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

By Karsten Hahn

Published: 2022-04-21 · Archived: 2026-04-05 20:22:44 UTC

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.
