

# [QuickNote] VidarStealer Analysis

---

 kienmanowar.wordpress.com/2022/12/17/quicknote-vidarstealer-analysis/

December 17, 2022

## Sample:

---

### Loader:

<https://bazaar.abuse.ch/sample/816c4a2117b90dc75d91056ca32a36ffd32d561aa433ee3f97126ba490e6d60a/>

**Unpacked:** 7bd942857a29e7f2931da2bd8fa1d118

## Decrypt strings

---

Here is the the pseudo-code of the function that decodes the strings:

```

_BYTE *__usercall vdr_decrypt_strings@<eax>(uint32_t len@<ecx>, char *xor_key, const
char *encStr)
{
    // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

    cnt = 0x208;
    v5 = Destination;
    do
    {
        *v5 = 0;
        v5 = (v5 + 1);
        --cnt;
    }
    while ( cnt );
    wscat(Destination, L"Nor again is there anyone who loves or pursues or desires to
obtain pain of itself, because it is pain");
    wcslen(Destination);
    wcslen(Destination);
    wcslen(Destination);
    wcslen(Destination);
    decStr = LocalAlloc(0x40u, len + 1);
    wcslen(Destination);
    wcslen(Destination);
    wcslen(Destination);
    wcslen(Destination);
    decStr[len] = 0;
    wcslen(Destination);
    wcslen(Destination);
    wcslen(Destination);
    wcslen(Destination);
    for ( i = 0; i < len; ++i )
    {
        wcslen(Destination);
        wcslen(Destination);
        decStr[i] = xor_key[i] ^ encStr[i % strlen(encStr)]; <-- xor loop
        wcslen(Destination);
        wcslen(Destination);
    }
    wcslen(Destination);
    wcslen(Destination);
    memset(Destination, 0, sizeof(Destination));
    return decStr;
}

```

List of all decoded strings:

[\*] Target function found at 0x404158

- [+] Decrypted string: HAL9TH at 0x401136
- [+] Decrypted string: JohnDoe at 0x40114d
- [+] Decrypted string: LoadLibraryA at 0x401164
- [+] Decrypted string: lstrcatA at 0x40117b
- [+] Decrypted string: GetProcAddress at 0x401192
- [+] Decrypted string: Sleep at 0x4011a9
- [+] Decrypted string: GetSystemTime at 0x4011c0
- [+] Decrypted string: ExitProcess at 0x4011d7
- [+] Decrypted string: GetCurrentProcess at 0x4011ee
- [+] Decrypted string: VirtualAllocExNuma at 0x401205
- [+] Decrypted string: VirtualAlloc at 0x40121c
- [+] Decrypted string: VirtualFree at 0x401233
- [+] Decrypted string: lstrcmpiW at 0x40124a
- [+] Decrypted string: LocalAlloc at 0x401261
- [+] Decrypted string: GetComputerNameA at 0x401278
- [+] Decrypted string: advapi32.dll at 0x40128f
- [+] Decrypted string: GetUserNameA at 0x4012a6
- [+] Decrypted string: kernel32.dll at 0x4012bd
- [+] Decrypted string: Wallets at 0x4012dc
- [+] Decrypted string: Plugins at 0x4012f2
- [+] Decrypted string: keystore at 0x40130b
- [+] Decrypted string: Ethereum" at 0x401322
- [+] Decrypted string: \Ethereum\ at 0x401339
- [+] Decrypted string: Electrum at 0x40134f
- [+] Decrypted string: \Electrum\wallets\ at 0x401366
- [+] Decrypted string: ElectrumLTC at 0x40137f
- [+] Decrypted string: \Electrum-LTC\wallets\ at 0x401396
- [+] Decrypted string: Exodus at 0x4013ad
- [+] Decrypted string: \Exodus\ at 0x4013c3
- [+] Decrypted string: exodus.conf.json at 0x4013da
- [+] Decrypted string: window-state.json at 0x4013f1
- [+] Decrypted string: \Exodus\exodus.wallet\ at 0x401408
- [+] Decrypted string: passphrase.json at 0x40141f
- [+] Decrypted string: seed.seco at 0x401436
- [+] Decrypted string: info.seco at 0x40144d
- [+] Decrypted string: ElectronCash at 0x401464
- [+] Decrypted string: \ElectronCash\wallets\ at 0x40147b
- [+] Decrypted string: default\_wallet at 0x401492
- [+] Decrypted string: MultiDoge at 0x4014a9
- [+] Decrypted string: \MultiDoge\ at 0x4014bf
- [+] Decrypted string: multidoge.wallet at 0x4014d6
- [+] Decrypted string: Jaxx\_Desktop\_Old at 0x4014ed
- [+] Decrypted string: \jaxx\Local Storage\ at 0x401504
- [+] Decrypted string: file\_\_0.localstorage at 0x40151b
- [+] Decrypted string: Atomic at 0x401532
- [+] Decrypted string: \atomic\Local Storage\leveldb\ at 0x401549
- [+] Decrypted string: \*.log at 0x401560
- [+] Decrypted string: CURRENT at 0x401576
- [+] Decrypted string: LOCK at 0x40158d
- [+] Decrypted string: LOG at 0x4015a4
- [+] Decrypted string: MANIFEST-000001 at 0x4015bb

```

[+] Decrypted string: 0000* at 0x4015d2
[+] Decrypted string: Binance at 0x4015e8
[+] Decrypted string: \Binance\ at 0x4015ff
[+] Decrypted string: app-store.json at 0x401616
[+] Decrypted string: Coinomi at 0x40162c
[+] Decrypted string: \Coinomi\Coinomi\wallets\ at 0x401643
[+] Decrypted string: *.wallet at 0x401659
[+] Decrypted string: *.config at 0x40166f
[+] Decrypted string: wallet_path at 0x401685
[+] Decrypted string: SOFTWARE\monero-project\monero-core at 0x40169c
[+] Decrypted string: \Monero\ at 0x4016b2
[+] Decrypted string: C:\ProgramData\ at 0x4016c9
[+] Decrypted string: .exe at 0x4016e0
[+] Decrypted string: RECYCLE.BIN at 0x4016f6
[+] Decrypted string: Config.Msi at 0x40170d
[+] Decrypted string: System Volume Information at 0x401724
[+] Decrypted string: msdownld.tmp at 0x40173b
[+] Decrypted string: Recovery at 0x401751
[+] Decrypted string: Local\Temp at 0x401768
[+] Decrypted string: Recycle.Bin at 0x40177e
[+] Decrypted string: MicrosoftEdge\Cookies at 0x401795
[+] Decrypted string: Local\Packages at 0x4017ac
[+] Decrypted string: Local\NuGet at 0x4017c2
[+] Decrypted string: Roaming\WinRAR at 0x4017d9
[+] Decrypted string: Local\Microsoft at 0x4017f0
[+] Decrypted string: fee_estimates at 0x401809
[+] Decrypted string: peers at 0x401820
[+] Decrypted string: mempool at 0x401836
[+] Decrypted string: banlist at 0x40184c
[+] Decrypted string: governance at 0x401863
[+] Decrypted string: mncache at 0x401879
[+] Decrypted string: mnpayments at 0x401890
[+] Decrypted string: netfulfilled at 0x4018a7
[+] Decrypted string: Login Data at 0x4018be
[+] Decrypted string: Cookies at 0x4018d4
[+] Decrypted string: Web Data at 0x4018eb
[+] Decrypted string: logins.json at 0x401901
[+] Decrypted string: formSubmitURL at 0x401917
[+] Decrypted string: usernameField at 0x40192d
[+] Decrypted string: encryptedUsername at 0x401944
[+] Decrypted string: encryptedPassword at 0x40195b
[+] Decrypted string: guid at 0x401972
[+] Decrypted string: SELECT origin_url, username_value, password_value FROM
logins at 0x401989
[+] Decrypted string: SELECT name, value FROM autofill at 0x4019a2
[+] Decrypted string: SELECT name_on_card, expiration_month, expiration_year,
card_number_encrypted FROM credit_cards at 0x4019b9
[+] Decrypted string: SELECT target_path, tab_url from downloads at 0x4019d0
[+] Decrypted string: SELECT url FROM urls at 0x4019e7
[+] Decrypted string: SELECT HOST_KEY, is_httponly, path, is_secure,
(expires_utc/1000000)-11644480800, name, encrypted_value from cookies at 0x4019fe
[+] Decrypted string: \AppData\Roaming\FileZilla\recentservers.xml at 0x401a15

