FORTALICE CLIENT ADVISORY

What does the recent hacking of a CEO's smartphone mean for you?

January 24, 2020

Fortalice

Fortalice

Executive Summary

The UN released a report recently identifying that Jeff Bezos' iPhone was hacked in 2018. The report further alleges that the hack is explicitly connected to Saudi Arabian Crown Prince Mohammed bin Salman.

We know that many of you are incredibly busy and will not have the time to read the full report, so we took the time to read it for you and offer an assessment of what may have happened and, more importantly, how to protect your work and personal communications.

So, who hacked Mr. Bezos? And what do we mean by "hacked"? Perhaps his private messages were accessed by more than one method and/or by multiple actors.

More importantly, if the richest man in the world, who has the resources to assemble one of the best digital security teams in the world, cannot protect his phone, what does that mean for the rest of us?

This is not the time to fear the unknown. Now is the time to analyze the puzzle pieces laid out before us and assess what went wrong and how we can learn from it to protect our workplaces and our loved ones.

Based on the UN report, we at Fortalice are offering a peek behind the digital curtain at what this all may mean. The report does not provide all of the forensic details or processes used; however, the analysis it does provide is worth heeding.

BEST PRACTICES MENTIONED IN THE REPORT

We know from the report that the forensics team created a lab for the examination which is a best practice to ensure the evidence isn't accidentally contaminated. They note that they did not find malware on the phone, however the absence of malware does not indicate a hack did not happen. They did find a video file that seemed suspicious. They combined their digital findings with research and collected intelligence information to conclude his phone had in fact been hacked.

According to the report's timeline, a WhatsApp message allegedly sent by Saudi Arabian leader Mohammed bin Salman was sent to Jeff Bezos on November 8, 2018. It included a photo of a woman who resembled Lauren Sanchez. The photograph may have had malware installed in it; if so, a method called steganography would have been used to hide the malware in plain sight. We have experience with clients who've fallen victim to malware hidden behind steganography at Fortalice and have seen tracking software and malware hidden in photographs and even innocuous images such as a signature block. It's important to note the video file could not be analyzed due to encryption, so there is no direct evidence that this file is the smoking gun or the initial source of compromise. Additionally, WhatsApp has stated that they were not contacted to aide in the investigation.

Another best practice is to put a confidence rating on your report; FTI rated the confidence of their findings appropriately at "medium to high". This appears to be appropriate given the timeframe they were allotted for the investigation, the evidence they had available to analyze, and the assignment they were given.

Could the attacker have actually been Saudi Arabian leader Mohammed bin Salman? Perhaps or perhaps not. For the record, he denies it. Attribution is hard but spoofing, or pretending to use someone else's phone number, is relatively easy to do. The WhatsApp account could have been created to make it look as if it were Mohammed bin Salman, or the authentic account could have been hacked into and used to hide the real identity of the perpetrator. Unless the accounts and the phone of Mohammed bin Salman undergo a thorough forensic review of dates, times,

phone logs, geocoded locations, and logins, it'll be hard to know for sure who was behind that WhatsApp message.

The FTI report does not directly insinuate that NSO Group's tools were used, but it does indicate that tools similar to theirs could be used to track and exfiltrate data. The NSO Group denies being involved saying in a statement, "As we stated unequivocally in April 2019 to the same false assertion, our technology was not used in this instance. Our technology cannot be used on US phone numbers. Our products are only used to investigate terror and serious crime. Any suggestion that NSO is involved is defamatory."

The FTI forensics summary notes that once the hacker had access to Jeff Bezos' phone, the phone's data was accessed at a much larger data rate than it had been prior to the alleged hacking. This could indicate files being sent to cloud instances and other means of remote access and data exfiltration. This is something our team commonly sees after a perpetrator gets access to a smartphone.

What does "hacking" a smartphone mean? In this report, they point to potential surveillance tools used. We have also seen instances where the attackers gain access to a phone's contents by accessing the cloud account of the owner and then using that cloud account to take photos, contacts, and messages and move laterally to gain further access.

The publicly available FTI report does not specifically mention whether or not they thoroughly investigated the cloud accounts and other services of Jeff Bezos. A best practice we typically undertake in forensics is to analyze the cloud accounts; in this case, because Bezos has an iPhone, it would have been an iCloud account. First, we would go to the access logs to look at who accessed the account and when. Then, we would look at all other accounts that could sync data from the device, such as photo sharing and backup sites.

So, how can you protect what matters to you most: your photos, messages, contacts, and more? What follows is not an exhaustive list but includes my favorite tips for phone safety.

PERSONAL PROTECTION STRATEGIES

1. Don't click on links in messaging apps or text messages unless you can verify their legitimacy. Pay careful attention when clicking on photos, images, and videos,
2. Consider providing a burner phone number from services such as Google Voice or Talkatone instead of giving out your actual telephone number. You can have the burner number forwarded to your real number.
3. Consider using phone anti-malware and anti-virus software; there are several great products out there.
4. If your phone acts oddly, consider doing a backup followed by a factory reset (it's hard for attackers to maintain persistence if you do a factory reset).
5. Two-factor authentication is time-consuming and no fun to use but often can be the extra lock necessary to keep attackers from taking over all of your information,
6. Turn on notifications to inform you if your accounts and/or devices are being accessed from a new location and/or device.
7. Disable "Auto Download Media" features in messaging apps such as WhatsApp, Signal, etc.

CONTACT FORTALICE

Fortalice Solutions, LLC. remains the cybersecurity and intelligence operations expert companies and people turn to regarding efforts to strengthen their privacy and cybersecurity. If you'd like to step up your cybersecurity defenses or need help complying with existing or future regulations, give us a call. We are highly skilled in disaster planning and recovery, incident response exercises and cyber risk assessment and we are standing by to aid you and your team.

Contact:

Call 877.487.8160 or email Watchmen@FortaliceSolutions.com