Cellebrite - Review

Task Force Cybercrime Insights

Cellebrite capabilities check
Analytics Series
Mobile device forensic on Android and iOS

www.cotech.de
contact@cotech.de
+49 531 3913154

Confidential Technologies GmbH
Wilhelmsgarten 3
D-38100 Braunschweig

Introduction

Cotech as experts for applied cryptography was invited to get an exclusive view on the labs of the Task Force Cybercrime. This labs is the center of all electronic surveillance and forensic measures in the federal state. By court order they can monitor all Internet traffic of a suspect. Internet providers must provide an interface where connection data can be fetched. This surveillance is passive. German authorities are not allowed to actively intercept communications. In addition they are not allowed to plant malicious devices on suspects. Forensic evidence from physical devices is collected on court order. Conservation of evidence on mobile devices is usually made with Cellebrite software.

Cellebrite

This software vendor calls itself leader of the market of device forensic. Software is only provided to government agencies. Users gets UI-based analysis tools. Data inspection is made by searching, grouping and visualization. It reads all device data from all apps. Data from common apps (e.g. WhatsApp, Instagram) is grouped separately. A data explorer give access to data. It shows images, GPS locations, messages, calls, contacts and browsing history. The forensic scientists are generally more interested in metadata than content. Metadata provides complex graphs about local movement, social milieu and activity timeline.

Set-up

For phone investigations a normal personal computer with Windows is used. An adapter kit makes sure that all kind of phones can be connected properly. For demonstration purposes, three phones were tested. The first was Armadillo Phone followed by iPhone 6 and a Google Nexus 5.

The Armadillo Phone were provided with the screen lock activated. This already fully blocked the analysis of the data and would have required to send the device to Cellbrite for further cracking (see discussion later). In a second test, the Armadillo phone was provided with an unlocked screen. This scenario conforms with real conditions (e.g. avoiding repressions from authorities at border crossing). The lab employee tried starting the developer mode of Android. The Armadillo OS prevented that. They informed us that they have never seen this being blocked before. This is the second barrier that prevented an investigation. Conclusively, the easy countermeasures of having a lock screen and disabled developer mode already prevented the investigators of gaining access to the phone's data

The only way to proceed for them, is to order a deeper device analysis by using Cellebrite's unlock service. In the following, both processes will be described.

Common way of gaining data access

An agent gets a convenient access to raw data and visualization. Before forensic work can be started full access to all data of the mobile device must be obtained. A common entry point for this are physical ports. The USB interface is predestined for copying massive data amounts. In normal state mobile devices are secure and this kind of access are prevented by the operating system. This security mechanism must be bypassed. Access is bypassed on different levels: jailbroken/rooted device, device in debugging mode and normal state. As declared previously the normal state is the securest. Criminologists have the same barrier as criminals. This is why politicians often demand backdoors for authorities.

The main strategy in mobile device forensic is to get root access on the device that may contain evidence. This is done in the same way IT hobbyists would approach it. They are using common information sources like XDA and blogs of security researchers. In a common cyber crime unit in Germany three criminologists doing that in their main work time. If a way of getting root access is available on the Internet, it is certain that German authorities are getting access to the device.

In the Android device range, many devices are rootable. Sometimes one-click root tools and step-by-step guides are available. But for many devices at least some information about getting root access is available online. The conclusion is that Android devices with an average market share are definitely not secure and authorities are able to sweep the devices.

The iOS side is slightly better. All phones are sharing the same operation system. On the one hand, this means that on availability of jailbreak the complete device range is vulnerable for device inspections. But on the other hand, iOS is getting more secure over time and Apple provides timely security updates. In iOS 12 the USB Restricted Mode was

www.cotech.de
contact@cotech.de
+49 531 3913154

Confidential Technologies GmbH
Wilhelmsgarten 3
D-38100 Braunschweig

introduced. This makes device inspections even harder. The USB port is just opened for battery charging and not for data exchange. The restricted mode is activated after one hour. This is enough to protect devices in normal investigations.

Cases described before are the common case. Investigations are made because of crime that are less important. Examples for that kind of crimes are small quantities of drug ownership, criminal assault and minor financial crimes. In other cases where criminal prosecution has more importance to authorities (e.g. murder, gang crime, illegal possession of firearms and serious financial offenses) another way of gaining data access is available.

Unlock services

Cellebrite offers a device unlock service. In special cases authorities can ship devices to Munich, where a Cellebrite's office is located. There, Cellebrite employed researchers with more methods to get data access on a device. They perform deep dives in the system and develop their own exploits. In addition they are buying exploits exclusively.

This kind of device attacks are a cat-and-mouse game between developers and attackers. In a scenario of limited resources, a strategy of minimizing data access from persistent memory might be the best strategy. Most times a hardware based encryption is available on persistent memory and attackers have not enough time to get access to key material with complex key extraction methods.

Generally this kind of service is not available for normal investigation. Cellebrite's business model depends on that service. In order to that one single usage of this service is to costly for investigations on petty criminals. Usually the average process time takes three weeks and the data gets extracted by experts.

Conclusion

Depending on the priority of an attack most devices are secure enough. Main attack vectors are Android's debugging mode and jailbreaks. All of them are performed over the USB port of the devices. Disabling USB data exchange and debugging exclude most attackers.

High priority targets shouldn't rely on the security of the hardware. The quality of Cellebrite's data extraction services is uncertain. We strongly advise to not saving any application data on persistent memory. In worst case the hardware encryption is not reliable. If application data must be saved persistently. It should saved with a high level encryption. In order of reaching the state of data is unencrypted just when it is loaded in RAM. The encryption key must not stored on the devices. It should derived from a user input (e.g. PIN, Passwort or Security Key or combination of factors). Biometric key derivation procedures are strongly not advised. Biometric targets are exposed every day and should only used for convenience.

In the beginning, the attempt of doing a quick analysis on Armadillo were described. The common way of extracting evidence from an Android phone is by activating the developer mode and using the Android Debug Bridge. Thus, in a scenario were users were forced to unlock the phone, a decoy password is a great way to lead the investigators into a unsuspicious Android environment. Here, developer mode and ADB emulation with fake output could help even more to let the investigators believe that there isn't any hidden data on the device. Conclusively, in order to achieve evasion from law enforcement repressions, even simple countermeasures and a fake Android environment helps enormously.

www.cotech.de
contact@cotech.de
+49 531 3913154

Confidential Technologies GmbH
Wilhelmsgarten 3
D-38100 Braunschweig