Malware Analysis Report

Executive overview

Users were prompted to upgrade for the newer version of Electrum wallet (4.0.0), which wasn’t an official release at the time, using one of the following URLs:

- https://my.electroneum.com/4.0.0/electrim-4.0.0.exe
- https://my.electroneum.com/4.0.0/electrim-4.0.0-setup.exe

Once run, the malware can steal seed phrases, private keys and request 2FA codes, then use these codes to transfer funds for external wallets.

Identification

Filename	electrum-4.0.0-setup.exe
File type	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
File Size	31484611 bytes (30.03 MB)
MD5	Afa8b4c6ca15a66d1a8b5399e45ebe06
SHA1	7EFBD3DAD2552E6BF4A447B5D54D9D1BBCD8FA0A
SHA256	C11F3E8D3A2CBC5C0334968EE5483EEEB0BA083B700A12AFACD8B857CA036855
SSDEEP	786432:m8uYa4paBoIHvAwU2SnH9xjk6Gr1/dHkHscxbQeztqiHRL:bavBTH4wKxw6 81lwVQ ep
Entropy	7.999881809582273
Tools	Visual Studio 2003

Static Analysis

Sections

Name	MD5	Virtual Address	Virtual Size	Raw Size	Entropy
.text	de10f6d8b01c12ec29a35514cd8d49da	0x001000	0x006077	0x6200	6.40397
.rdata	421f9404c16c75fa4bc7d37da19b3076	0x008000	0x001248	0x1400	5.04426
.data	9b72314b8d9ad5c72778b00cdf336e2	0x00A000	0x1A838	0x400	5.22445
data	D41d8cd98f00b204e9800998ecf8427e	0x025000	0x0F000	0x00	0
.rsrc	b371501e9fccd8c12c9ab45ff29d5849	0x034000	0x0DB58	0xDC00	6.07447

Resources

Title	Type	Entropy	Size
1	RT_MANIFEST	5.28813	1070
2	RT_ICON	3.20642	9640
3	RT_ICON	3.52336	4264
4	RT_ICON	2.80722	3752
5	RT_ICON	2.47831	2216
6	RT_ICON	2.66811	1640
7	RT_ICON	1.15935	1384
8	RT_ICON	4.17452	1128
9	RT_ICON	2.65167	744
10	RT_ICON	1.734	296
103	RT_GROUP_ICON	2.90294	146
105	RT_ICON	2.73893	514
106	RT_ICON	2.91148	248
107	RT_ICON	2.52183	160
111	RT_DIALOG	2.89887	238

Imports

- ADVAPI32.dll
- COMCTL32.dll
- GDI32.dll
- KERNEL32.dll
- SHELL32.dll
- USER32.dll
- Ole32.dll

Overlay

The overlay represents the bigger chunk of file

File type	NSIS data
entropy	7.999995231628418
offset	88576
size	31396035 (99.72% of the file)
MD5	5bb021ca20d0a96a61686edbcff4ac47

Interesting Strings

a full list can be found in the attachments, the list includes Function names that weren't obfuscated.

Offset	Size	Type	String
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.
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
00007b90	13	A	SeShutdownPrivilege
00007bd4	05	A	\Temp
00007bec	0a	A	NSIS Error
00007c24	09	A	%u.%u%s%s

Dynamic analysis

File activity

Here we will show additional files that were not present in the legitimate electrum-ssetup 4.0.0.exe. For the complete list, please refer to the Full_Files_Activity.txt attachment.