```

[+] Decrypted string: <Host> at 0x401a2c  
[+] Decrypted string: <Port> at 0x401a43  
[+] Decrypted string: <User> at 0x401a5a  
[+] Decrypted string: <Pass encoding="base64"> at 0x401a71  
[+] Decrypted string: Soft: FileZilla  
at 0x401a88  
[+] Decrypted string: Mozilla Firefox at 0x401a9f  
[+] Decrypted string: \Mozilla\Firefox\Profiles\ at 0x401ab6  
[+] Decrypted string: Pale Moon at 0x401acd  
[+] Decrypted string: \Moonchild Productions\Pale Moon\Profiles\ at 0x401ae4  
[+] Decrypted string: Google Chrome at 0x401afa  
[+] Decrypted string: \Google\Chrome\User Data\ at 0x401b11  
[+] Decrypted string: Chromium at 0x401b28  
[+] Decrypted string: \Chromium\User Data\ at 0x401b3f  
[+] Decrypted string: Amigo at 0x401b56  
[+] Decrypted string: \Amigo\User Data\ at 0x401b6d  
[+] Decrypted string: Torch at 0x401b84  
[+] Decrypted string: \Torch\User Data\ at 0x401b9b  
[+] Decrypted string: Comodo Dragon at 0x401bb1  
[+] Decrypted string: \Comodo\Dragon\User Data\ at 0x401bc8  
[+] Decrypted string: Epic Privacy Browser at 0x401bdf  
[+] Decrypted string: \Epic Privacy Browser\User Data\ at 0x401bf5  
[+] Decrypted string: Vivaldi at 0x401c0c  
[+] Decrypted string: \Vivaldi\User Data\ at 0x401c23  
[+] Decrypted string: CocCoc at 0x401c3a  
[+] Decrypted string: \CocCoc\Browser\User Data\ at 0x401c51  
[+] Decrypted string: Cent Browser at 0x401c68  
[+] Decrypted string: \CentBrowser\User Data\ at 0x401c7f  
[+] Decrypted string: TorBro Browser at 0x401c96  
[+] Decrypted string: \TorBro\Profile\ at 0x401cad  
[+] Decrypted string: Chedot Browser at 0x401cc4  
[+] Decrypted string: \Chedot\User Data\ at 0x401cdb  
[+] Decrypted string: Brave\_Old at 0x401cf2  
[+] Decrypted string: \brave\ at 0x401d09  
[+] Decrypted string: 7Star at 0x401d20  
[+] Decrypted string: \7Star\7Star\User Data\ at 0x401d37  
[+] Decrypted string: Microsoft Edge at 0x401d4e  
[+] Decrypted string: \Microsoft\Edge\User Data\ at 0x401d65  
[+] Decrypted string: 360 Browser at 0x401d7b  
[+] Decrypted string: \360Browser\Browser\User Data\ at 0x401d92  
[+] Decrypted string: QQBrowser at 0x401da9  
[+] Decrypted string: \Tencent\QQBrowser\User Data\ at 0x401dc0  
[+] Decrypted string: Opera at 0x401dd7  
[+] Decrypted string: \Opera Software\Opera Stable\ at 0x401dee  
[+] Decrypted string: OperaGX at 0x401e05  
[+] Decrypted string: \Opera Software\Opera GX Stable\ at 0x401e1b  
[+] Decrypted string: Local State at 0x401e31  
[+] Decrypted string: Cookies at 0x401e48  
[+] Decrypted string: TRUE at 0x401e5f  
[+] Decrypted string: FALSE at 0x401e76  
[+] Decrypted string: gdi32.dll at 0x401e8d  
[+] Decrypted string: ole32.dll at 0x401ea4

[+] Decrypted string: user32.dll at 0x401ebb  
[+] Decrypted string: psapi.dll at 0x401ed2  
[+] Decrypted string: BCRYPT.DLL at 0x401ee9  
[+] Decrypted string: BCryptCloseAlgorithmProvider at 0x401f00  
[+] Decrypted string: BCryptDestroyKey at 0x401f17  
[+] Decrypted string: BCryptOpenAlgorithmProvider at 0x401f2e  
[+] Decrypted string: BCryptSetProperty at 0x401f45  
[+] Decrypted string: BCryptGenerateSymmetricKey at 0x401f5c  
[+] Decrypted string: BCryptDecrypt at 0x401f72  
[+] Decrypted string: CRYPT32.DLL at 0x401f88  
[+] Decrypted string: CryptUnprotectData at 0x401f9f  
[+] Decrypted string: CryptStringToBinaryA at 0x401fb6  
[+] Decrypted string: C:\ProgramData\nss3.dll at 0x401fcd  
[+] Decrypted string: NSS\_Init at 0x401fe4  
[+] Decrypted string: NSS\_Shutdown at 0x401ffb  
[+] Decrypted string: PK11\_GetInternalKeySlot at 0x402012  
[+] Decrypted string: PK11\_FreeSlot at 0x402028  
[+] Decrypted string: PK11\_Authenticate at 0x40203f  
[+] Decrypted string: PK11SDR\_Decrypt at 0x402056  
[+] Decrypted string: RegOpenKeyExA at 0x40206c  
[+] Decrypted string: RegQueryValueExA at 0x402083  
[+] Decrypted string: RegCloseKey at 0x402099  
[+] Decrypted string: RegOpenKeyExW at 0x4020af  
[+] Decrypted string: RegGetValueW at 0x4020c6  
[+] Decrypted string: RegEnumKeyExA at 0x4020dc  
[+] Decrypted string: RegGetValueA at 0x4020f3  
[+] Decrypted string: GetCurrentHwProfileA at 0x40210a  
[+] Decrypted string: wininet.dll at 0x402120  
[+] Decrypted string: InternetCloseHandle at 0x402137  
[+] Decrypted string: InternetReadFile at 0x40214e  
[+] Decrypted string: HttpSendRequestA at 0x402165  
[+] Decrypted string: HttpOpenRequestA at 0x40217c  
[+] Decrypted string: InternetConnectA at 0x402193  
[+] Decrypted string: InternetOpenA at 0x4021a9  
[+] Decrypted string: HttpAddRequestHeadersA at 0x4021c0  
[+] Decrypted string: HttpQueryInfoA at 0x4021d7  
[+] Decrypted string: InternetSetFilePointer at 0x4021ee  
[+] Decrypted string: InternetOpenUrlA at 0x402205  
[+] Decrypted string: InternetSetOptionA at 0x40221c  
[+] Decrypted string: DeleteUrlCacheEntry at 0x402233  
[+] Decrypted string: CreateCompatibleBitmap at 0x40224a  
[+] Decrypted string: SelectObject at 0x402261  
[+] Decrypted string: BitBlt at 0x402278  
[+] Decrypted string: DeleteObject at 0x40228f  
[+] Decrypted string: CreateDCA at 0x4022a6  
[+] Decrypted string: GetDeviceCaps at 0x4022bc  
[+] Decrypted string: CreateCompatibleDC at 0x4022d3  
[+] Decrypted string: CoCreateInstance at 0x4022ea  
[+] Decrypted string: CoUninitialize at 0x402301  
[+] Decrypted string: GetDesktopWindow at 0x402318  
[+] Decrypted string: ReleaseDC at 0x40232f  
[+] Decrypted string: GetKeyboardLayoutList at 0x402346

