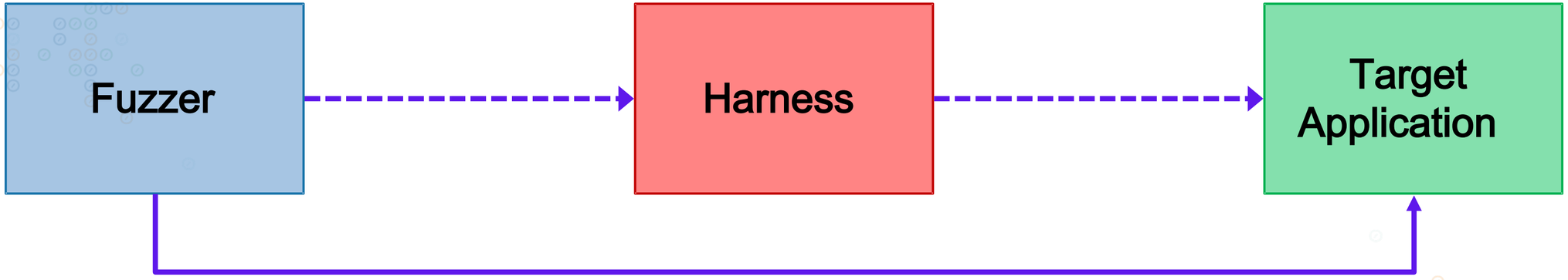
MANTODEA
SECURITY

Finding 0days with snapshot-based fuzzing

Presented By: Niels Pfau

The Fuzzing Process

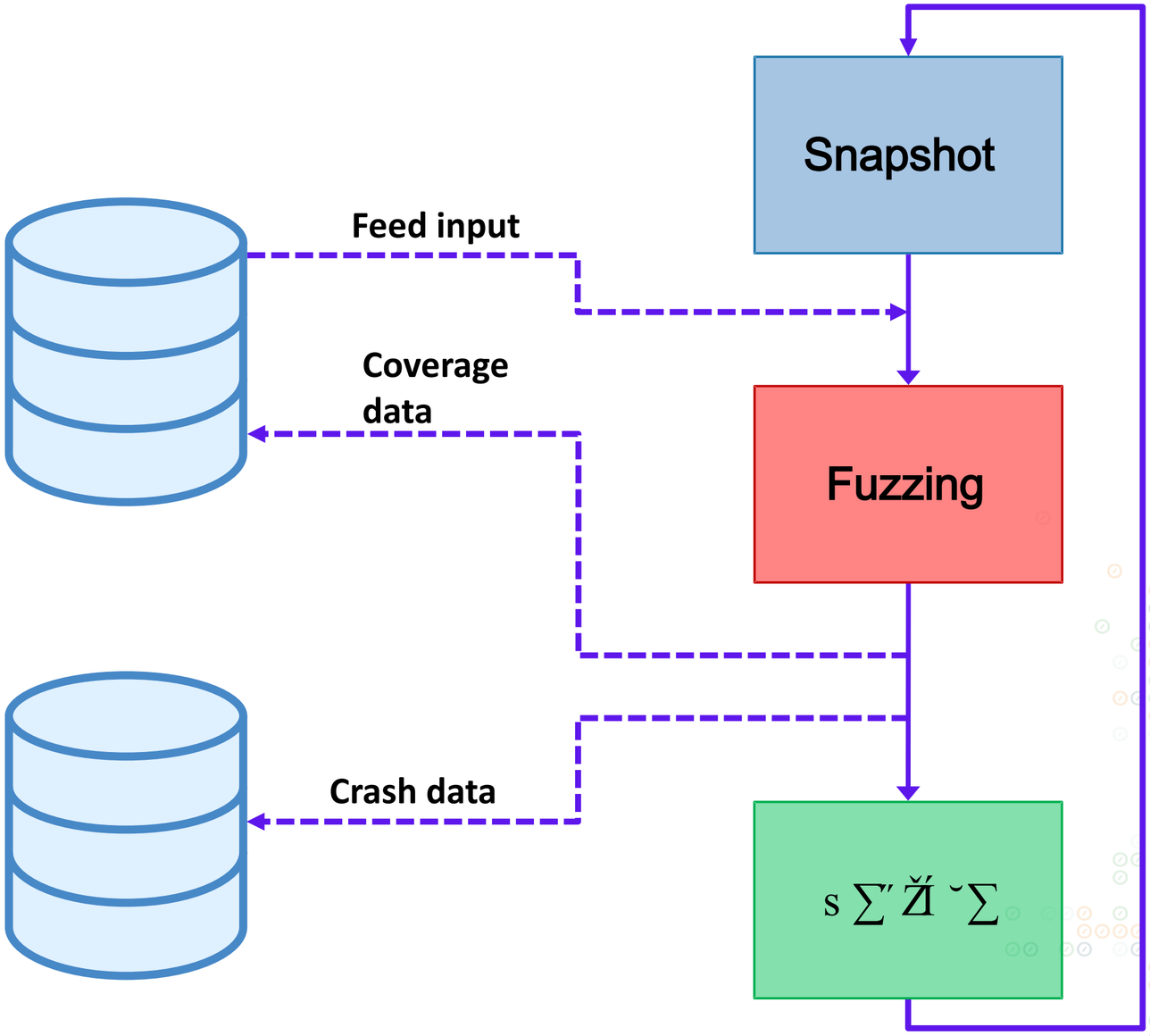
Traditional vs. Snapshot-based



UŒ¢• Ê• ‹« ¥»¥‡«

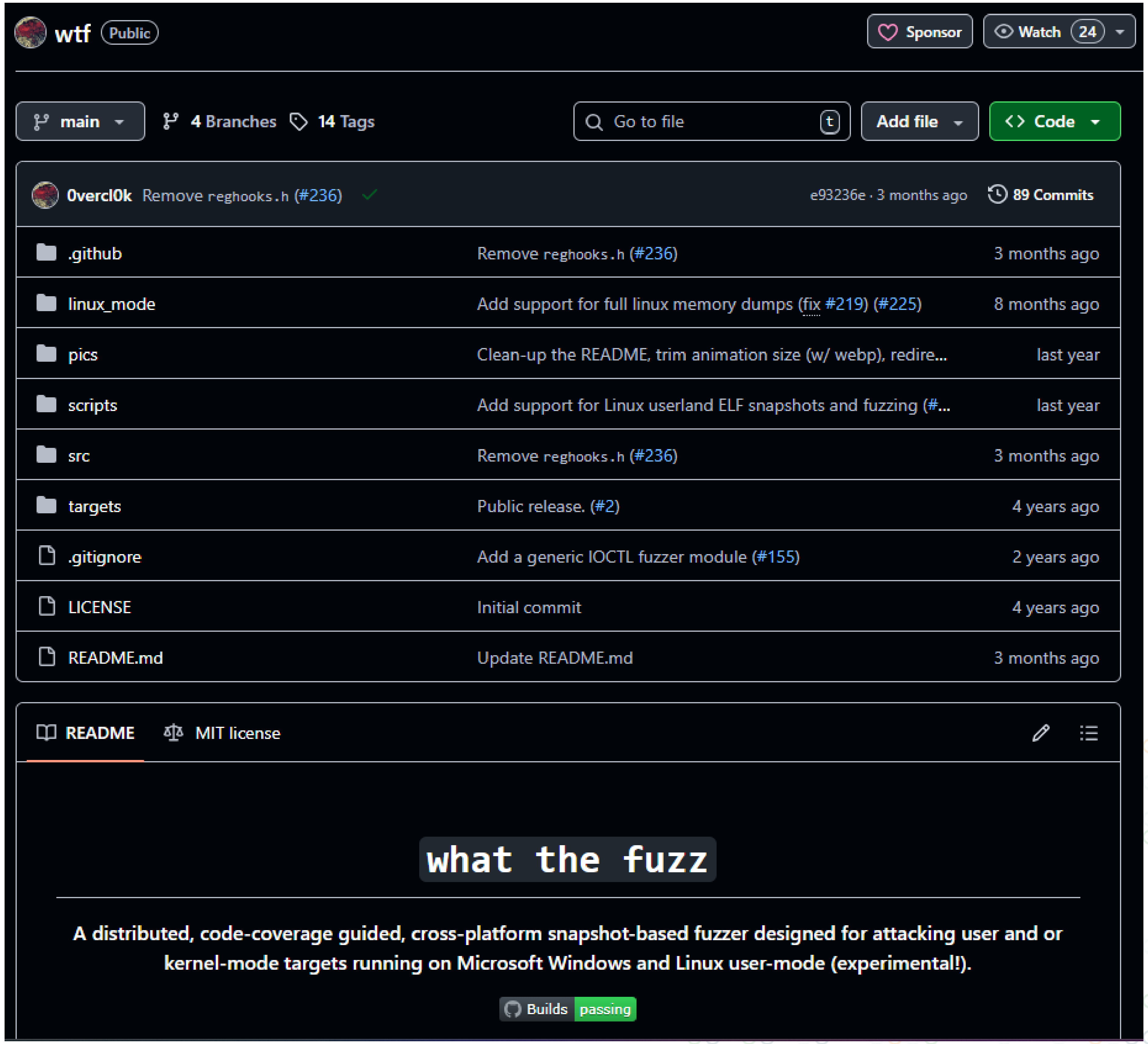
Complex States

Hard-to-reach code


Snapshot
Feed input
Coverage data
Fuzzing
Crash data
s ∑′ ŽÍ ˘∑

ŏ LLĂĆĆḷś ẑĵ ūū

A snapshot-based fuzzer for Windows applications



https://github.com/0vercl0k/wt
f

CVE-2024-22058 Detail