Dropped files

- C:\ProgramData\Microsoft\Windows\WER\Temp\WER27A9.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER27A9.tmp.txt
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER27AA.tmp
- C:\ProgramData\Microsoft\Windows\WER\Temp\WER27AA.tmp.txt
- C:\Windows\System32\spp\store\2.0\cache\cache.dat
- C:\Windows\System32\spp\store\2.0\data.dat.tmp
- C:\Users\<USER>\AppData\Local\Temp\nsq256.tmp\UserInfo.dll
- C:\Program Files (x86)\Electrum\Cryptodome\PublicKey_ec_ws.cp37-win32.pyd
- C:\Program Files (x86)\Electrum\Qt5Network.dll
- C:\Program Files (x86)\Electrum\Qt5Widgets.dll
- C:\Program Files (x86)\Electrum\electrum\checkpoints.json
- C:\Program Files (x86)\Electrum\electrum\checkpoints_testnet.json
- C:\Program Files (x86)\Electrum\electrum\lnwire\onion_wire.csv
- C:\Program Files (x86)\Electrum\electrum\lnwire\peer_wire.csv
- C:\Program Files (x86)\Electrum\electrum\plugins\README
- C:\Program Files (x86)\Electrum\electrum\plugins\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\audio_modem\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\audio_modem\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\bitbox02\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\bitbox02\bitbox02.py
- C:\Program Files (x86)\Electrum\electrum\plugins\bitbox02\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\coldcard\README.md
- C:\Program Files (x86)\Electrum\electrum\plugins\coldcard\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\coldcard\cmdline.py
- C:\Program Files (x86)\Electrum\electrum\plugins\coldcard\coldcard.py
- C:\Program Files (x86)\Electrum\electrum\plugins\coldcard\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\cosigner_pool\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\cosigner_pool\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\digitalbitbox\__init__.py

- C:\Program Files (x86)\Electrum\electrum\plugins\digitalbitbox\cmdline.py
- C:\Program Files (x86)\Electrum\electrum\plugins\digitalbitbox\digitalbitbox.py
- C:\Program Files (x86)\Electrum\electrum\plugins\digitalbitbox\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\email_requests\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\email_requests\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\hw_wallet\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\hw_wallet\cmdline.py
- C:\Program Files (x86)\Electrum\electrum\plugins\hw_wallet\plugin.py
- C:\Program Files (x86)\Electrum\electrum\plugins\hw_wallet\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\keepkey\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\keepkey\client.py
- C:\Program Files (x86)\Electrum\electrum\plugins\keepkey\clientbase.py
- C:\Program Files (x86)\Electrum\electrum\plugins\keepkey\cmdline.py
- C:\Program Files (x86)\Electrum\electrum\plugins\keepkey\keepkey.py
- C:\Program Files (x86)\Electrum\electrum\plugins\keepkey\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\labels\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\labels\cmdline.py
- C:\Program Files (x86)\Electrum\electrum\plugins\labels\kivy.py
- C:\Program Files (x86)\Electrum\electrum\plugins\labels\labels.py
- C:\Program Files (x86)\Electrum\electrum\plugins\labels\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\ledger\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\ledger\auth2fa.py
- C:\Program Files (x86)\Electrum\electrum\plugins\ledger\cmdline.py
- C:\Program Files (x86)\Electrum\electrum\plugins\ledger\ledger.py
- C:\Program Files (x86)\Electrum\electrum\plugins\ledger\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\revealer\DejaVuSansMono-Bold.ttf
- C:\Program Files (x86)\Electrum\electrum\plugins\revealer\LICENSE_DEJAVU.txt
- C:\Program Files (x86)\Electrum\electrum\plugins\revealer\SIL Open Font License.txt
- C:\Program Files (x86)\Electrum\electrum\plugins\revealer\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\revealer\hmac_drbg.py
- C:\Program Files (x86)\Electrum\electrum\plugins\revealer\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\revealer\revealer.py
- C:\Program Files (x86)\Electrum\electrum\plugins\safe_t\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\safe_t\client.py
- C:\Program Files (x86)\Electrum\electrum\plugins\safe_t\clientbase.py
- C:\Program Files (x86)\Electrum\electrum\plugins\safe_t\cmdline.py
- C:\Program Files (x86)\Electrum\electrum\plugins\safe_t\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\safe_t\safe_t.py