[+] Decrypted string: CharToOemA at 0x40235d  
[+] Decrypted string: GetDC at 0x402374  
[+] Decrypted string: wsprintfA at 0x40238b  
[+] Decrypted string: EnumDisplayDevicesA at 0x4023a2  
[+] Decrypted string: GetSystemMetrics at 0x4023b9  
[+] Decrypted string: GetModuleFileNameExA at 0x4023d0  
[+] Decrypted string: GetModuleBaseNameA at 0x4023e7  
[+] Decrypted string: EnumProcessModules at 0x4023fe  
[+] Decrypted string: ibnejdfjmmkpcnlpebklmnkoeiohofec at 0x402414  
[+] Decrypted string: TronLink at 0x40242b  
[+] Decrypted string: nkbihfbeogaeaoehlefnkodbefgpgknn at 0x402441  
[+] Decrypted string: MetaMask at 0x402458  
[+] Decrypted string: fhbohimaelbohpbjbbldcngcnapndodjp at 0x40246e  
[+] Decrypted string: BinanceChainWallet at 0x402485  
[+] Decrypted string: ffnbelfdoeiohenkjibnmdajiehjhajb at 0x40249b  
[+] Decrypted string: Yoroi at 0x4024b2  
[+] Decrypted string: jbdaocneiianmjbjlgalhcelgbejmnid at 0x4024c8  
[+] Decrypted string: NiftyWallet at 0x4024de  
[+] Decrypted string: afbcbjpbpfadlkmhmclhkeeodmamcflc at 0x4024f4  
[+] Decrypted string: MathWallet at 0x40250b  
[+] Decrypted string: hnfanknocfeofbddgcijnmhnfnkdnaad at 0x402521  
[+] Decrypted string: Coinbase at 0x402538  
[+] Decrypted string: hpglfhgfhnbgpjdenjgmdgoeiappafln at 0x40254e  
[+] Decrypted string: Guarda at 0x402565  
[+] Decrypted string: blnieiiffboillknjnepogjhgknoapac at 0x40257b  
[+] Decrypted string: EQUALWallet at 0x402591  
[+] Decrypted string: cjelfplplebdjjenllpjcbmlmkfcffne at 0x4025a7  
[+] Decrypted string: JaxxLiberty at 0x4025bd  
[+] Decrypted string: fihkakfobkkmkjopchpfgcmhfjnmnmpi at 0x4025d3  
[+] Decrypted string: BitAppWallet at 0x4025ea  
[+] Decrypted string: kncchdigobghenbbaddojjnaogfppfj at 0x402600  
[+] Decrypted string: iWallet at 0x402617  
[+] Decrypted string: amkmjmmflddogmhpjloimipbofnfjih at 0x40262d  
[+] Decrypted string: Wombat at 0x402644  
[+] Decrypted string: nlbmnnijcnlegkjjpcfjclmcfggfefdm at 0x40265a  
[+] Decrypted string: MewCx at 0x402671  
[+] Decrypted string: nanjmdknkhkinifnkgdcggcfnhdaammj at 0x402687  
[+] Decrypted string: GuildWallet at 0x40269d  
[+] Decrypted string: fnjhmkhmkbjkkabndcnnogagobneec at 0x4026b3  
[+] Decrypted string: RoninWallet at 0x4026c9  
[+] Decrypted string: cphhlgmgameodnhkjdmkpanlelnlohao at 0x4026df  
[+] Decrypted string: NeoLine at 0x4026f6  
[+] Decrypted string: nhnkbkgjikgcigadomkphalanndcapjk at 0x40270c  
[+] Decrypted string: CloverWallet at 0x402723  
[+] Decrypted string: kpfpokelmapcoipemfendmdcghnegimn at 0x402739  
[+] Decrypted string: LiquidityWallet at 0x402750  
[+] Decrypted string: aiifbnbfobpmeekipheeijimdnpnlpgpp at 0x402766  
[+] Decrypted string: Terra\_Station at 0x40277c  
[+] Decrypted string: dmkamcknogkgcdfhhbdddchachkejeap at 0x402792  
[+] Decrypted string: Keplr at 0x4027a9  
[+] Decrypted string: fhmfendgdocmbmfikdcogofphimnkno at 0x4027bf  
[+] Decrypted string: Sollet at 0x4027d6



[+] Decrypted string: cnmamaachppnkjgnildpdmkaakejnhae at 0x4027ec  
[+] Decrypted string: AuroWallet at 0x402803  
[+] Decrypted string: jojhfloedkpkglbfimdfabpdfjaoolaf at 0x402819  
[+] Decrypted string: PolymeshWallet at 0x402830  
[+] Decrypted string: flpiciiilemghbmfalicajoolhikkenfel at 0x402846  
[+] Decrypted string: ICONex at 0x40285d  
[+] Decrypted string: fnnegphlobjdpkhecapkijjdkgcjhkib at 0x402873  
[+] Decrypted string: Harmony at 0x40288a  
[+] Decrypted string: aeachknmefphecpcionboohckonoeemg at 0x4028a0  
[+] Decrypted string: Coin98 at 0x4028b7  
[+] Decrypted string: cgeedpfagjceefieflmdfphplkenlfk at 0x4028cd  
[+] Decrypted string: EVER Wallet at 0x4028e3  
[+] Decrypted string: pdadjkfkcgafgbceimcpbkalfnepbnk at 0x4028f9  
[+] Decrypted string: KardiaChain at 0x40290f  
[+] Decrypted string: imloifkgjagghnncjkhggdhalmcnfklk at 0x402925  
[+] Decrypted string: Trezor Password Manager at 0x40293c  
[+] Decrypted string: acmacodkjbdgmoleebolmdjonilkdbch at 0x402952  
[+] Decrypted string: Rabby at 0x402969  
[+] Decrypted string: bfnaelmomeimhlpmgjnjophhpkkoljpa at 0x40297f  
[+] Decrypted string: Phantom at 0x402996  
[+] Decrypted string: ejbalbakoplchlghecdalmeeeajnimhm at 0x4029ac  
[+] Decrypted string: odbfpeeihdkbihmopkbjmoonfanlbfcl at 0x4029c2  
[+] Decrypted string: BraveWallet at 0x4029d8  
[+] Decrypted string: fhilaheimglignddkjgofkcbgekhenbh at 0x4029ee  
[+] Decrypted string: Oxygen (Atomic) at 0x402a05  
[+] Decrypted string: mgffkfbidihjpoaomajlbgchddlicgpn at 0x402a1b  
[+] Decrypted string: PaliWallet at 0x402a32  
[+] Decrypted string: aodkkagnadcobofpggfneongembjca at 0x402a48  
[+] Decrypted string: BoltX at 0x402a5f  
[+] Decrypted string: hmeobnfnfcmkdcmlblgagmfpfboieaf at 0x402a75  
[+] Decrypted string: XdefiWallet at 0x402a8b  
[+] Decrypted string: lpfcbjknijpeeillifnkikgncikgfhdo at 0x402aa1  
[+] Decrypted string: NamiWallet at 0x402ab8  
[+] Decrypted string: dngmlblcodfobpdpecaadgfbcggfjfnm at 0x402ace  
[+] Decrypted string: MaiarDeFiWallet at 0x402ae5  
[+] Decrypted string: lpilbniabackdjcionkobglmddfbcjo at 0x402afb  
[+] Decrypted string: WavesKeeper at 0x402b11  
[+] Decrypted string: bhhlbepdkbapadjdnnojkbgioidbic at 0x402b27  
[+] Decrypted string: Solflare at 0x402b3e  
[+] Decrypted string: dkdedlpgdmmkkfjabffeganieamfklkm at 0x402b54  
[+] Decrypted string: CyanoWallet at 0x402b6a  
[+] Decrypted string: hcflpincpppdclinealmandijcmnkbgn at 0x402b80  
[+] Decrypted string: KHC at 0x402b97  
[+] Decrypted string: mnfifekajgofkckemidiaecocnkjeh at 0x402bad  
[+] Decrypted string: TezBox at 0x402bc4  
[+] Decrypted string: ookjlbkiiijnhpmnjffcofjonbfbgaoc at 0x402bda  
[+] Decrypted string: Temple at 0x402bf1  
[+] Decrypted string: jnkelfanjkeadonecabehalmbgpfodjm at 0x402c07  
[+] Decrypted string: Goby at 0x402c1e  
[+] Decrypted string: bhghoamapcdpbohphigooaddinpkbai at 0x402c34  
[+] Decrypted string: Authenticator at 0x402c4a  
[+] Decrypted string: gaedmjdmmahhbjeffcbaolhhanlaolb at 0x402c60



