Yahoo: An Innocent Victim Or A Government Stooge?

Thomas Brewster

October 5, 2016

To the Yahoo security team it looked like the company had been hacked. Again.

Someone in mid-2015 had installed software that scanned emails containing a string of characters, just as a nation state hacker might if they sought specific information without having to go through each message manually. It turned out, though, that unlike a recently-revealed 2014 attack, a foreign state was not to blame. Instead, according to a Reuters report, Yahoo executives helped the US government install a tool that would scan every email for that string, still unknown outside of those who carried out the surveillance project. CEO Marissa Mayer and her lawyers decided not to tell the Yahoo security team, a group called the Paranoids well-known for its dislike of invasive state surveillance. When security chief Alex Stamos found out, he quit.

Yahoo, however, has now criticised the report, claiming it misled readers. "The article is misleading. We narrowly interpret every government request for user data to minimize disclosure. The mail scanning described in the article does not exist on our systems."

Regardless of Yahoo's claims, critics have been brutal in their assessment of its actions. After the Snowden leaks revealed Yahoo was one of numerous tech giants said to have assisted the NSA in mass surveillance of US citizens, it was one of the most vocal opponents of bulk spying, promising to boost security. It did just that with a layer of encryption for emails in transit in 2014 and promised to deliver end-to-end crytography (it still hasn't turned up, though). The company also opposed government requests for data in court, even if it ultimately lost its most notable battle.

That it appeared yesterday to have reneged on its promise to protect user privacy incensed onlookers. "If true, this news will greatly undermine trust in the internet. For a company to secretly search all incoming emails of all its customers in response to a broad government directive would be a blow to privacy and a serious threat to freedom of expression," said Sherif Elsayed-Ali, head of technology and human rights at Amnesty International. "Tech companies want us to believe that they are pushing back against intrusive government surveillance but these reports could cast their ability to do so – if not their willingness – into doubt."

But is it possible Yahoo is telling the truth? Going further, could it be that the tool described was not for mass surveillance but something entirely different? And, following damaging reports of two major hacks, is Yahoo an innocent party?

Email scanning for good and bad

The language in yesterday's bombshell story was understandably vague. The words "scanning" and "searching" can be interpreted in many ways. It could be that the US government was looking for signs of cybercriminal or digital espionage passing through Yahoo's network. Email providers scan messages every day for malware and other security threats. No person reads the message, only automated systems look for telltale signs of criminal code and behaviour. That could be a signature known to represent malware, or an attachment that's been seen in previous attacks. Yahoo even notes in its privacy policy that it will perform some analysis on email content, whether incoming or going out: "Yahoo analyzes and stores all communications content, including email content from incoming and outgoing email."

The NSA or FBI may have sought information on illegal activity only they, and not Yahoo, knew about. "Well designed malware – the stuff the NSA is going to be taking point on – isn't likely to have some simple 'character string' you can match to detect it, though that's not impossible. This could also be some sort of phishing or spear phishing attack, or frankly any number of other possibilities given the vagueness of the article," said Julian Sanchez, a senior fellow at the Cato Institute.

Amongst those possibilities is that Yahoo was asked to assist the NSA on a project to uncover foreign spy activity, as exposed in Snowden files. That was revealed in the New York Times last year, which reported the NSA would monitor email addresses and "cyber signatures" — patterns linked to certain hacks – and attempt to find connections to espionage. "We know they're using these authorities for detecting network security threats at scale. This would be a natural extension," Sanchez added.

Some are therefore cutting Yahoo some slack. "I can't help feeling that the possible acquisition of Yahoo and Ms Mayer's potential payoff are encouraging some ill-informed speculation about what they have been doing with people's emails. I suspect Yahoo have acted very little differently from other large US service providers," said Professor Alan Woodward, a security expert from the UK's University of Surrey Computing department.

Even if Yahoo was helping the US with a security programme, major questions about its legality remain. "It's not any less a big deal if that's the case. If they're secretly getting providers to build architecture for bulk realtime content scanning, that's huge and needs to be debated publicly," added Sanchez.

Yahoo CISO Stamos, as noted in Reuters, pointed out another worrying problem with Yahoo's implementation of the government's request: the tool, whatever it did, had opened the door to other hackers. If it was a backdoor, it was a backdoor for anyone who wanted to get at Yahoo information. "They could have been voluntarily scanning for malware signatures. But even if they were doing this, it opens the door for abuse," noted Matthew Green, assistant professor at the Johns Hopkins Information Security Institute.

If Yahoo was allowing the government access into user's email messages, it has a lot to answer for. Even if it was joining the administration's hacker hunt, in trying to do something good Yahoo shot itself in the foot, a depressingly-prevalent theme at the firm soon to be acquired by Verizon for $5 billion.

Yahoo hacks

The Reuters story came hot on the heels of another nasty surprise from Yahoo: in mid-2014 it was hacked by an unnamed nation state and at least 500 million of its users had their usernames and encrypted passwords pilfered. It came on the back of a claim that 200 million had their information stolen, though sources close to that investigation said they had uncovered no evidence any such breach took place. Ironically, the latter probe revealed the real state-sponsored hack.

Former Yahoo employees have complained about a disconnect between Mayer and the security team. A New York Times report indicated Stamos was not given the budget and support he'd expected, and that secrets were kept from the Paranoids. That could well have been Yahoo's biggest mistake. If it hasn't been made painfully clear already, where execs and security teams don't get on, vulnerabilities often appear. When Yahoo failed to foster that relationship, it ended up losing Stamos, one of the most respected security chiefs on the planet, who now earns his keep at Facebook. And in upsetting concerned security engineers, it has another PR disaster on its hands.

"The bit of the story that really worried me was that allegedly whatever was done was done without the security team and that it left the systems open to hackers. If that is true it shows a remarkable lapse in judgement," Woodward added.

Yahoo has undoubtedly been victimized by criminal hackers. It's also had to bow to government pressure like many others. But, most damagingly of all, it's a victim of its own repeated mistakes, both in implementing a vulnerable scanning initiative and failing to support a security team that's done its darnedest to improve the public image of a company that badly needs it.