IS JP MORGAN CRYING CYBERWOLF ABOUT RUSSIA? OR IS MIKE ROGERS?

There was a weird spate of reporting on the cyberthreat to banks last week. Normally, security firms (and occasionally really good tech journalists) report under their own name on such attacks — after all, they have businesses to run! But not the story — first reported by Bloomberg Wednesday evening — that Russia had attacked JP Morgan. At first, these reports appeared to be coming from FBI — given that the FBI investigation served as the lede of the story.

> Russian hackers attacked the U.S. financial system in mid-August, infiltrating and stealing data from JPMorgan Chase & Co. (JPM) and at least one other bank, an incident the FBI is investigating as a possible retaliation for government-sponsored sanctions, according to *two people familiar with the probe*.
>
> The attack resulted in the loss of gigabytes of sensitive data, said the people, who asked not to be identified because the probe is still preliminary.

But over the course of the story — and two more sources introduced with no description beyond that they had been briefed on the probe — the FBI officially gave no comment.

> The sophistication of the attack and technical indicators extracted from the banks' computers provide some evidence of a government link. Still, the trail is muddy enough that investigators are considering the possibility that it's cyber criminals from Russia or elsewhere

> in Eastern Europe. Other federal agencies, including the National Security Agency, are now aiding the investigation, *a third person familiar with the probe said*.
>
> [snip]
>
> J. Peter Donald, an FBI spokesman in New York, declined to comment.
>
> [snip]
>
> In at least one of the attacks, the hackers grabbed sensitive data from the files of bank employees, including executives, *according to a fourth person briefed on the probe*, who, like the other individuals with knowledge of the matter, declined to divulge the name of victims other than JPMorgan. Some data related to customers may also have been accessed, the person said.

The NYT's version of the story, published later on Wednesday, also cited a bunch of people described only as "briefed on the continuing investigation."

> 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.
>
> [snip]
>
> 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.

The NYT was able to get the FBI (as well as JP Morgan) on the record.

> “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.

This article (published midday on Thursday) – which casts doubt on the seriousness of the attack – seems to suggest that JPMC leaked to the press, not the FBI.

> “There are no credible threats posed to the financial services sector at this time,” [Financial Services Information Sharing and Analysis Center] said in an email to its members.
>
> [snip]
>
> JPMorgan had said early on Thursday that it was working with U.S. law enforcement authorities to investigate a possible cyber attack.
>
> The bank provided little information

> about the suspected attack, declining to say whether it believed hackers had stolen any data or who might be responsible.
>
> “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,” it said in a statement.
>
> The FBI had said late on Wednesday that it was looking into media reports on a spate of attacks on U.S. banks, raising concerns that the sector was under siege by sophisticated hackers.
>
> Yet several cyber security experts said that they believe those concerns are overblown.
>
> “Banks are getting attacked every single day. These comments from FS-ISAC and its members indicate that this is not a major new offensive,” said Dave Kennedy, chief executive officer of TrustedSEC LLC, whose clients include several large U.S. banks.

See this Time piece for more reasons why this is probably not the Russian hack it has been pitched as. And the WaPo – in their Wednesday report relying on “officials” – also cast doubt on the claimed motive for the attack, if it is Russia.

But even after the Reuters report casting doubt on the claims about the hack, Bloomberg continued its reporting – this time suggesting the attack began in June and ended several weeks ago, when previous report said it had started (and this time focusing on JP Morgan alone).

> Hackers burrowed into the databanks of JPMorgan Chase & Co. and deftly dodged one of the world’s largest arrays of sophisticated detection systems for

> months.
>
> The attack, an outline of which was provided by two people familiar with the firm's investigation, started in June at the digital equivalent of JPMorgan's front door, exploiting an overlooked flaw in one of the bank's websites. From there, it quickly developed into any security team's worst nightmare.
>
> The hackers unleashed malicious programs that had been designed to penetrate the corporate network of JPMorgan — the largest U.S. bank, which had vowed two months before the attack began to spend a quarter-billion dollars a year on cybersecurity. With sophisticated tools, the intruders reached deep into the bank's infrastructure, silently siphoning off gigabytes of information, including customer-account data, until mid-August.
>
> [snip]
>
> Evidence of advanced planning and the access to elaborate resources, as well as information provided by the FBI, led some members of the bank's security team to tell outside consultants that they believed the hackers had been aided by the hidden hand of the Russian government, possibly as retribution for U.S.- imposed sanctions.

Bloomberg also made clear that Mike Rogers served as a source of some kind.

> The Federal Bureau of Investigation and other agencies are working on the JPMorgan probe, and House Intelligence Committee Chairman Michael Rogers has been briefed on the bank attacks.

It was all very convenient, blaming Russia (even though investigators hadn't confirmed that's

where the attack originated) for scary financial threats.

And then, after several days of all this, Bloomberg published this story, citing the gigabytes of data allegedly taken from JP Morgan, warning that we're all going to have to bail out Jamie Dimon again.

> A worst-case event that destroyed records, drained accounts and froze networks could hurt the economy on the scale of the terrorist attacks of Sept. 11, 2001. The government response, though, might be more akin to that following the 2008 credit meltdown, when the Federal Reserve invoked "unusual and exigent circumstances" to lend billions of dollars.
>
> The government might have little choice but to step in after an attack large enough to threaten the financial system. Federal deposit insurance would apply only if a bank failed, not if hackers drained accounts. The banks would have to tap their reserves and then their private insurance, which wouldn't be enough to cover all claims from a catastrophic event, DeMarco and other industry officials said.
>
> [snip]
>
> Discussions about the government's role in cleaning up after a catastrophic cyber assault have centered on the Terrorism Risk Insurance Act, or TRIA.
>
> [snip]
>
> The insurance law, enacted after the 2001 attacks, authorizes the government to provide financial support for insurance companies in the wake of terrorism. It is up for renewal this year. Under TRIA, insurers cover a fixed amount of losses from terrorist attacks with the government backstopping

> additional costs up to $100 billion. The law gives the Treasury secretary broad latitude to invoke the backstop.
>
> In private meetings, Treasury officials have told insurance industry lobbyists that the department would treat cyber-terror like a physical attack under TRIA, said the people involved with the talks, who spoke on condition of anonymity because the discussions were private.

There has been a whole lot of fearmongering over this attack, which insiders doubt happened as billed and/or as attributed to Russia.

But if something like it does happen — gigabytes! — you can be sure Jamie Dimon will stiff us with the bill.