The New York Times | http://nyti.ms/1nF1uJc



**TECHNOLOGY** | NYT NOW

# JPMorgan and Other Banks Struck by Hackers

By NICOLE PERLROTH AUG. 27, 2014

A number of United States banks, including JPMorgan Chase and at least four others, were struck by hackers in a series of coordinated attacks this month, according to four people briefed on a continuing investigation into the crimes.

The hackers infiltrated the networks of the banks, siphoning off gigabytes of data, including checking and savings account information, in what security experts described as a sophisticated cyberattack.

The motivation and origin of the attacks are not yet clear, according to investigators. The F.B.I. is involved in the investigation, and in the past few weeks a number of security firms have been brought in to conduct forensic studies of the penetrated computer networks.

According to two other people briefed on the matter, hackers infiltrated the computer networks of some banks and stole checking and savings account information from clients. It was not clear whether the attacks were financially motivated, or if they were collecting intelligence as part of an espionage effort.

JPMorgan has not seen any increased fraud levels, one person familiar with the situation said.

“Companies of our size unfortunately experience cyberattacks nearly every day,” said Patricia Wexler, a JPMorgan spokeswoman. “We have multiple layers of defense to counteract any threats and constantly monitor fraud levels.” Joshua Campbell, an F.B.I. spokesman, said the agency was working with the Secret Service to assess the full scope of

attacks. “Combating cyberthreats and criminals remains a top priority for the United States government,” he said.

The intrusions were first reported by Bloomberg, which indicated that they were the work of Russian hackers. But security experts and government officials said they had not yet made that conclusion.

Earlier this year, iSight Partners, a security firm in Dallas that provides intelligence on online threats, warned companies that they should be prepared for cyberattacks from Russia in retaliation for Western economic sanctions.

But Adam Meyers, the head of threat intelligence at CrowdStrike, a security firm that works with banks, said that it would be “premature” to suggest the attacks were motivated by sanctions.

Russian hackers began a monthlong online assault on Estonia in 2007 that nearly crippled the Baltic nation, after Estonian government workers moved a Soviet-era war memorial from the Estonian capital.

Still, security experts say that the stealthy nature of the recent attacks suggests that their motivation was not political.

The American banking sector has been a frequent target for hackers in recent years, with the vast majority of attacks motivated by financial theft.

But not all of them. Over the past two years, banks have been targeted in a series of politically motivated attacks from Iran, in which a group of Iranian hackers flooded United States banking sites with so much online traffic — a method called a distributed denial of service, or DDoS, attack — that the websites slowed or intermittently collapsed.

Hackers who took credit for those attacks said they went after the banks in retaliation for an anti-Islam video that mocked the Prophet Muhammad, and pledged to continue the attacks until the video was removed from the Internet.

American intelligence officials said the group was actually a cover for the Iranian government. Officials claimed Iran was waging the attacks in retaliation for Western economic sanctions and for attacks on its own systems.

Unlike the attacks traced to Iran, the recent hacks against the American banks were not intended to disrupt the bank's services but appeared to be part of a financial or intelligence-gathering effort, three people briefed on the investigations said.

Mr. Meyers, of CrowdStrike, said hackers could have been after account information, or even intelligence about a potential merger or acquisition. Security experts said the hackers chose to pursue account information, not disruption, which is the earmark of state-sponsored attacks.

Because JPMorgan had not seen any unusual incidences of fraud, however, it was too early to conclude that the attacks were solely financially motivated.

So why were the banks targeted? Security experts said they could not yet determine whether the attacks over the past few weeks were the work of Russians, or whether they were politically motivated. Indeed, Mr. Meyers said, any such conclusions at this point would be the result of what he said was an effort by security firms to be the first to present conclusive evidence.

Banks are also frequent targets for intelligence agencies looking to collect information about their targets. In 2012, Russian security researchers uncovered a computer virus on 2,500 computers, many of them inside major Lebanese banks, including the Bank of Beirut and Blom Bank. The virus was specifically intended to steal customers' login credentials to their bank accounts.

The researchers believed the computer virus was state-sponsored and said they had found evidence it had been created by the same programmers who created Flame and Stuxnet, two computer viruses that officials have said were unleashed by the United States and Israel to spy on computers inside Iran.

Jessica Silver-Greenberg, Nathaniel Popper, Michael Corkery, David Gelles and Matt Apuzzo contributed reporting.

A version of this article appears in print on August 28, 2014, on page B1 of the New York edition

with the headline: 5 U.S. Banks Hit in Attack by Hackers.

---