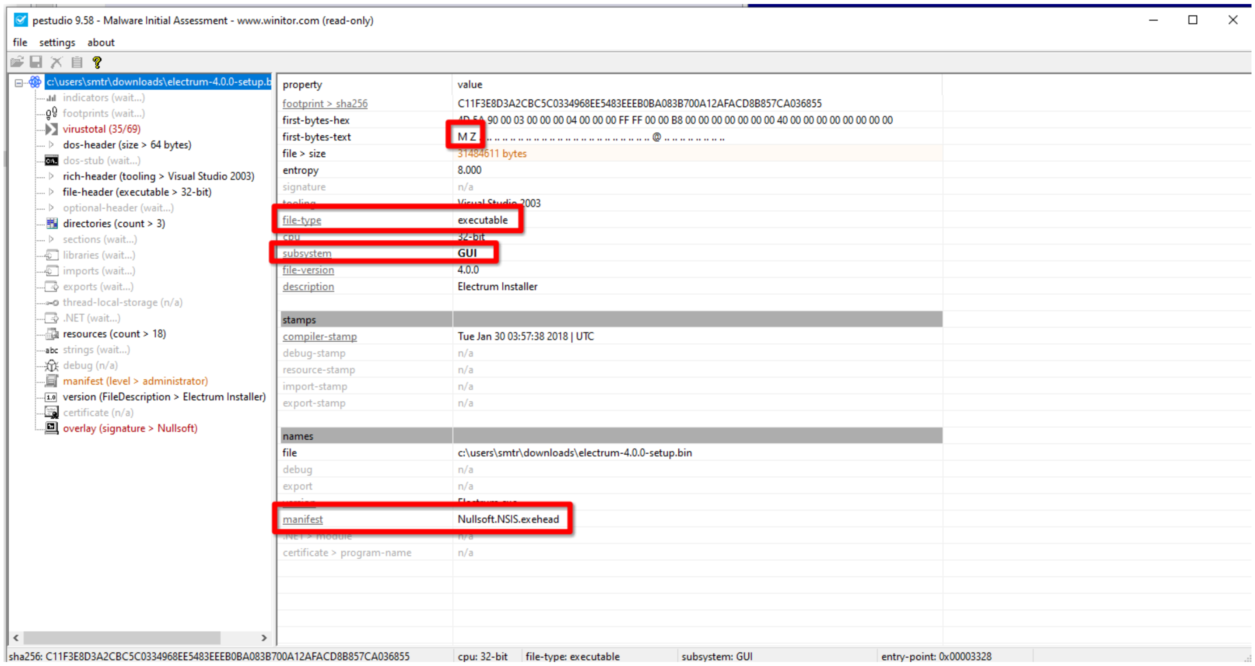
Electrum-4.0.0-setup.exe

Static Analysis

- starting with identifying the file and getting its fingerprint



pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)
file settings about

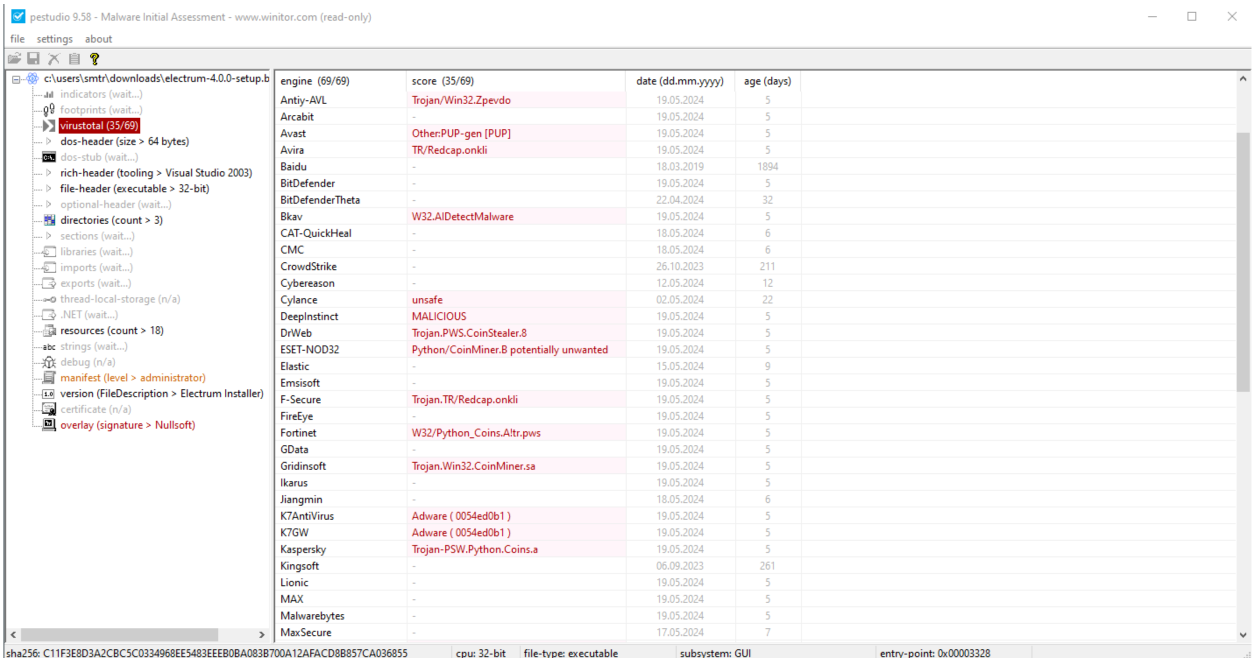
```
c:\users\smtr\downloads\electrum-4.0.0-setup.b
  indicators (wait...)
  footprints (wait...)
  virustotal (35/69)
  dos-header (size > 64 bytes)
  dos-stub (wait...)
  rich-header (tooling > Visual Studio 2003)
  file-header (executable > 32-bit)
  optional-header (wait...)
  directories (count > 3)
  sections (wait...)
  libraries (wait...)
  imports (wait...)
  exports (wait...)
  thread-local-storage (n/a)
  .NET (wait...)
  resources (count > 18)
  strings (wait...)
  debug (n/a)
  manifest (level > administrator)
  version (FileDescription > Electrum Installer)
  certificate (n/a)
  overlay (signature > Nullsoft)
```

property	value
footprint > sha256	C11F3E8D3A2CBC5C0334968EE5483EEEB0BA083B700A12AFACD8B857CA036855
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z . .. . @ .. ..
file > size	31484611 bytes
entropy	8.000
signature	n/a
tooling	Visual Studio 2003
file-type	executable
cpu	32-bit
subsystem	GUI
file-version	4.0.0
description	Electrum Installer
stamps	
compiler-stamp	Tue Jan 30 03:57:38 2018 | UTC
debug-stamp	n/a
resource-stamp	n/a
import-stamp	n/a
export-stamp	n/a
names	
file	c:\users\smtr\downloads\electrum-4.0.0-setup.bin
debug	n/a
export	n/a
version	Electrum.exe
manifest	Nullsoft.NSIS.exehead
.NET > module	n/a
certificate > program-name	n/a

```
sha256: C11F3E8D3A2CBC5C0334968EE5483EEEB0BA083B700A12AFACD8B857CA036855   cpu: 32-bit   file-type: executable   subsystem: GUI   entry-point: 0x00003328
```

the file is found to be a PE32 with a NSIS installer and isn't signed by ant certificate.

