TL;DR

Coinomi multi-asset wallet poor implementation leads to sharing your plain-text passphrase with a third-party server. My passphrase was compromised and $60K-$70K worth of crypto-currency assets were stolen because of Coinomi wallet and how the wallet handled my passphrase. I'm disclosing this issue publicly because Coinomi refused to take the responsibility and all my attempts through private channels have failed.

Please note that this security issue cannot be exploited by anyone except by the people who created it or have control over the backend. To everyone who is using or used Coinomi wallet, make sure to remove your funds from the wallet and change your passphrase by creating a new wallet using another application otherwise your funds might get stolen sooner or later.

To understand how catastrophic the security issue is, they simply take your crypto-currency wallet's passphrases/seeds and spell check it by sending it remotely to Google servers in clear plain text!

They did not take the responsibility of my loss, I gave them more than 24 hours before full disclosure, they fixed the issue without notifying their users and they kept procrastinating like scumbags to buy more time.

Below is a link to their final response to my request after going back and forth with them for over 3 days to get my stolen funds back, even after they confirmed the security issue and you can clearly see how silly and reckless their responses are (these responses are just examples):
https://avoid-coinomi.com/files/coinomi_final_response.png

My advice never ever trust Coinomi with your hard earned crypto-currency assets. Read this post entirely to understand why because this is not their first time reflecting this kind behavior.

The Incident

First of all I admit it was my mistake trusting Coinomi wallet by inserting one of my main wallets (Exodus wallet) passphrase into their application. I trusted them because I downloaded the software from their website, the setup file was digitally signed and was mentioned by several reputable websites such as bitcoinwiki.org. I wanted to shift some of the assets that were not supported by Exodus wallet using the same passphrase/seed.

The incident began on 14th February, 2019. I downloaded and installed Coinomi application (Windows version) and noticed that their setup file was digitally signed but their main application was NOT signed after the installation process was completed.

I contacted them publicly through twitter (@warith2020) and they confirmed the issue then uploaded a new version with the main application signed. At that time I had already entered my Exodus's wallet passphrase into Coinomi's application.

On 22nd February 2019, I noticed that more than 90% of my Exodus wallet assets were transferred to multiple wallet addresses and the first transaction began with BTC on 19th February 2019 around 3:30 am UTC. Then followed by ETH (including ERC20 tokens), LTC and finally BCH.

Technical Analysis

I started going back in time and arranging the events. The only new thing that I did was installing and running Coinomi wallet so my first conclusion was that the unsigned version of the application had a backdoor.

I did further investigation and compared both the unsigned version of the setup file and the signed version. The only difference was they added digital signature to the main executable file and the Java file (the main application).

At that stage I thought that there is probably something suspicious about the application apart from having their main executable unsigned, so I started replicating what I did in a new virtual machine but this time I installed "Fiddler". A software that allows you to monitor and debug HTTP/HTTPS traffic of all applications running on your machine.

I started monitoring the traffic by running Fiddler in the background and then started Coinomi wallet. The first thing I noticed is that Coinomi application starts downloading dictionary wordlist from the following web address:
https://redirector.gvt1.com/edgedl/chrome/dict/en-us-8-0.bdic

Then I clicked on restore wallet and pasted a random passphrase and suddenly the screen screamed SURPRISE MOTHER****** (boom puzzle solved!)

The WHOLE passphrase in plain-text is sent to googleapis.com a domain name owned by Google! It was sending it as a spelling check function! Here is sample of the screenshot of the HTTP request:
https://avoid-coinomi.com/files/coinomi_screenshot_1.png

To verify my findings I have uploaded a video for anyone who wants to test and replicate what I did:
https://avoid-coinomi.com/files/coinomi_http_traffic_video.mp4

You can also simply paste any random sentence with spelling mistake in the textbox in Coinomi's "Restore Wallet" form/page and you will see that it gets underlined with red line after being sent in clear text to googleapis.com.

To understand what's going on, I will explain it technically. Coinomi core functionality is built using Java programming language. The user interface is designed using HTML/JavaScript and rendered using integrated Chromium (Google's open-source project) based browser.

The whole thing is done using JxBrowser to build cross-platform applications and before you say (like Coinomi's CTO did) that it's JxBrowser issue, let me tell you that they mentioned this on their website in 2016 and how to disable the spell checking default behavior:
https://jxbrowser.support.teamdev.com/support/solutions/articles/9000044250-configuring-spell-checker

So essentially the textbox which you enter your passphrase in, is basically an HTML file ran by Chromium browser component and once you type or paste anything in that textbox it will immediately and discreetly send it remotely to googleapis.com for spelling check (how awesome is that!).

As a result, someone from Google's team or whoever had access to the HTTP requests that are sent to googleapis.com found the passphrase and used it to steal my $60K-$70K worth crypto assets (at current market price). Anyone who is involved in technology and crypto-currency knows that a 12 random English words separated by spaces will probably be a passphrase to a crypto-currency wallet!

Coinomi's Response

The team behind Coinomi are either extremely smart to add such backdoor so that when they get caught they would simply say it was an honest mistake or they are extremely stupid to overlook such security bug.

I will not be surprised if they intentionally created this backdoor behavior function and had an insider at Google especially when you learn from recent news about a founder of crypto-currency exchange claiming weird suspicious death while no one except him has access to the crypto-currency assets!

