FTI CONSULTING | CYBERSECURITY

PROJECT CATO

Anthony J. Ferrante
Senior Managing Director and
Global Head of Cybersecurity

November 2019

Confidential

Project Cato
Executive Summary

In February of 2019, intelligence information warning of possible targeting of Jeff Bezos' phone by an Advanced Persistent Threat (APT)[1] was sent to Bezos' security advisor, Gavin de Becker. De Becker is Founder of Gavin de Becker & Associates (GDBA), a 900-person consulting and services firm that advises at-risk public figures.

On February 24, 2019, GDBA retained Anthony J. Ferrante of the business advisory firm FTI Consulting, Inc. (FTI) to manage and direct a complex investigation and forensic analysis of the personal iPhone X[2] of Bezos.

Ferrante served as Chief of Staff of the Federal Bureau of Investigation's (FBI) Cyber Division. More recently, he was Director for Cyber Incident Response at The White House, assigned to the National Security Council (2015 – 2017).

Extensive forensic study of Bezos' phone was undertaken in a well-equipped and secure lab environment, including forensic imaging of Bezos' phone and analysis of phone behavior in a sandboxed network.[3]

The digital forensic results, combined with investigation, interviews, research, and expert intelligence information, lead FTI to assess Bezos' phone was compromised, possibly via tools procured by Saud al Qahtani. Al Qahtani is/was known to be a close friend and advisor of Saudi Crown Prince Mohamed bin Salman (MBS).[4] At the time of the Bezos iPhone compromise, al Qahtani was President and Chairman of the Saudi Federation for Cybersecurity, Programming and Drones,[5] through which he directed cyber and hacking programs for the Saudi regime.[6]

As has been widely reported, al Qahtani directed a massive online campaign against Bezos, including thousands of artificially-trending tweets excoriating *The Washington Post* and calling for boycotts of other Bezos companies.[7] More significantly, al Qahtani is known to have played a key and senior role in the killing of *Washington Post* columnist Jamal Khashoggi.

[1] An Advanced Persistent Threat (APT) is a prolonged and targeted cyber attack in which an intruder gains access to a network and remains undetected for an extended period of time. The intention of an APT attack is usually to monitor network activity and steal data rather than to cause damage to the network.

[2] Jeff Bezos' iPhone X device was model number A1901.

[3] See Page 8, Section 5 for a detailed description of the sandboxed network and the secure forensic lab environment.

[4] https://www.bellingcat.com/wp-content/uploads/2019/06/Lord-of-the-Flies_Redacted_6-25-19.pdf, https://www.nytimes.com/2018/11/14/world/middleeast/saudi-arabia-crown-prince-loyalists.html

[5] https://archive.fo/20181030152706/https://www.spa.gov.sa/viewfullstory.php?lang=en&newsid=1756908

[6] https://www.bellingcat.com/news/mena/2019/06/26/lord-of-the-flies-an-open-source-investigation-into-saud-al-qahtani/

[7] https://www.thedailybeast.com/how-the-saudis-made-jeff-bezos-public-enemy-1, https://www.bloomberg.com/news/articles/2018-11-04/saudis-call-for-amazon-boycott-over-anger-at-washington-post

Al Qahtani has long worked with a company called Hacking Team, developers of programs used by many nation-states to spy on dissidents and other adversaries. Al Qahtani eventually purchased 20 percent ownership in Hacking Team, apparently acquired on behalf of the Saudi government.[8] In 2015, leaked documents[9] revealed that at least two (2) customers of Hacking Team had asked the company to create the capability to infect devices via a video sent in WhatsApp:

Expéditeur: REDACTED
Date: 3 mai 2015 20:18:16 UTC−4
Destinataire: REDACTED
Cc: REDACTED
Objet: (SEDENA) Meeting Questions and Comments

Hola REDACTED,
I'm taking advantage of my flight from Mexico to Washington to send you, as promised, the **main questions that the attendees of SEDENA asked** you during your presentation/demo. [..] Below are the questions raised during the meeting with SEDENA that would require a further answer to them:

- [..]
- Can we do an infection through a picture or a video (in WhatsApp for instance) as they are automatically downloaded in the App ? this is a question that was asked in Colombia also.

Figure 1: Internal leaked email from Hacking Team revealing clients' requests to infect devices via an attached photo or video in WhatsApp.

Source: https://wikileaks.org/hackingteam/emails/emailid/821469

Keeping that information in mind, note that Bezos exchanged phone numbers with MBS at a dinner in Los Angeles on April 4, 2018. In the following days, MBS and Bezos communicated via WhatsApp:

*Figure 2: **Texts between Bezos and MBS**.*

Source: Bezos' iPhone, WhatsApp application

[8] https://www.vice.com/en_us/article/8xvzyp/hacking-team-investor-saudi-arabia

[9] https://www.forbes.com/sites/thomasbrewster/2015/07/06/hacking-team-hacked/#3960ae626cfe

On May 1, 2018, Bezos received a text from the WhatsApp account used by MBS. This WhatsApp message contained a large video attachment that arrived unexpectedly and without explanation, meaning it was not discussed by the parties in advance of being sent.

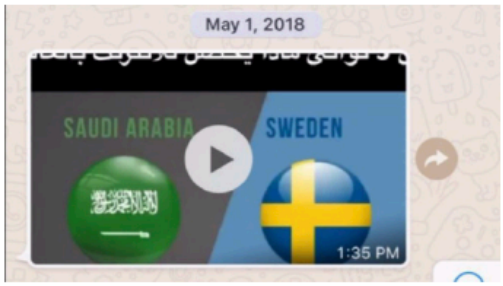

Figure 3: The text containing video file sent to Bezos from MBS account.