- C:\Program Files (x86)\Electrum\electrum\plugins\safe_t\transport.py
- C:\Program Files (x86)\Electrum\electrum\plugins\trezor\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\trezor\clientbase.py
- C:\Program Files (x86)\Electrum\electrum\plugins\trezor\cmdline.py
- C:\Program Files (x86)\Electrum\electrum\plugins\trezor\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\trezor\trezor.py
- C:\Program Files (x86)\Electrum\electrum\plugins\trustedcoin\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\trustedcoin\cmdline.py
- C:\Program Files (x86)\Electrum\electrum\plugins\trustedcoin\kivy.py
- C:\Program Files (x86)\Electrum\electrum\plugins\trustedcoin\qt.py
- C:\Program Files (x86)\Electrum\electrum\plugins\trustedcoin\trustedcoin.py
- C:\Program Files (x86)\Electrum\electrum\plugins\virtualkeyboard\__init__.py
- C:\Program Files (x86)\Electrum\electrum\plugins\virtualkeyboard\qt.py
- C:\Program Files (x86)\Electrum\electrum\wordlist\english.txt
- C:\Program Files (x86)\Electrum\google\protobuf\internal_api_implementation.cp37-win32.pyd
- C:\Program Files (x86)\Electrum\google\protobuf\pyext_message.cp37-win32.pyd
- C:\Program Files (x86)\Electrum\safetlib\tests\txcache\insight_bitcoin_gold_tx_25526bf06c76ad3082bba930cf627cdd5f1b3cd0b9907dd7ff1a07e14addc985.json
- C:\Program Files (x86)\Electrum\safetlib\tests\txcache\insight_bitcoin_gold_tx_db77c2461b840e6edbe7f9280043184a98e020d9795c1b65cb7cef2551a8fb18.json

Deleted files

- C:\Users\<USER>\AppData\Local\Temp\nslAEBF.tmp
- C:\Users\<USER>\AppData\Local\Temp\nsmAF5E.tmp
- C:\Users\user\AppData\Local\Temp\nse7168.tmp
- C:\Users\user\AppData\Local\Temp\nso7108.tmp

Written files

- C:\Users\<USER>\AppData\Local\Temp\nsgAF3D.tmp
- C:\Users\<USER>\AppData\Local\Temp\nsmAF5E.tmp\UserInfo.dll
- C:\Program Files (x86)\Electrum\LIBEAY32.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtBluetooth.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtDBus.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtDesigner.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtHelp.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtLocation.pyd

- C:\Program Files (x86)\Electrum\PyQt5\QtMultimedia.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtMultimediaWidgets.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtNetwork.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtNetworkAuth.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtNfc.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtOpenGL.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtPositioning.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtQml.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtQuick.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtQuickWidgets.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtSensors.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtSerialPort.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtSql.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtSvg.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtTest.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtWebChannel.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtWebSockets.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtWinExtras.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtXml.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtXmlPatterns.pyd
- C:\Program Files (x86)\Electrum\PyQt5\Qt\bin
- C:\Program Files (x86)\Electrum\PyQt5\Qt\bin\d3dcompiler_47.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\bin\libEGL.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\bin\libGLESv2.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\bin\libeay32.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\bin\opengl32sw.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\bin\ssleay32.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\audio
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\audio\qtaudio_wasapi.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\audio\qtaudio_windows.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\bearer
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\bearer\qgenericbearer.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\mediaservice
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\mediaservice\dsengine.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\mediaservice\qtmedia_audioengine.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\mediaservice\wmfengine.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\sensorgestures
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\sensorgestures\qtsensorgestures_plugin.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\sensorgestures\qtsensorgestures_shakeplugin.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\sensors
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\sensors\qtsensors_generic.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\sqldrivers

- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\sqldrivers\qsqlite.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\sqldrivers\qsqlmysql.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\sqldrivers\qsqlodbc.dll
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\sqldrivers\qsqlpsql.dll

Opened files

- C:\Users\<USER>\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000017.db
- C:\Users\<USER>\AppData\Local\Temp\nsgAF3D.tmp
- C:\Users\<USER>\AppData\Local\Temp\nslAEBF.tmp
- C:\Users\<USER>\AppData\Local\Temp\nsmAF5E.tmp
- C:\Users\<USER>\AppData\Local\Temp\nsmAF5E.tmp\UserInfo.dll
- C:\Users\azure
- C:\Windows\system32\ntmarta.dll
- C:\Program Files (x86)\Electrum\LIBEAY32.dll
- C:\Program Files (x86)\Electrum\LIBEAY32.dll
- C:\Program Files (x86)\Electrum\PyQt5\QtDBus.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtDBus.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtDesigner.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtDesigner.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtHelp.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtHelp.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtLocation.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtLocation.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtMultimedia.py\
- C:\Program Files (x86)\Electrum\PyQt5\QtMultimedia.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtMultimediaWidgets.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtMultimediaWidgets.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtNetwork.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtNetwork.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtNetworkAuth.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtNetworkAuth.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtNfc.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtNfc.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtOpenGL.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtOpenGL.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtPositioning.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtPositioning.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtQml.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtQml.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtQuick.pyd