Description

A buffer overflow allows a low privilege user on the local machine that has the EPM Agent installed to execute arbitrary code with elevated permissions in Ivanti EPM 2021.1 and older.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NVD	**NIST:** NVD	**Base Score:** N/A	NVD assessment not yet provided.
R	**CNA:** HackerOne	**Base Score:** 7.8 HIGH	**Vector:** CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

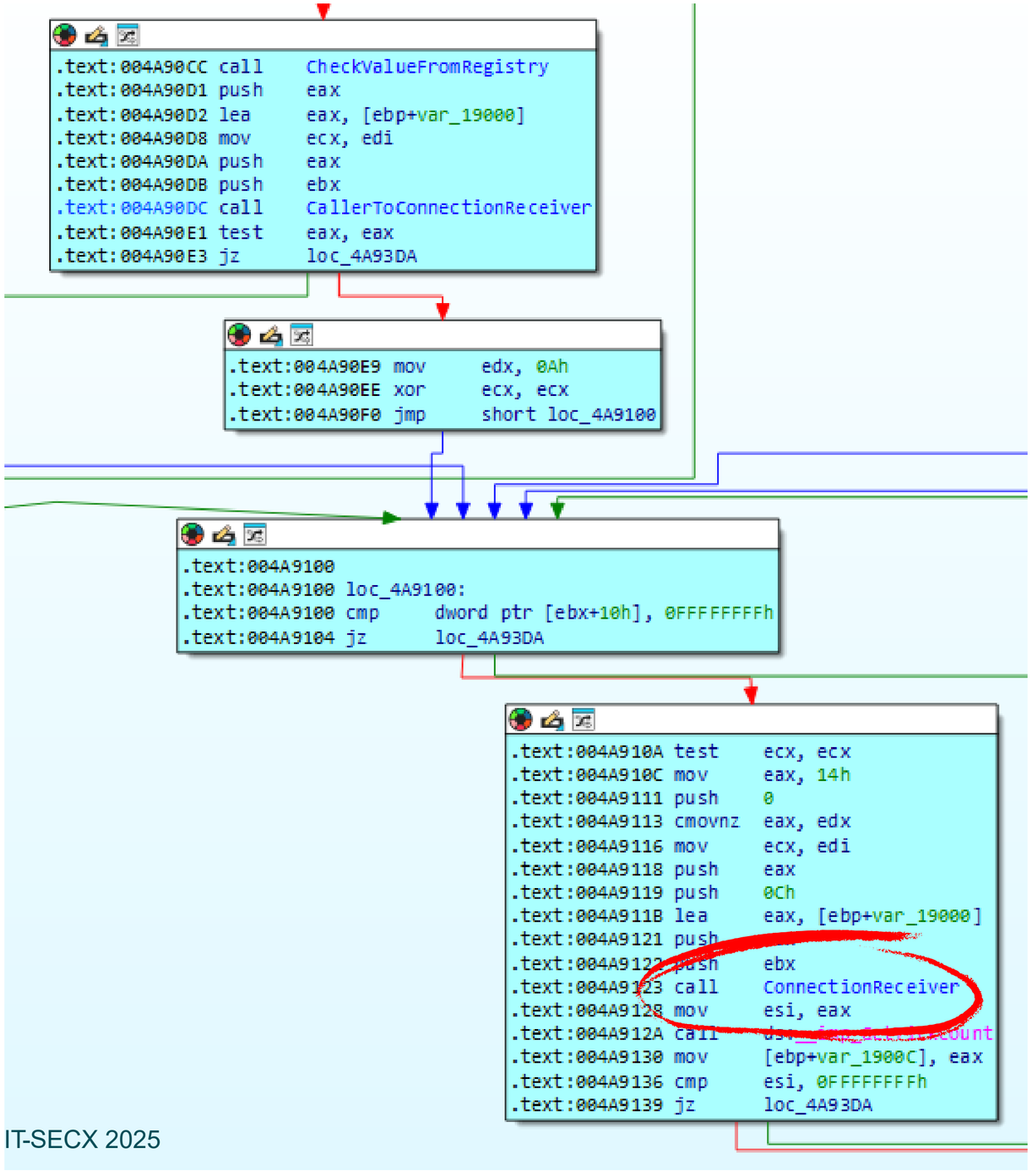
Unauthorized Access or You Are Not Logged In

