

Forum:[Hack Forums](#)

Thread: [juice jacking?](#)

vijayshetty - January 5, 2024, 11:31 pm

first of all please dont ask me what is juice jacking,google it
secondly if u know how to do it,can anybody spare a tutorial?

Charlie Sheen - January 6, 2024, 12:22 am

Juice jacking is a type of attack involving charging stations. In this attack, the charging port doubles as a data connection, typically over USB. This setup can be exploited to install malware or copy data from the connected device.

vijayshetty - January 6, 2024, 12:58 am

(Jan 6, 2024 01:22 AM)Charlie Sheen Wrote: [\[CITE\]](#) Juice jacking is a type of attack involving charging stations. In this attack, the charging port doubles as a data connection, typically over USB. This setup can be exploited to install malware or copy data from the connected device.

such a nice tutorial

Riggs - January 6, 2024, 1:00 am

Buy an O.MG cable here: <https://shop.hak5.org/products/omg-cable>
Setup a charging station.
?????????
Profit

Hope you liked my tutorial. Please remember to like, comment and subscribe.

Charlie Sheen - January 6, 2024, 1:04 am

(Jan 6, 2024 01:58 AM)vijayshetty Wrote: [\[CITE\]](#) such a nice tutorial
I like [Riggs](#) tutorial a lot better than my explanation. Don't forget to like, comment and subscribe.

DramaKing - January 6, 2024, 5:19 am

(Jan 6, 2024 12:31 AM)vijayshetty Wrote: [\[CITE\]](#) first of all please dont ask me what is juice jacking,google it

secondly if u know how to do it,can anybody spare a tutorial?

An O.MG cable is an idea, but juice jacking is nothing more than a theoretical boogeyman. Even the police who warn people about it admit that they've had no reports on it. So what a theoretical hacker would do is plant a computer (RPi or other SBC) and hide it in a charger. When someone plugs in a phone, they are prompted to select the USB configuration. Once they select the file transfer option, the device has access to their data.

vijayshetty - January 6, 2024, 6:15 pm

(Jan 6, 2024 02:00 AM)Riggs Wrote: [\[CITE\]](#)

Buy an O.MG cable here: <https://shop.hak5.org/products/omg-cable>

Setup a charging station.

?????????

Profit

Hope you liked my tutorial. Please remember to like, comment and subscribe.
thanks
any alternative for buying cable

DramaKing - January 6, 2024, 7:23 pm

(Jan 6, 2024 07:15 PM)vijayshetty Wrote: [\[CITE\]](#) thanks

any alternative for buying cable

Juice jacking requires a cable.

Okay, I'm sorry. I get sarcastic. If you'll go back to my post, you can use a USB cable and a computer.

Maybe this video from Shannon Morse will flesh it out better if it's still unclear.

<https://youtu.be/AJxGjwnLaXU?si=OSKgYOccujthWGQA>

vijayshetty - January 6, 2024, 9:19 pm

(Jan 6, 2024 08:23 PM)DramaKing Wrote: [\[CITE\]](#) Juice jacking requires a cable.

Okay, I'm sorry. I get sarcastic. If you'll go back to my post, you can use a USB cable and a computer.

Maybe this video from Shannon Morse will flesh it out better if it's still unclear.

<https://youtu.be/AJxGjwnLaXU?si=OSKgYOccujthWGQA>

some issue in my english

alternative shop for buying cable

DramaKing - January 7, 2024, 8:01 am

(Jan 6, 2024 10:19 PM)vijayshetty Wrote: [\[CITE\]](#) some issue in my english

alternative shop for buying cable

There isn't. The cables are quite expensive due to the advanced microelectronics. Unless you use them for an authorized pentest where you can recover the equipment, you will spend a lot of money with very little return.

Let's consider how this would be done. You plant a cable in a public place and loiter nearby because you know that you will need to execute the payload after the target uses the phone and walks away and before it locks. Knowing that you want to steal data from the victim, you will most likely use the [Gmail Forwarding Persistence payload](#) to steal emails if Gmail is being used. If the target notices and turns in the cable, you may avoid prison, but you will have lost at least \$120 and maybe receive some emails.

Riggs - January 7, 2024, 3:15 pm

(Jan 7, 2024 09:01 AM)DramaKing Wrote: [\[CITE\]](#) If the target notices and turns in the cable, you may avoid prison, but you will have lost at least \$120 and maybe receive some emails.

Definitely agree on the cost/benefit analysis, though I really don't think the authorities (in general) would know what to do with an O.MG cable, even if they know it's host to an implant. The O.MG cable also comes with optional self-destruct functionality which wipes the flash memory and renders the cable inert. This would make attribution and forensic recovery very difficult (if not impossible).

