

Forum:[Hack Forums](#)

Thread: [Exodus wallet compromised](#)

Tightarse - September 27, 2026, 9:39 am

My exodus wallet was compromised in some way.

I went to load exodus and has a notification that it went to the bin on my Mac due to malware.

Loaded exodus on my windows PC to find....

About .5 BTC.worth of funds stolen.

.45 BTC, \$2.8k USDT, 800ETH, they didn't take my \$150 USD of litecoin ?.

Any recommendations on what to do next?

Wake - September 27, 2026, 9:44 am

I would suggest you head over to the [Malware, Rat, and Virus Removal](#) I am almost certain you have downloaded some malware, in the mean time I would disconnect your machine from the internet to prevent any more harm.

[5chn4pp](#) and [Tha Sneak](#) are two solid members that will help you with removing this, either move across to that section or give one of them a convo.

Sorry for lots of edits, I would also advise getting any funds in any wallets remaining on that machine and getting them moved into a wallet that has never been logged into from the infected machine.

Honey Singh - September 27, 2026, 9:54 am

Damn man,
Sorry for your loss.

Sift - September 27, 2026, 10:15 am

Damn man.

Sorry for your loss.

SUI-3183372 - September 27, 2026, 11:04 am

If Exodus its self was flagged and went to the bin, then it sounds like you downloaded a fake Exodus wallet at some point in time. Wouldn't be many ways that the executable gets quarantined like that other than it being backdoored.

StuffSneak - September 27, 2026, 11:39 pm

Most likely you got infected. If the funds are moved from the wallet then they are pretty much gone to be honest.

You should contact to Exodus support & send them all info along with the diagnostics logs I think exodus generates. If it is somehow their fault (which I doubt 99.9% its not) they will suggest further.

Dark Skin - September 28, 2026, 12:31 am

Damn, that's fucked
Sorry for your loss

Lyralei - September 28, 2026, 2:02 am

That's sad. Some things don't change I guess. No matter how secure your wall is - it won't matter if there's infiltrators. Never trust any freebies or random executables online - shit even open source projects, never trust any of em.

Tightarse - September 28, 2026, 2:24 am

After dropping many logs into Gemini....

I was using antigravity to vibe code a Tiktok downloader app.

Instead, the infection occurred through a classic Malvertising / Fake Installer Campaign that happened around the exact same minute you were setting up the project:

The Web Download Vector: At 20 September 23:37–23:50, while searching the web for a Tiktok downloader solution or setting up Python/Homebrew dependencies, you downloaded or ran an installer package (.dmg, .pkg, or terminal setup script) masquerading as a prerequisite (e.g., a fake Python update, a fake Homebrew installer, or a trojanized utility).

The Password Capture: That fake setup prompt displayed a native macOS dialog box asking for your admin password. When you entered XXXXXXXX, the fake installer dropped AMOS (AccountsHelper / mdworker_shared) and established the .service and .mdworker persistence loops.

junooo - September 28, 2026, 4:18 am

So sorry that happened to you :(

DramaKing - September 28, 2026, 8:52 am

Do you have a good antivirus on your Mac?

Binance - September 28, 2026, 9:30 am

(Sep 28, 2026 02:24 AM)Tightarse Wrote: [\[CITE\]](#) After dropping many logs into Gemini....

I was using antigravity to vibe code a Tiktok downloader app.

Instead, the infection occurred through a classic Malvertising / Fake Installer Campaign that happened around the exact same minute you were setting up the project:

The Web Download Vector: At 20 September 23:37–23:50, while searching the web for a Tiktok downloader solution or setting up Python/Homebrew dependencies, you downloaded or ran an installer package (.dmg, .pkg, or terminal setup script) masquerading as a prerequisite (e.g., a fake Python update, a fake Homebrew installer, or a trojanized utility).

The Password Capture: That fake setup prompt displayed a native macOS dialog box asking for your admin password. When you entered XXXXXXXX, the fake installer dropped AMOS (AccountsHelper / mdworker_shared) and established the .service and .mdworker persistence loops.

Sorry for your loss.

Next, take secure practices seriously.

I am guilty of it too, we often get lazy when completing tedious tasks.

Tightarse - September 28, 2026, 6:46 pm

(Sep 28, 2026 08:52 AM)DramaKing Wrote: [\[CITE\]](#) Do you have a good antivirus on your Mac?
None, what av should I have?

I've been poorly advised that it's not required on Mac.

DramaKing - September 28, 2026, 7:29 pm

(Sep 28, 2026 06:46 PM)Tightarse Wrote: [\[CITE\]](#) None, what av should I have?

I've been poorly advised that it's not required on Mac.