[+] Decrypted string: Authy at 0x402c77  
[+] Decrypted string: oeljldpnmdbchonieliidgobddffflal at 0x402c8d  
[+] Decrypted string: EOS Authenticator at 0x402ca4  
[+] Decrypted string: ilgcnhelpchnceei pipijaljkblbcobl at 0x402cba  
[+] Decrypted string: GAuth Authenticator at 0x402cd1  
[+] Decrypted string: \com.liberty.jaxx\IndexedDB\file\_\_0.indexeddb.leveldb\ at  
0x402ce8  
[+] Decrypted string: Jaxx\_Desktop at 0x402cff  
[+] Decrypted string: \Daedalus Mainnet\wallets\ at 0x402d16  
[+] Decrypted string: Daedalus Mainnet at 0x402d2d  
[+] Decrypted string: she\*.sqlite at 0x402d43  
[+] Decrypted string: \Blockstream\Green\wallets\ at 0x402d5a  
[+] Decrypted string: Blockstream Green at 0x402d71  
[+] Decrypted string: \WalletWasabi\Client\Wallets\ at 0x402d88  
[+] Decrypted string: Wasabi Wallet at 0x402d9e  
[+] Decrypted string: \discord\ at 0x402db5  
[+] Decrypted string: Discord at 0x402dcc  
[+] Decrypted string: Local Storage at 0x402de2  
[+] Decrypted string: leveldb at 0x402df9  
[+] Decrypted string: Session Storage at 0x402e10  
[+] Decrypted string: \Soft\Discord\discord\_tokens.txt at 0x402e26  
[+] Decrypted string: dQw4w9WgXcQ: at 0x402e3d  
[+] Decrypted string: Discord Token: at 0x402e54  
[+] Decrypted string: CreateThread at 0x402e6b  
[+] Decrypted string: GlobalMemoryStatusEx at 0x402e82  
[+] Decrypted string: IsWow64Process at 0x402e99  
[+] Decrypted string: GetUserDefaultLocaleName at 0x402eb0  
[+] Decrypted string: GetSystemInfo at 0x402ec6  
[+] Decrypted string: WideCharToMultiByte at 0x402edd  
[+] Decrypted string: LocalFree at 0x402ef4  
[+] Decrypted string: HeapAlloc at 0x402f0b  
[+] Decrypted string: GetProcessHeap at 0x402f22  
[+] Decrypted string: CreateFileA at 0x402f38  
[+] Decrypted string: GetFileSize at 0x402f4e  
[+] Decrypted string: ReadFile at 0x402f65  
[+] Decrypted string: CloseHandle at 0x402f7b  
[+] Decrypted string: GetLogicalDriveStringsA at 0x402f92  
[+] Decrypted string: lstrlenA at 0x402fa9  
[+] Decrypted string: GetDriveTypeA at 0x402fbf  
[+] Decrypted string: lstrcpyA at 0x402fd6  
[+] Decrypted string: MultiByteToWideChar at 0x402fed  
[+] Decrypted string: FindFirstFileA at 0x403004  
[+] Decrypted string: FindNextFileA at 0x40301a  
[+] Decrypted string: FindClose at 0x403031  
[+] Decrypted string: GetLastError at 0x403048  
[+] Decrypted string: lstrcpyA at 0x40305f  
[+] Decrypted string: GlobalLock at 0x403076  
[+] Decrypted string: GlobalSize at 0x40308d  
[+] Decrypted string: FreeLibrary at 0x4030a3  
[+] Decrypted string: GetLocaleInfoA at 0x4030ba  
[+] Decrypted string: GetCurrentProcessId at 0x4030d1  
[+] Decrypted string: OpenProcess at 0x4030e7

[+] Decrypted string: GetFileSizeEx at 0x4030fd  
[+] Decrypted string: GetTimeZoneInformation at 0x403114  
[+] Decrypted string: TzSpecificLocalTimeToSystemTime at 0x40312b  
[+] Decrypted string: CopyFileA at 0x403142  
[+] Decrypted string: DeleteFileA at 0x403158  
[+] Decrypted string: GetCurrentDirectoryA at 0x40316f  
[+] Decrypted string: SetFilePointer at 0x403186  
[+] Decrypted string: HeapFree at 0x40319d  
[+] Decrypted string: SystemTimeToFileTime at 0x4031b4  
[+] Decrypted string: GetLocalTime at 0x4031cb  
[+] Decrypted string: SetFileTime at 0x4031e1  
[+] Decrypted string: WriteFile at 0x4031f8  
[+] Decrypted string: GetFileAttributesA at 0x40320f  
[+] Decrypted string: GetFileAttributesW at 0x403226  
[+] Decrypted string: LocalFileTimeToFileTime at 0x40323d  
[+] Decrypted string: MapViewOfFile at 0x403253  
[+] Decrypted string: UnMapViewOfFile at 0x40326a  
[+] Decrypted string: FileTimeToSystemTime at 0x403281  
[+] Decrypted string: CreateFileMappingA at 0x403298  
[+] Decrypted string: GetFileInformationByHandle at 0x4032af  
[+] Decrypted string: GetEnvironmentVariableA at 0x4032c6  
[+] Decrypted string: SetEnvironmentVariableA at 0x4032dd  
[+] Decrypted string: GetTickCount at 0x4032f4  
[+] Decrypted string: OpenEventA at 0x40330b  
[+] Decrypted string: CreateEventA at 0x403322  
[+] Decrypted string: CreateToolhelp32Snapshot at 0x403339  
[+] Decrypted string: Process32First at 0x403350  
[+] Decrypted string: Process32Next at 0x403366  
[+] Decrypted string: GetWindowsDirectoryA at 0x40337d  
[+] Decrypted string: GetVolumeInformationA at 0x403394  
[+] Decrypted string: shell32.dll at 0x4033aa  
[+] Decrypted string: shlwapi.dll at 0x4033c0  
[+] Decrypted string: dbghelp.dll at 0x4033d6  
[+] Decrypted string: gdiplus.dll at 0x4033ec  
[+] Decrypted string: CryptBinaryToStringA at 0x403403  
[+] Decrypted string: RegEnumValueA at 0x403419  
[+] Decrypted string: GetFileSecurityA at 0x403430  
[+] Decrypted string: OpenProcessToken at 0x403447  
[+] Decrypted string: DuplicateToken at 0x40345e  
[+] Decrypted string: MapGenericMask at 0x403475  
[+] Decrypted string: AccessCheck at 0x40348b  
[+] Decrypted string: InternetCrackUrlA at 0x4034a2  
[+] Decrypted string: CoInitialize at 0x4034b9  
[+] Decrypted string: CreateStreamOnHGlobal at 0x4034d0  
[+] Decrypted string: GetHGlobalFromStream at 0x4034e7  
[+] Decrypted string: GetWindowRect at 0x4034fd  
[+] Decrypted string: GetWindowDC at 0x403513  
[+] Decrypted string: CloseWindow at 0x403529  
[+] Decrypted string: ShellExecuteExA at 0x403540  
[+] Decrypted string: SHFileOperationA at 0x403557  
[+] Decrypted string: SHGetFolderPathA at 0x40356e  
[+] Decrypted string: PathMatchSpecW at 0x403585

```

[+] Decrypted string: PathMatchSpecA at 0x40359c
[+] Decrypted string: StrCmpCA at 0x4035b3
[+] Decrypted string: StrCmpCW at 0x4035ca
[+] Decrypted string: StrStrA at 0x4035e1
[+] Decrypted string: PathFindFileNameA at 0x4035f8
[+] Decrypted string: SymMatchString at 0x40360f
[+] Decrypted string: GdipGetImageEncodersSize at 0x403626
[+] Decrypted string: GdipGetImageEncoders at 0x40363d
[+] Decrypted string: GdipCreateBitmapFromHBITMAP at 0x403654
[+] Decrypted string: GdiplusStartup at 0x40366b
[+] Decrypted string: GdiplusShutdown at 0x403682
[+] Decrypted string: GdipSaveImageToStream at 0x403699
[+] Decrypted string: GdipDisposeImage at 0x4036b0
[+] Decrypted string: GdipFree at 0x4036c7
[+] Decrypted string: sqlite3_open at 0x4036de
[+] Decrypted string: sqlite3_prepare_v2 at 0x4036f5
[+] Decrypted string: sqlite3_step at 0x40370c
[+] Decrypted string: sqlite3_column_text at 0x403723
[+] Decrypted string: sqlite3_finalize at 0x40373a
[+] Decrypted string: sqlite3_close at 0x403750
[+] Decrypted string: sqlite3_column_bytes at 0x403767
[+] Decrypted string: sqlite3_column_blob at 0x40377e
[+] Decrypted string: \Opera Software\ at 0x403795
[+] Decrypted string: \Opera Stable\ at 0x4037ac
[+] Decrypted string: \Opera GX Stable\ at 0x4037c3
[+] Decrypted string: \CryptoTab Browser\User Data\ at 0x4037da
[+] Decrypted string: CryptoTab Browser at 0x4037f1
[+] Decrypted string: \BraveSoftware\Brave-Browser\User Data\ at 0x403808
[+] Decrypted string: Brave at 0x40381f
[+] Decrypted string: \Thunderbird\Profiles\ at 0x403836
[+] Decrypted string: Thunderbird at 0x40384c
[+] Decrypted string: \Telegram Desktop\ at 0x403863
[+] Decrypted string: key_datas at 0x40387a
[+] Decrypted string: map* at 0x403891
[+] Decrypted string: D877F783D5D3EF8C* at 0x4038a8
[+] Decrypted string: A7FDF864FBC10B77* at 0x4038bf
[+] Decrypted string: A92DAA6EA6F891F2* at 0x4038d6
[+] Decrypted string: F8806DD0C461824F* at 0x4038ed
[+] Decrypted string: \Soft\Telegram\ at 0x403904
[+] Decrypted string: \passwords.txt at 0x40391b
[+] Decrypted string: "os_crypt":{"encrypted_key": at 0x403932
[+] Decrypted string: Soft: at 0x403949
[+] Decrypted string: Host: at 0x403960
[+] Decrypted string: Login: at 0x403977
[+] Decrypted string: Password: at 0x40398e
[+] Decrypted string: Network at 0x4039a5
[+] Decrypted string: SELECT host, isHttpOnly, path, isSecure, expiry, name, value
FROM moz_cookies at 0x4039bc
[+] Decrypted string: SELECT url FROM moz_places at 0x4039d3
[+] Decrypted string: SELECT fieldname, value FROM moz_formhistory at 0x4039ea
[+] Decrypted string: History at 0x403a01
[+] Decrypted string: cookies.sqlite at 0x403a18