Source: Bezos' iPhone, WhatsApp application

The downloader that delivered the 4.22MB video was encrypted, delaying or preventing further study of the code delivered along with the video. It should be noted that the encrypted WhatsApp file sent from MBS' account was slightly larger than the video itself. We know from a comprehensive examination of forensic artifacts on Bezos' phone that within hours of the encrypted downloader being received, a massive and unauthorized exfiltration of data from Bezos' phone began, continuing and escalating for months thereafter.

The amount of data being transmitted out of Bezos' phone changed dramatically after receiving the WhatsApp video file and never returned to baseline. Following execution of the encrypted downloader sent from MBS' account, egress on the device immediately jumped by approximately 29,000 percent.

Forensic artifacts show that in the six (6) months prior to receiving the WhatsApp video, Bezos' phone had an average of 430KB of egress per day, fairly typical of an iPhone. Within hours of the WhatsApp video, egress jumped to 126MB. The phone maintained an unusually high average of 101MB of egress data per day for months thereafter, including many massive and highly atypical spikes of egress data. Forensic artifacts demonstrated that this unauthorized data was transmitted from Bezos' phone via the cellular network.

In addition to digital forensic artifacts, our investigation learned of at least two (2) instances in which texts sent to Bezos from MBS' WhatsApp account may reveal an awareness of private information that was not known publicly at the time.

The first such text was sent to Bezos from MBS' account on November 8, 2018, and contained a single photograph of a woman resembling Lauren Sanchez, with whom Bezos was having a then-secret personal relationship. For context, this was after the relationship would have been obvious to persons with access to private texts, calls, and images on Bezos' phone, but months before the relationship was known or reported publicly. The photo and cryptic caption were sent precisely during the period Bezos and his wife were exploring divorce. "Arguing with a woman is like reading the Software License agreement. In the end you have to ignore everything and click I agree." (Memes such as this were available on the Internet, however the content of the text was not typical of any past communication from MBS, making it likely it was sent with reference to Bezos' personal life events at that time.)

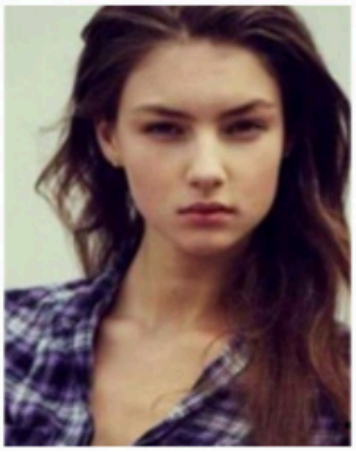

Figure 4: Photo sent to Bezos.

Source: Bezos' iPhone, WhatsApp application

Figure 5: Lauren Sanchez.

Source: The Mega Agency

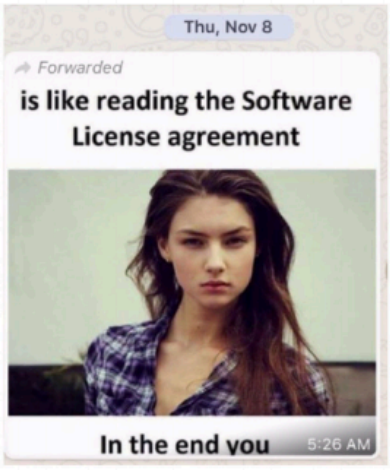

Figure 6: Text sent to Bezos from MBS account.

Source: Bezos' iPhone, WhatsApp application

The second text that demonstrates an awareness of non-public information that could have been gained via surveillance of Bezos' phone was sent to Bezos from MBS' WhatsApp account, after more than three (3) months of no communication between the parties. On February 14, 2019, Bezos was provided a detailed briefing about the extent of the Saudi online campaign against him. The briefing was provided in two (2) calls on the Bezos' phone. This text evinces an awareness of what Bezos had just been told:

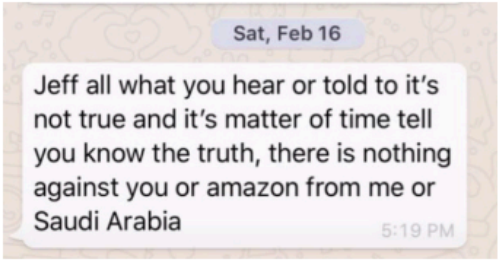

Figure 7: Text sent to Bezos from MBS WhatsApp account after months of no communication.

Source:Bezos' iPhone, WhatsApp application

Several elements of context also informed FTI's conclusions, notably that the Saudi regime is known to use phone spyware against its adversaries. The Saudi regime was by all accounts very concerned about Jamal Khashoggi and *The Washington Post* at the time the encrypted video file was sent to Bezos; Bezos owns *The Washington Post*.

Based upon the results of a full forensic examination of the logical file system of Bezos' phone, including network analysis, and an in-depth investigation conducted over several months, FTI reports with medium to high confidence that Bezos' iPhone X was compromised via malware sent from a WhatsApp account used by Saudi Crown Prince Mohamed bin Salman.

See below for a step-by-step technical account of our work in this matter thus far.

The Digital Forensic Study

1. On February 17, 2019, de Becker was advised by a leading intelligence expert closely familiar with Saudi Arabia to perform a forensic imaging and analysis of the personal iPhone X of Jeff Bezos due to suspicions of targeting and possible compromise by an Advanced Persistent Threat (APT) actor. Ferrante assembled a team of cybersecurity and investigative experts to perform the requested work. Ferrante led all aspects of the work, to include oversight and direction of technical, intelligence, and investigative processes.

