Hackers' $1 billion bank theft may still impact consumers

February 17 2015, byJosh Boak

In this Saturday, Jan. 5, 2013 file photo, a person inserts a debit card into an ATM in Pittsburgh. Security experts say consumers still need to keep a close eye on their checking and savings, as epic computer breaches are becoming all too common. (AP Photo/Gene J. Puskar, File)

The hacker gang that looted as much as $1 billion worldwide from banks was unusual: It stole directly from the banks, instead of ripping off their customers.

But this was hardly a bit of Robin Hood banditry that spared innocent account holders. Security experts say consumers still need to keep a close eye on their checking and savings, as epic computer breaches such as this theft—documented in a report issued Monday—are becoming all too common.

"Customers are still at risk," said Sergey Golovanov, a researcher at the Russian cybersecurity firm Kaspersky Lab that released the report. "Criminals had access to all banking infrastructure, so they were able to get any data about customers."

Doug Johnson, senior vice president at the American Bankers Association, said there's no evidence that any U.S. bank has been a victim of this particular breach. Still, the report found that some of the proceeds were deposited with banks in China and the United States.

The hacks detailed in the report, which was presented at a security conference in Cancun, Mexico, are the latest twist on data breaches that have struck not just banks but the health insurer Anthem and major retailers such as Target and Home Depot. And just like those thefts, experts say there are simple protections that consumers can take.

For starters, most American bank customers are insured against theft by the Federal Deposit Insurance Corp. The insurance applies to any sum up to $250,000 in checking, a savings account or a certificate of deposit at a U.S. bank.

Still, more people have become vigilant about monitoring their transactions and responding to alerts from their banks if a charge or withdrawal appears to be suspicious.

"We all look at our bank statements a hell of a lot more carefully than 20 years ago," said John Gunn, vice president of communications at

VASCO Data Security, which provides authentication software for financial institutions.

There are other simple moves that individuals can do to guard their financial data, said Stu Sjouwerman, founder of the data security firm KnowBe4.

Even if it appears to be from their bank, people should never open email attachments that they didn't request. Nor should they click on links inside emails, but instead type the name of their bank into the Web browser address bar. And they should only provide a Social Security number or account information over the phone on calls that they initiated.

"Those are the normal things you would recommend consumers to use," Sjouwerman said.

It appears as though the hacker gang accessed computers by having bank employees click on email attachments.

The hackers relied on a technique known as "spear phishing," in which they sent emails from a fake account that looked familiar to the bank workers. Those emails infected the computer with a form of malware called Carbanak and gave the gang entry into the internal network, allowing them to mimic the actions of workers responsible for the cash transfer systems.

In a plan that smacked of a Hollywood thriller, the hackers then lurked unseen in the systems of more than 100 banks in 30 countries, according to the Kaspersky Lab report. Working in stealth for months, the group would learn how each bank operated and used that knowledge to steal up to about $10 million in each raid, a sum just small enough to go nearly undetected in the daily shuffle of money.

Their intended targets were primarily in Russia, followed by the United States, Germany, China and Ukraine, Kaspersky says. One bank lost $7.3 million when its ATMs were programmed to spew cash at certain times that henchmen would then collect, while a separate firm had $10 million taken via its online platform. The attacks remain active after about two years of thefts.

The report did not identify the banks involved and Kaspersky is partnering with law enforcement agencies to investigate the hacking that allegedly came out of Russia, Ukraine, and other parts of Europe and China.

Just as the hacking has grown more persistent, banks say their defenses have improved. Johnson of the American Bankers Association said that $10 worth of fraud is stopped for every $1 that succeeds, compared to a ratio of one-to-one roughly a decade ago. The banks also insure against their computer networks being compromised and set aside capital to withstand any losses from fraud.

Yet the hacking attempts continue to evolve in ways that indicate the battle may never end.

"These exploits are going to continue," Johnson said.

Citation: Hackers' $1 billion bank theft may still impact consumers (2015, February 17) retrieved 5 June 2023 from https://phys.org/news/2015-02-hackers-billion-bank-theft-impact.html