- using PE-Studio we have a fingerprint we can use on virus total to check previous reports

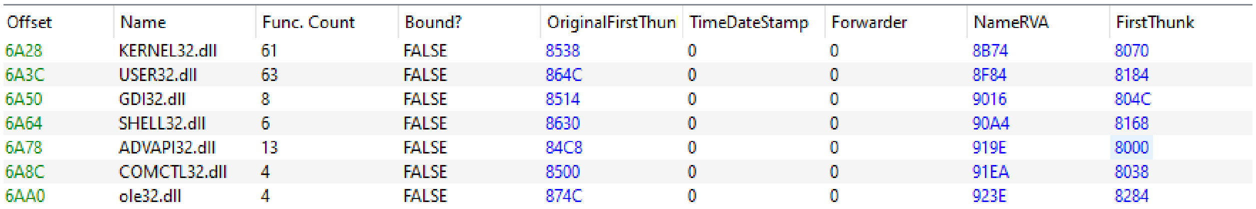

pestudio 9.58 - Malware Initial Assessment - www.winitor.com (read-only)
file
settings
about

c:\users\smtr\downloads\electrum-4.0.0-setup.b
- indicators (wait...)
- footprints (wait...)
- virustotal (35/69)
- dos-header (size > 64 bytes)
- dos-stub (wait...)
- rich-header (tooling > Visual Studio 2003)
- file-header (executable > 32-bit)
- optional-header (wait...)
- directories (count > 3)
- sections (wait...)
- libraries (wait...)
- imports (wait...)
- exports (wait...)
- thread-local-storage (n/a)
- .NET (wait...)
- resources (count > 18)
- strings (wait...)
- debug (n/a)
- manifest (level > administrator)
- version (FileDescription > Electrum Installer)
- certificate (n/a)
- overlay (signature > Nullsoft)

engine (69/69)	score (35/69)	date (dd.mm.yyyy)	age (days)
Antiy-AVL	Trojan/Win32.Zpevdo	19.05.2024	5
Arcabit	-	19.05.2024	5
Avast	Other:PUP-gen [PUP]	19.05.2024	5
Avira	TR/Redcap.onkli	19.05.2024	5
Baidu	-	18.03.2019	1894
BitDefender	-	19.05.2024	5
BitDefenderTheta	-	22.04.2024	32
Bkav	W32.AIDetectMalware	19.05.2024	5
CAT-QuickHeal	-	18.05.2024	6
CMC	-	18.05.2024	6
CrowdStrike	-	26.10.2023	211
Cybereason	-	12.05.2024	12
Cylance	unsafe	02.05.2024	22
DeepInstinct	MALICIOUS	19.05.2024	5
DrWeb	Trojan.PWS.CoinStealer.8	19.05.2024	5
ESET-NOD32	Python/CoinMiner.B potentially unwanted	19.05.2024	5
Elastic	-	15.05.2024	9
Emsisoft	-	19.05.2024	5
F-Secure	Trojan.TR/Redcap.onkli	19.05.2024	5
FireEye	-	19.05.2024	5
Fortinet	W32/Python_Coins.A!tr.pws	19.05.2024	5
GData	-	19.05.2024	5
Gridinsoft	Trojan.Win32.CoinMiner.sa	19.05.2024	5
Ikarus	-	19.05.2024	5
Jiangmin	-	18.05.2024	6
K7AntiVirus	Adware (0054ed0b1)	19.05.2024	5
K7GW	Adware (0054ed0b1)	19.05.2024	5
Kaspersky	Trojan-PSW.Python.Coins.a	19.05.2024	5
Kingsoft	-	06.09.2023	261
Lionic	-	19.05.2024	5
MAX	-	19.05.2024	5
Malwarebytes	-	19.05.2024	5
MaxSecure	-	17.05.2024	7

sha256: C11F3E8D3A2CBC5C0334968EE5483EEEB0BA083B700A12AFACD8B857CA036855 | cpu: 32-bit | file-type: executable | subsystem: GUI | entry-point: 0x00003328

- checking the imports using PE-Bear



Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Forwarder	NameRVA	FirstThunk
6A28	KERNEL32.dll	61	FALSE	8538	0	0	8B74	8070
6A3C	USER32.dll	63	FALSE	864C	0	0	8F84	8184
6A50	GDI32.dll	8	FALSE	8514	0	0	9016	804C
6A64	SHELL32.dll	6	FALSE	8630	0	0	90A4	8168
6A78	ADVAPI32.dll	13	FALSE	84C8	0	0	919E	8000
6A8C	COMCTL32.dll	4	FALSE	8500	0	0	91EA	8038
6AA0	ole32.dll	4	FALSE	874C	0	0	923E	8284

by checking the imported Dlls and the exact used functions we have an idea about the functionality

File Operations

- **Create, Delete, Find, Move, and Copy Files:**
  - `DeleteFileA`
  - `FindFirstFileA`
  - `FindNextFileA`

  - `FindClose`
  - `CreateFileA`
  - `MoveFileA`
  - `MoveFileExA`
  - `CopyFileA`
  - `GetFileSize`
  - `SetFilePointer`
  - `GetFileAttributesA`
  - `SetFileAttributesA`
  - `GetShortPathNameA`
  - `GetFullPathNameA`
  - `GetTempFileNameA`
  - `ReadFile`
  - `WriteFile`
  - `SetFileTime`
  - `CompareFileTime`
  - `GetDiskFreeSpaceA`
  - `GetWindowsDirectoryA`
  - `GetTempPathA`

Registry Operations

- **Create, Delete, Query, and Set Registry Values**:
  - `RegEnumValueA`
  - `RegEnumKeyA`
  - `RegQueryValueExA`

- `RegSetValueExA`
- `RegCloseKey`
- `RegDeleteValueA`
- `RegDeleteKeyA`
- `RegOpenKeyExA`
- `RegCreateKeyExA`
- `RegDeleteKeyExA`

Process and Thread Management

- **Create and Manage Processes and Threads:**
  - `CreateProcessA`
  - `ExitProcess`
  - `CreateThread`
  - `GetCurrentProcess`
  - `GetExitCodeProcess`
  - `WaitForSingleObject`
  - `SetEnvironmentVariableA`
  - `GetEnvironmentVariableA`
  - `Sleep`
  - `GetTickCount`
  - `GetLastError`
  - `SetErrorMode`