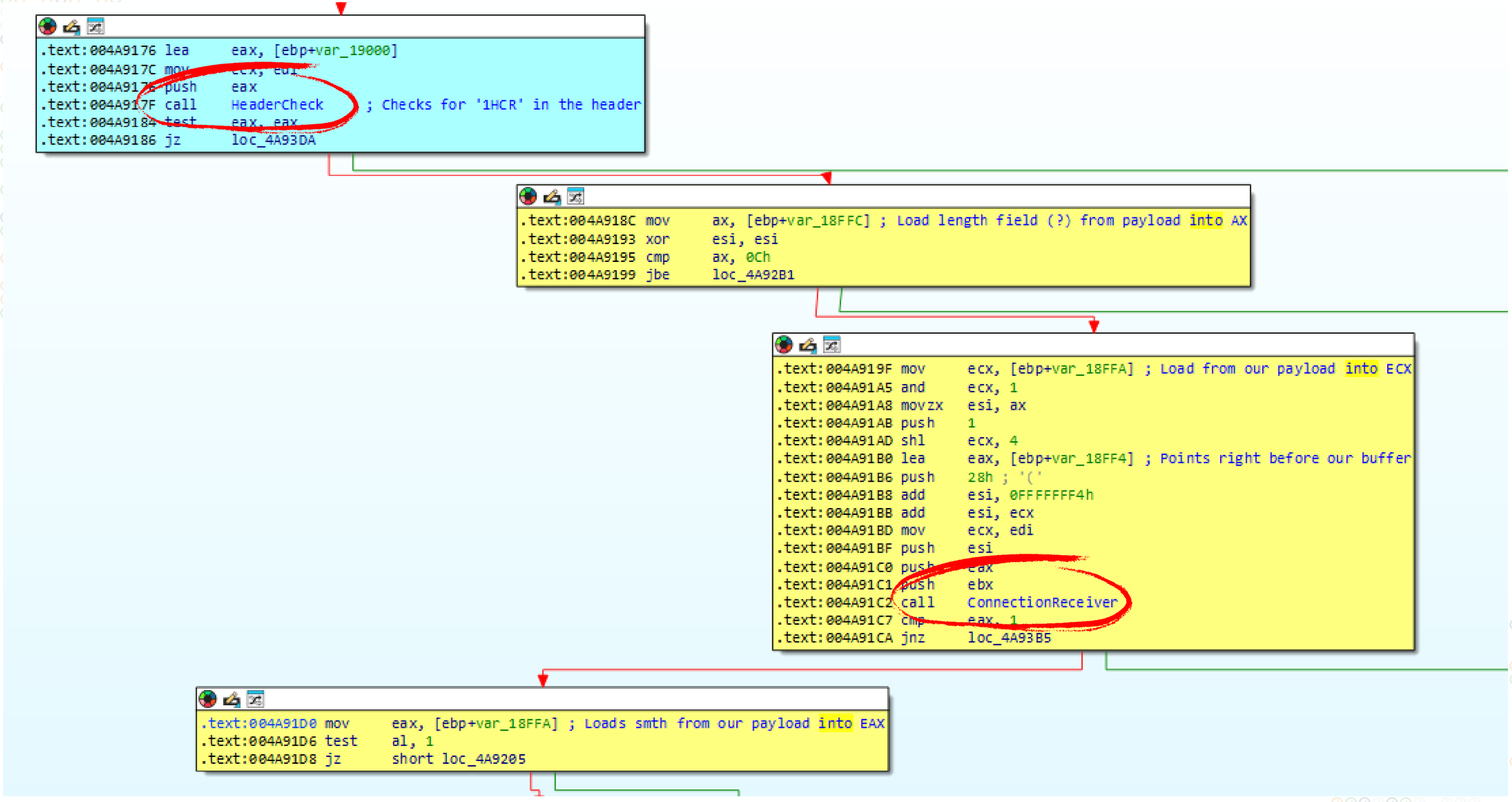
Your access to the Ivanti knowledge base doesn't allow you to view this knowledge article or you need to be logged in.

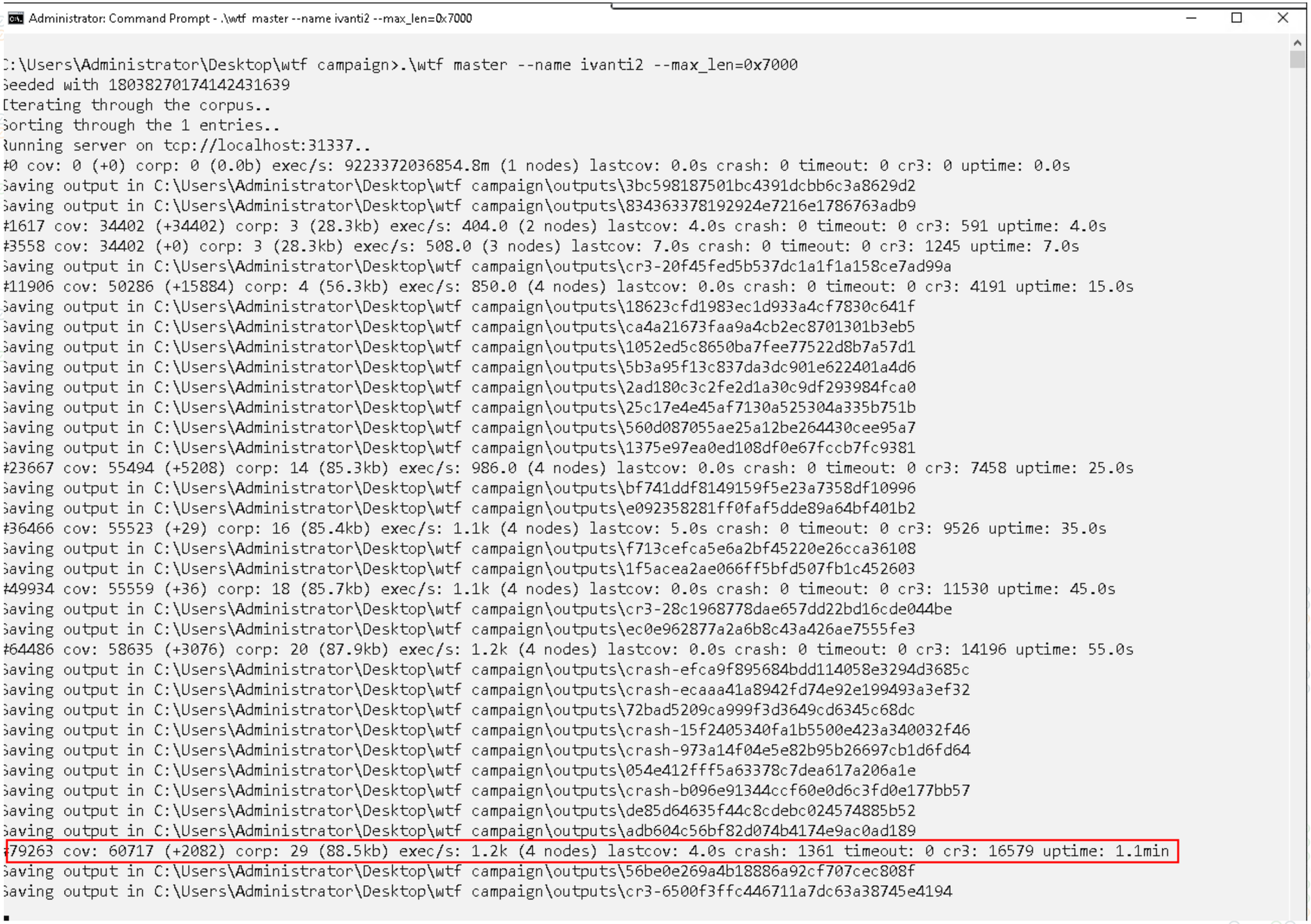
PLEASE NOTE: Only customers with an active maintenance contract can access the Ivanti product DOWNLOADS, KNOWN ISSUE articles and other specific customer content.

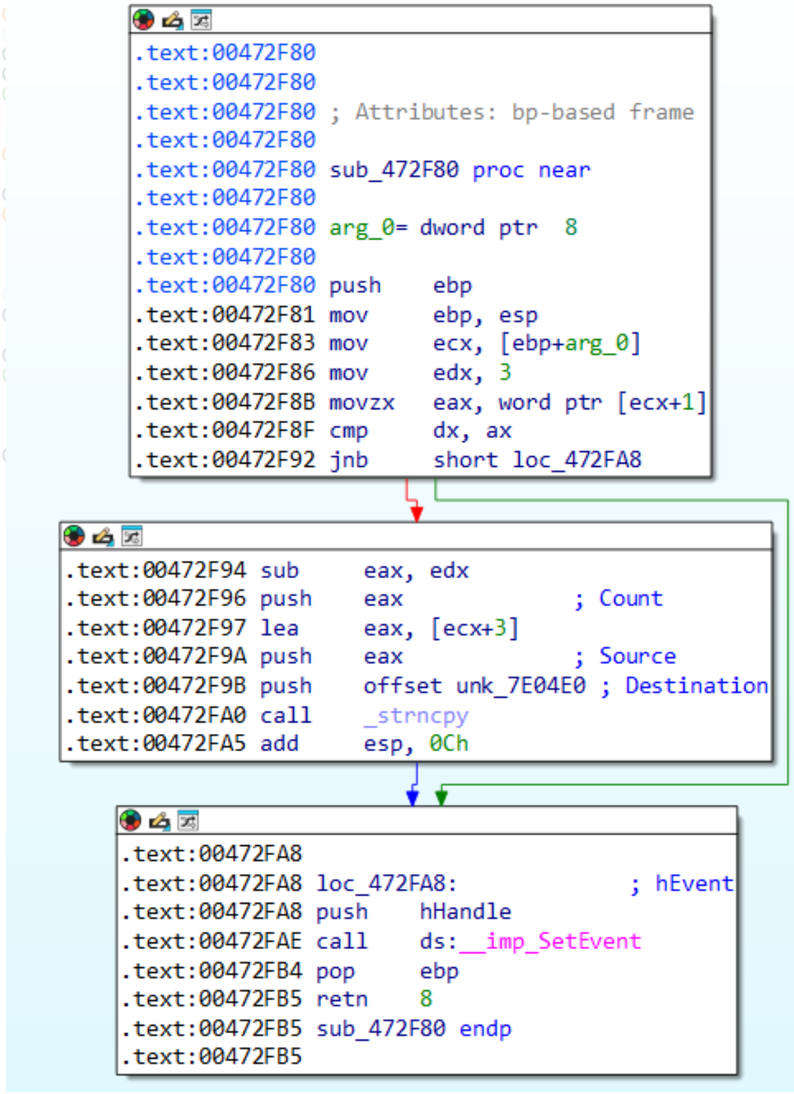
If you believe you should have access and need assistance with accessing this article please contact Ivanti Customer Care.

