State actors targeting mobile phones

Threat Memo - Date: 24/01/2020 - Version: 1.0

TLP:WHITE

FOR	Category	Type	Domain(s)	Sector(s)	Confidence
INFORMATION	Cyberespionage	Targeted attack	World	Digital services	A1

Key Points

- Amazon CEO's mobile was highly likely infected by espionage malware, that exfiltrated personal information.
- The infection was highly likely caused by Saudi Arabia rulers' messages.
- Likely candidates for the malware used are a number of espionage platforms marketed to governments.
- Mobile devices continuously seen as valuable resources of personal and financial information by state and criminal actors.

Summary

On January 22, 2020, news media around the world reported[1] on the almost certain breach of the mobile device of Amazon's CEO, Jeff Bezos by cyberespionage malware installed during message exchanges with the de facto ruler of Saudi Arabia, Prince Mohamed bin Salman (MBS). According to the forensic investigation[2], by the consulting firm FTI:

- No specific malware has been discovered up to the time of writing, pending a forensic investigation of the root file system.
- After the reception of attached videos by MBS, the outgoing traffic of the mobile device increased way above any possible normal use (increases in the area of 29 000% to 56 000 000%), a strong indication of data exfiltration.
- Personal messages by MBS to Bezos suggest direct and timely knowledge of non-public information the mobile phone owner was discussing.

Based on the above, the investigation team assessed with medium to high confidence that the mobile device in question had been compromised since May 2018. Such a surveillance operation would require a highly advanced technical capability. It is highly likely that the Saudi government used a specialised mobile phone espionage platform: either a version of the Pegasus malware by the Israeli NSO group or the Galileo Remote Control System (RCS) by the Italian company Hacking Team (of which a Saudi investor owns 20%).

NSO is a known developer of cyber espionage tools. Their prime product, Pegasus, can infect mobile devices and intercept all types of communications. NSO has repeatedly been accused of supplying oppressive regimes with malware enable them to closely monitor dissident activities. Characteristically, it has become the subject of several lawsuits: in November 2019 by WhatsApp for targeting about 1400 individuals, in May 2019 by Amnesty International, and in December 2019 by human rights groups for alleged assistance to the Saudi government to the October 2018 murder of Saudi journalist Jamal Khashoggi.

The Italian company Hacking Team markets the RCS products Galileo and Da Vinci as "investigative tools" for law enforcement and security agencies. The malware can infect computer and mobile operating systems, including Apple iOS, Linux, Mac OS X, and Microsoft Windows and gives almost complete access to the victim's device. Crucially for the Bezos case, a number of internal Hacking Team documents[3], leaked in 2015 show that the Galileo RCS should have the capability to infect iPhones via the WhatsApp application by presenting a malicious picture or video.

Comments

Mobile devices have been targeted in the past both by criminal and state actors as valuable resources of personal and financial information for any individual. Recent examples of such state surveillance are:

- The Egyptian government's surveillance on citizens using malicious mobile applications, revealed in October 2019.
- The large-scale, highly technical, Chinese surveillance campaign targeting groups perceived dissident, especially the Uyghur Muslim population in 2019 (please see CERT-EU Memo 190919-1).
- The report of August 2019 that Huawei technicians in African countries aid governments in monitoring of political opponents. Allegedly the technicians penetrated WhatsApp using NSO's Pegasus, used phones to geo-locate dissidents, and performed surveillance.
- An Iranian espionage application disguised as a calendar, disseminated in February 2019.

[1] https://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince

[2] FTI Consulting, Cyber Security, Project Cato. Project report, November 2019.
https://assets.documentcloud.org/documents/6668313/FTI-Report-into-Jeff-Bezos-Phone-Hack.pdf

[3] Ibid.

Concerning people at important positions, personal information found on their devices makes them prone to blackmail and political influence. This has happened, for example, during the electoral campaign in Israel in March 2019, where the candidate Benny Gantz had his voice recordings leaked, after his phone had most likely been hacked.

The case of Bezos' phone is unique, however, as a state actor (Saudi Arabia) appears to be taking advantage of personal/trust relationships between leaders and people in positions of power in order to acquire unauthorized access (infection highly likely caused by the exchange of messages with Saudi Arabia's rulers). Another similar case of trust abuse has been the report[4] that during the 2013 G20 summit, Russia distributed as gifts to delegates (including heads of state) USB flash drives and mobile phone chargers that were actually infected with surveillance malware.

Another issue in the Bezos-MBS case is that the latter also had relations with several people with influential roles in the US (e.g. the US president), especially in the high-tech sector. It is plausible to consider additional cases of cyberespionage with the goal to acquire information suitable to blackmail powerful individuals in favor of Saudi interests.

[4] https://www.theguardian.com/world/2013/oct/29/russia-denies-spying-g20-putin-spokesman