Library and Module Management

- **Load, Free, and Get Modules:**

    - `LoadLibraryExA`
    - `FreeLibrary`
    - `GetModuleHandleA`
    - `GetModuleFileNameA`
    - `GetProcAddress`

String and Character Operations

- **Compare, Copy, and Manipulate Strings**:
    - `lstrcmpA`
    - `lstrcmpiA`
    - `lstrlenA`
    - `lstrcpynA`
    - `lstrcpyA`
    - `lstrcatA`
    - `MultiByteToWideChar`

Window and UI Management

- **Create and Manage Windows, Dialogs, and Messages**:
    - `CreateWindowExA`
    - `CreateDialogParamA`
    - `EndDialog`
    - `DestroyWindow`
    - `ExitWindowsEx`
    - `SendMessageA`
    - `SendMessageTimeoutA`

- `PostQuitMessage`
- `ShowWindow`
- `SetWindowTextA`
- `SetForegroundWindow`
- `InvalidateRect`
- `EnableWindow`
- `SetWindowPos`
- `SetWindowLongA`
- `GetWindowLongA`
- `FindWindowExA`
- `IsWindow`
- `IsWindowVisible`
- `IsWindowEnabled`
- `SetClassLongA`
- `GetClassInfoA`
- `DefWindowProcA`
- `GetClientRect`
- `GetWindowRect`
- `TrackPopupMenu`
- `AppendMenuA`
- `CreatePopupMenu`
- `GetSystemMetrics`
- `GetMessagePos`
- `CheckDlgButton`
- `EnableMenuItem`
- `GetSystemMenu`

  - `SystemParametersInfoA`
  - `RegisterClassA`
  - `ScreenToClient`
  - `SetDlgItemTextA`
  - `GetDlgItemTextA`
  - `GetDlgItem`
  - `DispatchMessageA`
  - `PeekMessageA`

Clipboard Operations

- **Open, Close, Set, and Empty Clipboard**:
  - `OpenClipboard`
  - `CloseClipboard`
  - `SetClipboardData`
  - `EmptyClipboard`

Graphics and Drawing

- **Draw Text, Fill Rectangles, Select Objects, and Set Colors**:
  - `DrawTextA`
  - `FillRect`
  - `BeginPaint`
  - `EndPaint`
  - `GetDC`
  - `ReleaseDC`
  - `SelectObject`
  - `SetTextColor`
  - `SetBkMode`

    - `SetBkColor`

Security and Privileges

- **Adjust and Lookup Privileges, Set File Security**:
    - `AdjustTokenPrivileges`
    - `LookupPrivilegeValueA`
    - `OpenProcessToken`
    - `SetFileSecurityA`

Miscellaneous Operations

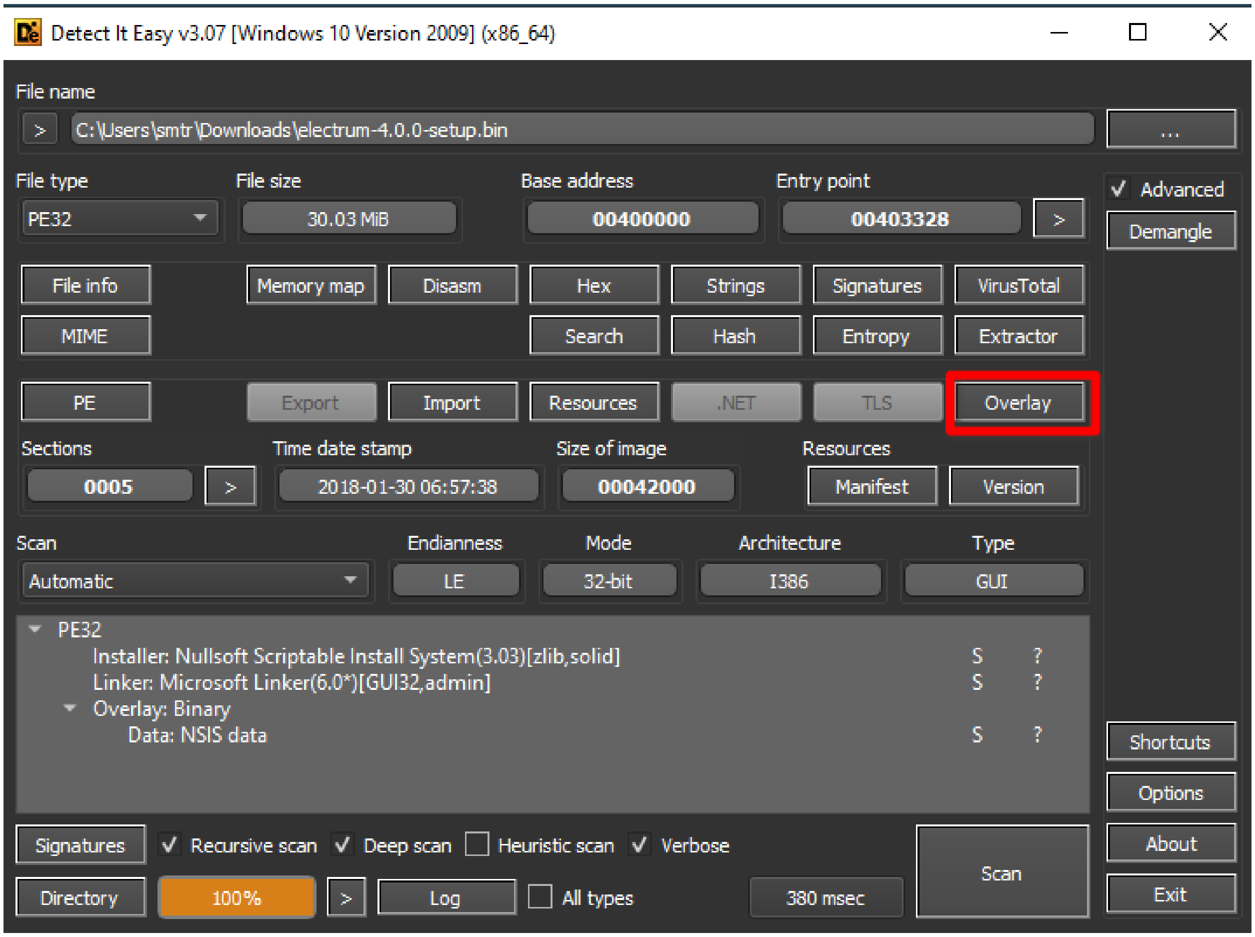
- **File and System Paths, Error Handling, Sleep, etc.**:
    - `GetPrivateProfileStringA`
    - `WritePrivateProfileStringA`
    - `ExpandEnvironmentStringsA`
    - `CloseHandle`
    - `GlobalAlloc`
    - `GlobalFree`
    - `GlobalLock`
    - `GlobalUnlock`
    - `KERNEL32.dll`
    - `USER32.dll`
    - `GDI32.dll`
    - `SHELL32.dll`
    - `ADVAPI32.dll`
    - `COMCTL32.dll`