2. FTI first deployed a forensic investigator on February 25, 2019[10] to undertake a cursory study of one attachment sent to Bezos from MBS' WhatsApp account.
3. Following the cursory study of the item, it was determined that FTI would conduct full forensic imaging and analysis of the device to more completely identify any evidence of compromise, espionage, or data theft. FTI provided a list of hardware and software that would be acquired on behalf of Bezos and used to conduct the full forensic imaging and analysis at a secure location.[11] The following items were acquired by GDBA and used to perform forensic acquisition and analysis of Bezos' iPhone X:
    a. Cellebrite software and hardware components including:
        i. UFED 4PC Ultimate (FileSystemDump, PhysicalDump, ExtractPassword, CloneSim, ExtractSim, ExtractPhone): License and Dongle
        ii. Phone Detective: License and Dongle
        iii. Physical Analyzer (GPS, PhysicalDecoding, iPhone, Other_Plugins): License and Dongle
    b. Two (2) Microsoft Surface Laptops with the following specifications:
        i. Memory: 16GB
        ii. Processor: Intel Core i7
        iii. Storage: 512GB
    c. NETGEAR R6700 Nighthawk AC1750 Wireless Router
4. On May 17, 2019, a team of FTI technical experts and forensic investigators arrived at a secure location to establish the forensic lab for studying Bezos' iPhone X. Installation, configuration, and testing of the forensic lab environment were completed over two (2) days. The forensic lab consisted of the following components:
    a. NETGEAR R6700 Nighthawk AC1750 wireless router configured with a hidden Extended Service Set Identification (ESSID)[12] and WPA2[13] 128bit encryption for security. The wireless router was configured to provide internal only (non-Internet) network connectivity to the lab environment.[14]
    b. Two (2) Microsoft Surface Laptops configured with:
        i. Cellebrite UFED 4PC Ultimate and Physical Analyzer
        ii. Telerik Fiddler configured as a man-in-the-middle proxy[15] for use in live network traffic capture and sandbox analysis of Bezos' iPhone X[16]. The Fiddler proxy was configured to run on the internal network and redirect all requests to a local web server in order to more accurately simulate a live Internet connection when conducting a sandbox analysis of Bezos' iPhone X.

[12] Extended Service Set Identification or ESSID is the identifying name of a wireless network.

[13] WPA2 is a security standard for securing a wireless network using a 128bit encryption key.

[14] The configuration of the forensic lab environment was done with an active Internet connection to allow for installation, patching, and updates of all necessary tools and technologies. Once fully configured, and prior to commencing and forensic acquisition and analysis, the lab environment was disconnected from the Internet and connected to the internal only network that was configured via the wireless router.

[15] The Fiddler tool facilitates the capturing of network traffic between the Internet and test computers and phones by establishing a proxy to act as an intermediary. The tool enables the inspection of incoming and outgoing data and to monitor and modify requests and responses before the browser or application receives them.

[16] A sandboxed network is an isolated network environment that is not connected to the Internet in any way. It was used to monitor and capture network traffic in a secure environment while simulating Internet activity.

iii. Wireshark[17] for use in live network packet capture of Bezos' iPhone X

iv. Oracle VirtualBox configured with Ubuntu 18.04 LTS virtual machines (VMs) for running various Linux utilities for data processing, network packet analysis, and malware analysis

v. Windows Subsystem for Linux running Ubuntu 18.04 LTS SSH servers for sharing of data between the two analysis machines

vi. PowerGREP for data processing and matching against an internally loaded intelligence database[18]

5. On May 18, 2019, at approximately 22:32 PDT, FTI received Bezos' iPhone X. (From this point forward, the lab was secured and staffed 24-hours a day, no electronic devices were allowed in or out, all persons entering passed through metal-detector screening, and technicians worked round the clock.)

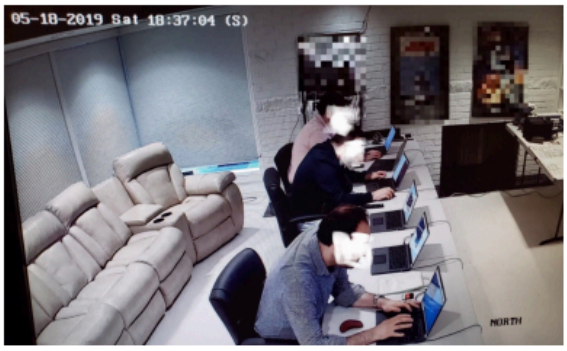

Figure 8: Temporary secure forensic lab.
Source: Security footage from secure forensic lab

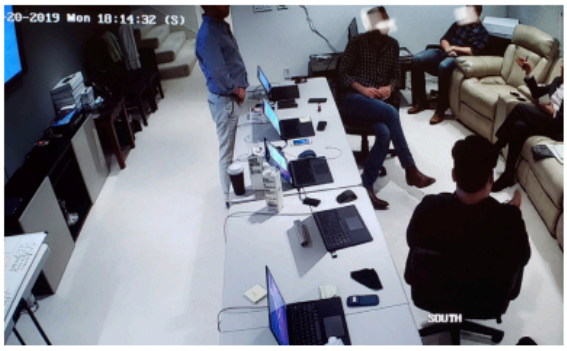

Figure 9: Gavin de Becker (sitting) is briefed at secure forensic lab.
Source: Security footage from secure forensic lab

6. During the initial attempt to collect a forensic image of the iPhone, FTI determined that the device had iTunes backup encryption enabled, and that full analysis of the contents of the forensic image would require the encryption password. Awaiting the password, FTI started a logical mobile acquisition via Cellebrite's UFED 4PC[19] on May 19, 2019 at 1:05 PDT, and the forensic acquisition concluded at 4:02 PDT. Upon completion of the forensic acquisition, a malware scan and hash[20] list of all contents on the forensic image was run using Cellebrite's Physical Analyzer.[21] Both processes ended at 11:33 PDT. Cellebrite's Physical Analyzer did not identify any malware on the device using its built-in scanner.

[17] Wireshark is an open-source network packet analyzer that allows for the capturing of raw network packets from a live network-connected device.

[18] FTI provided an offline intelligence database for use in the forensic lab environment.

[19] UFED 4PC is a product from Cellebrite that allows for forensic acquisition of mobile devices.

[20] In digital forensics, a hash is a type of digital fingerprint useful for identifying a file and correlating it against various intelligence databases.