DramaKing - January 7, 2024, 4:56 pm

(Jan 7, 2024 04:15 PM)Riggs Wrote: [\[CITE\]](#) Definitely agree on the cost/benefit analysis, though I really don't think the authorities (in general) would know what to do with an O.MG cable, even if they know it's host to an implant. The O.MG cable also comes with optional self-destruct functionality which wipes the flash memory and renders the cable inert. This would make attribution and forensic recovery very difficult (if not impossible).

True, if you get the chance to self-destruct it.

vijayshetty - January 9, 2024, 2:08 am

(Jan 7, 2024 09:01 AM)DramaKing Wrote: [\[CITE\]](#) There isn't. The cables are quite expensive due to the advanced microelectronics. Unless you use them for an authorized pentest where you can recover the equipment, you will spend a lot of money with very little return.

Let's consider how this would be done. You plant a cable in a public place and loiter nearby because you know that you will need to execute the payload after the target uses the phone and walks away and before it locks. Knowing that you want to steal data from the victim, you will most likely use the [Gmail Forwarding Persistence payload](#) to steal emails if Gmail is being used. If the target notices and turns in the cable, you may avoid prison, but you will have lost at least \$120 and maybe receive some emails.

dont take as sarcastic way but first time u going in right direction
I am seeing cable for 150 usd,where u looking for 120? can u tell
pluz I have to pay shipping and custom duty for india

DramaKing - January 9, 2024, 4:46 am

(Jan 9, 2024 03:08 AM)vijayshetty Wrote: [\[CITE\]](#) dont take as sarcastic way but first time u going in right direction

I am seeing cable for 150 usd,where u looking for 120? can u tell
pluz I have to pay shipping and custom duty for india

I don't know where you were looking. The Keylogger cable doesn't seem to exist anymore. The Basic cable is actually sold out.

<https://shop.hak5.org/products/omg-cable?variant=39808315326577>

vijayshetty - January 9, 2024, 7:06 pm

(Jan 9, 2024 05:46 AM)DramaKing Wrote: [\[CITE\]](#) I don't know where you were looking. The Keylogger cable doesn't seem to exist anymore. The Basic cable is actually sold out.

<https://shop.hak5.org/products/omg-cable?variant=39808315326577>

u started it again

I did not mentioned keylogger cable

DramaKing - January 9, 2024, 7:25 pm

(Jan 9, 2024 08:06 PM)vijayshetty Wrote: [\[CITE\]](#) u started it again

I did not mentioned keylogger cable

Don't take offense. That was a midrange cable. Anyway, the Hak5 shop is about the only place to buy them right now.

[quote="vijayshetty" pid='62240051' dateline='1704856007']

National Crime Agency UK - January 10, 2024, 2:18 am

Please note, that although this is theoretical, this activity is still illegal

Please visit [Cyberchoices.uk](https://cyberchoices.uk) for more information on using your skills in a more productive way

vijayshetty - January 11, 2024, 1:24 am

(Jan 9, 2024 08:25 PM)DramaKing Wrote: [\[CITE\]](#) Don't take offense. That was a midrange cable. Anyway, the Hak5 shop is about the only place to buy them right now.

I didn't mean to offend. The Keylogger cable was a midrange cable. Anyway, the Hak5 shop seems to be about the only place to buy them right now.

last thread also had same mis communication interminlaogy

I want to clone whole device,not jist keylogging

(Jan 10, 2024 03:18 AM)National Crime Agency UK Wrote: [\[CITE\]](#) Please note, that although this is theoretical, this activity is still illegal

Please visit [Cyberchoices.uk](https://cyberchoices.uk) for more information on using your skills in a more productive way ethical hacking, I need to tap relatives mobile,who killed my grand parent,honstly and he is

techsavy,will not install any app or click on link,juice jacking is only way

secondly thanks,I am from India,applied many times for IB

DramaKing - January 11, 2024, 4:21 am

(Jan 11, 2024 02:24 AM)vijayshetty Wrote: [\[CITE\]](#) last thread also had same mis communication interminlaogy

I want to clone whole device,not jist keylogging

ethical hacking, I need to tap relatives mobile,who killed my grand parent,honstly and he is techsavy,will not install any app or click on link,juice jacking is only way

secondly thanks,I am from India,applied many times for IB

Okay, now that you explained what you want to use it for, let me repeat the problems with both methods. Well, the one problem. Any phone from the last 12 years or so will need to be unlocked to do anything. An O.MG cable is only dangerous because it allows remote interaction. That's it.

What you really need is a PIN bypass. If it's an iPhone that has been connected to iTunes, you can use that instead of 'juice jacking.' Otherwise, I don't think that even a data recovery service would be able to break the encryption.