  - `CoCreateInstance`
  - `OleInitialize`
  - `OleUninitialize`
  - `CoTaskMemFree`
  - `ImageList_Create`
  - `ImageList_Destroy`
  - `ImageList_AddMasked`
  - `SHFileOperationA`
  - `SHGetFileInfoA`
  - `SHBrowseForFolderA`
  - `SHGetPathFromIDListA`
  - `SHGetSpecialFolderLocation`
  - `MessageBoxIndirectA`
  - `CharNextA`
  - `CharPrevA`
  - `wsprintfA`
  - `LoadImageA`
  - `LoadCursorA`
  - `LoadBitmapA`
  - `GetSysColor`
  - `GetSystemDirectoryA`
  - `GetTempPathA`

all of the previous functions do exist in the legit electrum installer, which does give us much of an idea about the malicious functionality present in our sample.

- check the overlay

using DIE we dumped the overlay and started checking it



Detect It Easy v3.07 [Windows 10 Version 2009] (x86_64)

File name: C:\Users\smtr\Downloads\electrum-4.0.0-setup.bin

File type	File size	Base address	Entry point
PE32	30.03 MiB	00400000	00403328

Sections	Time date stamp	Size of image
0005	2018-01-30 06:57:38	00042000

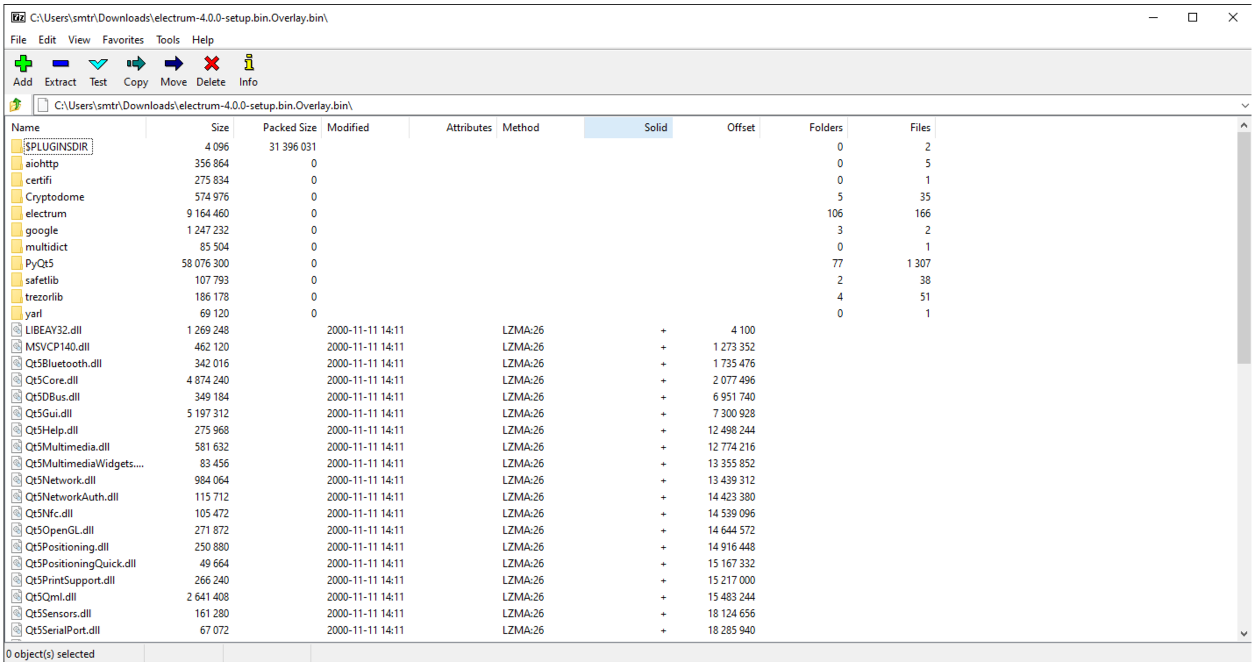
Scan	Endianness	Mode	Architecture	Type
Automatic	LE	32-bit	I386	GUI

```
PE32
    Installer: Nullsoft Scriptable Install System(3.03)[zlib,solid]    S  ?
    Linker: Microsoft Linker(6.0*)[GUI32,admin]                        S  ?
  Overlay: Binary
      Data: NSIS data                                                  S  ?
```

☑ Advanced ☑ Recursive scan ☑ Deep scan ☐ Heuristic scan ☑ Verbose ☐ All types

100% 380 msec

the overlay is a NSIS installer, so we can use 7zip to open the archive and check what it has:

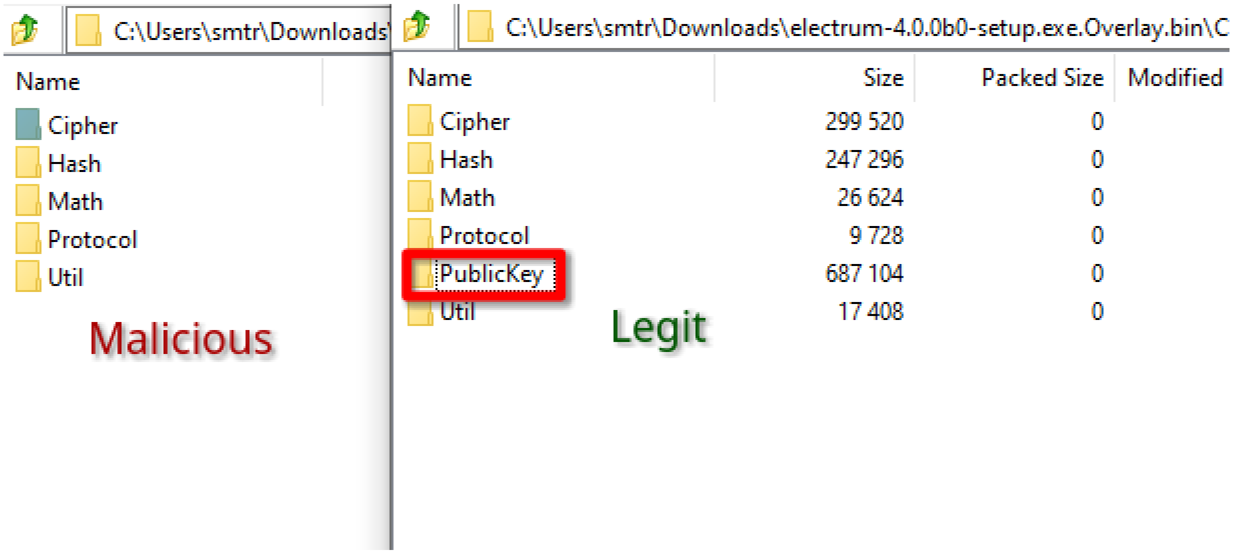

C:\Users\smtr\Downloads\electrum-4.0.0-setup.bin.Overlay.bin\
File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info
C:\Users\smtr\Downloads\electrum-4.0.0-setup.bin.Overlay.bin\