[21] Physical Analyzer is a product from Cellebrite that takes a forensic image and consolidates device data from variety of sources.

7. At 4:51 PDT on May 19, 2019, FTI initiated network packet collection[22] of Bezos' iPhone X, using Wireshark and Fiddler. This was done by configuring the iPhone X to direct all Wi-Fi traffic to the Fiddler proxy which acted as an intermediary and running Wireshark on the proxy machine to capture all network packets originating from the iPhone. FTI used four different techniques while collecting network traffic, each being logged separately. These included collecting network traffic while the device was locked, unlocked, idle, and while simulating user activity (opening and closing apps). At 12:19 PDT on May 21, 2019, the collection of network traffic concluded.
8. On May 20, 2019, FTI provided and tested options for bypassing the iTunes backup encryption password. FTI advised resetting "All Settings" on Bezos' iPhone X to restore the device's settings to factory defaults — removing the encryption password while preserving the file system and any relevant data and artifacts. FTI received authorization to perform this resetting step, did so, and then commenced acquisition of an unencrypted Cellebrite forensic image at 12:27 PDT.
9. Upon completion of the forensic image at 15:17 PDT, another malware scan and hash of all files was run using Cellebrite's Physical Analyzer. Cellebrite's Physical Analyzer again did not identify any obvious malware on the device using its built-in scanner.
10. FTI returned Bezos' iPhone X to GDBA on May 22, 2019 at approximately 16:30 PDT.
11. FTI used the reporting tool on Cellebrite's Physical Analyzer to export data from both acquired forensic images into Microsoft Excel format and redacted all sensitive data that was included in the reports. As requested by GDBA, FTI used Cellebrite's Physical Analyzer to extract a suspect video file from Bezos' iPhone X for further analysis. FTI departed the secure location on May 22, 2019 at 16:41 PDT with copies of the redacted Cellebrite reports that were generated from the acquired forensic images, network capture logs generated in step 7, and the suspect video file.
12. Between May 22, 2019, and July 19, 2019, FTI conducted in-depth analysis of forensic artifacts from the redacted Cellebrite reports and captured network logs. FTI extracted 350,579 unique hashes from the Cellebrite reports and correlated them against a variety of open source and proprietary cyber threat intelligence databases. There were no matches against known conventional or typical malicious software.
13. FTI additionally identified 1,290 unique URLs[23] and 378 unique domain names[24] from the network capture logs. FTI correlated these network artifacts against a variety of open source and proprietary cyber threat intelligence databases and identified 192 potentially suspect indicators of compromise (IOCs)[25] that required further vetting.
14. Each of these 192 suspect IOCs was related to domain names and URLs that various malware samples had been observed communicating with historically. Malware typically communicates with a website or server that acts as a command and control (C2) server which is used to issue commands to a compromised device, conduct espionage, and steal or exfiltrate data. However, malware will also communicate with legitimate websites and servers for a variety of reasons, such as to generate advertising revenue through click fraud, track user activity, or generate noise to obfuscate C2 activity towards actual malicious websites.

[22] Packet capture and proxying applications are useful for identifying network communication with suspect remote servers that are used to control and spy on the compromised device.

[23] A URL or Uniform Resource Locator is the address of a particular web page or resource. For example: http://www.example.com/index.html is a URL with example.com being the domain name of the particular website.

[24] Domain name is simply a human readable form of an IP address.

[25] Indicator of Compromise (IOC) is a term used in cyber threat intelligence and digital forensics to refer to network or host-based artifacts, such as IP addresses, domain names, URLs, hashes, et cetera related to potential malicious activity.

15. FTI conducted an in-depth audit of the 192 suspect IOCs and did not find evidence that any of the identified domain names or URLs were related to C2 type traffic or any other malicious traffic. FTI thus concluded that they were all false positives.[26] The following chart shows the top 50 suspect network artifacts, all of which were determined to be legitimate and reputable websites categorized as search engines, news or media companies, technology companies, or social networks, et cetera (this stands true for the full list of 192 IOCs).

	IOC	Category		IOC	Category
1.	bing.com	Search Engines/ Portals	26.	dailymail.co.uk	News/Media
2.	en.wikipedia.org	Reference	27.	dropbox.com	File Storage/Sharing
3.	medium.com	News/Media	28.	go.microsoft.com	Technology/Internet
4.	outlook.com	Email	29	imdb.com	Entertainment
5.	ieee.org	Technology/Internet	30.	login.live.com	Technology/Internet
6.	apple.com	Technology/Internet	31.	reddit.com	Newsgroups/Forums
7.	google.com	Search Engines/ Portals	32.	spotify.com	Entertainment
8.	icloud.com	Office/Business Applications	33.	twitter.com	Social Networking
9.	live.com	Technology/Internet	34.	mobile.pipe.aria.micro-soft.com	Technology/Internet
10.	update.googleapis.com	Technology/Internet	35.	client-office365-tas.msedge.net	Technology/Internet
11.	buffalo.edu	Education	36.	config.edge.skype.com	Chat (IM)/SMS
12.	people.com	Entertainment	37.	googleapis.com	Technology/Internet
13.	skype.com	Chat (IM)/SMS	38.	microsoft.com	Technology/Internet
14.	wikipedia.org	Reference	39.	safebrowsing.googleapis.com	Technology/Internet
15.	amazon.com	Shipping	40.	support.apple.com	Technology/Internet
16.	cnn.com	News/Media	41.	yahoo.com	Search Engines/ Portals
17.	gstatic.com	Search Engines/ Portals	42.	clients4.google.com	Technology/Internet
18.	settings-win.data.microsoft.com	Technology/Internet	43.	facebook.com	Social Networking
19.	techcrunch.com	Technology/Internet	44.	s.amazon-adsystem.com	Web Ads/Analytics
20.	washingtonpost.com	News/Media	45.	trc.taboola.com	Web Ads/Analytics
21.	wsj.com	News/Media	46.	doubleclick.net	Web Ads/Analytics
22.	edition.cnn.com	News/Media	47.	google.ru	Search Engines/ Portals
23.	nyu.edu	Education	48.	unity3d.com	Technology/Internet
24.	wired.com	News/Media	49.	de.ioam.de	Web Ads/Analytics
25.	dailymail.co.uk	News/Media	50.	en.m.wikipedia.org	Reference

Figure 10: Top 50 suspect network artifacts based on aggregated risk score from open source and proprietary threat intelligence sources.

