The Guardian

This article is more than **5 months old**

How the UN unearthed a possible Saudi Arabian link to Jeff Bezos hack

Analysis by cybersecurity firm suggested Amazon founder was target of advanced malware

Alex Hern

Wed 22 Jan 2020 18.05 GMT

The UN's demand for law enforcement authorities to conduct a proper investigation into the alleged hacking of Jeff Bezos's mobile phone came after it reviewed the findings of a cybersecurity firm, FTI.

The firm carried out a forensic analysis of Bezos' phone last year and concluded with "medium to high confidence" that it had been compromised because of actions attributable to a WhatsApp account used by the Saudi crown prince, Mohammed bin Salman.

As a result of this study, the UN said that Bezos, who also owns the Washington Post, had probably been hit by a piece of sophisticated malware, and it cited two firms - NSO and Hacking Team - as potential sources for this technology.

The UN was careful not to be definitive. Instead of pointing the finger, its statement said the apparent hack had been achieved using software "such as NSO Group's Pegasus or, less likely, Hacking Team's Galileo, that can hook into legitimate applications to bypass detection and obfuscate activity".

The NSO Group, an Israeli cyber-surveillance firm, strongly denied that its surveillance tools were responsible.

“NSO is shocked and appalled by the story that has been published with respect to alleged hacking of the phone of Mr Jeff Bezos,” the company said in a statement. “These types of abuses of surveillance systems blacken the eye of the cyber-intelligence community and put a strain on the ability to use legitimate tools to fight serious crime and terror. We expect that all actors in this arena put in place stringent procedures and technological controls, such as those that we have put in place, to assure that their systems are not used in an abusive manner.”

Jeff Bezos owns the Washington post, employer of the murdered Saudi journalist Jamal Khashoggi Photograph: Joshua Roberts/Reuters

The FTI report cited by the UN special rapporteurs, Agnes Callamard and David Kaye, noted that both NSO and Hacking Team, an Italian company, offered tools that could theoretically have performed the attack.

The report also highlighted that Saudi Arabia’s chief cybersecurity specialist, a close friend of Prince Mohammed named Saud al-Qahtani, “had long worked with” Hacking Team, and “eventually purchased 20% ownership” of the company, “apparently acquired on behalf of the Saudi government”.

Whatever spyware was used, descriptions of the attack point to the use of a sophisticated piece of software, which was delivered through a video file, received from Mohammed’s personal phone number.

The video appeared to describe the relationship between Saudi Arabia and Sweden, with closely cropped Arabic captions.

It is unclear whether Bezos clicked on the video. He may not have had to.

It appears the malware was not actually in the video itself but in the encrypted “envelope” in which it was contained.

When the message reached Bezos’s phone, and it decrypted to reveal the video, the malicious code was released.

“The downloader that delivered the 4.22MB video was encrypted, delaying or preventing further study of the code delivered along with the video,” the FTI analysis said. “It should be noted that the encrypted WhatsApp file sent from [Prince Mohammed’s] account was slightly larger than the video itself.”

Within hours of receipt of the video, data usage on Bezos’s phone began to spike, rising 30-fold over the day, and eventually peaking at multiple gigabytes of data sent in a single day.

That spike, FTI says, is the best evidence of a hack. “Anomalous spikes in egress data can often be attributed to malware activity such as spyware and backdoor trojans.”

The firm ruled out other explanations.

But while investigators identified the suspicious video that seems to have caused the hack, and the massive spike in data usage, the FTI report found no hard evidence of an actual hack.

After cloning the device and examining its file system they found “no matches against known … malicious software”. They “did not identify any malware on the device” when they scanned it with one of their forensic tools.

They did find 192 “potentially suspect” web addresses that the phone had connected to, but a review of those found no further malicious traffic. In fact, one of the potentially suspect URLs was “amazon.com”, and another was

“washingtonpost.com”, two sites Bezos owns. “Malware will also communicate with legitimate websites and servers for a variety of reasons,” FTI said, explaining why it had flagged those URLs.

The report argues the absence of hard evidence is not unusual, “since sophisticated malware often contains self-destruction capabilities that may activate if certain conditions or objectives are met”.

The final red flag, however, is Saudi Arabia’s alleged history of use of precisely the same type of malware it is thought to have sent to Bezos.The UN report places the attack in a “brief timeline of key events” that begins with the Washington Post journalist Jamal Khashoggi’s censorship by the Saudi state in 2016, and highlights the hacking of other Saudi activists at the hands of the state, including Yahya Assiri in May 2018 and Omar Abdulaziz in June 2018. Both men were “in frequent communication with Mr Khashoggi” at the time, and he was employed by Bezos’s newspaper.

