7-CSO Online-Yahoo breach exposes

Yahoo breach exposes the drawbacks of state-sponsored hacking

Relying on private hackers gives governments some deniability, but it can bring the whole scheme down

U.S. Correspondent, IDG News Service |

REUTERS/Yuri Gripas

When governments turn to private hackers to carry out state-sponsored attacks, as the FBI alleges Russia did in the 2014 breach of Yahoo, they're taking a big risk.

On the one hand, it gives them a bit of plausible deniability while reaping the potential spoils of each attack, but if the hackers aren't kept on a tight leash things can turn bad.

Karim Baratov, the 22-year-old Canadian hacker who the FBI alleges Russia's state security agency hired to carry out the Yahoo breach, didn't care much for a low profile.

His Facebook and Instagram posts boasted of the million-dollar house he bought in a Toronto suburb and there were numerous pictures of him with expensive sports cars — the latest an Aston Martin DB9 with the license plate "MR KARIM."

But forget those for a moment and consider he wasn't very careful in hiding his hacking work.

His name is registered to several Russian-language websites that offer email hacking for between $80 and $90 per account. In the domain name records, he listed his home address.

“When you bring in amateurs who don’t follow standard protocol, that carries risk,” said Alex Holden, chief information security officer at Hold Security.

Piknu

Pictures from Baratov’s Instagram account.

The breach of Yahoo happened in 2014. At the time, the company notified the FBI but only believed 26 accounts had been targeted. It wasn’t until mid 2016 that the true enormity of the hack started to become apparent.

Security experts say it’s possible Baratov or a second hacker hired to help might have bragged online about the hack at some point, tipping off U.S. investigators.

And then in August 2016 a database allegedly stolen from Yahoo was found circulating on the black market.

“Some of the information about this hack was basically leaked,” Holden said. “That’s not a sign of a mature intelligence operation.”

So why did Russia turn to a 22-year-old from Canada? Language might have played a role.

According to the indictment, Baratov broke into the accounts through spear phishing email attacks, which are often designed to dupe victims into handing over password information.

However, spear phishing only works best if the emails appear authentic.

“The benefit of having Karim, the Canadian, on the team probably allowed creation of far more believable phishing attacks due to his being a native English speaker,” said Chester Wisniewski, a research scientist at security firm Sophos, in an email.

In addition to Baratov, the Russian agents allegedly hired a 29-year-old Latvian named Aleksey Belan, who pulled off the main hack against Yahoo, and stole the database involving 500 million user accounts.

By outsourcing the operation to Belan, Russia probably wanted to conceal the true motives for the Yahoo breach, Wisniewski said. Prior to Wednesday's indictment, Belan himself was already a wanted man for hacks against U.S. e-commerce companies.

"Who better to assist in a break-in?" he said. "There is also the 'cover' of criminal actions to potentially obfuscate the spying that was allegedly the real purpose."

In response to Wednesday's criminal indictments by the FBI, the Russian government is denying any involvement, and calling the allegations a distraction.

Baratov, who has been arrested in Canada, is also claiming innocence, according to his lawyer. Meanwhile, Belan remains at large.

But if the allegations are true, it does show one example of how Russia is harnessing the power of cybercriminals for spying purposes — and how it can get sloppy.

Next read this