Source: FTI Cybersecurity

[26] A false positive is a result that indicates a certain result is present when it really is not.

16. It should be noted that the lack of identified malicious traffic does not disprove the existence of current or previous compromise on a device.
17. FTI captured network traffic from Bezos' iPhone X using a sandboxed network that attempted to simulate an active Internet connection. Advanced malware variants are known to employ sophisticated methods to avoid discovery, such as detecting sandboxing and analysis techniques, testing for an active Internet connection, and remaining dormant or destroying evidence of itself if certain conditions exist.[27] These factors can prevent detection of some indications of compromise.
18. FTI also conducted an in-depth investigation of the artifacts related to the iPhone X's logical file system from the redacted Cellebrite report, and audited 274,515 directories, subdirectories, and filenames. Special care was taken to identify evidence of jailbreaking[28] tools and known iOS exploits tools.[29] After a comprehensive review of the logical file system and a validation of all false positives, FTI assesses with medium confidence that no evidence of these types of tools were identified on Bezos' iPhone X to date. As previously stated, lack of evidence of malicious tools of this nature does not refute their existence since sophisticated malware often contains self-destruction capabilities that may activate if certain conditions or objectives are met.
19. While the above investigative avenues did not provide evidence to confidently state whether Bezos' iPhone X had been compromised, an additional lead proved more fruitful. On May 1, 2018 at approximately 13:35 PDT, a WhatsApp message from an account utilized by MBS, the Crown Prince of Saudi Arabia, was sent to Bezos' phone. It contained an embedded video attachment.[30] This message was considered suspicious and was flagged for additional investigation by FTI:

WhatsApp Message Details	
Source	WhatsApp
Instant Message #	6
Platform	Mobile
Timestamp: Date	5/1/2018
Timestamp: Time	5/1/2018 8:35:21 PM(UTC+0)
Attachment #1	96d9a338-b75c-4fd8-a541-620421f0ade0.mp4
Attachment #1 - Details	https://mmg-fna.whatsapp.net/d/f/REDACTED.enc

Figure 11: Suspect WhatsApp message with video attachment.

Source: FTI Cybersecurity

20. Though the parties knew each other, this message was sent without any advance indication or explanation. The video appears to be an Arabic language promotional film about telecommunications (the file containing the video is slightly larger than the video itself).
21. Cursory analysis of the video file did not identify any embedded malicious code, however, further analysis of the WhatsApp artifacts from the redacted Cellebrite reports revealed that the video was delivered via an encrypted downloader hosted on WhatsApp's media server:
    a. https://mmg-fna.whatsapp.net/d/f/REDACTED.enc

[27] FTI's subject matter experts have in-depth experience analyzing malware with sophisticated discovery avoidance capabilities.
[28] Jailbreaking is the process by which full execute and write access is obtained on all the partitions of a device. This process involves the use of custom built or open source jailbreaking tools and exploits.
[29] There are certain indicators in the device's file system that are created/edited when a device has been compromised or jailbroken. See https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf
[30] Embedded video was a .mov file.

22. Due to end-to-end encryption[31] employed by WhatsApp, it is virtually impossible to decrypt the contents of the downloader to determine if it contained any malicious code in addition to the delivered video. However, an examination of forensic artifacts from the redacted Cellebrite reports identified an anomalous and extreme change in behavior of the phone following delivery of the video. A timeline analysis of cellular data originating from Bezos' iPhone X reveals a 29,156 percent increase in unauthorized egress data within hours of the video's delivery. There were also several additional notable spikes in egress data following the initial spike on May 2, 2018, ranging from 221MB through a highly atypical 4.6GB.
23. A comparison of the data egress against a baseline timeline analysis prior to the initial spike on May 2, 2018 shows a stark variance. Prior to May 2, 2018, Bezos' iPhone X had fairly typical average of 430KB of egress data per day. In sharp contrast with the previous average, 126MB of unauthorized egress data occurred on May 2, 2018. In stark contrast to the previous daily average of 430KB of egress data, the daily average in the months after the WhatsApp video jumped to 101MB of egress data. Before May 2, 2018, only one (1) minimal spike in egress data was detected, totaling 14.43MB, and determined to be authorized. This traffic took place on December 30, 2017, and can be attributed to iMessage usage by Bezos on that day.