Name	Size	Packed Size	Modified	Attributes	Method	Solid	Offset	Folders	Files
$PLUGINSDIR	4 096	31 396 031						0	2
aiohttp	356 864	0						0	5
certifi	275 834	0						0	1
Cryptodome	574 976	0						5	35
electrum	9 164 460	0						106	166
google	1 247 232	0						3	2
multidict	85 504	0						0	1
PyQt5	58 076 300	0						77	1 307
safetlib	107 793	0						2	38
trezorlib	186 178	0						4	51
yarl	69 120	0						0	1
LIBEAY32.dll	1 269 248		2000-11-11 14:11		LZMA:26	+	4 100		
MSVCP140.dll	462 120		2000-11-11 14:11		LZMA:26	+	1 273 352		
Qt5Bluetooth.dll	342 016		2000-11-11 14:11		LZMA:26	+	1 735 476		
Qt5Core.dll	4 874 240		2000-11-11 14:11		LZMA:26	+	2 077 496		
Qt5DBus.dll	349 184		2000-11-11 14:11		LZMA:26	+	6 951 740		
Qt5Gui.dll	5 197 312		2000-11-11 14:11		LZMA:26	+	7 300 928		
Qt5Help.dll	275 968		2000-11-11 14:11		LZMA:26	+	12 498 244		
Qt5Multimedia.dll	581 632		2000-11-11 14:11		LZMA:26	+	12 774 216		
Qt5MultimediaWidgets....	83 456		2000-11-11 14:11		LZMA:26	+	13 355 852		
Qt5Network.dll	984 064		2000-11-11 14:11		LZMA:26	+	13 439 312		
Qt5NetworkAuth.dll	115 712		2000-11-11 14:11		LZMA:26	+	14 423 380		
Qt5Nfc.dll	105 472		2000-11-11 14:11		LZMA:26	+	14 539 096		
Qt5OpenGL.dll	271 872		2000-11-11 14:11		LZMA:26	+	14 644 572		
Qt5Positioning.dll	250 880		2000-11-11 14:11		LZMA:26	+	14 916 448		
Qt5PositioningQuick.dll	49 664		2000-11-11 14:11		LZMA:26	+	15 167 332		
Qt5PrintSupport.dll	266 240		2000-11-11 14:11		LZMA:26	+	15 217 000		
Qt5Qml.dll	2 641 408		2000-11-11 14:11		LZMA:26	+	15 483 244		
Qt5Sensors.dll	161 280		2000-11-11 14:11		LZMA:26	+	18 124 656		
Qt5SerialPort.dll	67 072		2000-11-11 14:11		LZMA:26	+	18 285 940		

0 object(s) selected

by walking through the archive we notice the absence of directories addition of some new files and DLLs . (in comparison with the legit installer)

1. Cryptodome\publicKey



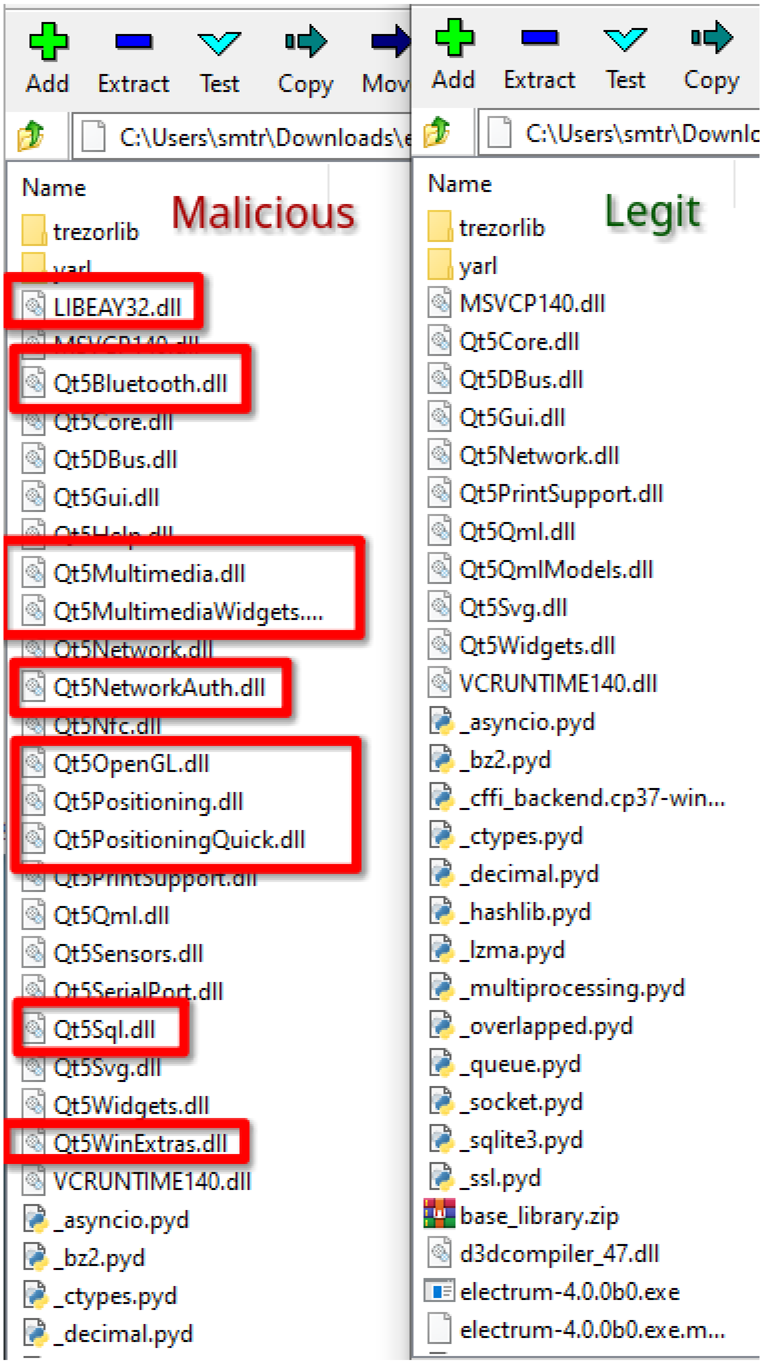
C:\Users\smtr\Downloads\

Name
Cipher
Hash
Math
Protocol
Util

C:\Users\smtr\Downloads\electrum-4.0.0b0-setup.exe.Overlay.bin\C

Name	Size	Packed Size	Modified
Cipher	299 520	0	
Hash	247 296	0	
Math	26 624	0	
Protocol	9 728	0	
PublicKey	687 104	0	
Util	17 408	0	