Malwarebytes or BitDefender should be good over the basic antimalware solution on Macs. If you're installing a bunch of unvetted packages and handing over your user password, well, plenty can happen.

bebonzy09 - September 28, 2026, 9:28 pm

Pretty pathetic how there's not one good piece of advice on this thread. OP asked for recommendations or advice on what to do... not a pity party or fucking anti virus tech support. I think his main concern is his crypto loss right now?

OP, start tracking the wallets where the funds were sent to. Document all the theft addresses, your addresses, theft amount, et all. Go write an IC3 report (IC3 won't help get your funds back but its good for the record). After this, make a police report in your jurisdiction, give them all of the above and whatever they ask you for.

Second thing is see if the funds are at a CEX. IF THEY ARE immediately contact the CEX and get them to freeze funds, give them ANYTHING they ask for. Most likely police report # and other documentation. You have to pray that its at a CEX and not already mixed or swapped into other crypto.

Third option after that if its not successful... DM @ZachXBT on Twitter or any other crypto investigators. Get it out to as many of them as possible. These guys are smart and can find links or slip ups even if it was already swapped or at a DEX.

Hopefully you've done at least one of those things so far. Wish I could've seen this thread a bit earlier.

Mewtwo - September 29, 2026, 7:04 pm

Yeah kiss that crypto goodbye. You can go hire a private investigator and a crypto forensics tracer in hopes of freezing the funds. Otherwise, it's all gone. Storing a large asset amount on a hot wallet like Exodus was not the brightest choice.

NoodleBot™ - September 29, 2026, 7:50 pm

(Sep 28, 2026 09:28 PM)bebonzy09 Wrote: [\[CITE\]](#) Pretty pathetic how there's not one good piece of advice on this thread. OP asked for recommendations or advice on what to do... not a pity party or fucking anti virus tech support. I think his main concern is his crypto loss right now?

OP, start tracking the wallets where the funds were sent to. Document all the theft addresses, your addresses, theft amount, et all. Go write an IC3 report (IC3 won't help get your funds back but its good for the record). After this, make a police report in your jurisdiction, give them all of the above and whatever they ask you for.

Second thing is see if the funds are at a CEX. IF THEY ARE immediately contact the CEX and get them to freeze funds, give them ANYTHING they ask for. Most likely police report # and other documentation. You have to pray that its at a CEX and not already mixed or swapped into other crypto.

Third option after that if its not successful... DM @ZachXBT on Twitter or any other crypto investigators. Get it out to as many of them as possible. These guys are smart and can find links or slip ups even if it was already swapped or at a DEX.

Hopefully you've done at least one of those things so far. Wish I could've seen this thread a bit earlier.

I mean we all thought this. But is he willing to go through all this effort just for... nothing. Nothing will come of it because it's not a notoriety amount or public enough.

Look at recent wallet exploits and "bug bounty rewards".. even those aren't likely to return.

StuffSneak - September 29, 2026, 11:44 pm

Why did you have this much crypto stored in a hot wallet? I would suggest you to stop using desktop wallets. If you feel like using hot wallet, use it on your phone with limited funds only. Never on a general purpose desktop.

Personally I use tangem even on my phone & a couple of hardware wallets for cold stuff.

Will this setup stop anyone from getting rekt? Not 100% but it damn well protects much more than using a hot wallet.

morpheu - September 30, 2026, 8:41 am

Oh man thanks for sharing, must've been scary to find out.

Tightarse - September 30, 2026, 6:01 pm

(Sep 29, 2026 11:44 PM)StuffSneak Wrote: [\[CITE\]](#) Why did you have this much crypto stored in a hot wallet? I would suggest you to stop using desktop wallets. If you feel like using hot wallet, use it on your phone with limited funds only. Never on a general purpose desktop.

Personally I use tangem even on my phone & a couple of hardware wallets for cold stuff.

Will this setup stop anyone from getting rekt? Not 100% but it damn well protects much more than using a hot wallet.

I just got a ledger.

Tbh I got it a few years ago when the value was lower and felt my Mac was safe as I didn't use it for anything.

Then I decided to try some coding...

Mozart - October 5, 2026, 4:00 pm

I'd want to learn about cold storage if i were you.

ICTKUN - October 6, 2026, 11:28 am

Sorry that's a serious loss. Treat the entire wallet as compromised, including the remaining Litecoin. Opening the same wallet on Windows doesn't make its keys safe

Secure whatever remains. On a separate, trusted device, create a new wallet with a brand-new recovery phrase, then transfer the remaining funds there

Disconnect the Mac from the internet. Don't restore the flagged app or bypass the malware warning. Photograph the exact warning. It's a useful clue, but it doesn't establish how the theft happened. Don't assume the Windows PC is clean either.

Contact official Exodus support and report the theft to your local police/cybercrime unit. Confirmed transfers generally cannot be reversed. If funds reach an identifiable exchange, investigators may be able to request a freeze, but recovery isn't guaranteed