Data Breach
Prevention. Response. Notification. TODAY

New JPMorgan Chase Breach Details Emerge

Other U.S. Banks Distance Themselves, See Isolated Event

By Mathew J. Schwartz, *August 29, 2014.* Follow Mathew J. @euroinfosec

Details continue to emerge about the probe into a suspected breach at **JPMorgan Chase**, as well as the implications of the investigation for the U.S. financial services industry.

The **breach** appears to have begun in early June, but wasn't detected - and stopped - until mid-August, when a routine **investigation** uncovered signs that customized malware was being used to exfiltrate gigabytes' worth of data, including some customer information, from the bank's network, reports **Bloomberg**, citing two unnamed sources with knowledge of the investigation. The report says attackers appear to have exploited multiple zero-day vulnerabilities in their attack, and to have routed stolen data through multiple countries, including Brazil, before finally routing much of it to a large city in Russia.

The FBI and U.S. Secret Service have confirmed that they're investigating the potential breach. A JPMorgan Chase spokeswoman says the bank is working with the agencies to identify the scope of the potential breach. The National Security Agency is also assisting with the investigation - which is common in large attacks believed to have been launched from abroad - and the bank has brought in multiple digital forensic investigation firms with law enforcement ties, including CrowdStrike, FireEye, and Stroz Friedberg, reports ***The Wall Street Journal***.

Representatives from CrowdStrike, FireEye and Stroz Friedberg all declined to comment on that report.

Broader Attack?

The JPMorgan probe is reportedly part of a broader investigation, which is examining if a larger, coordinated attack campaign also compromised other U.S. banks.

But other U.S. financial firms have moved to distance themselves from the breach investigation, with representatives from Bank of America, Bank of New York Mellon, PNC Financial Services Group, State Street, SunTrust Banks, U.S. Bancorp, and Wells Fargo all telling *The Wall Street Journal* they've uncovered no signs of a similar intrusion.

Meanwhile, the Financial Services Information Sharing and Analysis Center, or FS-ISAC, which works with both big and small financial services firms in the United States, as well as some firms in Europe, says it's seen no signs of a broader attack campaign.

"There are no credible threats posed to the financial services sector at this time," the group says in an update e-mailed to its members, adding that it is "unaware of any significant cyber-attacks causing unauthorized access to sensitive information at any member institutions," reports **Reuters**.

No Surprise: Banks Are Big Targets

Information security experts say it's no surprise that firms such as JPMorgan Chase are being pummeled by cyber-attacks - given the financial upsides for successful hackers. "Hackers are always probing bank systems, and even a year ago or so, law enforcement authorities and regulators put out an advisory to banks about criminals hacking into bank employee accounts to infiltrate their computer networks, and in some selected cases to steal funds," says Gartner financial services cybersecurity analyst **Avivah Litan** in a blog post.

"Frankly, this isn't new news - it's just the culmination of old news," Litan adds. "I imagine that the authorities and security staff never were able to eliminate the hackers from their systems. They have probably been in there for years, and there have probably been multiple actors, ranging from financial hackers to state-sponsored cyberspies."

JPMorgan spokeswoman Trish Wexler says in a statement: "Companies of our size unfortunately experience cyber-attacks nearly every day. We have multiple layers of defense to counteract any threats and constantly monitor fraud levels."

JPMorgan CEO **Jamie Dimon**, in fact, has promised that by the end of 2014, the bank will be spending $250 million annually on cybersecurity and employing 1,000 related personnel.

Early news reports about the investigation said that U.S. law enforcement agencies were reviewing whether the Russian government might be behind the attack, potentially in retaliation for U.S. sanctions imposed on Russia over the Ukraine. "Everyone is trying hard to tie this [to] the whole political situation with Russia," says Amichai Shulman, CTO of security firm Imperva. "However, it is well known that for a few years now, a large portion of banking attacks and financially related hacking has consistently been coming from Eastern Europe," meaning that criminal gangs could just as easily be behind the attacks.

Indeed, numerous security experts have cautioned against rushing to nation-state conclusions. "I think it's a little bit early to say it's the Russians, or worse still, the Russian government. One needs to be slightly certain of facts," says Alan Woodward, a professor in the department of computing at the University of Surrey in the United Kingdom. "It's like any crime, you don't go around alleging any crime unless you can prove it."

Furthermore, it can be incredibly difficult to amass enough evidence to solidly attribute online attacks. "I do work with Europol, and one of the big bugbears these agencies have is, it's quite difficult to track the sources of these attacks down," Woodward says.

The challenge is compounded by having to identify the people who actually launched an attack. "While an attack may be traced back to an IP address, it takes a lot of additional evidence and expert analysis to identify the person sitting at the keyboard at the computer behind that IP address," says Dublin-based cybersecurity consultant and Europol adviser Brian Honan.