2. Network/Graphics/SQL Dlls



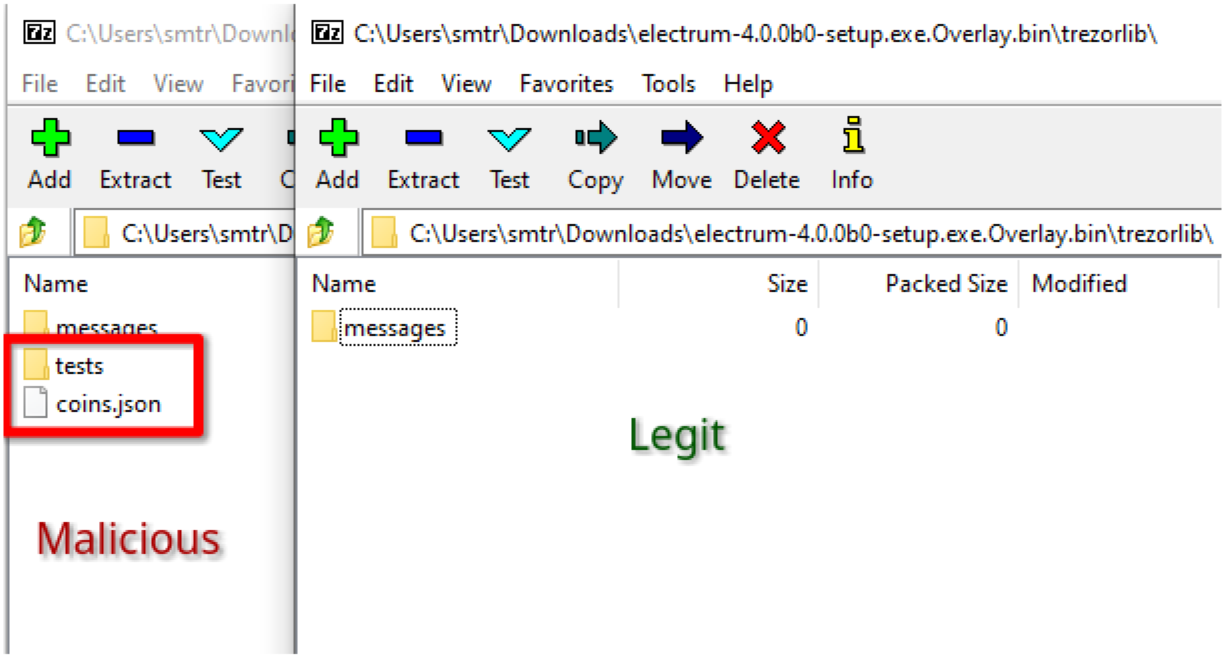
Malicious

Name
trezorlib
yarl
LIBEAY32.dll
MSVCP140.dll
Qt5Bluetooth.dll
Qt5Core.dll
Qt5DBus.dll
Qt5Gui.dll
Qt5Help.dll
Qt5Multimedia.dll
Qt5MultimediaWidgets....
Qt5Network.dll
Qt5NetworkAuth.dll
Qt5Nfc.dll
Qt5OpenGL.dll
Qt5Positioning.dll
Qt5PositioningQuick.dll
Qt5PrintSupport.dll
Qt5Qml.dll
Qt5Sensors.dll
Qt5SerialPort.dll
Qt5Sql.dll
Qt5Svg.dll
Qt5Widgets.dll
Qt5WinExtras.dll
VCRUNTIME140.dll
_asyncio.pyd
_bz2.pyd
_ctypes.pyd
_decimal.pyd

Legit

Name
trezorlib
yarl
MSVCP140.dll
Qt5Core.dll
Qt5DBus.dll
Qt5Gui.dll
Qt5Network.dll
Qt5PrintSupport.dll
Qt5Qml.dll
Qt5QmlModels.dll
Qt5Svg.dll
Qt5Widgets.dll
VCRUNTIME140.dll
_asyncio.pyd
_bz2.pyd
_cffi_backend.cp37-win...
_ctypes.pyd
_decimal.pyd
_hashlib.pyd
_lzma.pyd
_multiprocessing.pyd
_overlapped.pyd
_queue.pyd
_socket.pyd
_sqlite3.pyd
_ssl.pyd
base_library.zip
d3dcompiler_47.dll
electrum-4.0.0b0.exe
electrum-4.0.0b0.exe.m...

3. Extra Coin Wallet Addresses



C:\Users\smtr\Downl

C:\Users\smtr\D

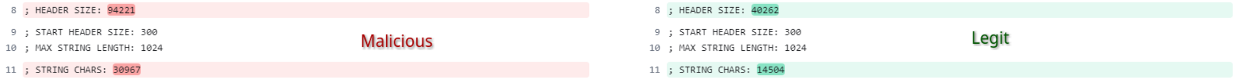
Name
messages
tests
coins.json

C:\Users\smtr\Downloads\electrum-4.0.0b0-setup.exe.Overlay.bin\trezorlib\

Name	Size	Packed Size	Modified
messages	0	0	

4. [NSIS].nsi scripts

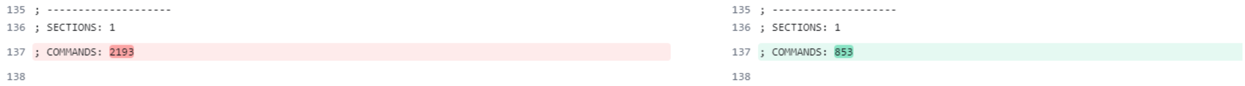
   a. size



```
; HEADER SIZE: 94221
; START HEADER SIZE: 300
; MAX STRING LENGTH: 1024
; STRING CHARS: 30967
```

```
; HEADER SIZE: 40262
; START HEADER SIZE: 300
; MAX STRING LENGTH: 1024
; STRING CHARS: 14504
```

   b. number of commands



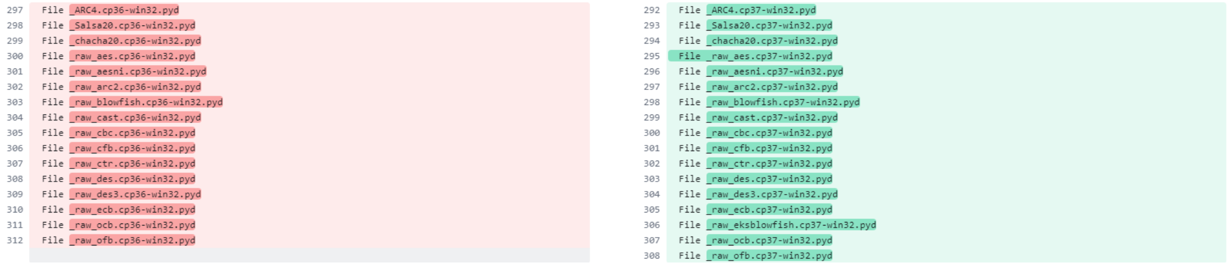
```
; --------------------
; SECTIONS: 1
; COMMANDS: 2193