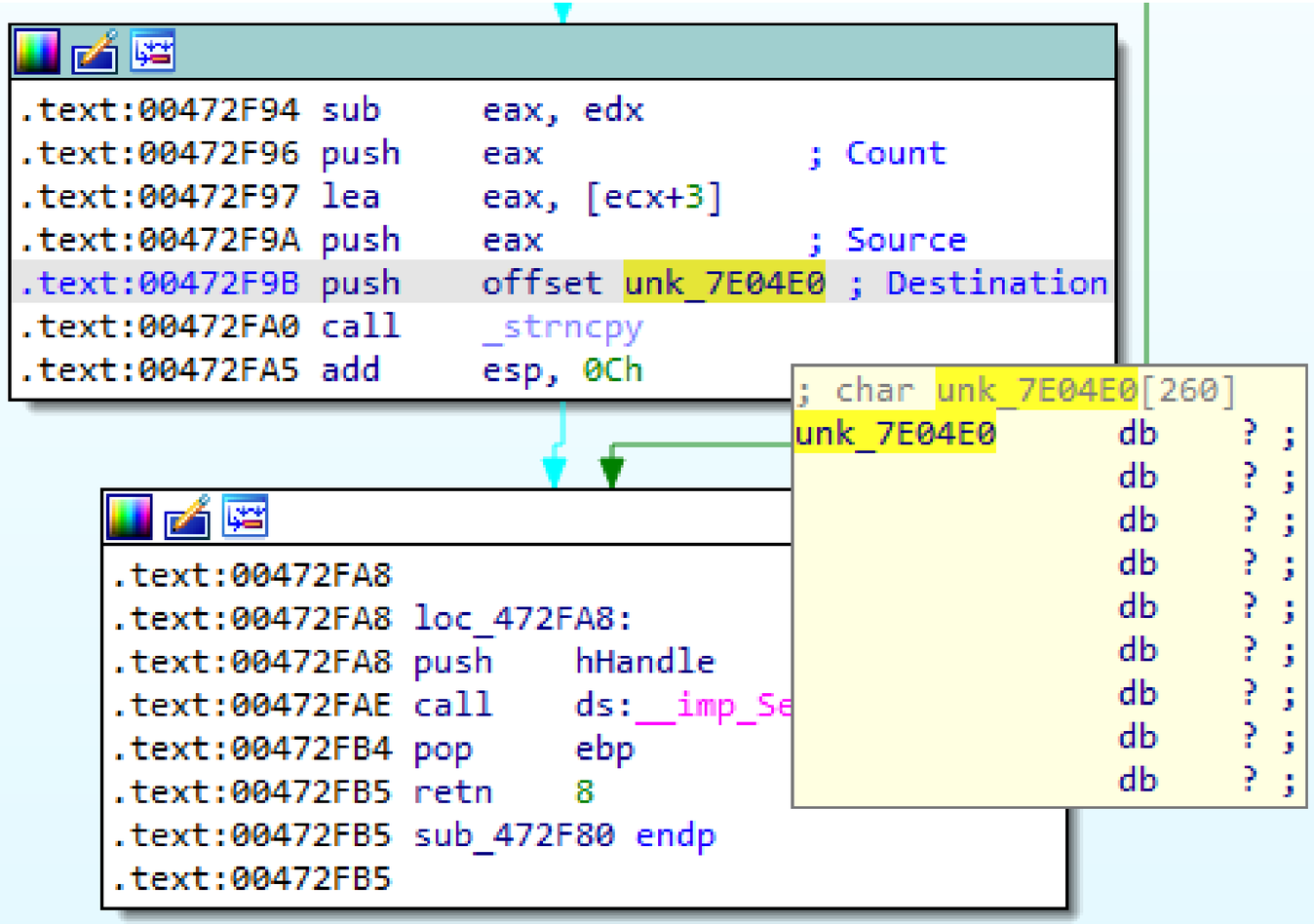
https://forums.ivanti.com/s/article/CVE-2024-22058-Privilege-Escalation-for-Ivanti-Endpoint-Manager-EPM


.text:004A90CC call CheckValueFromRegistry
.text:004A90D1 push eax
.text:004A90D2 lea eax, [ebp+var_19000]
.text:004A90D8 mov ecx, edi
.text:004A90DA push eax
.text:004A90DB push ebx
.text:004A90DC call CallerToConnectionReceiver
.text:004A90E1 test eax, eax
.text:004A90E3 jz loc_4A93DA
.text:004A90E9 mov edx, 0Ah
.text:004A90EE xor ecx, ecx
.text:004A90F0 jmp short loc_4A9100
.text:004A9100
.text:004A9100 loc_4A9100:
.text:004A9100 cmp dword ptr [ebx+10h], 0FFFFFFFFh
.text:004A9104 jz loc_4A93DA
.text:004A910A test ecx, ecx
.text:004A910C mov eax, 14h
.text:004A9111 push 0
.text:004A9113 cmovnz eax, edx
.text:004A9116 mov ecx, edi
.text:004A9118 push eax
.text:004A9119 push 0Ch
.text:004A911B lea eax, [ebp+var_19000]
.text:004A9121 push
.text:004A9122 push ebx
.text:004A9123 call ConnectionReceiver
.text:004A9128 mov esi, eax
.text:004A912A call
.text:004A9130 mov [ebp+var_1900C], eax
.text:004A9136 cmp esi, 0FFFFFFFFh
.text:004A9139 jz loc_4A93DA


.text:004A9176 lea eax, [ebp+var_19000]
.text:004A917C mov ecx, edi
.text:004A917E push eax
.text:004A917F call HeaderCheck ; Checks for '1HCR' in the header
.text:004A9184 test eax, eax
.text:004A9186 jz loc_4A93DA
.text:004A918C mov ax, [ebp+var_18FFC] ; Load length field (?) from payload into AX
.text:004A9193 xor esi, esi
.text:004A9195 cmp ax, 0Ch
.text:004A9199 jbe loc_4A92B1
.text:004A919F mov ecx, [ebp+var_18FFA] ; Load from our payload into ECX
.text:004A91A5 and ecx, 1
.text:004A91A8 movzx esi, ax
.text:004A91AB push 1
.text:004A91AD shl ecx, 4
.text:004A91B0 lea eax, [ebp+var_18FF4] ; Points right before our buffer
.text:004A91B6 push 28h ; '('
.text:004A91B8 add esi, 0FFFFFFF4h
.text:004A91BB add esi, ecx
.text:004A91BD mov ecx, edi
.text:004A91BF push esi
.text:004A91C0 push eax
.text:004A91C1 push ebx
.text:004A91C2 call ConnectionReceiver
.text:004A91C7 cmp eax, 1
.text:004A91CA jnz loc_4A93B5
.text:004A91D0 mov eax, [ebp+var_18FFA] ; Loads smth from our payload into EAX
.text:004A91D6 test al, 1
.text:004A91D8 jz short loc_4A9205