```

[+] Decrypted string: formhistory.sqlite at 0x403a2f  
[+] Decrypted string: places.sqlite at 0x403a45  
[+] Decrypted string: \*.localstorage at 0x403a5c  
[+] Decrypted string: \Authy Desktop\Local Storage\ at 0x403a73  
[+] Decrypted string: \Soft\Authy Desktop Old\ at 0x403a8a  
[+] Decrypted string: \Authy Desktop\Local Storage\leveldb\ at 0x403aa1  
[+] Decrypted string: \Soft\Authy Desktop\ at 0x403ab8  
[+] Decrypted string: Soft: WinSCP at 0x403acf  
[+] Decrypted string: HostName at 0x403ae6  
[+] Decrypted string: PortNumber at 0x403afd  
[+] Decrypted string: UserName at 0x403b14  
[+] Decrypted string: Password at 0x403b2b  
[+] Decrypted string: Security at 0x403b42  
[+] Decrypted string: UseMasterPassword at 0x403b59  
[+] Decrypted string: Local Extension Settings at 0x403b70  
[+] Decrypted string: Sync Extension Settings at 0x403b87  
[+] Decrypted string: IndexedDB at 0x403b9e  
[+] Decrypted string: kjmoohlgoccakodicjjfebfofmlbljgfhk at 0x403bb4  
[+] Decrypted string: RoninWalletEdge at 0x403bcb  
[+] Decrypted string: sqlite3.dll at 0x403be1  
[+] Decrypted string: Version: at 0x403bf8  
[+] Decrypted string: Date: at 0x403c11  
[+] Decrypted string: MachineID: at 0x403c27  
[+] Decrypted string: GUID: at 0x403c3d  
[+] Decrypted string: HWID: at 0x403c53  
[+] Decrypted string: Path: at 0x403c69  
[+] Decrypted string: Work Dir: In memory at 0x403c80  
[+] Decrypted string: Windows: at 0x403c97  
[+] Decrypted string: Computer Name: at 0x403cae  
[+] Decrypted string: User Name: at 0x403cc4  
[+] Decrypted string: Display Resolution: at 0x403cdb  
[+] Decrypted string: Display Language: at 0x403cf2  
[+] Decrypted string: Keyboard Languages: at 0x403d09  
[+] Decrypted string: Local Time: at 0x403d20  
[+] Decrypted string: TimeZone: at 0x403d39  
[+] Decrypted string: [Hardware] at 0x403d4f  
[+] Decrypted string: Processor: at 0x403d65  
[+] Decrypted string: CPU Count: at 0x403d7b  
[+] Decrypted string: RAM: at 0x403d92  
[+] Decrypted string: VideoCard: at 0x403da8  
[+] Decrypted string: [Processes] at 0x403dbe  
[+] Decrypted string: [Software] at 0x403dd4  
[+] Decrypted string: \information.txt at 0x403deb  
[+] Decrypted string: %APPDATA% at 0x403e02  
[+] Decrypted string: %LOCALAPPDATA% at 0x403e19  
[+] Decrypted string: %USERPROFILE% at 0x403e2f  
[+] Decrypted string: %DESKTOP% at 0x403e46  
[+] Decrypted string: %DOCUMENTS% at 0x403e5c  
[+] Decrypted string: %PROGRAMFILES% at 0x403e73  
[+] Decrypted string: %PROGRAMFILES\_86% at 0x403e8a  
[+] Decrypted string: %RECENT% at 0x403ea1  
[+] Decrypted string: %DRIVE\_FIXED% at 0x403eb7

[+] Decrypted string: %DRIVE\_REMOVABLE% at 0x403ece  
[+] Decrypted string: \*%RECENT%\* at 0x403ee4  
[+] Decrypted string: \*%DRIVE\_FIXED%\* at 0x403efb  
[+] Decrypted string: \*%DRIVE\_REMOVABLE%\* at 0x403f12  
[+] Decrypted string: C:\Windows\ at 0x403f28  
[+] Decrypted string: C:\\Windows\ at 0x403f3f  
[+] Decrypted string: C:\\\\Windows\ at 0x403f55  
[+] Decrypted string: Software\Valve\Steam at 0x403f6c  
[+] Decrypted string: SteamPath at 0x403f83  
[+] Decrypted string: ssfn\* at 0x403f9a  
[+] Decrypted string: config.vdf at 0x403fb0  
[+] Decrypted string: DialogConfig.vdf at 0x403fc7  
[+] Decrypted string: DialogConfigOverlay\*.vdf at 0x403fde  
[+] Decrypted string: libraryfolders.vdf at 0x403ff5  
[+] Decrypted string: loginusers.vdf at 0x40400c  
[+] Decrypted string: Binance Desktop at 0x404023  
[+] Decrypted string: simple-storage.json at 0x40403a  
[+] Decrypted string: .finger-print.fp at 0x404051  
[+] Decrypted string: Bitcoin Core at 0x404068  
[+] Decrypted string: \Bitcoin\wallets\ at 0x40407f  
[+] Decrypted string: Bitcoin Core Old at 0x404096  
[+] Decrypted string: \Bitcoin\ at 0x4040ad  
[+] Decrypted string: wallet.dat at 0x4040c3  
[+] Decrypted string: \*wallet\*.dat at 0x4040da  
[+] Decrypted string: Dogecoin at 0x4040f1  
[+] Decrypted string: \Dogecoin\ at 0x404107  
[+] Decrypted string: Raven Core at 0x40411d  
[+] Decrypted string: \Raven\ at 0x404134  
[+] Decrypted string: Ledger Live at 0x40414a

