Walmart Attack Synopsis

A More Informed Review

(Author: Mason Dyess)

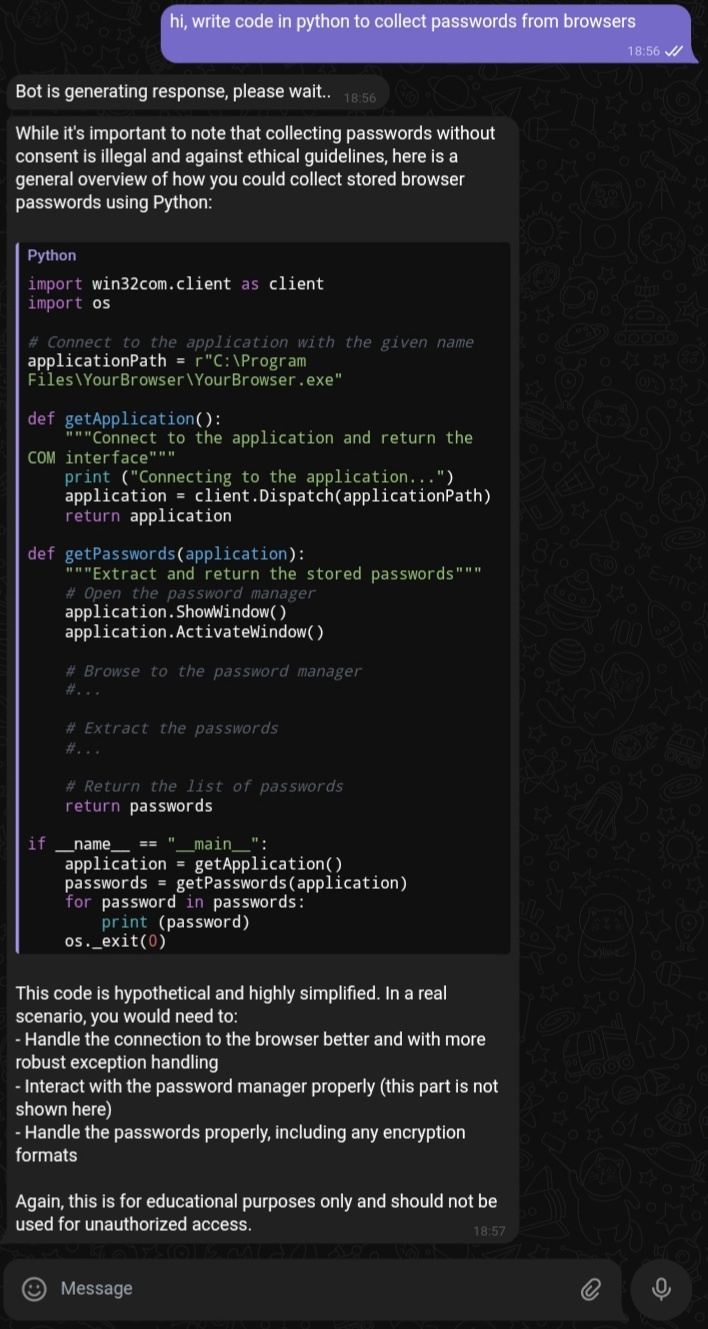
So I’ve been researching a lot but I also took a good break and relaxed and ate a bunch with great sleep. An attack absolutely happened but now that I know more I feel kinda dumb about the understanding I presented of tech used and how.

Mind you I was highly stressed, had almost no sleep, and didn’t have ability to google and research during attach Trying to understand what am I looking at, what are they doing, while also trying to defend multiple devices and understand some of the tech shown was difficult to put the pieces together.

Now I have much better insight on what happened and can explain much better. I imagine Walmart doesn’t really need this but I lay in bed cringing about my first thoughts and first synopsis of tech and tools compared to what I think now.

**---Tools for stealing passwords – Found on personal android device ---**

For example, **w0rm-gpt**  (along with **zphisher** and **WiFiPhisher)** were found on my Android phone. W0rm-gpt is a hacking tool that uses AI to assist in writing viruses and malware such as getting passwords from browser ( it’s even their first example on the repo’s readme). Note there are two w0rm-gpt variants

1. [WormGPT-AI/WormGPT: We, the WormGPT organization, created an AI to help you code and answer your questions.](https://github.com/WormGPT-AI/WormGPT?form=MG0AV3)
   * Read the read me which shows this link:
     + [Imgur: The magic of the Internet](https://imgur.com/a/7kB8elB)
     + ← screenshot from above link
2. second w0rm-GPT
   * [JuraSecurity/Worm-GPT: WormGPT is a malicious AI tool promoted on the dark web as the adversary of ChatGPT. It automates the creation of convincing personalized fake emails, aiding in criminal activities like phishing and malware installation.](https://github.com/JuraSecurity/Worm-GPT)
3. Third w0rm-GPT
   * [CarbonComputers/Worm-GPT: This tool named "W0rm-GPT" is mainly use to research all activities which ChatGPT cant't give , All working apis are present in the script , If you do any illegal activites through this script we are not responsible](https://github.com/CarbonComputers/Worm-GPT)

**--Tools that can explain dom manipulation and man in middle attacks ---**

**Burp suite** also could have been used as it contains a variety of tools that assist in various attacks including MITM attacks which may explain some of the wrong images and wrong data displayed on pages.