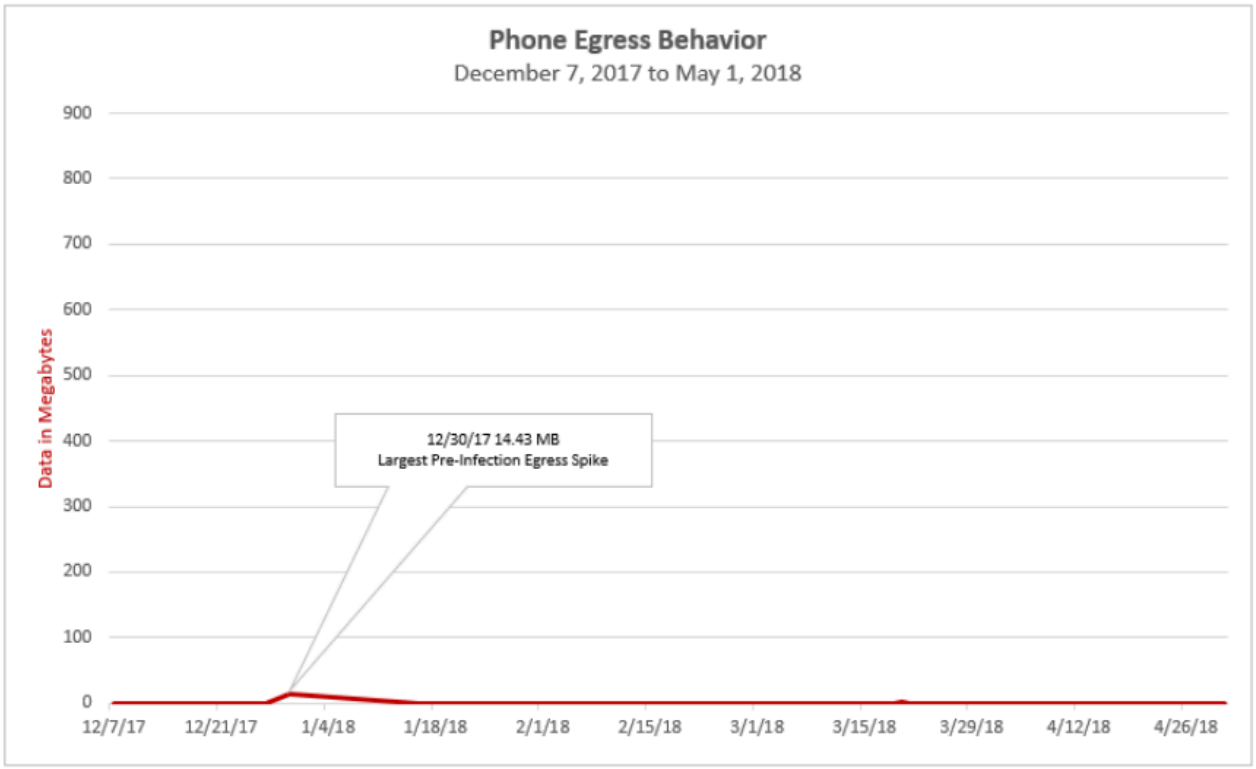

Figure 12: Normal egress of data from Bezos' phone during the 6-month period prior to the WhatsApp video sent from account used by MBS. Daily average was a fairly typical 430KB of data transmitted out of the phone. The one spike of 14.43MB is attributed to authorized iMessage usage.

Source: FTI Cybersecurity

[31] End-to-end encryption is a highly secure method to communicate privately over a network. By encrypting messages at both ends of a conversation, end-to-end encryption prevents anyone in the middle from reading private communications.

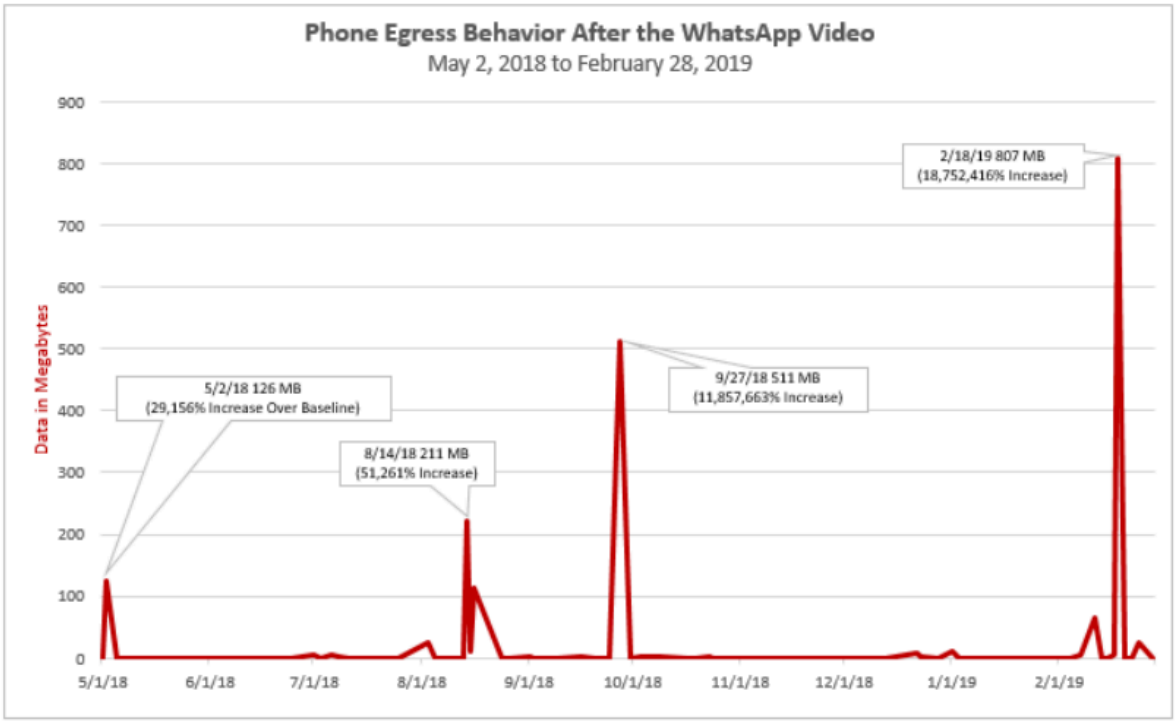

Figure 13: Increase in unauthorized exfiltration of data from Bezos' phone starting hours after the MBS text on May 2, 2018. and continuing through February 28, 2019. In addition to spikes, the daily average jumped from 430KB to 101MB.

