

Forum:[Hack Forums](#)

Thread: [cellebrite can only govs access it?](#)

Roberto Scorpius Malfoy - November 16, 2024, 5:13 am

<https://cellebrite.com/>

Its a program where you can bruteforce attack into devices, is this a program that only governments can use? I heard that this is the program that governments are using to bruteforce ppl's pincodes.

Does anyone know if this program can try unlimited attempts until the codes is correct?

Bastille - November 16, 2024, 5:28 am

Interesting topic, I've heard about this many times while watching french documentaries about police investigations.

I'm pretty sure this is related to the OS version of the smartphone, I don't think it works on all, especially on iOS, but has a higher success rate on Android. You need to subscribe to updates, and as you receive updates, you're able to brute-force more OS versions.

It seems that there are different type of products, and those with the label "UFED" seem to be for gov only, as they are capable of "brute-forcing" pin codes.

You can see that there are many of those machines (non-UFED) available on eBay

EDIT : I'm adding this video as it provides lot of information, this a UFED version (as you can see on the frame of the display) :

Roberto Scorpius Malfoy - November 16, 2024, 5:50 am

(Nov 16, 2024 06:28 AM)Bastille Wrote: [\[CITE\]](#) Interesting topic, I've heard about this many times while watching french documentaries about police investigations.

I'm pretty sure this is related to the OS version of the smartphone, I don't think it works on all, especially on iOS, but has a higher success rate on Android. You need to subscribe to updates, and as you receive updates, you're able to brute-force more OS versions.

It seems that there are different type of products, and those with the label "UFED" seem to be for gov only, as they are capable of "brute-forcing" pin codes.

You can see that there are many of those machines (non-UFED) available on eBay

EDIT : I'm adding this video as it provides lot of information, this a UFED version (as you can see on the frame of the display) :

Interesting stuff, if you try multiple times wrong codes on iphone it takes longer and longer to be able to try a new code like it takes 1 hour 2 hour, how can they bypass that when they bruteforce?

Bastille - November 16, 2024, 6:11 am

(Nov 16, 2024 06:50 AM)Roberto Scorpius Malfoy Wrote: [\[CITE\]](#) Interesting stuff, if you try multiple

times wrong codes on iPhone it takes longer and longer to be able to try a new code like it takes 1 hour 2 hours, how can they bypass that when they bruteforce?

I guess it's a flaw on the iOS version, maybe when you type the pincode WITH the display the system knows that he has to block after X unsuccessful tries, but if you "inject" the pincode through the cable maybe the OS is not designed to block it after too many unsuccessful tries (I'm just assuming, I don't know if this works like that)

?rew - November 16, 2024, 6:52 pm

It's not government only just expensive as if you are non government. GrayKey is kind of the same and they have a non police version too. The video referenced is how we did it back in like 2012 era

UFED Universal Forensics Extraction Device are basic units that are used but very outdated. A lot of people push fake articles on it due to they can pump and dump the units on eBay for \$\$

Depicide - November 16, 2024, 7:34 pm

Cellebrite is one of the only programs that the US Supreme Court qualifies as evidentiary value when it comes to DFL of electronics. This and one other program, but I forget what it is.

A lot of agencies use it because of the easy user interface and the information is categorized neatly. It is very effective if you have a password for the phone but bypassing certain phones can be a pain and when the phone is first turned on after being turned off. This is the Before First Unlock which is when your phone is the most secure.

Roberto Scorpius Malfoy - November 17, 2024, 5:36 am

(Nov 16, 2024 08:34 PM) iRoTOnOT Wrote: [\[CITE\]](#) Cellebrite is one of the only programs that the US Supreme Court qualifies as evidentiary value when it comes to DFL of electronics. This and one other program, but I forget what it is.

A lot of agencies use it because of the easy user interface and the information is categorized neatly. It is very effective if you have a password for the phone but bypassing certain phones can be a pain and when the phone is first turned on after being turned off. This is the Before First Unlock which is when your phone is the most secure.

I heard that bypassing the pincode of the phone is pretty easy since the program can try multiple codes per second, but what makes me confused is when you try wrong password several times Apple will tell you to wait like 2mins-10 mins-1 hour after repeatedly wrong attempts.

Bastille - November 17, 2024, 5:39 am

(Nov 17, 2024 06:36 AM) Roberto Scorpius Malfoy Wrote: [\[CITE\]](#) I heard that bypassing the pincode of the phone is pretty easy since the program can try multiple codes per second, but what makes me confused is when you try wrong password several times Apple will tell you to wait like 2mins-10 mins-1 hour after repeatedly wrong attempts.

From ChatGPT :

Exploitation of vulnerabilities:

Cellebrite often exploits software vulnerabilities in phone operating systems. These exploits allow bypassing security measures, including lockout delays, by directly accessing the data without needing to unlock the device.

Optimized brute-force attacks outside the device:

In some cases, Cellebrite clones the phone's memory (dumping the flash memory content). The brute-force process is then carried out on the cloned data rather than the original device, avoiding delays or data erasure caused by failed attempts.

Access via developer or recovery modes:

Some phones have diagnostic ports or developer modes that grant limited but sufficient access for data extraction or for injecting code to unlock the device.