Coinomi's team did not reflect any responsible behavior and they kept asking me about the technical issue behind the bug because they were worried about their public image and reputation. They kept ignoring my request of taking the responsibility and ignored my solid facts regarding it. They didn't give a single **** about my stolen crypto assets. They kept reminding me (kinda threatening me) of the legal implications if I go public with the information I have and they forgot their legal responsibility for my stolen crypto assets as well as the risk that impacts other users of the wallet.

In fact, Coinomi's team discreetly deleted their reply to my tweets to hide the evidence regarding their unsigned main executable in which they confirmed the issue and they didn't respond to my requests as shown in the following screenshots:
https://avoid-coinomi.com/files/coinomi_tweets.pdf

Such behavior was a clear evidence for me that there is something suspicious about their wallet and they didn't want to expose it. It seems the founders are the developers of the application and they don't like anyone who criticizes their ugly baby creation "Coinomi" wallet. They think that they are the code gurus fallen from the heavens who write perfect code.

However, before I published my findings I sent them the whole thing giving them more than 12 hours heads-up because they requested a clear technical evidence. Their CTO told me that he will download the report within 3 hours (they downloaded the report after 5-6 hours). Imagine someone tells you that you have a CRITICAL vulnerability in your software which holds users' hard earned crypto assets and yet you act carelessly because somehow you think you are a superior creature (*Khan from Star Trek Into Darkness movie*).

Below are the screenshots of the private messages between Coinomi's CTO and me:
https://avoid-coinomi.com/files/coinomi_cto_private_messages.pdf

This is not their first time behaving this way especially when someone finds an issue with their application. Luke Childs previously published a security vulnerability/misconfiguration and their response was somehow similar:
https://bitsonline.com/coinomi-vulnerability-respond/
https://imnotdead.co.uk/blog/coinomi

Recap

To recap the events for further investigation:

- My first passphrase attempt was sent to googleapis.com through Coinomi wallet was on 14th February 2019
- Google's employee or whoever has control over the data that are sent to googleapis.com processed the data that had my passphrase and that was between 14th and 19th February 2019
- My crypto assets were stolen on 19th February 2019 starting around 3:30 am UTC and the transactions continued for 15 minutes. At the end 90% of the assets were gone and remaining assets were only left because these assets were supported by Exodus wallet but NOT Coinomi wallet (what a coincidence you say!)

Please note that I took all the security precaution to keep my passphrase and wallet safe. I have a separate isolated virtual machine for it with Anti-Virus/Anti-Malware and firewall installed. I also had other wallets on the same virtual machine for years. Nothing was stolen except for the wallet which I recently used my passphrase in, which is Coinomi wallet!

What's Next

I will start taking legal actions against the company behind Coinomi if they don't act and take the responsibility. The company is registered in UK as "Coinomi LTD" if anyone one has faced or facing similar case were you suddenly lost your crypto assets and you happen to have used Coinomi wallet. The funny thing is that they state on their website:

"*Most importantly, no Coinomi wallet has ever been hacked or otherwise compromised to date.*" (bull****!)

Be aware that probably all desktop versions are affected (I'm not sure about the mobile versions) and the guy/group who is/are capturing the passphrases, possibly targeting only wallets with decent amount of assets to stay low profile as long as he/they can.

I have also uploaded copy of the latest version of Coinomi application in case they take down the links to hide the facts:

- UNSIGNED version (proof that the main application was not signed): *https://avoid-coinomi.com/files/coinomi-wallet-1.0.4-win64_UNSIGNED.exe*
- Signed version (proof that the wallet sends passphrase to a remote server): *https://avoid-coinomi.com/files/coinomi-wallet-1.0.4-win64_signed.exe*
- Screenshot of the SHA256SUM hashes before the patch: *https://avoid-coinomi.com/files/coinomi_hashes.png*

Final Thoughts

This was an expensive and mentally painful experience to learn from and hopefully after publishing this post no one will experience the same. The lessons learned so far:

- Never trust any multi-asset crypto wallet unless they have done an external security audit by a trusted third-party and their security audit is publicly available.
- Never ever trust Coinomi with your hard earned crypto-currencies. They do not take any responsibility and when they f***-up things they just run away like it's not their business.
- Never ever trust Google services/products with your sensitive information. They have great control over the data and it seems their policy isn't that strict which results in taking advantage and the power of the collected data by their employees especially who have malicious intents.

At the end I need to make it clear again why I published this:

- Spread awareness among users who are using or used Coinomi wallet.
- Demand my stolen crypto-currency assets from the company behind Coinomi wallet either in terms of crypto currency or in terms of fiat currency. The more they procrastinate the more the value of the assets increase by time.
- Force Google to start investigating the issue. I'm pretty sure this is a serious issue not only in regards of my stolen crypto-currency assets but also in terms of users' privacy and their data being maliciously used by Google's employees or whoever have control over these data.

Finally I hope the readers share this website to spread the awareness. I'm pretty sure hundred thousands of crypto assets will be saved and many users will have the opportunity to save their hard earned crypto assets!

Next time if you need to spell check your passphrase/seed and to make sure that you are following the English dictionary just use Coinomi wallet LMAO!