

Forum:[Hack Forums](#)

Thread: [MassJacker Clipper Malware Targeting Users Who Install Pirated Software](#)

JoseMar - March 18, 2025, 7:15 am

MassJacker Clipper Malware Targeting Users Who Install Pirated Software

A recently found cryptojacking malware named “MassJacker” is focusing on clients who download pilfered programs, supplanting cryptocurrency wallet addresses to divert stores to attackers.

The malware acts as a clipboard robber, checking when clients duplicate crypto wallet addresses and noiselessly supplanting them with addresses controlled by the risk actors.

The disease chain starts at locales like pesktop[.]com, which promotes pilfered programs but really disperses malware.

When clients download these apparently authentic programs, the malware executes a command script taken after by a PowerShell script that downloads numerous extra executables.

CYBERARK Security analysts recognized that MassJacker utilizes advanced anti-analysis strategies to avoid discovery, counting JIT snaring, metadata token mapping, and a custom virtual machine usage to jumble its code.

The malware’s structure recommends associations to a prior risk called MassLogger, in spite of the fact that its usefulness is centered particularly on cryptocurrency theft.

“MassJacker works by supplanting the addresses of crypto wallets replicated by the client, with the ones having a place for the aggressor in the clipboard. By doing so, the aggressor endeavors to trap the casualty into exchanging cash to the attacker’s address instead of the planning target,” clarifies the report specifying the threat.

The malware employs AES-encrypted records of attacker-controlled wallets, downloaded as recovery.dat and recovery.sol.dat files.

Infection Chain

When analyzing the disease preparation, analysts found that MassJacker utilizes different packers and prepares infusion to cover up the noxious payload in an apparently authentic prepare called InstalUtil.exe.

The Gigantic Scale of the Robbery Operation

In a dazzling disclosure, analysts found that the dangerous on-screen characters behind MassJacker have sent an operation utilizing over 778,531 one-of-a-kind cryptocurrency wallet addresses.

The examination revealed one especially dynamic Solana wallet with the address “CJpe4dUcV5Knc2XZKTVsTNHm2MpmJGJNWCJdkfbNdYF5” that contained roughly \$87,000 worth of Solana tokens at the time of discovery.

Historical investigation appeared that this single wallet had already held over 2075 SOL, which was worth more than \$300,000.

The wallet's broad exchange history, counting NFT exchanges, proposes it may be included in numerous criminal operations past fair crypto jacking.

One casualty tweeted that almost all reserves were being stolen and exchanged in this particular wallet, demonstrating the broad effect of this operation.

The broad number of exchanges makes it improbable that all reserves came exclusively from clipboard seizing, indicating extra noxious exercises by the same risk-performing artists.

Don't forget to check your address 3 times before to send!?

Additional sources to explore: You can also search directly on Google for more information:

<https://cointelegraph.com/news/new-massjacker-malware-targets-piracy-users-steals-crypto>

<https://www.cyberark.com/resources/threat-research-blog/captain-massjacker-sparrow-uncovering-the-malwares-buried-treasure>

<https://www.binance.com/en/square/post/03-14-2025-new-cryptojacking-malware-massjacker-targets-cryptocurrency-transactions-21553263933889>