- C:\Program Files (x86)\Electrum\PyQt5\QtQuick.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtQuickWidgets.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtQuickWidgets.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtSensors.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtSensors.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtSerialPort.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtSerialPort.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtSql.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtSql.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtSvg.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtSvg.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtTest.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtTest.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtWebChannel.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtWebChannel.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtWebSockets.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtWebSockets.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtWinExtras.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtWinExtras.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtXml.pyd
- C:\Program Files (x86)\Electrum\PyQt5\QtXml.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\QtXmlPatterns.pyd
- C:\Program Files (x86)\Electrum\PyQt5\Qt\bin
- C:\Program Files (x86)\Electrum\PyQt5\Qt\bin\
- C:\Program Files (x86)\Electrum\PyQt5\QtXmlPatterns.pyd\
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\audio
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\bearer
- C:\Program Files (x86)\Electrum\PyQt5\Qt\plugins\mediaservice

Registry Activity

To get a list of all modifications, refer to Full_Registry_activity.pdf

Note: these key modifications were done by the installed exe, electrum.exe (not electrum-4.0.0-setup.exe)

Opened keys

- HKEY_CURRENT_USER\Software\Electrum
- HKEY_CURRENT_USER\Software\Classes\bitcoin
- HKEY_CURRENT_USER\Software\Classes\bitcoin\shell\open\command
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Electrum

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Electrum.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\CTF\Compatibility\Electrum.exe
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath

Sat Keys

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\GoogleUpdaterInternalService126.0.6462.0\Start HKEY_USERS\S-1-5-21-4270068108-2931534202-3907561125-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.exe\OpenWithProgids\exefile
HKEY_CURRENT_USER\Software\Classes\bitcoin HKEY_CURRENT_USER\Software\Electrum
HKEY_CURRENT_USER\Software\Electrum\NULL
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Electrum
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Electrum\DisplayIcon
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Electrum\DisplayName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Electrum\DisplayVersion
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Electrum\EstimatedSize
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Electrum\Publisher
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Electrum\URLInfoAbout
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Electrum\UninstallString
HKEY_CURRENT_USER_Classes\bitcoin\DefaultIcon HKEY_CURRENT_USER_Classes\bitcoin\NULL
HKEY_CURRENT_USER_Classes\bitcoin\URL Protocol HKEY_CURRENT_USER_Classes\bitcoin\shell
HKEY_CURRENT_USER_Classes\bitcoin\shell\open
HKEY_CURRENT_USER_Classes\bitcoin\shell\open\command
HKEY_CURRENT_USER_Classes\bitcoin\shell\open\command\NULL

Network Activity

DNS requests

- Hsmiths4fyqlw5xw.onion
- Wsw6tua3xl24gsmi264zaep6seppjyrkyucpsmuxnjzyt3f3j6swshad.onion
- domain electrum.bip.click
- domain oneweek.duckdns.org
- domain electrum.electrumxm.com
- domain qtornadoklbgdyww.onion

- domain electrum.livex.biz
- domain electrum.fullhealth.net
- domain electrum.arcade.tel
- domain electrum.rollerco.xyz
- domain electrum.esrv.one
- domain electrum.lightspeed.tel
- domain electrum.xs500.net
- domain bauerjhejlv6di7s.onion
- domain bauerjda5hnedjam.onion

IP Traffic

- 20.199.120.85
- 40.79.189.58
- 13.107.246.63
- 20.54.25.34
- 20.49.150.241
- 34.104.35.123
- 185.167.160.30

Process Activity

Shell commands

- %PATH%\Electrum.exe

Process tree

- C:\Users\user\Desktop\Electrum.exe

IOCs

Dropped executable file

- C:\Users\admin\AppData\Local\Temp\nsaAB4A.tmp\UserInfo.dll
  0073337816509851476c2cc154f471a3e3a1a2806b97c363870acc09a30a5ed7