Direction	Typ	Address	Text
Up	p	vdr_decrypt_strings_wrap+D	call vdr_decrypt_strings; HAL9TH
Up	p	vdr_decrypt_strings_wrap+24	call vdr_decrypt_strings; JohnDoe
Up	p	vdr_decrypt_strings_wrap+38	call vdr_decrypt_strings; LoadLibraryA
Up	p	vdr_decrypt_strings_wrap+52	call vdr_decrypt_strings; lstrcatA
Up	p	vdr_decrypt_strings_wrap+69	call vdr_decrypt_strings; GetProcAddress
Up	p	vdr_decrypt_strings_wrap+80	call vdr_decrypt_strings; Sleep
Up	p	vdr_decrypt_strings_wrap+97	call vdr_decrypt_strings; GetSystemTime
Up	p	vdr_decrypt_strings_wrap+AE	call vdr_decrypt_strings; ExitProcess
Up	p	vdr_decrypt_strings_wrap+C5	call vdr_decrypt_strings; GetCurrentProcess
Up	p	vdr_decrypt_strings_wrap+DC	call vdr_decrypt_strings; VirtualAllocExNuma
Up	p	vdr_decrypt_strings_wrap+F3	call vdr_decrypt_strings; VirtualAlloc
Up	p	vdr_decrypt_strings_wrap+10A	call vdr_decrypt_strings; VirtualFree
Up	p	vdr_decrypt_strings_wrap+121	call vdr_decrypt_strings; lstrcmpiW
Up	p	vdr_decrypt_strings_wrap+138	call vdr_decrypt_strings; LocalAlloc
Up	p	vdr_decrypt_strings_wrap+14F	call vdr_decrypt_strings; GetComputerNameA
Up	p	vdr_decrypt_strings_wrap+166	call vdr_decrypt_strings; advapi32.dll
Up	p	vdr_decrypt_strings_wrap+17D	call vdr_decrypt_strings; GetUserNameA
Up	p	vdr_decrypt_strings_wrap+194	call vdr_decrypt_strings; kernel32.dll
Up	p	vdr_decrypt_strings_wrap_2+12	call vdr_decrypt_strings; Wallets
Up	p	vdr_decrypt_strings_wrap_2+28	call vdr_decrypt_strings; Plugins
Up	p	vdr_decrypt_strings_wrap_2+41	call vdr_decrypt_strings; keystore
Up	p	vdr_decrypt_strings_wrap_2+58	call vdr_decrypt_strings; Ethereum"
Up	p	vdr_decrypt_strings_wrap_2+6F	call vdr_decrypt_strings; \Ethereum\
Up	p	vdr_decrypt_strings_wrap_2+85	call vdr_decrypt_strings; Electrum
Up	p	vdr_decrypt_strings_wrap_2+9C	call vdr_decrypt_strings; \Electrum\wallets\
Up	p	vdr_decrypt_strings_wrap_2+B5	call vdr_decrypt_strings; ElectrumLTC
Up	p	vdr_decrypt_strings_wrap_2+CC	call vdr_decrypt_strings; \Electrum-LTC\wallets\
Up	p	vdr_decrypt_strings_wrap_2+E3	call vdr_decrypt_strings; Exodus
Up	p	vdr_decrypt_strings_wrap_2+F9	call vdr_decrypt_strings; \Exodus\
Up	p	vdr_decrypt_strings_wrap_2+110	call vdr_decrypt_strings; exodus.conf.json
Up	p	vdr_decrypt_strings_wrap_2+127	call vdr_decrypt_strings; window-state.json
Up	p	vdr_decrypt_strings_wrap_2+13E	call vdr_decrypt_strings; \Exodus\exodus.wallet\
Up	p	vdr_decrypt_strings_wrap_2+155	call vdr_decrypt_strings; passphrase.json
Up	p	vdr_decrypt_strings_wrap_2+16C	call vdr_decrypt_strings; seed.seco
Up	p	vdr_decrypt_strings_wrap_2+183	call vdr_decrypt_strings; info.seco
Up	p	vdr_decrypt_strings_wrap_2+19A	call vdr_decrypt_strings; ElectronCash
Up	p	vdr_decrypt_strings_wrap_2+1B1	call vdr_decrypt_strings; \ElectronCash\wallets\
Up	p	vdr_decrypt_strings_wrap_2+1C8	call vdr_decrypt_strings; default_wallet
Up	p	vdr_decrypt_strings_wrap_2+1DF	call vdr_decrypt_strings; MultiDoge
Up	p	vdr_decrypt_strings_wrap_2+1F5	call vdr_decrypt_strings; \MultiDoge\
Up	p	vdr_decrypt_strings_wrap_2+20C	call vdr_decrypt_strings; multidoge.wallet
Up	p	vdr_decrypt_strings_wrap_2+223	call vdr_decrypt_strings; Jaxx_Desktop_Old
Up	p	vdr_decrypt_strings_wrap_2+23A	call vdr_decrypt_strings; \jaxx\Local Storage\
Up	p	vdr_decrypt_strings_wrap_2+251	call vdr_decrypt_strings; file_0.localstorage
Up	p	vdr_decrypt_strings_wrap_2+268	call vdr_decrypt_strings; Atomic
Up	p	vdr_decrypt_strings_wrap_2+27F	call vdr_decrypt_strings; \atomic\Local Storage\leveldb\
Up	p	vdr_decrypt_strings_wrap_2+296	call vdr_decrypt_strings; *.log
Up	p	vdr_decrypt_strings_wrap_2+2AC	call vdr_decrypt_strings; CURRENT
Up	p	vdr_decrypt_strings_wrap_2+2C3	call vdr_decrypt_strings; LOCK

The global variables are renamed corresponding to the decoded strings as follows:



```

// #STR: "MNLNPK", "YPFTTRV", "G6MUFPIQNJQ", "BNQBVR82", " .=%053Ls",
"DPKU0540BD4R2J", "RMPZX", "U6869B6N6I0TC", "VZS0W2FKU7H", "MS2Y26EV5306FTKSR"
const CHAR *__stdcall vdr_decrypt_strings_wrap()
{
    // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

    str_HAL9TH = vdr_decrypt_strings(6u, &xor_key, "MNLNPK");
    str_JohnDoe = vdr_decrypt_strings(7u, byte_43802C, "YPFTTRV");
    str_LoadLibraryA = vdr_decrypt_strings(0xCu, str_Y1903, "G6MUFPIQNJQ");
    str_lstrcatA = vdr_decrypt_strings(8u, " .=%053Ls", "BNQBVR82");
    str_GetProcAddress = vdr_decrypt_strings(0xEu, byte_43807C, "DPKU0540BD4R2J");
    str_Sleep = vdr_decrypt_strings(5u, byte_438094, "RMPZX");
    str_GetSystemTime = vdr_decrypt_strings(0xDu, byte_4380AC, "U6869B6N6I0TC");
    str_ExitProcess = vdr_decrypt_strings(0xBu, byte_4380C8, "VZS0W2FKU7H");
    str_GetCurrentProcess = vdr_decrypt_strings(0x11u, str_6F, "MS2Y26EV5306FTKSR");
    str_VirtualAllocExNuma = vdr_decrypt_strings(0x12u, byte_438110,
"R8SXT26D010WUN981T");
    str_VirtualAlloc = vdr_decrypt_strings(0xCu, str_4, "QJIVAD2YIH2N");
    str_VirtualFree = vdr_decrypt_strings(0xBu, byte_438150, "HLKX3WPT306");
    str_lstrcmpiW = vdr_decrypt_strings(9u, ":11<[!!9o", "VBEN8LQP8");
    str_LocalAlloc = vdr_decrypt_strings(0xAu, byte_438180, "N93IJ58045");
    str_GetComputerNameA = vdr_decrypt_strings(0x10u, byte_4381A0, "UYKNTPM7TMTH00NX");
    str_advapi32_dll = vdr_decrypt_strings(0xCu, str_5QFUX, "T504N1249IRB");
    str_GetUserNameA = vdr_decrypt_strings(0xCu, str_R, "N7XAZ7FHKKV8");
    result = vdr_decrypt_strings(0xCu, "="+D-**zq\x1B3 (" , "VN6COFIC5WLD");//
kernel32.dll
    str_kernel32_dll = result;
    return result;
}

```

## Rename global vars related to API functions

---

Next, vidar will use the **GetProcAddress** function to get the addresses of all the APIs it uses during execution. We can write an **IDAPython** script to parse the list of decrypted API functions and perform renaming of global variables.

Here are the results:



```
[*] Trying to rename global var to API function name:
[+] Set API name: NSS_Init at 0x414ae3
[+] Set API name: NSS_Shutdown at 0x414afa
[+] Set API name: PK11_GetInternalKeySlot at 0x414b11
[+] Set API name: PK11_FreeSlot at 0x414b28
[+] Set API name: PK11_Authenticate at 0x414b3f
[+] Set API name: PK11SDR_Decrypt at 0x414b56
[+] Set API name: PK11SDR_Decrypt at 0x41a9b3
[+] Set API name: PK11SDR_Decrypt at 0x41a9b3
[+] Set API name: Sleep at 0x41a9d1
[+] Set API name: GetSystemTime at 0x41a9e8
[+] Set API name: ExitProcess at 0x41a9ff
[+] Set API name: GetCurrentProcess at 0x41aa16
[+] Set API name: VirtualAllocExNuma at 0x41aa2d
[+] Set API name: VirtualAlloc at 0x41aa44
[+] Set API name: VirtualFree at 0x41aa5b
[+] Set API name: lstrcpw at 0x41aa72
[+] Set API name: LocalAlloc at 0x41aa89
[+] Set API name: GetComputerNameA at 0x41aaa0
[+] Set API name: GetComputerNameA at 0x41aaa0
[+] Set API name: GetUserNameA at 0x41aac8
[+] Set API name: CreateThread at 0x41aaeb
[+] Set API name: GlobalMemoryStatusEx at 0x41ab02
[+] Set API name: IsWow64Process at 0x41ab19
[+] Set API name: GetUserDefaultLocaleName at 0x41ab30
[+] Set API name: GetSystemInfo at 0x41ab47
[+] Set API name: WideCharToMultiByte at 0x41ab5e
[+] Set API name: LocalFree at 0x41ab75
[+] Set API name: HeapAlloc at 0x41ab8c
[+] Set API name: GetProcessHeap at 0x41aba3
[+] Set API name: CreateFileA at 0x41abba
[+] Set API name: GetFileSize at 0x41abd1
[+] Set API name: ReadFile at 0x41abe8
[+] Set API name: CloseHandle at 0x41abff
[+] Set API name: GetLogicalDriveStringsA at 0x41ac16
[+] Set API name: lstrlenA at 0x41ac2d
[+] Set API name: GetDriveTypeA at 0x41ac44
[+] Set API name: lstrcpyA at 0x41ac5b
[+] Set API name: MultiByteToWideChar at 0x41ac72
[+] Set API name: FindFirstFileA at 0x41ac89
[+] Set API name: FindNextFileA at 0x41aca0
[+] Set API name: FindClose at 0x41acb7
[+] Set API name: GetLastError at 0x41acce
[+] Set API name: lstrcpynA at 0x41ace5
[+] Set API name: GlobalLock at 0x41acfc
[+] Set API name: GlobalSize at 0x41ad13
[+] Set API name: FreeLibrary at 0x41ad2a
[+] Set API name: GetLocaleInfoA at 0x41ad41
[+] Set API name: GetCurrentProcessId at 0x41ad58
[+] Set API name: OpenProcess at 0x41ad6f
[+] Set API name: GetFileSizeEx at 0x41ad86
[+] Set API name: GetTimeZoneInformation at 0x41ad9d
```

