

NYT NOW

Neglected Server Provided Entry for JPMorgan Hackers

By **Matthew Goldstein, Nicole Perlroth and Michael Corkery**

December 22, 2014 8:41 pm

The computer breach at JPMorgan Chase this summer — the largest intrusion of an American bank to date — **might have been thwarted if the bank had installed a simple security fix to an overlooked server in its vast network**, said people who have been briefed on internal and outside investigations into the attack.

Big corporations like JPMorgan spend millions — \$250 million in the bank's case — on computer security every year to guard against increasingly sophisticated attacks like the one on Sony Pictures. But the weak spot at JPMorgan appears to have been a very basic one, the people said. They did not want to be identified publicly because the investigation into the attack is incomplete.

The attack against the bank began last spring, after hackers stole the login credentials for a JPMorgan employee, these people said. Still, the attack could have been stopped there.

Most big banks use a double authentication scheme, known as two-factor authentication, which requires a second one-time password to gain access to a protected system. But JPMorgan's security team had apparently neglected to upgrade one of its network servers with the dual password scheme, the people briefed on the matter said. That left the bank vulnerable to intrusion.

The oversight is now the focus of an internal review at JPMorgan that seeks to identify whether there are any other unguarded holes in the bank's vast network, several of the people briefed on the matter said, adding that, internally, the episode is seen as an embarrassment.

The relatively simple nature of the attack — some details of which have not been previously reported — puts the breach in a new light. In August, when Bloomberg News first reported on the attack, which ultimately compromised some account information for 83 million households and small businesses, the bank’s security experts and the Federal Bureau of Investigation feared a sophisticated adversary. Some suspected the attack, possibly with backing from Russia, was intended as retaliation against economic sanctions levied by the United States and its allies in response to Russia’s policies in Ukraine. By mid-October, however, that theory began to fray, and the F.B.I. officially ruled out the Russian government as a culprit.

It is still not known where the attack originated.

The internal investigation at the bank is known as Rio. Though early on some officials suspected that at least one of the attackers’ computers was in Brazil, the attack could have been routed through computers anywhere. The basis for the internal name is unclear.

In the aftermath of the attack, JPMorgan has set up a “business control group” of about a dozen technology and cybersecurity executives to assess the fallout and to prevent hackers from breaching its network in the future. The group has been holding meetings once every few weeks.

The bank maintains that the damage to customers was limited to the theft of email passwords, home addresses and phone numbers.

“These criminals accessed customer contact information, but no account information,” said Patricia Wexler, a bank spokeswoman. “We have seen no evidence of fraud as a result of this.”

JPMorgan discovered the hackers inside its systems in August, after first finding that the same group of hackers had breached a website for a charitable race that the bank sponsors.

The revelation that a simple flaw was at issue may help explain why several other financial institutions that were targets of the same hackers were not ultimately affected nearly as much as JPMorgan Chase was. “To date, only two other institutions

have suffered some kind of intrusion, but those breaches were said to be relatively minor by people briefed on the attacks.

What is clear is JPMorgan's attack did not involve the use of a so-called zero day attack — the kind of sophisticated, completely novel software bug that can sell for a million dollars on the black market. Nor did hackers use the kind of destructive malware that government officials say hackers in North Korea used to sabotage data at Sony Pictures.

Nonetheless, once inside JPMorgan, hackers did manage to gain high-level access to more than 90 bank servers, but were caught before they could retrieve private customer financial information, the people briefed on the investigations said.

The breach, which the F.B.I. and federal prosecutors in Manhattan are treating as a criminal investigation, was not stopped until the second week of August.

The National Security Agency — which does not often get involved in most attacks on a private company — has been working with JPMorgan because the bank, particularly given its size, is considered to be part of the nation's "critical infrastructure." Two people briefed on the matter said that an N.S.A. special team will sometimes work with a corporate victim of hackers to ensure that no trap doors remain.

It is not clear why the vulnerability in the bank's network had gone unaddressed previously. But this summer's hack occurred during a period of high turnover in the bank's cybersecurity team with many departing for First Data, a payments processor.

A large part of the problem, security experts say, is that it has become nearly impossible for banks of JPMorgan's size to secure their networks, particularly as they integrate the networks of companies they acquire with their own. This has been a particular headache at JPMorgan, where it is still not uncommon for the name "Bank One" — a lender JPMorgan merged with a decade ago — to pop up in a web URL.

In August, the same month JPMorgan discovered hackers had been lurking in its system for months, the Department of Homeland Security warned companies

that such acquisitions posed a critical threat. The agency said then that a critical American manufacturing company had been infiltrated by “multiple, sophisticated threat actors over a period of several months” using the networks of companies it had acquired in recent years.

JPMorgan’s push to fortify its computer security comes as regulators prod banks to better vet their vendors. JPMorgan, for example, has yet to give the green light to Simmco Data Systems, the small Michigan company that runs the website of JPMorgan’s Corporate Challenge charitable race website, to resume operations. It was only after JPMorgan found that the Corporate Challenge website had been breached that it learned its own network had been attacked by the same hackers.

David Simms, chief executive of Simmco, declined to comment, noting that “this is an active federal investigation.”

Several state attorneys general, led by George Jepsen of Connecticut, are still investigating the breach, as are federal prosecutors in Manhattan under Preet Bharara, the United States attorney for the borough.

Representatives for the F.B.I., Mr. Bharara and Mr. Jepsen all declined to comment. An N.S.A. spokesman said the intelligence agency would defer to the F.B.I., which has been overseeing the investigation.

About two weeks ago, JPMorgan’s legal department sent an email to a number of its technology and cybersecurity employees reminding them not to “destroy or delete” any relevant documents about the breach, as well as about a smaller intrusion one year ago that affected 465,000 customers who used the bank’s prepaid cash cards.

Companies customarily send out these “hold” notices when they receive subpoenas or request for documents from regulators and law enforcement agencies.