- C:\Program Files\Electrum\MSVCP140.dll
  75ddc9778c23ee95b6c57db6b689f11c07d164d5a4c158d4c0acb87a520b8004
- C:\Program Files\Electrum\Qt5Bluetooth.dll
  469985a272f420b78d50581766d5721d32e74d44e686ec7fec65093ab9696313
- C:\Program Files\Electrum\LIBEAY32.dll
  b61de59000c6b130e0163358fb9c1f20bcc5dff3d17ff5a0c235b744f6181295
- C:\Program Files\Electrum\Qt5Core.dll
  4fbca3dac52f6ca7d40c97e8d6e0d5a38f44ddafaf383a66323979d2c1217a76
- C:\Program Files\Electrum\Qt5DBus.dll
  94c2ae7816eac0527eb5585e4a3eb025eb69130dd6339709365dcf133fc442d6
- C:\Program Files\Electrum\Qt5Widgets.dll
  efc6ac346c11dbbc68e30038898f3a05e875f9c3958954978c52ccec17bb0410
- C:\Program Files\Electrum\electrum-4.0.0.exe
  e1f489197aa4689a309eec0aad514b7f974f10e0cfebf8ed753d006f839c32cf
- C:\Program Files\Electrum\Qt5WinExtras.dll
  28ac8a83f083a7cfddcbb0d19cd1b7a31d582ed93883de72da9761b6ead58ec0
- C:\Program Files\Electrum\Qt5Gui.dll
  2ec2c15ae82a3c402d9d3f7e4dd2d4da3b295ecb9e495b04eec7c098793af952
- C:\Program Files\Electrum\PyQt5\Qt\bin\d3dcompiler_47.dll
  efbdbbcd0d954f8fdc53467de5d89ad525e4e4a9cfff8a15d07c6fdb350c407f
- C:\Program Files\Electrum\PyQt5\Qt\bin\opengl32sw.dll
  25ae7577e066fa80519a8f1c314b15cdd22e4a8d3ecd2a36eccc79e40714a91d
- C:\Program Files\Electrum\PyQt5\Qt\bin\libEGL.dll
  93e3efd164501b39a476ce081298673304446d0933145ba36fdc010a943be325
- C:\Program Files\Electrum\Qt5MultimediaWidgets.dll
  1193d334e10b8d831e8f6d90390fb0693eae9c67a98869ad6363d26c8c0a7ace
- C:\Program Files\Electrum\Qt5Help.dll
  1f8c7f3930ecc455cdc4aacbf4142a3b345840029d51c9dfa8e8b2c088aa4589
- C:\Program Files\Electrum\Qt5Multimedia.dll
  8219e39bfb8ac7d97436555e53b66838812f9b166bb8198fd56e073b7209b14d
- C:\Program Files\Electrum\PyQt5\Qt\bin\libGLESv2.dll
  2e3c98f0bae29819b0a1fa2b2e82c43425dcbd2516fc0213adcb7bd793ae4356
- C:\Program Files\Electrum\Qt5PositioningQuick.dll
  e3b32e30811b07bde5f3617192f71b2d10f874ec540c59818a91dc0921293d17
- C:\Program Files\Electrum\Qt5Nfc.dll
  f0345a0602ad0d91deb109542fe01a19b733e8b416f407948199016f97b48c65
- C:\Program Files\Electrum\Qt5NetworkAuth.dll
  9d674e6d594aac02e2e980cb11f76579cb2ac5ea055a197632bd069f167b3faf
- C:\Program Files\Electrum\Qt5Positioning.dll
  5acf35fede4861f4ba658698b6822539a4e7208807632c92a1b183b785238ae1
- C:\Program Files\Electrum\Qt5OpenGL.dll
  25b07afb02d92c83ef198028a0f8717058cbf2512bb8649927b91668db95e209
- C:\Program Files\Electrum\Qt5PrintSupport.dll
  077339d4017bc8fb3a8cd0e3233775f3ae5df0f8f18507b4539f92e133965b38