```

```
; --------------------
; SECTIONS: 1
; COMMANDS: 853

```

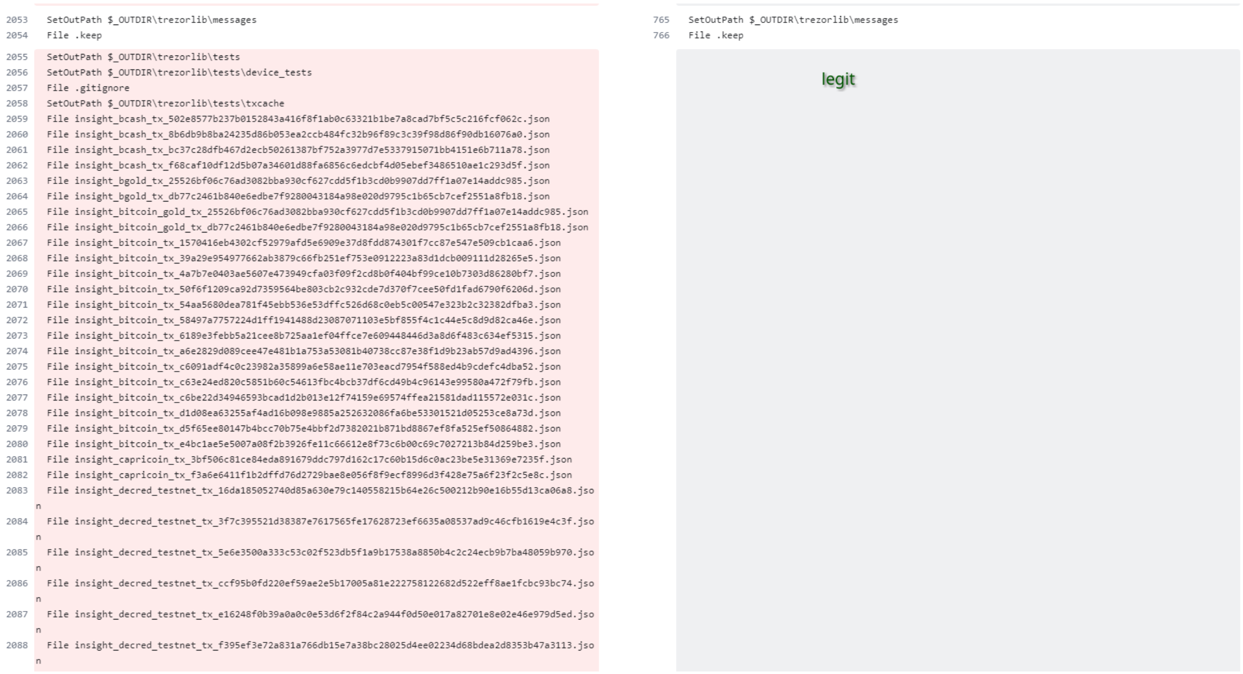
   c. pyd versions used



```
  File _ARC4.cp36-win32.pyd
  File _Salsa20.cp36-win32.pyd
  File _chacha20.cp36-win32.pyd
  File _raw_aes.cp36-win32.pyd
  File _raw_aesni.cp36-win32.pyd
  File _raw_arc2.cp36-win32.pyd
  File _raw_blowfish.cp36-win32.pyd
  File _raw_cast.cp36-win32.pyd
  File _raw_cbc.cp36-win32.pyd
  File _raw_cfb.cp36-win32.pyd
  File _raw_ctr.cp36-win32.pyd
  File _raw_des.cp36-win32.pyd
  File _raw_des3.cp36-win32.pyd
  File _raw_ecb.cp36-win32.pyd
  File _raw_ocb.cp36-win32.pyd
  File _raw_ofb.cp36-win32.pyd
```

```
  File _ARC4.cp37-win32.pyd
  File _Salsa20.cp37-win32.pyd
  File _chacha20.cp37-win32.pyd
  File _raw_aes.cp37-win32.pyd
  File _raw_aesni.cp37-win32.pyd
  File _raw_arc2.cp37-win32.pyd
  File _raw_blowfish.cp37-win32.pyd
  File _raw_cast.cp37-win32.pyd
  File _raw_cbc.cp37-win32.pyd
  File _raw_cfb.cp37-win32.pyd
  File _raw_ctr.cp37-win32.pyd
  File _raw_des.cp37-win32.pyd
  File _raw_des3.cp37-win32.pyd
  File _raw_ecb.cp37-win32.pyd
  File _raw_eksblowfish.cp37-win32.pyd
  File _raw_ocb.cp37-win32.pyd
  File _raw_ofb.cp37-win32.pyd
```