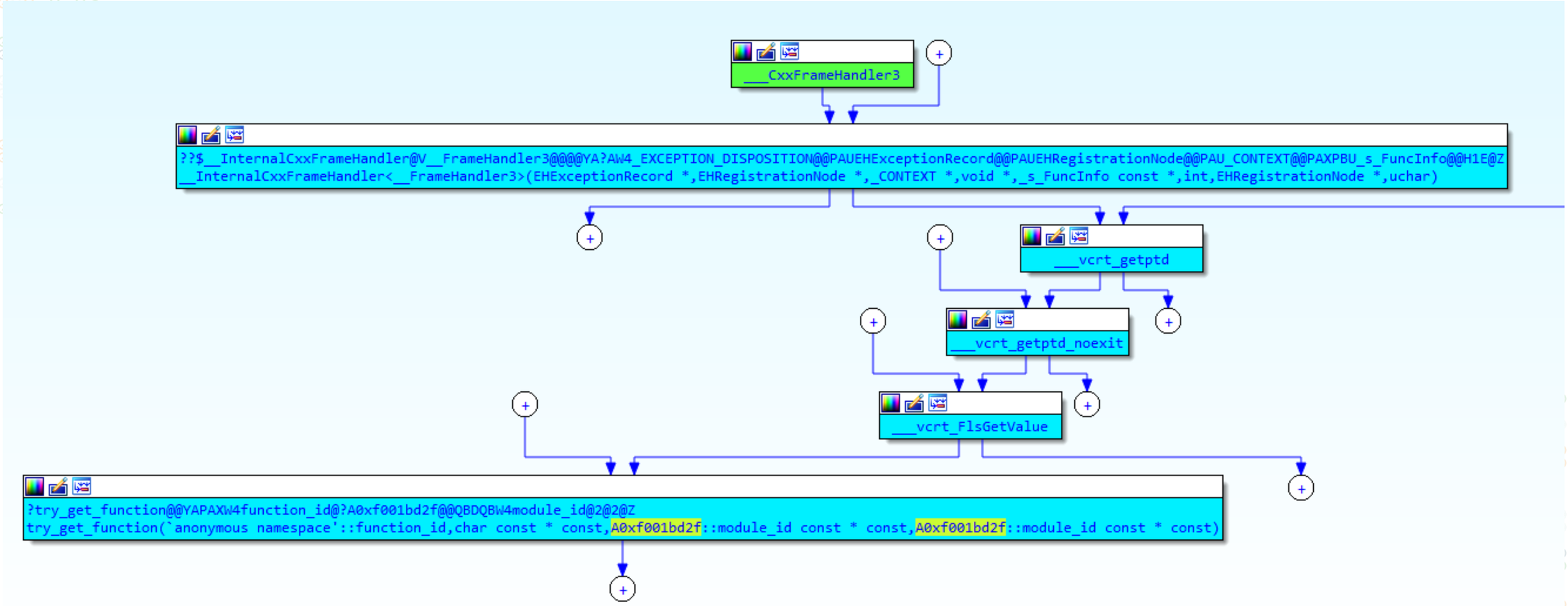

Administrator: Command Prompt - .\wtf master --name ivanti2 --max_len=0x7000
C:\Users\Administrator\Desktop\wtf campaign>.\wtf master --name ivanti2 --max_len=0x7000
Seeded with 18038270174142431639
Iterating through the corpus..
Sorting through the 1 entries..
Running server on tcp://localhost:31337..
#0 cov: 0 (+0) corp: 0 (0.0b) exec/s: 9223372036854.8m (1 nodes) lastcov: 0.0s crash: 0 timeout: 0 cr3: 0 uptime: 0.0s
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\3bc598187501bc4391dcbb6c3a8629d2
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\834363378192924e7216e1786763adb9
#1617 cov: 34402 (+34402) corp: 3 (28.3kb) exec/s: 404.0 (2 nodes) lastcov: 4.0s crash: 0 timeout: 0 cr3: 591 uptime: 4.0s
#3558 cov: 34402 (+0) corp: 3 (28.3kb) exec/s: 508.0 (3 nodes) lastcov: 7.0s crash: 0 timeout: 0 cr3: 1245 uptime: 7.0s
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\cr3-20f45fed5b537dc1a1f1a158ce7ad99a
#11906 cov: 50286 (+15884) corp: 4 (56.3kb) exec/s: 850.0 (4 nodes) lastcov: 0.0s crash: 0 timeout: 0 cr3: 4191 uptime: 15.0s
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\18623cfd1983ec1d933a4cf7830c641f
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\ca4a21673faa9a4cb2ec8701301b3eb5
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\1052ed5c8650ba7fee77522d8b7a57d1
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\5b3a95f13c837da3dc901e622401a4d6
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\2ad180c3c2fe2d1a30c9df293984fca0
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\25c17e4e45af7130a525304a335b751b
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\560d087055ae25a12be264430cee95a7
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\1375e97ea0ed108df0e67fccb7fc9381
#23667 cov: 55494 (+5208) corp: 14 (85.3kb) exec/s: 986.0 (4 nodes) lastcov: 0.0s crash: 0 timeout: 0 cr3: 7458 uptime: 25.0s
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\bf741ddf8149159f5e23a7358df10996
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\e092358281ff0faf5dde89a64bf401b2
#36466 cov: 55523 (+29) corp: 16 (85.4kb) exec/s: 1.1k (4 nodes) lastcov: 5.0s crash: 0 timeout: 0 cr3: 9526 uptime: 35.0s
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\f713cefca5e6a2bf45220e26cca36108
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\1f5acea2ae066ff5bfd507fb1c452603
#49934 cov: 55559 (+36) corp: 18 (85.7kb) exec/s: 1.1k (4 nodes) lastcov: 0.0s crash: 0 timeout: 0 cr3: 11530 uptime: 45.0s
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\cr3-28c1968778dae657dd22bd16cde044be
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\ec0e962877a2a6b8c43a426ae7555fe3
#64486 cov: 58635 (+3076) corp: 20 (87.9kb) exec/s: 1.2k (4 nodes) lastcov: 0.0s crash: 0 timeout: 0 cr3: 14196 uptime: 55.0s
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\crash-efca9f895684bdd114058e3294d3685c
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\crash-ecaaa41a8942fd74e92e199493a3ef32
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\72bad5209ca999f3d3649cd6345c68dc
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\crash-15f2405340fa1b5500e423a340032f46
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\crash-973a14f04e5e82b95b26697cb1d6fd64
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\054e412fff5a63378c7dea617a206a1e
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\crash-b096e91344ccf60e0d6c3fd0e177bb57
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\de85d64635f44c8cdebc024574885b52
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\adb604c56bf82d074b4174e9ac0ad189
#79263 cov: 60717 (+2082) corp: 29 (88.5kb) exec/s: 1.2k (4 nodes) lastcov: 4.0s crash: 1361 timeout: 0 cr3: 16579 uptime: 1.1min
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\56be0e269a4b18886a92cf707cec808f
Saving output in C:\Users\Administrator\Desktop\wtf campaign\outputs\cr3-6500f3ffc446711a7dc63a38745e4194


