

"Cybercriminals will share their exploits with one another and all it takes is another ringleader to take the ball and run with it," Elmer said. "Also we will oftentimes see threats being recycled, where hacks that were popular five years ago are modified and re-released."

Total Networx customers, primarily community banks, have generally protected their networks, he said. The bigger problem is the banks' corporate customers who have looser security, he said.

"What banks have really been after is something that can cheaply and effectively put their users in a bubble," Elmer said.

His company has devised a way to effectively segregate users from the bank network, he said. He said he couldn't divulge details. Before the latest Gozi threat he expected to set up about 1,000 such segregations in six months. If Gozi materializes, it could be four to five times that, he said.

It represents progress, he said. Banks have often kept the problem secret; it's easier to put the lost money back into a customer account and move on. Now trade associations, regulators and the FBI are pushing to get all banks to discuss the problem with their customers.

The various entities have started the push to make sure every bank is broaching the topic with customers.

"Up until this point," he said, "there were only a handful of banks that were comfortable talking about it with their customers."

—-

MODERN BANK ROBBERS:

An Eastern European cybergang supposedly has been gathering recruits in recent months to wage a large-scale attack that would drain money from customer accounts at 30 U.S. financial institutions.

-How it works: The Gozi malware lets thieves impersonate both a financial institution and its customer, making detection difficult.

-Who's behind it: Underground forums have pointed to a Russian hacker nicknamed "VorVzakone."

-Status: Recent UnderWeb posts suggest the attack is off for now, but cybercriminals like to stay unpredictable.

Citation: For banks, cyberattacks lurk as constant threat (2012, November 16) retrieved 12 May 2024 from https://phys.org/news/2012-11-banks-cyberattacks-lurk-constant-threat.html