d. Bitcoin wallet addresses



```
SetOutPath $_OUTDIR\trezorlib\messages
File .keep
SetOutPath $_OUTDIR\trezorlib\tests
SetOutPath $_OUTDIR\trezorlib\tests\device_tests
File .gitignore
SetOutPath $_OUTDIR\trezorlib\tests\txcache
File insight_bcash_tx_502e8577b237b0152843a416f8f1ab0c63321b1be7a8cad7bf5c5c216fcf062c.json
File insight_bcash_tx_8b6db9b8ba24235d86b053ea2ccb484fc32b96f89c3c39f98d86f90db16076a0.json
File insight_bcash_tx_bc37c28dfb467d2ecb50261387bf752a3977d7e5337915071bb4151e6b711a78.json
File insight_bcash_tx_f68caf10df12d5b07a34601d88fa6856c6edcbf4d05ebef3486510ae1c293d5f.json
File insight_bgold_tx_25526bf06c76ad3082bba930cf627cdd5f1b3cd0b9907dd7ff1a07e14addc985.json
File insight_bgold_tx_db77c2461b840e6edbe7f9280043184a98e020d9795c1b65cb7cef2551a8fb18.json
File insight_bitcoin_gold_tx_25526bf06c76ad3082bba930cf627cdd5f1b3cd0b9907dd7ff1a07e14addc985.json
File insight_bitcoin_gold_tx_db77c2461b840e6edbe7f9280043184a98e020d9795c1b65cb7cef2551a8fb18.json
File insight_bitcoin_tx_1570416eb4302cf52979afd5e6909e37d8fdd874301f7cc87e547e509cb1caa6.json
File insight_bitcoin_tx_39a29e954977662ab3879c66fb251ef753e0912223a83d1dcb009111d28265e5.json
File insight_bitcoin_tx_4a7b7e0403ae5607e473949cfa03f09f2cd8b0f404bf99ce10b7303d86280bf7.json
File insight_bitcoin_tx_50f6f1209ca92d7359564be803cb2c932cde7d370f7cee50fd1fad6790f6206d.json
File insight_bitcoin_tx_54aa5680dea781f45ebb536e53dffc526d68c0eb5c00547e323b2c32382dfba3.json
File insight_bitcoin_tx_58497a7757224d1ff1941488d23087071103e5bf855f4c1c44e5c8d9d82ca46e.json
File insight_bitcoin_tx_6189e3febb5a21cee8b725aa1ef04ffce7e609448446d3a8d6f483c634ef5315.json
File insight_bitcoin_tx_a6e2829d089cee47e481b1a753a53081b40738cc87e38f1d9b23ab57d9ad4396.json
File insight_bitcoin_tx_c6091adf4c0c23982a35899a6e58ae11e703eacd7954f588ed4b9cdefc4dba52.json
File insight_bitcoin_tx_c63e24ed820c5851b60c54613fbc4bcb37df6cd49b4c96143e99580a472f79fb.json
File insight_bitcoin_tx_c6be22d34946593bcad1d2b013e12f74159e69574ffea21581dad115572e031c.json
File insight_bitcoin_tx_d1d08ea63255af4ad16b098e9885a252632086fa6be53301521d05253ce8a73d.json
File insight_bitcoin_tx_d5f65ee80147b4bcc70b75e4bbf2d7382021b871bd8867ef8fa525ef50864882.json
File insight_bitcoin_tx_e4bc1ae5e5007a08f2b3926fe11c66612e8f73c6b00c69c7027213b84d259be3.json
File insight_capricoin_tx_3bf506c81ce84eda891679ddc797d162c17c60b15d6c0ac23be5e31369e7235f.json
File insight_capricoin_tx_f3a6e6411f1b2dffd76d2729bae8e056f8f9ecf8996d3f428e75a6f23f2c5e8c.json
File insight_decred_testnet_tx_16da185052740d85a630e79c140558215b64e26c500212b90e16b55d13ca06a8.json
File insight_decred_testnet_tx_3f7c395521d38387e7617565fe17628723ef6635a08537ad9c46cfb1619e4c3f.json
File insight_decred_testnet_tx_5e6e3500a333c53c02f523db5f1a9b17538a8850b4c2c24ecb9b7ba48059b970.json
File insight_decred_testnet_tx_ccf95b0fd220ef59ae2e5b17005a81e222758122682d522eff8ae1fcbc93bc74.json
File insight_decred_testnet_tx_e16248f0b39a0a0c0e53d6f2f84c2a944f0d50e017a82701e8e02e46e979d5ed.json
File insight_decred_testnet_tx_f395ef3e72a831a766db15e7a38bc28025d4ee02234d68bdea2d8353b47a3113.json
```

```
SetOutPath $_OUTDIR\trezorlib\messages
File .keep
```

legit

- strings

```
00006914    24  A   .DEFAULT\Control Panel\International
0000693c    24  A   Control Panel\Desktop\ResourceLocale
000069a0    29  A   Software\Microsoft\Windows\CurrentVersion
000069cc    29  A   \Microsoft\Internet Explorer\Quick Launch

00007a20    19  A   verifying installer: %d%%
00007a3c    14  A   unpacking data: %d%%
00007a54    08  A   ... %d%%
00007a60    3b  A   Installer integrity check has failed. Common causes include
00007a9c    32  A   incomplete download and damaged media. Contact the
00007acf        28  A   installer's author to obtain a new copy.
00007af9        14  A   More information at:
00007b0e    1d  A   http://nsis.sf.net/NSIS_Error
00007b30    42  A   Error writing temporary file. Make sure your temp folder is valid.
00007b74    19  A   Error launching installer
```

```
00007bd4    05   A    \Temp
00007bec    0a   A    NSIS Error
00007c24    09   A    %u.%u%s%s
```

Advanced static

- opened IDA and didnt get much luck in identifying the malicious stub.

Dynamic Analysis:

File activity

the setup exe

- the installation files/DLLs

the executable itself

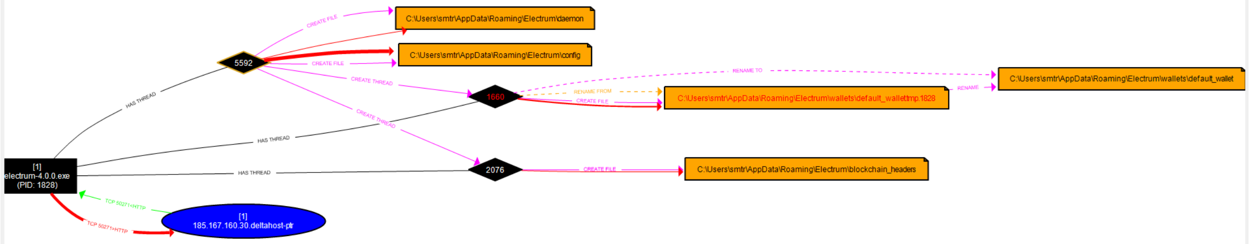
- the default wallet file

Registry activity

- as shown in the video and the key_findings report.

process activity

- ProcMon and procDot (activity of electrum.exe)


[1]
electrum-4.0.0.exe
(PID: 1828)
HAS THREAD
HAS THREAD
HAS THREAD
5592
1660
2076
CREATE FILE
CREATE FILE
CREATE THREAD
CREATE THREAD
C:\Users\smtr\AppData\Roaming\Electrum\daemon
C:\Users\smtr\AppData\Roaming\Electrum\config
RENAME TO
RENAME FROM
CREATE FILE
C:\Users\smtr\AppData\Roaming\Electrum\wallets\default_wallettmp.1828
RENAME
C:\Users\smtr\AppData\Roaming\Electrum\wallets\default_wallet
CREATE FILE
C:\Users\smtr\AppData\Roaming\Electrum\blockchain_headers
TCP 50271<HTTP
TCP 50271>HTTP
[1]
185.167.160.30.deltahost-ptr

network activity

1. HTTP requests
    a. 185.167.160.30/pdata.php

2. DNS queries
    a. apply wireshark filters

3. connections
    a. tcp and udp connections for different IPs