.text:00472F80
.text:00472F80
.text:00472F80 ; Attributes: bp-based frame
.text:00472F80
.text:00472F80 sub_472F80 proc near
.text:00472F80
.text:00472F80 arg_0= dword ptr 8
.text:00472F80
.text:00472F80 push ebp
.text:00472F81 mov ebp, esp
.text:00472F83 mov ecx, [ebp+arg_0]
.text:00472F86 mov edx, 3
.text:00472F8B movzx eax, word ptr [ecx+1]
.text:00472F8F cmp dx, ax
.text:00472F92 jnb short loc_472FA8
.text:00472F94 sub eax, edx
.text:00472F96 push eax ; Count
.text:00472F97 lea eax, [ecx+3]
.text:00472F9A push eax ; Source
.text:00472F9B push offset unk_7E04E0 ; Destination
.text:00472FA0 call _strncpy
.text:00472FA5 add esp, 0Ch
.text:00472FA8
.text:00472FA8 loc_472FA8: ; hEvent
.text:00472FA8 push hHandle
.text:00472FAE call ds:__imp_SetEvent
.text:00472FB4 pop ebp
.text:00472FB5 retn 8
.text:00472FB5 sub_472F80 endp
.text:00472FB5


.text:00472F94 sub eax, edx
.text:00472F96 push eax ; Count
.text:00472F97 lea eax, [ecx+3]
.text:00472F9A push eax ; Source
.text:00472F9B push offset unk_7E04E0 ; Destination
.text:00472FA0 call _strncpy
.text:00472FA5 add esp, 0Ch
; char unk_7E04E0[260]
unk_7E04E0 db ? ;
db ? ;
db ? ;
db ? ;
db ? ;
db ? ;
db ? ;
db ? ;
db ? ;
.text:00472FA8
.text:00472FA8 loc_472FA8:
.text:00472FA8 push hHandle
.text:00472FAE call ds:__imp_Se
.text:00472FB4 pop ebp
.text:00472FB5 retn 8
.text:00472FB5 sub_472F80 endp
.text:00472FB5

Command

```
0:000> !address 007e04e0


Mapping file section regions...
Mapping module regions...
Mapping PEB regions...
Mapping TEB and stack regions...
Mapping heap regions...
Mapping page heap regions...
Mapping other regions...
Mapping stack trace database regions...
Mapping activation context regions...

Usage:                  Image
Base Address:           007df000
End Address:            007e5000
Region Size:            00006000 (  24.000 kB)
State:                  00001000          MEM_COMMIT
Protect:                00000004          PAGE_READWRITE
Type:                   01000000          MEM_IMAGE
Allocation Base:        00400000
Allocation Protect:     00000080          PAGE_EXECUTE_WRITECOPY
Image Path:             issuser.exe
Module Name:            issuser
Loaded Image Name:      C:\Users\nop\Desktop\testingBin\issuser.exe
Mapped Image Name:
More info:              lmv m issuser
More info:              !lmi issuser
More info:              ln 0x7e04e0
More info:              !dh 0x400000
```


__CxxFrameHandler3
??$__InternalCxxFrameHandler@V__FrameHandler3@@@@YA?AW4_EXCEPTION_DISPOSITION@@PAUEHExceptionRecord@@PAUEHRegistrationNode@@PAU_CONTEXT@@PAXPBU_s_FuncInfo@@H1E@Z
__InternalCxxFrameHandler<__FrameHandler3>(EHExceptionRecord *,EHRegistrationNode *,_CONTEXT *,void *,_s_FuncInfo const *,int,EHRegistrationNode *,uchar)
__vcrt_getptd
__vcrt_getptd_noexit
__vcrt_FlsGetValue
?try_get_function@@YAPAXW4function_id@?A0xf001bd2f@@QBDQBW4module_id@2@2@Z
try_get_function(`anonymous namespace'::function_id,char const * const,A0xf001bd2f::module_id const * const,A0xf001bd2f::module_id const * const)

```
.text:00666CA8
.text:00666CA8
.text:00666CA8 ; Attributes: library function bp-based frame
.text:00666CA8
.text:00666CA8 ; int __cdecl __vcrt_FlsGetValue(DWORD dwTlsIndex)
.text:00666CA8 ___vcrt_FlsGetValue proc near
.text:00666CA8
.text:00666CA8 dwTlsIndex= dword ptr  8
.text:00666CA8
.text:00666CA8 push    ebp
.text:00666CA9 mov     ebp, esp
.text:00666CAB push    esi
.text:00666CAC push    offset unk_797200
.text:00666CB1 push    offset unk_7971F8
.text:00666CB6 push    offset aFlsgetvalue ; "FlsGetValue"
.text:00666CBB push    2
.text:00666CBD call    ?try_get_function@@YAPAXW4function_id@?A0xf001bd2f@@QBDQBW4module_id@2@2@Z ; try_get_function(`anonymous namesp
.text:00666CC2 add     esp, 10h
.text:00666CC5 mov     esi, eax
.text:00666CC7 push    [ebp+dwTlsIndex] ; dwTlsIndex
.text:00666CCA test    esi, esi
.text:00666CCC jz      short loc_666CDA
```

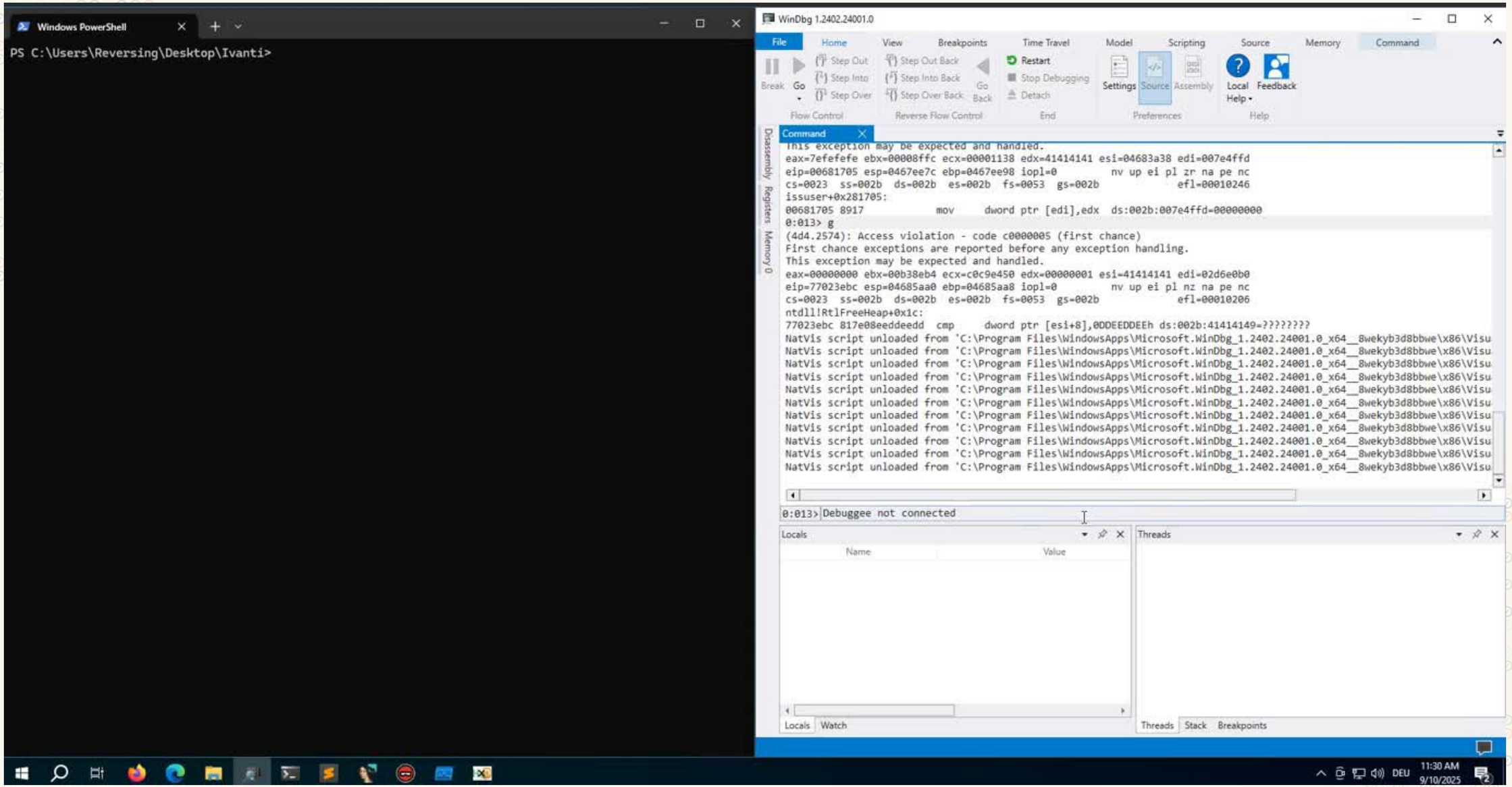
```
.text:00666CCE mov     ecx, esi
.text:00666CD0 call    ds:___guard_check_icall_fptr ; _guard_check_icall_nop(x) ...
.text:00666CD6 call    esi
.text:00666CD8 jmp     short loc_666CE0
```