- C:\Program Files\Electrum\Qt5Network.dll
  f104638510c03618edb54b717b8c25d6e5feb2a40e2b8f7df6ce52a211efb62b
- C:\Program Files\Electrum\Qt5Qml.dll
  3789dac5ae9cf2018e7cfb39fddb61f58f10614b45c53209ac1735e725bc4e3e
- C:\Program Files\Electrum_overlapped.pyd
  0fc5b875a5c5d1606aeece39ff604d495128ea303ebb327956049e59673e6a2d
- C:\Program Files\Electrum_ctypes.pyd
  b981c445eca5c7f1435b8311344b3ffe0ddb3a2fe2d6bfdcd82cbbae5ebbbdd4
- C:\Program Files\Electrum\Qt5SerialPort.dll
  e808282281ee88d6fde1d966cd061b4b9b010d9e06f9a0c8c728354300af05f1
- C:\Program Files\Electrum\VCRUNTIME140.dll
  6823b98c3e922490a2f97f54862d32193900077e49f0360522b19e06e6da24b4
- C:\Program Files\Electrum\Qt5Sensors.dll
  b1cb50c859002ad1a212f74048c00e6189ca9eab4087272291926ec31c4132ca
- C:\Program Files\Electrum\Qt5Sql.dll
  254825527a2e975397518892df772ed297f395d7d64dce44169fd7eaf7328707
- C:\Program Files\Electrum_multiprocessing.pyd
  3a6aaa3d489ee2e295838befc70a0f940c83749227e12a1d873481cdc4e365e8
- C:\Program Files\Electrum_bz2.pyd
  6086c281c1dc046b2274e6421058ba392fe55d48fbbb9f07fe193ac123027f41
- C:\Program Files\Electrum_asyncio.pyd
  e7c4c78aff9d6b18e062fabd6a2672cc50bfd9440ebc8509eb590585a6ba2497
- C:\Program Files\Electrum_socket.pyd
  3d438fbdb6285751c792fe7145f83bcf8d1d1aa769ba553f774861474079eadb
- C:\Program Files\Electrum_decimal.pyd
  743737dc8ead21fd36746a9c91d68dd9cb76209fb557efb77902140becad580a
- C:\Program Files\Electrum\Qt5Svg.dll
  7a5fd382b4a7991a30bb182690ada8685d8856795560c4cfef9a7a0091719b12
- C:\Program Files\Electrum_lzma.pyd
  6c76877ebfc25695893167aa92292352fa2409941258ccbee16c8db4ffbdc583
- C:\Program Files\Electrum_hashlib.pyd
  dd9f416c39cba25aa2c1f65058f85b9e21c3756e6e5c28eed0cf277927114caf
- C:\Program Files\Electrum\hid.cp36-win32.pyd
  b3a4b6c1c8cb5938f85e01632c64236f61098492ac14828b4288fe0e83a60b03
- C:\Program Files\Electrum_ssl.pyd
  be9b097bf2e0f91873ee6997a38b4458629249694790ea46d580bb5bf31161d7

DNS requests

- domain electrum.bip.click
- domain oneweek.duckdns.org
- domain electrum.electrumxm.com
- domain qtornadoklbgdyww.onion
- domain hsmiths5mjk6uijs.onion
- domain electrum.livex.biz

- domain electrum.fullhealth.net
- domain electrum.arcade.tel
- domain electrum.rollerco.xyz
- domain electrum.esrv.one
- domain electrum.lightspeed.tel
- domain electrum.xs500.net
- domain bauerjhejlv6di7s.onion
- domain bauerjda5hnedjam.onion
- domain hsmiths4fyqlw5xw.onion

Connections

- ip 104.31.234.6
- ip 185.167.160.30
- ip 91.211.88.33
- ip 185.25.48.104
- ip 111.90.159.213
- ip 46.227.71.107
- ip 46.227.71.110
- ip 46.227.71.106
- ip 46.227.71.108
- ip 46.227.71.109
- ip 185.8.177.126

HTTP requests

- url http://185.167.160.30/pdata.php

Conclusion

Electrum 4.0.0 malware used phishing and malicious updates as its attack vectors and caused financial losses. The key indicators included malicious domains, IP addresses, and file hashes. The network traffic showed connections to malicious domains and data transfers that weren't initiated by the user. The malware modified some registry keys and changed privileges to ensure persistence.

To protect against similar threats, make sure to use only signed installers from official websites.