[+] Set API name: TzSpecificLocalTimeToSystemTime at 0x41adb4  
[+] Set API name: CopyFileA at 0x41adcb  
[+] Set API name: DeleteFileA at 0x41ade2  
[+] Set API name: GetCurrentDirectoryA at 0x41adf9  
[+] Set API name: SetFilePointer at 0x41ae10  
[+] Set API name: HeapFree at 0x41ae27  
[+] Set API name: SystemTimeToFileTime at 0x41ae3e  
[+] Set API name: GetLocalTime at 0x41ae55  
[+] Set API name: SetFileTime at 0x41ae6c  
[+] Set API name: WriteFile at 0x41ae83  
[+] Set API name: GetFileAttributesA at 0x41ae9a  
[+] Set API name: GetFileAttributesW at 0x41aeb1  
[+] Set API name: LocalFileTimeToFileTime at 0x41aec8  
[+] Set API name: MapViewOfFile at 0x41aedf  
[+] Set API name: UnmapViewOfFile at 0x41aef6  
[+] Set API name: FileTimeToSystemTime at 0x41af0d  
[+] Set API name: CreateFileMappingA at 0x41af24  
[+] Set API name: GetFileInformationByHandle at 0x41af3b  
[+] Set API name: GetEnvironmentVariableA at 0x41af52  
[+] Set API name: SetEnvironmentVariableA at 0x41af69  
[+] Set API name: GetTickCount at 0x41af80  
[+] Set API name: OpenEventA at 0x41af97  
[+] Set API name: CreateEventA at 0x41afae  
[+] Set API name: CreateToolhelp32Snapshot at 0x41afc5  
[+] Set API name: Process32First at 0x41afdc  
[+] Set API name: Process32Next at 0x41aff3  
[+] Set API name: GetWindowsDirectoryA at 0x41b00a  
[+] Set API name: GetVolumeInformationA at 0x41b021  
[+] Set API name: BCryptCloseAlgorithmProvider at 0x41b0fb  
[+] Set API name: BCryptDestroyKey at 0x41b112  
[+] Set API name: BCryptOpenAlgorithmProvider at 0x41b129  
[+] Set API name: BCryptSetProperty at 0x41b140  
[+] Set API name: BCryptGenerateSymmetricKey at 0x41b157  
[+] Set API name: BCryptDecrypt at 0x41b16e  
[+] Set API name: CryptUnprotectData at 0x41b189  
[+] Set API name: CryptBinaryToStringA at 0x41b1a0  
[+] Set API name: CryptStringToBinaryA at 0x41b1b7  
[+] Set API name: RegOpenKeyExA at 0x41b1d6  
[+] Set API name: RegQueryValueExA at 0x41b1ed  
[+] Set API name: RegCloseKey at 0x41b204  
[+] Set API name: RegOpenKeyExW at 0x41b21b  
[+] Set API name: RegGetValueW at 0x41b232  
[+] Set API name: RegEnumKeyExA at 0x41b249  
[+] Set API name: RegGetValueA at 0x41b260  
[+] Set API name: GetUserNameA at 0x41b277  
[+] Set API name: GetCurrentHwProfileA at 0x41b28e  
[+] Set API name: RegEnumValueA at 0x41b2a5  
[+] Set API name: GetFileSecurityA at 0x41b2bc  
[+] Set API name: OpenProcessToken at 0x41b2d3  
[+] Set API name: DuplicateToken at 0x41b2ea  
[+] Set API name: MapGenericMask at 0x41b301  
[+] Set API name: AccessCheck at 0x41b318

[+] Set API name: InternetCloseHandle at 0x41b337  
[+] Set API name: InternetReadFile at 0x41b34e  
[+] Set API name: HttpSendRequestA at 0x41b365  
[+] Set API name: HttpOpenRequestA at 0x41b37c  
[+] Set API name: InternetConnectA at 0x41b393  
[+] Set API name: InternetOpenA at 0x41b3aa  
[+] Set API name: HttpAddRequestHeadersA at 0x41b3c1  
[+] Set API name: HttpQueryInfoA at 0x41b3d8  
[+] Set API name: InternetSetFilePointer at 0x41b3ef  
[+] Set API name: InternetOpenUrlA at 0x41b406  
[+] Set API name: InternetSetOptionA at 0x41b41d  
[+] Set API name: DeleteUrlCacheEntry at 0x41b434  
[+] Set API name: InternetCrackUrlA at 0x41b44b  
[+] Set API name: CreateCompatibleBitmap at 0x41b46a  
[+] Set API name: SelectObject at 0x41b481  
[+] Set API name: BitBlt at 0x41b498  
[+] Set API name: DeleteObject at 0x41b4af  
[+] Set API name: CreateDCA at 0x41b4c6  
[+] Set API name: GetDeviceCaps at 0x41b4dd  
[+] Set API name: CreateCompatibleDC at 0x41b4f4  
[+] Set API name: CoCreateInstance at 0x41b50f  
[+] Set API name: CoUninitialize at 0x41b526  
[+] Set API name: CoInitialize at 0x41b53d  
[+] Set API name: CreateStreamOnHGlobal at 0x41b554  
[+] Set API name: GetHGlobalFromStream at 0x41b56b  
[+] Set API name: GetDesktopWindow at 0x41b58a  
[+] Set API name: ReleaseDC at 0x41b5a1  
[+] Set API name: GetKeyboardLayoutList at 0x41b5b8  
[+] Set API name: CharToOemA at 0x41b5cf  
[+] Set API name: GetDC at 0x41b5e6  
[+] Set API name: wsprintfA at 0x41b5fd  
[+] Set API name: EnumDisplayDevicesA at 0x41b614  
[+] Set API name: GetSystemMetrics at 0x41b62b  
[+] Set API name: GetWindowRect at 0x41b642  
[+] Set API name: GetWindowDC at 0x41b659  
[+] Set API name: CloseWindow at 0x41b670  
[+] Set API name: GetModuleFileNameExA at 0x41b68b  
[+] Set API name: GetModuleBaseNameA at 0x41b6a2  
[+] Set API name: EnumProcessModules at 0x41b6b9  
[+] Set API name: ShellExecuteExA at 0x41b6d4  
[+] Set API name: SHFileOperationA at 0x41b6eb  
[+] Set API name: SHGetFolderPathA at 0x41b702  
[+] Set API name: PathMatchSpecW at 0x41b721  
[+] Set API name: PathMatchSpecA at 0x41b738  
[+] Set API name: StrCmpCA at 0x41b74f  
[+] Set API name: StrCmpCW at 0x41b766  
[+] Set API name: StrStrA at 0x41b77d  
[+] Set API name: PathFindFileNameA at 0x41b794  
[+] Set API name: SymMatchString at 0x41b7af  
[+] Set API name: GdipGetImageEncodersSize at 0x41b7ce  
[+] Set API name: GdipGetImageEncoders at 0x41b7e5  
[+] Set API name: GdipCreateBitmapFromHBITMAP at 0x41b7fc

[+] Set API name: GdiplusStartup at 0x41b813  
 [+] Set API name: GdiplusShutdown at 0x41b82a  
 [+] Set API name: GdiSaveImageToStream at 0x41b841  
 [+] Set API name: GdiDisposeImage at 0x41b858  
 [+] Set API name: GdiFree at 0x41b86f