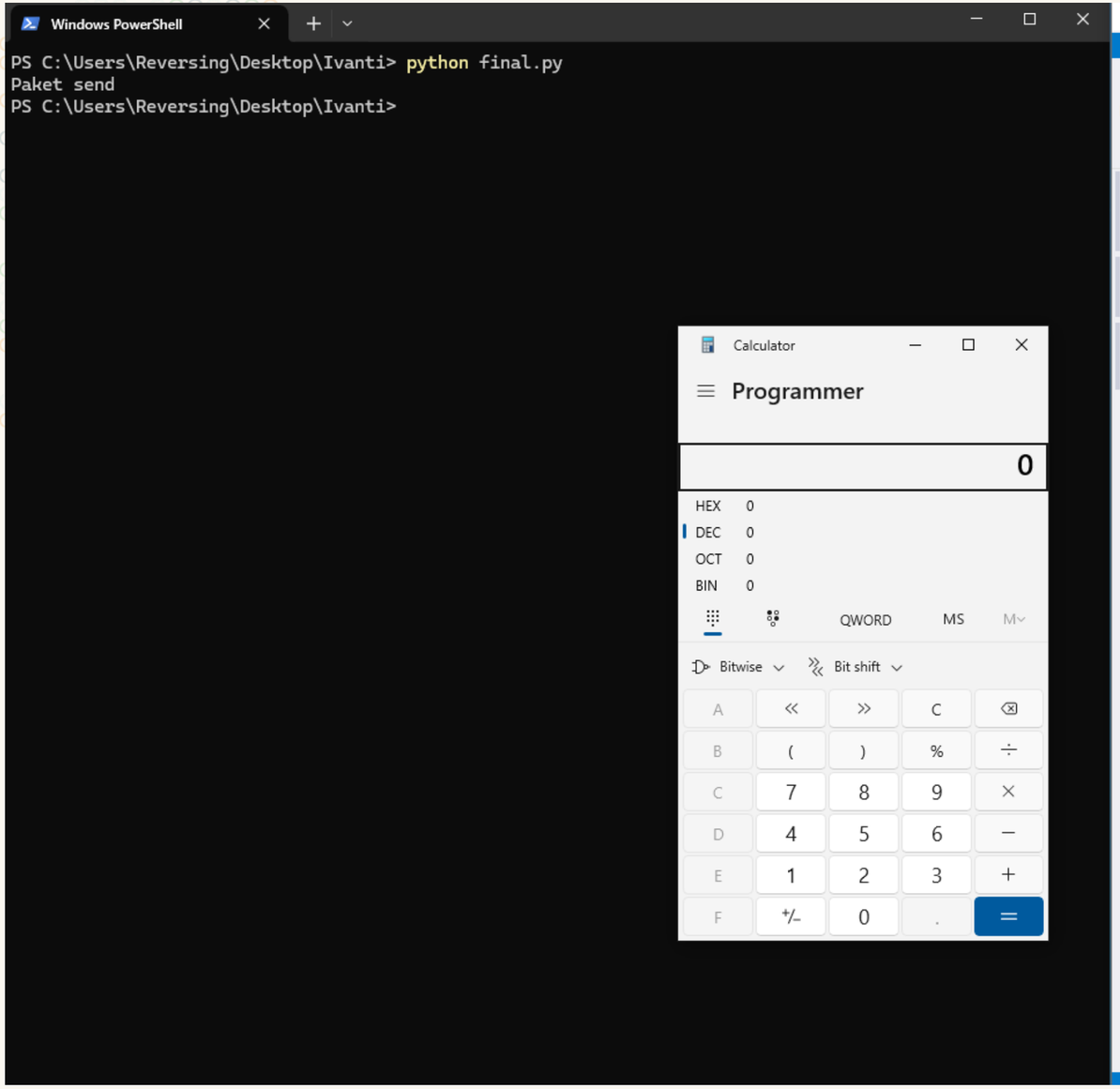
```
0:013> p
eax=42424242 ebx=00000000 ecx=42424242 edx=03e4eed0 esi=42424242 edi=00000000
eip=00666cd0 esp=03e4e858 ebp=03e4e860 iopl=0         nv up ei pl nz na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000206
issuser+0x266cd0:
00666cd0 ff1508787100    call    dword ptr [issuser+0x317808 (00717808)] ds:002b:00717808=0063d0d7
0:013> p
eax=42424242 ebx=00000000 ecx=42424242 edx=03e4eed0 esi=42424242 edi=00000000
eip=00666cd6 esp=03e4e858 ebp=03e4e860 iopl=0         nv up ei pl nz na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000206
issuser+0x266cd6:
00666cd6 ffd6            call    esi {42424242}

0:013>
```

But what about mitigations?