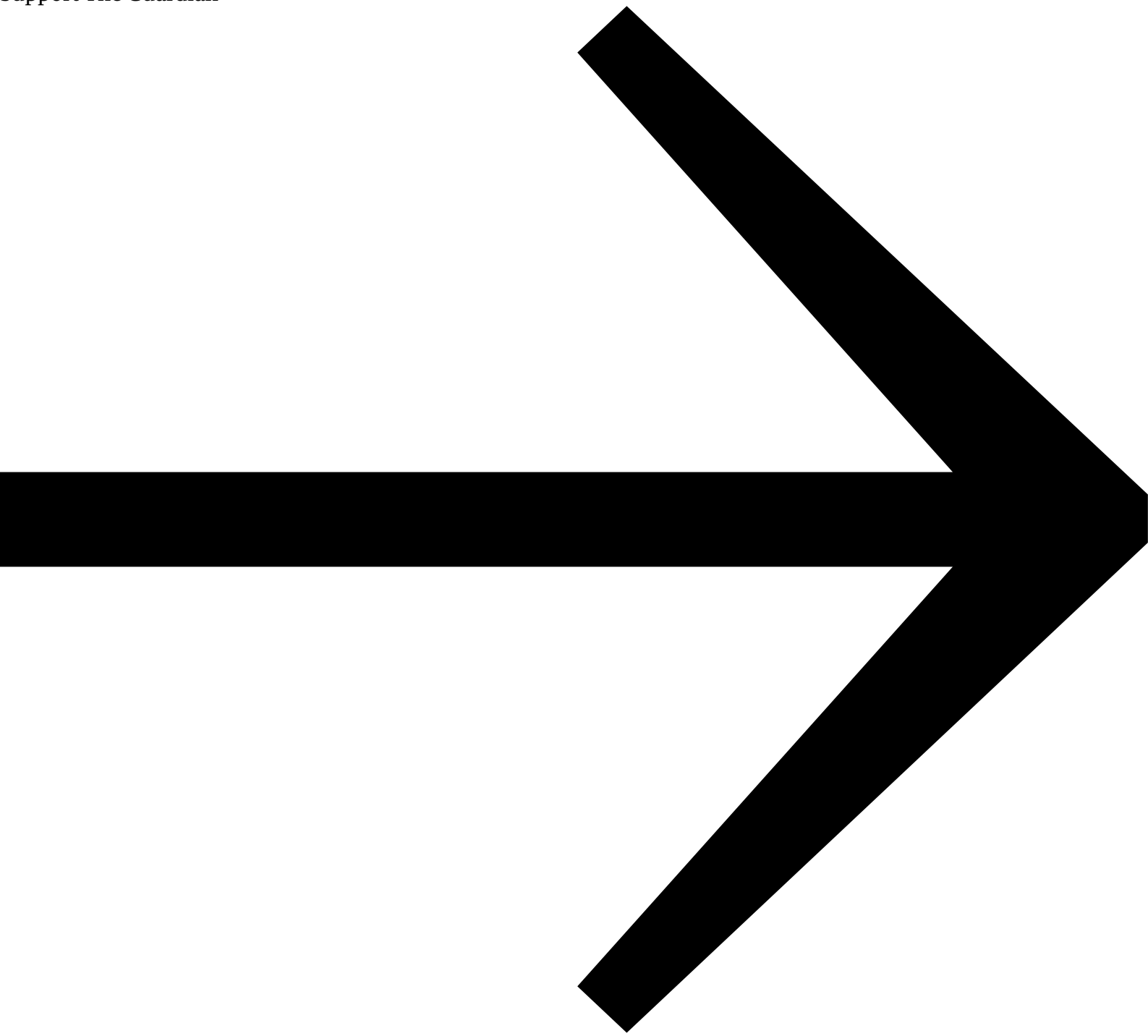
Other activists, including Ghanem al-Dosari and an Amnesty International official working in Saudi Arabia, were also targeted in June 2018 by text messages that led “to NSO infrastructure”, the UN report says. Khashoggi was murdered in the Saudi embassy in Turkey in October that year.

NSO has denied its technology has been used against activists.

Saudi Arabia has also denied using spyware to target dissidents and critics of the kingdom in this way.

Hacking Team has not responded to the UN report.

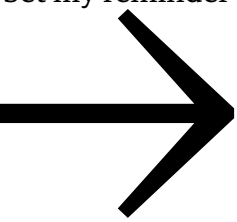
Support The Guardian



Remind me in September

Remind me in September
Email address

Set my reminder



We will use this to send you a single email in September 2020. To find out what personal data we collect and how we use it, please visit our Privacy Policy

We will be in touch to invite you to contribute. Look out for a message in your inbox in September 2020. If you have any questions about contributing, please contact us here.

Topics

- Jeff Bezos
- Mohammed bin Salman
- Saudi Arabia
- Middle East and North Africa
- WhatsApp
- analysis