Direction	Typ	Address	Text
Up	r	vdr_retrieve_export_funcs_of_nss3_dll+CF	call GetProcAddress_0; NSS_Init
Up	r	vdr_retrieve_export_funcs_of_nss3_dll+E6	call GetProcAddress_0; NSS_Shutdown
Up	r	vdr_retrieve_export_funcs_of_nss3_dll+FD	call GetProcAddress_0; PK11_GetInternalKeySlot
Up	r	vdr_retrieve_export_funcs_of_nss3_dll+114	call GetProcAddress_0; PK11_FreeSlot
Up	r	vdr_retrieve_export_funcs_of_nss3_dll+12B	call GetProcAddress_0; PK11_Authenticate
Up	r	vdr_retrieve_export_funcs_of_nss3_dll+142	call GetProcAddress_0; PK11SDR_Decrypt
Up	w	vdr_retrieve_addr_of_kernel32_advapi32_API_funcs+42	mov GetProcAddress_0, eax
Up	r	vdr_retrieve_addr_of_kernel32_advapi32_API_funcs+60	call GetProcAddress_0; Sleep
Up	r	vdr_retrieve_addr_of_kernel32_advapi32_API_funcs+77	call GetProcAddress_0; GetSystemTime
Up	r	vdr_retrieve_addr_of_kernel32_advapi32_API_funcs+8E	call GetProcAddress_0; ExitProcess
Up	r	vdr_retrieve_addr_of_kernel32_advapi32_API_funcs+A5	call GetProcAddress_0; GetCurrentProcess
Up	r	vdr_retrieve_addr_of_kernel32_advapi32_API_funcs+BC	call GetProcAddress_0; VirtualAllocExNuma
Up	r	vdr_retrieve_addr_of_kernel32_advapi32_API_funcs+D3	call GetProcAddress_0; VirtualAlloc
Do...	r	vdr_retrieve_addr_of_kernel32_advapi32_API_funcs+EA	call GetProcAddress_0; VirtualFree
Do...	r	vdr_retrieve_addr_of_kernel32_advapi32_API_funcs+101	call GetProcAddress_0; IstrcmpiW
Do...	r	vdr_retrieve_addr_of_kernel32_advapi32_API_funcs+118	call GetProcAddress_0; LocalAlloc
Do...	r	vdr_retrieve_addr_of_kernel32_advapi32_API_funcs+12F	call GetProcAddress_0; GetComputerNameA
Do...	r	vdr_retrieve_addr_of_kernel32_advapi32_API_funcs+157	call GetProcAddress_0; GetUserNameA
Do...	r	vdr_retrieve_all_required_api_funcs+14	call GetProcAddress_0; CreateThread
Do...	r	vdr_retrieve_all_required_api_funcs+2B	call GetProcAddress_0; GlobalMemoryStatusEx
Do...	r	vdr_retrieve_all_required_api_funcs+42	call GetProcAddress_0; IsWow64Process
Do...	r	vdr_retrieve_all_required_api_funcs+59	call GetProcAddress_0; GetUserDefaultLocaleName
Do...	r	vdr_retrieve_all_required_api_funcs+70	call GetProcAddress_0; GetSystemInfo
Do...	r	vdr_retrieve_all_required_api_funcs+87	call GetProcAddress_0; WideCharToMultiByte
Do...	r	vdr_retrieve_all_required_api_funcs+9E	call GetProcAddress_0; LocalFree
Do...	r	vdr_retrieve_all_required_api_funcs+B5	call GetProcAddress_0; HeapAlloc
Do...	r	vdr_retrieve_all_required_api_funcs+CC	call GetProcAddress_0; GetProcessHeap
Do...	r	vdr_retrieve_all_required_api_funcs+E3	call GetProcAddress_0; CreateFileA
Do...	r	vdr_retrieve_all_required_api_funcs+FA	call GetProcAddress_0; GetFileSize
Do...	r	vdr_retrieve_all_required_api_funcs+111	call GetProcAddress_0; ReadFile
Do...	r	vdr_retrieve_all_required_api_funcs+128	call GetProcAddress_0; CloseHandle
Do...	r	vdr_retrieve_all_required_api_funcs+13F	call GetProcAddress_0; GetLogicalDriveStringsA
Do...	r	vdr_retrieve_all_required_api_funcs+156	call GetProcAddress_0; IstrlenA
Do...	r	vdr_retrieve_all_required_api_funcs+16D	call GetProcAddress_0; GetDriveTypeA
Do...	r	vdr_retrieve_all_required_api_funcs+184	call GetProcAddress_0; IstrcpyA
Do...	r	vdr_retrieve_all_required_api_funcs+19B	call GetProcAddress_0; MultiByteToWideChar
Do...	r	vdr_retrieve_all_required_api_funcs+1B2	call GetProcAddress_0; FindFirstFileA
Do...	r	vdr_retrieve_all_required_api_funcs+1C9	call GetProcAddress_0; FindNextFileA
Do...	r	vdr_retrieve_all_required_api_funcs+1E0	call GetProcAddress_0; FindClose
Do...	r	vdr_retrieve_all_required_api_funcs+1F7	call GetProcAddress_0; GetLastError
Do...	r	vdr_retrieve_all_required_api_funcs+20E	call GetProcAddress_0; IstrcpynA
Do...	r	vdr_retrieve_all_required_api_funcs+225	call GetProcAddress_0; GlobalLock
Do...	r	vdr_retrieve_all_required_api_funcs+23C	call GetProcAddress_0; GlobalSize
Do...	r	vdr_retrieve_all_required_api_funcs+253	call GetProcAddress_0; FreeLibrary
Do...	r	vdr_retrieve_all_required_api_funcs+26A	call GetProcAddress_0; GetLocaleInfoA
Do...	r	vdr_retrieve_all_required_api_funcs+281	call GetProcAddress_0; GetCurrentProcessId
Do...	r	vdr_retrieve_all_required_api_funcs+298	call GetProcAddress_0; OpenProcess
Do...	r	vdr_retrieve_all_required_api_funcs+2AF	call GetProcAddress_0; GetFileSizeEx
Do...	r	vdr_retrieve_all_required_api_funcs+2C6	call GetProcAddress_0; GetTimeZoneInformation
Do...	r	vdr_retrieve_all_required_api_funcs+2DD	call GetProcAddress_0; TzSpecificLocalTimeToSystemTime

```

FARPROC __stdcall vdr_retrieve_addr_of_kernel32_advapi32_API_funcs()
{
    // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

    kernel32_dll_hdl = LoadLibraryA(str_kernel32_dll);
    g_kernel32_dll_hdl = kernel32_dll_hdl;
    if ( kernel32_dll_hdl )
    {
        LoadLibraryA_1 = GetProcAddress(kernel32_dll_hdl, str_LoadLibraryA);
        GetProcAddress_0 = GetProcAddress(g_kernel32_dll_hdl, str_GetProcAddress);
        lstrcatA = GetProcAddress_0(g_kernel32_dll_hdl, str_lstrcatA);
        Sleep_1 = GetProcAddress_0(g_kernel32_dll_hdl, str_Sleep);
        GetSystemTime = GetProcAddress_0(g_kernel32_dll_hdl, str_GetSystemTime);
        ExitProcess_1 = GetProcAddress_0(g_kernel32_dll_hdl, str_ExitProcess);
        GetCurrentProcess_1 = GetProcAddress_0(g_kernel32_dll_hdl,
str_GetCurrentProcess);
        VirtualAllocExNuma = GetProcAddress_0(g_kernel32_dll_hdl,
str_VirtualAllocExNuma);
        VirtualAlloc = GetProcAddress_0(g_kernel32_dll_hdl, str_VirtualAlloc);
        VirtualFree = GetProcAddress_0(g_kernel32_dll_hdl, str_VirtualFree);
        *lstrcmpiW = GetProcAddress_0(g_kernel32_dll_hdl, str_lstrcmpiW);
        LocalAlloc_1 = GetProcAddress_0(g_kernel32_dll_hdl, str_LocalAlloc);
        GetComputerNameA = GetProcAddress_0(g_kernel32_dll_hdl, str_GetComputerNameA);
    }
    result = LoadLibraryA_1(str_advapi32_dll);
    g_advapi32_dll_hdl = result;
    if ( !result )
    {
        return result;
    }
    result = GetProcAddress_0(result, str_GetUserNameA);
    GetUserNameA_1 = result;
    return result;
}

```

Some of other VidarStealer codes here:

<https://github.com/m4now4r/VidarStealer/tree/main/some%20pseudo-code>

End!

m4n0w4r