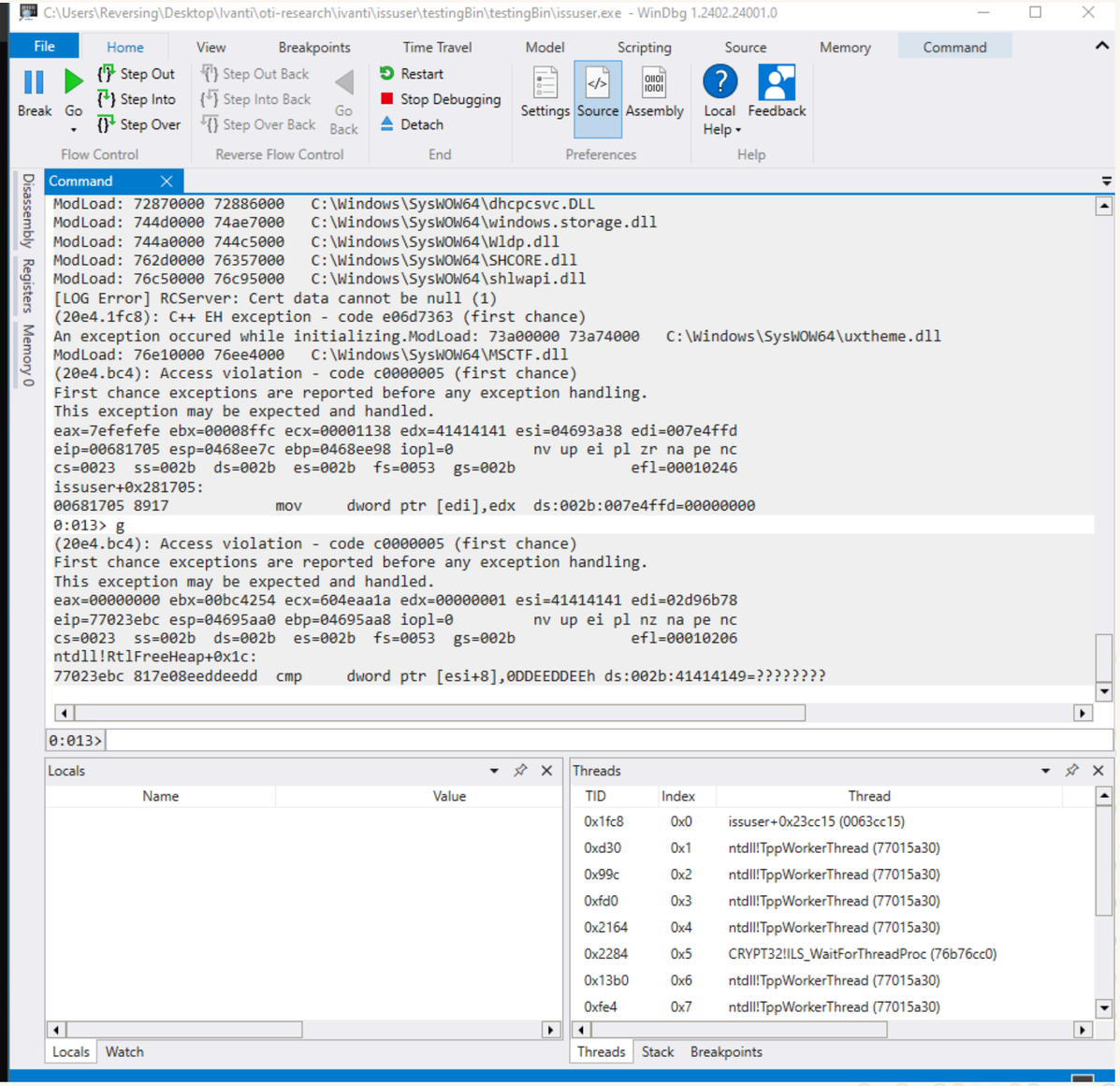
Command

```
0:013> .load C:\Users\Administrator\Desktop\narly.dll
0:013> !nmod
00400000 0085d000 issuser              /SafeSEH ON  /GS       *DEP C:\Users\Administrator\Desktop\testingBin\issuser.exe
01100000 01178000 ENUiuser             NO_SEH                *DEP C:\Users\Administrator\Desktop\testingBin\ENUiuser.dll
03380000 035f2000 curllib              /SafeSEH ON  /GS       *DEP C:\Users\Administrator\Desktop\testingBin\curllib.dll
03750000 03786000 ISSFTCLT             /SafeSEH ON  /GS       *DEP C:\Users\Administrator\Desktop\testingBin\ISSFTCLT.DLL
03a30000 03a6d000 irclog               /SafeSEH ON  /GS       *DEP C:\Users\Administrator\Desktop\testingBin\irclog.dll
10000000 10026000 RollingLog           /SafeSEH ON  /GS       *DEP C:\Users\Administrator\Desktop\testingBin\RollingLog.dll
749b0000 74a2c000 uxtheme              /SafeSEH ON  /GS *ASLR *DEP C:\Windows\system32\uxtheme.dll
74a30000 74a45000 dhcpcsvc             /SafeSEH ON  /GS *ASLR *DEP C:\Windows\SYSTEM32\dhcpcsvc.DLL
74a50000 750aa000 windows_storage      /SafeSEH ON  /GS *ASLR *DEP C:\Windows\SYSTEM32\windows.storage.dll
```


Windows PowerShell
PS C:\Users\Reversing\Desktop\Ivanti>
WinDbg 1.2402.24001.0
File
Home
View
Breakpoints
Time Travel
Model
Scripting
Source
Memory
Command
Break
Go
Step Out
Step Into
Step Over
Step Out Back
Step Into Back
Step Over Back
Go Back
Restart
Stop Debugging
Detach
Settings
Source
Assembly
Local Help
Feedback
Flow Control
Reverse Flow Control
End
Preferences
Help
Command
This exception may be expected and handled.
eax=7efefefe ebx=00008ffc ecx=00001138 edx=41414141 esi=04683a38 edi=007e4ffd
eip=00681705 esp=0467ee7c ebp=0467ee98 iopl=0 nv up ei pl zr na pe nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010246
issuser+0x281705:
00681705 8917 mov dword ptr [edi],edx ds:002b:007e4ffd=00000000
0:013> g
(4d4.2574): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=00b38eb4 ecx=c0c9e450 edx=00000001 esi=41414141 edi=02d6e0b0
eip=77023ebc esp=04685aa0 ebp=04685aa8 iopl=0 nv up ei pl nz na pe nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010206
ntdll!RtlFreeHeap+0x1c:
77023ebc 817e08eeddeedd cmp dword ptr [esi+8],0DDEEDDEEh ds:002b:41414149=????????
NatVis script unloaded from 'C:\Program Files\WindowsApps\Microsoft.WinDbg_1.2402.24001.0_x64__8wekyb3d8bbwe\x86\Visu
0:013> Debuggee not connected
Locals
Name
Value
Threads
Locals
Watch
Threads
Stack
Breakpoints
DEU
11:30 AM
9/10/2025


Windows PowerShell
PS C:\Users\Reversing\Desktop\Ivanti> python final.py
Paket send
PS C:\Users\Reversing\Desktop\Ivanti>

Calculator
Programmer
0
HEX 0
DEC 0
OCT 0
BIN 0
QWORD
MS
Bitwise
Bit shift


C:\Users\Reversing\Desktop\Ivanti\oti-research\ivanti\issuser\testingBin\testingBin\issuser.exe - WinDbg 1.2402.24001.0
File
Home
View
Breakpoints
Time Travel
Model
Scripting
Source
Memory
Command
Break
Go
Step Out
Step Into
Step Over
Restart
Stop Debugging
Detach
Settings
Source
Assembly
Local Help
Feedback
Flow Control
Reverse Flow Control
End
Preferences
Help
Command
ModLoad: 72870000 72886000 C:\Windows\SysWOW64\dhcpcsvc.DLL
ModLoad: 744d0000 74ae7000 C:\Windows\SysWOW64\windows.storage.dll
ModLoad: 744a0000 744c5000 C:\Windows\SysWOW64\Wldp.dll
ModLoad: 762d0000 76357000 C:\Windows\SysWOW64\SHCORE.dll
ModLoad: 76c50000 76c95000 C:\Windows\SysWOW64\shlwapi.dll
[LOG Error] RCServer: Cert data cannot be null (1)
(20e4.1fc8): C++ EH exception - code e06d7363 (first chance)
An exception occured while initializing.ModLoad: 73a00000 73a74000 C:\Windows\SysWOW64\uxtheme.dll
ModLoad: 76e10000 76ee4000 C:\Windows\SysWOW64\MSCTF.dll
(20e4.bc4): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=7efefefe ebx=00008ffc ecx=00001138 edx=41414141 esi=04693a38 edi=007e4ffd
eip=00681705 esp=0468ee7c ebp=0468ee98 iopl=0 nv up ei pl zr na pe nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010246
issuser+0x281705:
00681705 8917 mov dword ptr [edi],edx ds:002b:007e4ffd=00000000
0:013> g
(20e4.bc4): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=00bc4254 ecx=604eaa1a edx=00000001 esi=41414141 edi=02d96b78
eip=77023ebc esp=04695aa0 ebp=04695aa8 iopl=0 nv up ei pl nz na pe nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00010206
ntdll!RtlFreeHeap+0x1c:
77023ebc 817e08eeddeedd cmp dword ptr [esi+8],0DDEEDDEEh ds:002b:41414149=????????
0:013>
Locals
Name
Value
Threads
TID
Index
Thread
0x1fc8 0x0 issuser+0x23cc15 (0063cc15)
0xd30 0x1 ntdll!TppWorkerThread (77015a30)
0x99c 0x2 ntdll!TppWorkerThread (77015a30)
0xfd0 0x3 ntdll!TppWorkerThread (77015a30)
0x2164 0x4 ntdll!TppWorkerThread (77015a30)
0x2284 0x5 CRYPT32!ILS_WaitForThreadProc (76b76cc0)
0x13b0 0x6 ntdll!TppWorkerThread (77015a30)
0xfe4 0x7 ntdll!TppWorkerThread (77015a30)
Locals
Watch
Threads
Stack
Breakpoints

MANTODEA
SECURITY

THANK YOU