Source: FTI Cybersecurity

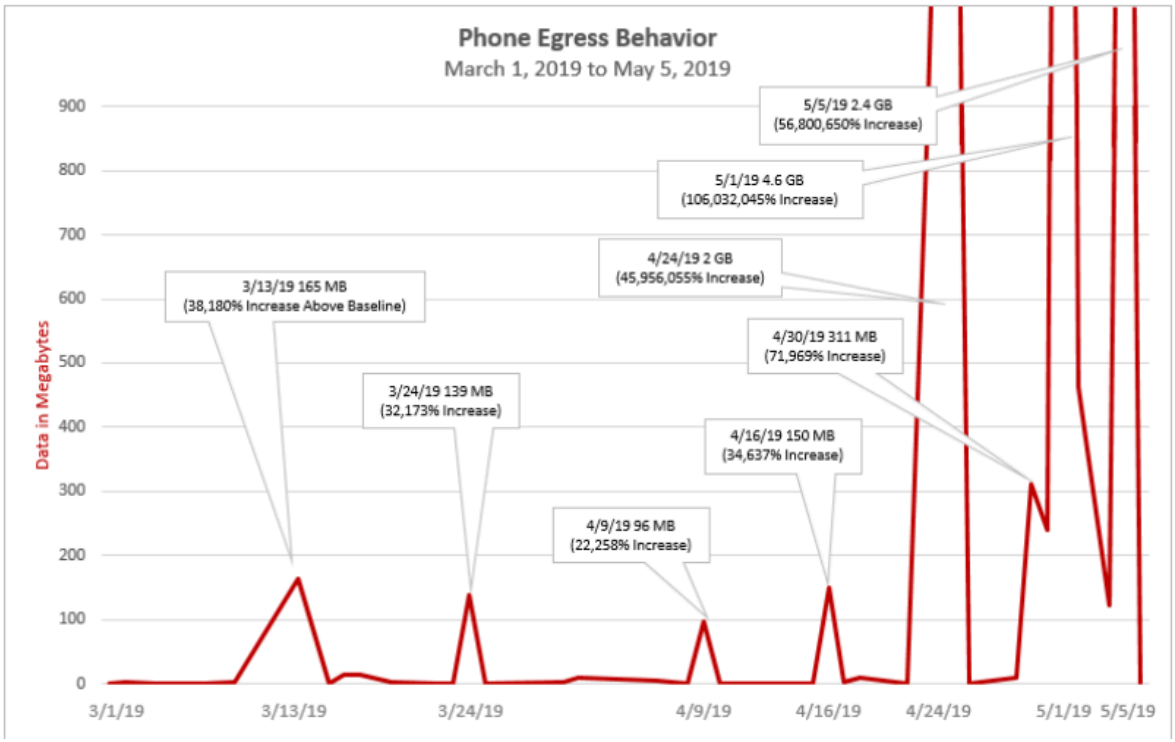

Figure 14: Escalating increase in frequency and amount of unauthorized exfiltration of data from Bezos' phone between March 1, 2019. and after May 5, 2019.

Source: FTI Cybersecurity

Date	Egress Data	Percent Change vs. Pre-Video Baseline
5/2/2018	126MB	29,156%
8/14/2018	221MB	51,261%
9/27/2018	511MB	11,857,663%
2/18/2019	807MB	18,752,416%
4/24/2019	2GB	45,956,055%
5/1/2019	4.6GB	106,032,045%
5/5/2019	2.4GB	56,800,650%

Figure 15: Notable spikes in egress traffic showing the percentage increase over the pre-video baseline average of 430KB per day.

Source: FTI Cybersecurity

24. Anomalous spikes in egress data can often be attributed to malware activity such as spyware and backdoor trojans[32] since they provide the ability to exfiltrate vast amounts of data including photos, videos, messages, and other private or sensitive files. It should be noted that spikes resembling these might occur legitimately if a user enabled iCloud backup over cellular data service. Bezos, however, had iCloud backups disabled on his device. Other legitimate causes of spikes in egress data could be if a user willingly uploaded or transmitted large amounts of data via a chat or messaging app, email client, or cloud storage service, but none of these activities were corroborated by GDBA or Bezos. Further, and significantly, FTI was able to study the history of this phone's behavior, and it never transmitted egress data in this way prior to execution of this WhatsApp video file.
25. FTI further conducted a comparative analysis against cellular data egress snapshots of five (5) FTI-owned iPhones to contrast activity from Bezos' iPhone both before and after the delivery of the suspicious WhatsApp video.[33] As can be seen in Figure 16, data egress originating from the five (5) devices is similar to Bezos' pre-May 2, 2018, baseline with a combined daily average of 1.9MB of egress data and only two (2) minimal spikes across two (2) devices — attributed to VoIP[34] calling and photo sharing activity, respectively. Similar to Bezos' initial baseline, this chart demonstrates typical iPhone behavior among a sample of five (5) iPhones that is in stark contrast to the spikes in egress data identified on Bezos' phone after delivery of the WhatsApp video.

[32] Backdoor Trojans refer to malicious software programs that share the primary functionality of enabling a remote attacker to have access to, or send commands, to a compromised device.

[33] FTI acquired network data from the five (5) iPhone devices using Cellebrite UFED 4PC and Physical Analyzer.

[34] VoIP or Voice over IP is a mechanism that allows placing voice calls over a data connection using specialized software. Common VoIP applications include Skype, Google Voice, and TalkU.