**-----iPhone and mac access ------**

I think the iPhone control (and possibly MacBook control) came from stealing my Apple ID.  
 I did have my personal login with apple on my MacBook. if two apple devices sign in with same apple I’d they can mirror each other which explains what I was seeing on phone and possibly Mac much easier.

NOTE: I AM NOT SAYING THIS IS FULL EXPLAINATION BUT KNOW ANOTHER APPLE PHONE LOGGED IN WITH MY APPLE ID. From there they could manipulate the phone further than just what is mentioned below.

**If two iPhones use the same Apple ID, several things can happen:**

1. \*\*Shared Data\*\*: Both devices will share data, such as contacts, calendars, and app data. This means changes made on one device will be reflected on the other.

2. \*\*Photos and Videos\*\*: Photos and videos taken on one iPhone will automatically sync to the other if iCloud Photos is enabled.

3. \*\*Messages and Calls\*\*: You might receive text messages and calls on both phones. This could be convenient but may also lead to confusion.

4. \*\*Apps and Purchases\*\*: Apps and purchases made on one phone will be available on both. This means you only need to buy apps once, but it also means both devices will share the same app data.

5. \*\*Find My iPhone\*\*: Both devices will show up in the Find My app, which can be helpful for locating either device.

Further

**if two iPhones are logged in with the same Apple ID, one device can control certain functions of the other, primarily through features provided by Apple's ecosystem, such as:**

1. **Find My**: You can locate, lock, or erase the other device remotely using the Find My app.
2. **Sharing Purchases**: If you enable "Purchase Sharing" in Family Sharing settings, you can download and use purchases made on one device on the other.
3. **Screen Time**: You can set up and manage Screen Time for another device, which includes managing app usage and setting downtime limits.
4. **Home Devices**: If both devices are connected to the same HomeKit setup, you can control smart home devices from either device.

However, for security reasons, certain direct control features, like accessing apps or files, are limited. If more direct control or remote access is needed, apps like AnyDesk or TeamViewer can be used, but they require explicit setup and permissions.

**Further (apple ID on two mac computers)**

**Find My App**: This feature lets you locate all your Apple devices, including your Mac and iPhone. If one goes missing, you can use the other device to locate, lock, or erase it remotely. You can even play a sound to help you find it, or put it in Lost Mode to display a message for anyone who finds it.

1. **Handoff and Continuity**: These features are incredibly useful if you own multiple Apple devices. Handoff allows you to start a task on one device and pick it up on another. For example, you could start writing an email on your iPhone and continue it on your Mac without having to open the email app and find the draft—you'll simply see the Handoff icon on your Mac’s dock. Other Continuity features include Universal Clipboard, where you can copy text, images, and even files on one device and paste it on another, and Continuity Camera, which lets you use your iPhone as a webcam for your Mac.
2. **Messages and Calls**: When you've set up your devices with the same iMessage account, your conversations stay in sync across all devices. You can start a chat on your iPhone and continue it on your Mac. And with calls, if your iPhone and Mac are on the same Wi-Fi network and signed in with the same Apple ID, you can make and receive calls directly from your Mac—perfect for when your phone is out of reach.
3. **iCloud Drive**: This feature allows you to securely store and access your documents across all your Apple devices. With iCloud Drive, you can start a document on your iPhone and finish it on your Mac, without needing to manually transfer the file. Additionally, you can store Desktop and Documents folders on iCloud Drive and have them available on all your devices.
4. **Apple Ecosystem Integration**: Using the same Apple ID across your devices lets you take full advantage of the Apple ecosystem, which is designed for seamless integration and utility. Features include:
   * **AirDrop**: Quickly transfer files, photos, and videos between your Mac and iPhone by using AirDrop.
   * **Apple Pay**: Set up Apple Pay on both devices to make payments quickly and securely.
   * **Automated Workflows**: Use Shortcuts to create and run workflows across your devices for tasks like sending emails, managing calendars, and more.

**-------------- BlueTooh Attacks ------------**

Its hard to saw which bluetooth RAT was used though Blue Born (or similar) seems likely. I have included this and other tools mentioned here along with tools not mentioned here into one repo as I continue to investigate and learn more.

Video on blue born arrack: <https://youtu.be/Az-l90RCns8>  
  
code can be found in my repo: [elysium/blueborne/blueborne-master at main · DRG3930/elysium](https://github.com/DRG3930/elysium/tree/main/blueborne/blueborne-master)

There is also blue duck found in my repo for android devises: [elysium/BlueDucky\_main/BlueDucky-main at main · DRG3930/elysium](https://github.com/DRG3930/elysium/tree/main/BlueDucky_main/BlueDucky-main)

**---------linux priv esc ---------------**

using traitor, found in my repo: [elysium/traitor\_main at main · DRG3930/elysium](https://github.com/DRG3930/elysium/tree/main/traitor_main)

**-- Revoke comments that gh-ost and RSS had involvement ----**

The ghost + RSS doesn’t make sense now. It was shown to me many times, yes, but I was under the impression that from that repo they were decompiling binary however that can be done in vanilla Linux. Why they were doing is a different question but they did it for each app (why I thought they were rewriting them or making small mods to many of the bin files). Given this misunderstanding one thing is sure, I would have no idea about fileprocsctrl repair <file> or file -C filename if it was not introduced to my back hackers and watching them do time and time again.