Backdoors or privileged access:

In rare instances, Cellebrite may work with phone manufacturers or obtain master keys to bypass security measures. However, this is uncommon and often controversial.

Advanced cryptographic analysis:

For certain phones, Cellebrite uses advanced techniques to analyze encryption systems, identifying weaknesses or patterns that allow faster code guessing compared to standard brute-force.

I didn't think about the second option, sounds realistic as you can clone smartphones, but I guess you also need a celebrité device to clone a smartphone without the pincode

?rew - November 17, 2024, 5:44 pm

(Nov 17, 2024 06:36 AM)Roberto Scorpius Malfoy Wrote: [\[CITE\]](#) I heard that bypassing the pincode of the phone is pretty easy since the program can try multiple codes per second, but what makes me confused is when you try wrong password several times Apple will tell you to wait like 2mins-10 mins-1 hour after repeatedly wrong attempts.

Using exploits to bypass that.

Look at iPhone jailbreaks look at who coded them ;)

DramaKing - November 18, 2024, 6:45 am

(Nov 16, 2024 06:50 AM)Roberto Scorpius Malfoy Wrote: [\[CITE\]](#) Interesting stuff, if you try multiple times wrong codes on iphone it takes longer and longer to be able to try a new code like it takes 1 hour 2 hour, how can they bypass that when they bruteforce?

iPhones permanently lock after 10 failed unlock attempts. Apple has patched the known exploit. Cellebrite software can be purchased by both governments, law enforcement, and any enterprise that can afford it.

(Nov 17, 2024 06:44 PM)?rew Wrote: [\[CITE\]](#) Using exploits to bypass that.

Look at iPhone jailbreaks look at who coded them ;)

Yeah, sure. Just jailbreak the locked phone.

I posted this a while back.

<https://www.macrumors.com/2024/07/18/cellebrite-unable-to-unlock-iphones-on-ios-17-4/> It's important to realize that Apple issues security patches to fix vulnerabilities, and therefore exploits only affect certain software versions.

?rew - November 19, 2024, 9:00 am

(Nov 18, 2024 07:45 AM)DramaKing Wrote: [\[CITE\]](#) iPhones permanently lock after 10 failed unlock attempts. Apple has patched the known exploit. Cellebrite software can be purchased by both governments, law enforcement, and any enterprise that can afford it.

Yeah, sure. Just jailbreak the locked phone.

I posted this a while back.

<https://www.macrumors.com/2024/07/18/cellebrite-unable-to-unlock-iphones-on-ios-17-4/> It's important to realize that Apple issues security patches to fix vulnerabilities, and therefore exploits

only affect certain software versions.

Apple fix vulnerabilities, but not 0 days.

Also you need to read into my comment a bit more, you are not jailbreaking locked phones. As I said look at who is credited and coded the jailbreak software ;)

https://youtu.be/1d_kyMw8unE?t=94

Also most media get their facts way wrong. They retain an "expert" to spew theories or go off old documents speculating they put 0 research into writing articles because its all about the clicks and views. If you can fear monger or set relief to the paranoid you completed the objective.

Going off this chart

<https://www.documentcloud.org/documents/24833832-cellebrite-ios-document-april-2024?ref=404media.co>

Majority of devices seized are supported to get forensic images so IDK what that author of the article is talking about. I get if you don't get forensics or mobile forensics how you can say that but to each their own.

DramaKing - November 19, 2024, 9:42 am

(Nov 19, 2024 10:00 AM)?rew Wrote: [\[CITE\]](#) Apple fix vulnerabilities, but not 0 days.

Also you need to read into my comment a bit more, you are not jailbreaking locked phones. As I said look at who is credited and coded the jailbreak software ;)

https://youtu.be/1d_kyMw8unE?t=94

Also most media get their facts way wrong. They retain an "expert" to spew theories or go off old documents speculating they put 0 research into writing articles because its all about the clicks and views. If you can fear monger or set relief to the paranoid you completed the objective.

Going off this chart

<https://www.documentcloud.org/documents/24833832-cellebrite-ios-document-april-2024?ref=404media.co>

Majority of devices seized are supported to get forensic images so IDK what that author of the article is talking about. I get if you don't get forensics or mobile forensics how you can say that but to each their own.

That chart is essentially what I linked to. Now some users dispute it and suggest that newer devices can be unlocked with more restricted and secret features.

And if you read what I posted, I said "known exploits." Of course there could be a zero-day that hasn't been made public, but what the public doesn't know has an incredibly small chance of hurting you.

?rew - November 20, 2024, 5:56 pm

(Nov 19, 2024 10:42 AM)DramaKing Wrote: [\[CITE\]](#) That chart is essentially what I linked to. Now some users dispute it and suggest that newer devices can be unlocked with more restricted and secret features.

And if you read what I posted, I said "known exploits." Of course there could be a zero-day that hasn't been made public, but what the public doesn't know has an incredibly small chance of hurting

you.

The whole concept is built off zero days, so saying Know exploits is pointless.

This is why they pump millions into their RnD team and hire top exploiters and zero day talent in the mobile area.

It's not really a dispute you can go on the discord and ask for devices and what is supported if you are a known entity and they will tell you.

The media has a lot of this all wrong because they did not investigate into it but just pumped out an article with scary scary things.