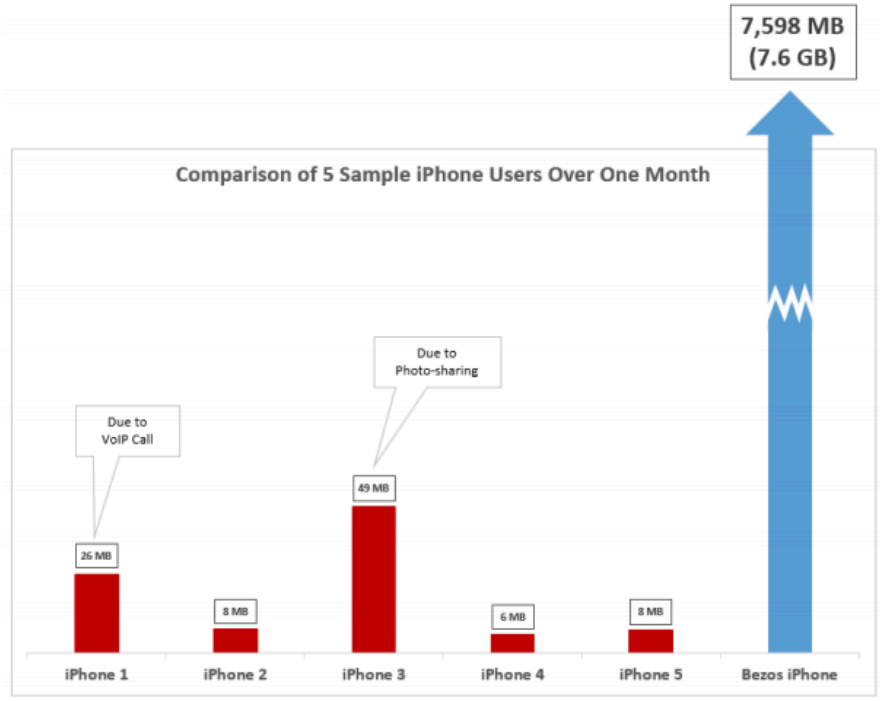

Figure 16: Comparative one-month timeline analysis of data egress (cellular) originating from five (5) sample iPhones, in megabytes.

Source: FTI Cybersecurity

26. Advanced mobile spyware, such as NSO Group's Pegasus[35] or Hacking Team's Galileo,[36] can hook into legitimate applications and processes on a compromised device as a way to bypass detection and obfuscate activity in order to ultimately intercept and exfiltrate data. The success of techniques such as these is a very likely explanation for the various spikes in traffic originating from Bezos' device. For example, more than 6GB of egress data was observed using exfiltration vectors such as nsurlsession, [37] Mobile Safari, and Apple's email client following the initial spike on May 2, 2018. It should be noted that these types of advanced cyber tools are typically employed by sophisticated nation-state actors. An investigation[38] into Saudi Arabian sponsored hacking activity demonstrates many examples of sophisticated espionage tools such as those provided by NSO Group or Hacking Team being used to spy on dissidents and political adversaries.
27. While the possibility exists that any number of sophisticated cyber weapons including NSO Group's Pegasus could have been used to compromise and exfiltrate data from Bezos' device, FTI's technicians also considered other possible cyber weapons. Note that al Qahtani, MBS' ex officio chief of hacking, owned a 20 percent stake in Hacking Team as of two (2) years prior to the compromise of Bezos device. It is likely that at the time in question, NSO Group and also Hacking Team — and likewise al Qahtani — would have possessed an exploit to infect devices via this very vector. FTI is aware that Hacking Team had specifically explored delivering cyber weapons via WhatsApp, and also aware of NSO Group's extensive use of WhatsApp as a delivery method.

[35] https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

[36] https://www.4armed.com/blog/galileo-rcs-running-espionage-operation/

[37] https://developer.apple.com/documentation/foundation/nsurlsession

[38] https://www.washingtonpost.com/opinions/2018/12/05/israel-is-selling-spy-software-dictators-betraying-its-own-ideals/?utm_term=.c4ae87b5be7e

Initial Disposition and Ongoing Investigation

Following a full forensic examination of the logical file system, network analysis, and an in-depth investigation of all available artifacts to date, FTI assesses with medium to high confidence that Bezos' iPhone X was compromised via a WhatsApp video attachment that was sent from an account utilized by Saudi Crown Prince Mohamed bin Salman (MBS). A review of external events, including apparent awareness of, and action upon, otherwise private information and events, supports these digital forensic conclusions. Based on the investigation to date and all available intelligence, it is believed that the compromise was likely facilitated by malicious tools procured by al Qahtani, such as a product of NSO (*e.g.*, Pegasus-3), or a product of Hacking Team (*e.g.*, Galileo).

FTI assesses that Bezos' device was compromised on May 1, 2018 and that the compromise resulted in gigabytes of data exfiltration that likely contained sensitive data such as personal photos, text messages, instant messages, emails, and possibly local (eavesdropped) recordings done via the phone's microphone.

FTI is pursuing several additional investigative avenues to further analyze and validate suspicious egress data, to corroborate malicious activity associated with the WhatsApp video and other elements of WhatsApp, and to further examine the device for the existence of past or present malicious software. The following investigative steps are currently pending.

1. Intercept and analyze live cellular data from Bezos' iPhone X.
    a. FTI will configure a new lab environment to capture and analyze live cellular data from Bezos' iPhone X. All network analysis thus far was captured via Wi-Fi in a sandboxed environment without an active Internet connection. As mentioned above, sophisticated malware often has network awareness and can employ methods to avoid discovery, such as detecting sandboxing and analysis techniques and testing for an active Internet connection. Intercepting live cellular data will aim to identify malware communication of this type while also analyzing cellular data egress as identified from the timeline analysis of Bezos' iPhone X.
2. Jailbreak Bezos' iPhone X and perform a forensic examination of the root file system.
    a. FTI will gain access to and conduct a forensic examination of the root filesystem of Bezos' iPhone X by jailbreaking it prior to analysis. Advanced weapons grade mobile malware typically installs itself to the root filesystem of a device to maintain persistence and avoid detection. Identifying evidence of malicious artifacts on this portion of the device could validate if an infection existed and corroborate evidence presented in this report.

FTI CONSULTING | CYBERSECURITY

About FTI Consulting

FTI Consulting, Inc. is an independent global business advisory firm dedicated to helping organizations manage change and mitigate risk: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. Connect with us on Twitter (@FTIConsulting), Facebook and LinkedIn.

www.fticonsulting.com