YAHOO'S THREE HACKS

As a number of outlets have reported, Yahoo has announced that 500 million of its users' accounts got hacked in 2014 by a suspected state actor.

But that massive hack is actually one of three interesting hacks of Yahoo in recent years.

2012 alleged Peace affiliated hack

In August, Motherboard reported — and reported to Yahoo — that the hacker known as Peace, who may have ties to Ukrainian and/or organized crime and also sold the MySpace and Linked In credentials, was selling credentials from what he said were 200 million accounts hacked in 2012. But when Motherboard tried to verify the data, some of it came back as out of date or invalid.

> According to a sample of the data, it contains usernames, hashed passwords (created with md5 algorithm), dates of birth, and in some cases back-up email addresses. The data is being sold for 3 bitcoins, or around $1,860, and supposedly contains 200 million records from "2012 most likely," according to Peace. Until Yahoo confirms a breach, however, or the full dataset is released for verification, it is possible that the data is collated and repackaged from other major data leaks.
>
> [snip]
>
> Motherboard obtained a very small sample of the data—only 5000 records—before it was publicly listed, and found that most of the two dozen Yahoo usernames tested by Motherboard did correspond to actual accounts on the service. (This was done by going to the login section of Yahoo, entering the email address, and clicking

> next; when the email address wasn't recognised, it was not possible to continue.)
>
> However, when Motherboard attempted to contact over 100 of the addresses in the sample set, many returned as undeliverable. "This account has been disabled or discontinued," read one autoresponse to many of the emails that failed to deliver properly, while others read "This user doesn't have a yahoo.com account."

2014 state actor hack

Yahoo claims it discovered the 500 million user hack in its investigation of the Peace allegations in August. The details being released now, in particular the encryption used with the account, vary from what Peace claimed in August.

> A source familiar with the investigation told Motherboard on Thursday that, although no direct evidence was found to support Peace's claims, Yahoo conducted a broader investigation, and during that time, they found the attack from what they described as a state-sponsored actor in 2014. The source declined to provide any evidence that the attack was state-sponsored, but said that the company strongly believed it to be the case.
>
> According to Yahoo's announcement, the majority of passwords were hashed with the strong hashing function bcrypt, meaning that hackers will have a much harder time at obtaining many users' real passwords. The source claimed that only a very small percentage of password hashes were not bcrypt.

Note, while Yahoo is claiming this was a hack done by a state actor, it has not said *what*

state actor.

Also, Yahoo appears to be suggesting that Peace's claim he had Yahoo credentials was not true. Though, given that Yahoo is being acquired by Verizon at the moment, they would have an incentive to claim they didn't know about this massive hack earlier.

2016 individual hack tied to DNC

Finally, an individualized hack of a Yahoo user — DNC consultant Alexandra Chalupa — was an independent source of the claim that DNC hackers might have ties to Russia or Ukraine. While the hack was evident from emails released by WikiLeaks, Chalupa had worked with Yahoo's Michael Isikoff previously and he added details explaining her suspicions about the timing.

> "I was freaked out," Chalupa, who serves as director of "ethnic engagement" for the DNC, told Yahoo News in an interview, noting that she had been in close touch with sources in Kiev, Ukraine, including a number of investigative journalists, who had been providing her with information about Manafort's political and business dealings in that country and Russia.
>
> "This is really scary," she said.
>
> [snip]
>
> Chalupa's message, which had not been previously reported, stands out: It is the first indication that the reach of the hackers who penetrated the DNC has extended beyond the official email accounts of committee officials to include their private email and potentially the content on their smartphones. After Chalupa sent the email to Miranda (which mentions that she had invited this reporter to a meeting with Ukrainian journalists in

> Washington), it triggered high-level concerns within the DNC, given the sensitive nature of her work. “That’s when we knew it was the Russians,” said a Democratic Party source who has knowledge of the internal probe into the hacked emails. In order to stem the damage, the source said, “we told her to stop her research.”
>
> A Yahoo spokesman said the pop-up warning to Chalupa “appears to be one of our notifications” and said it was consistent with a new policy announced by Yahoo on its Tumblr page last December to notify customers when it has strong evidence of “state sponsored” cyberattacks.

Significantly, this story, at least, claims this (and not cyber consultant CrowdStrike) is where DNC certainty that the hack was perpetrated by Russians came from.

Note that Chalupa’s Yahoo address was also affected in the Linked In hack, which exposed a simple password.

For now, I’m just presenting these three separate hacks as data points of interest.