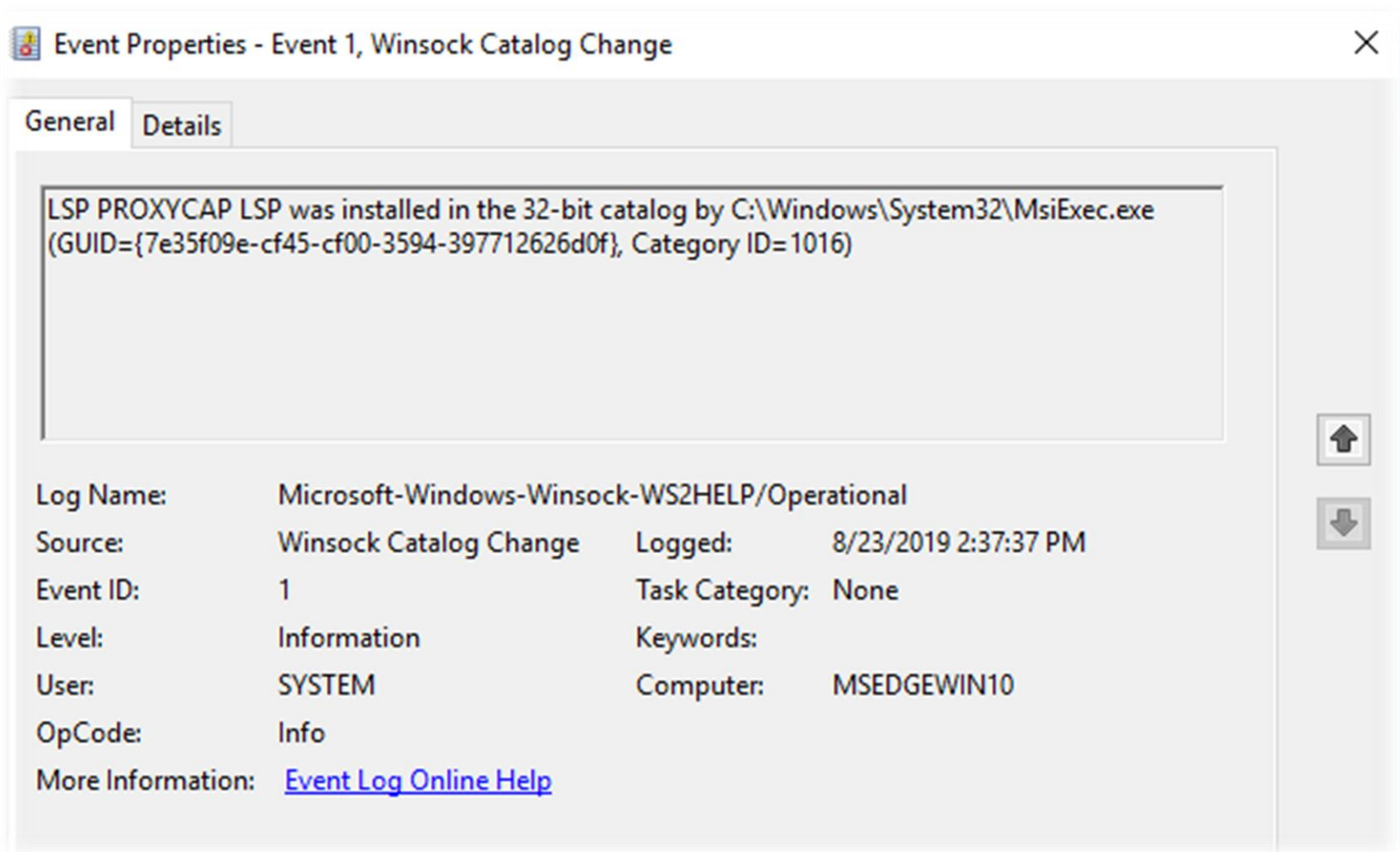Author: @SBousseaden

The Power of Windows EVT #DFIR – Collection of Events useful for Forensics
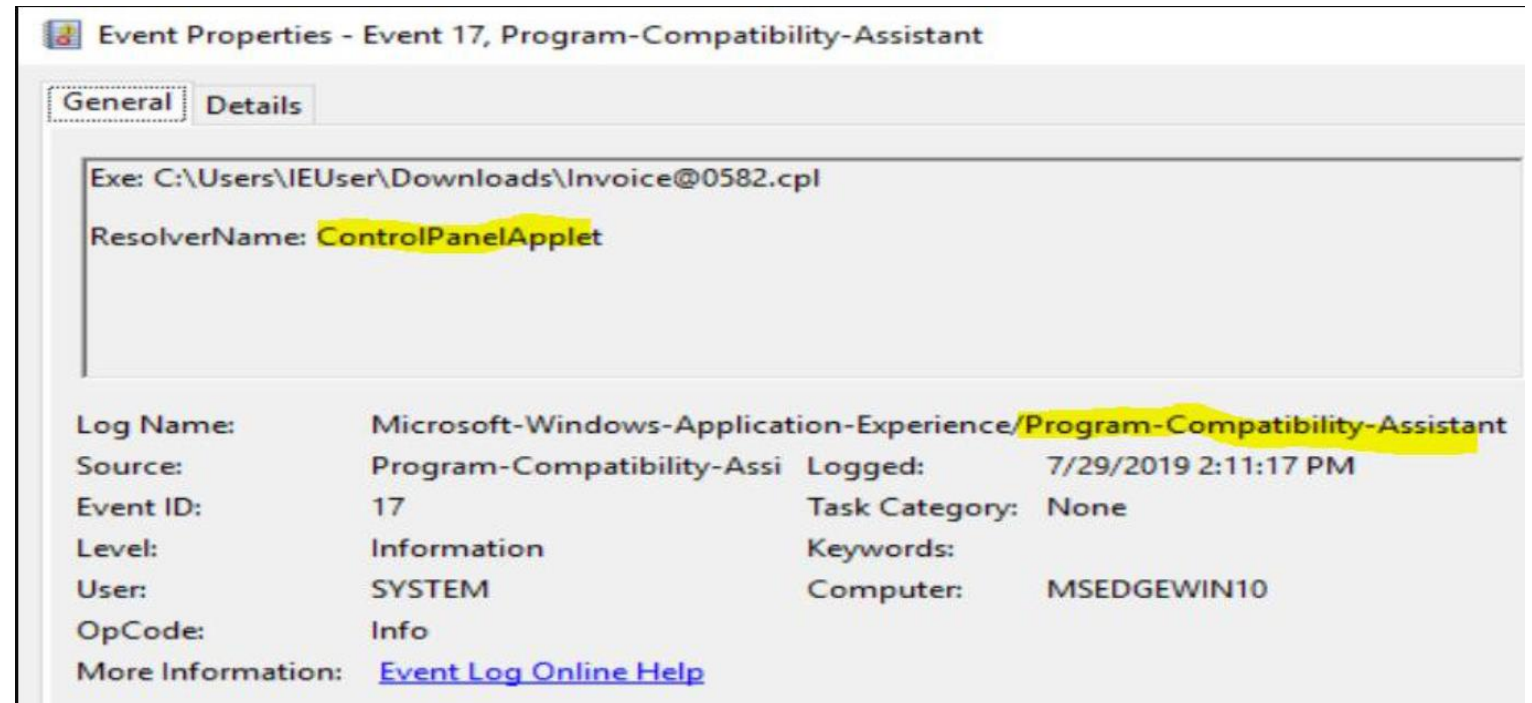
Persistence — WinSock

Event Properties - Event 1, Winsock Catalog Change

General | Details

LSP PROXYCAP LSP was installed in the 32-bit catalog by C:\Windows\System32\MsiExec.exe (GUID={7e35f09e-cf45-cf00-3594-397712626d0f}, Category ID=1016)

Log Name:	Microsoft-Windows-Winsock-WS2HELP/Operational		
Source:	Winsock Catalog Change	Logged:	8/23/2019 2:37:37 PM
Event ID:	1	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	MSEDGEWIN10
OpCode:	Info		
More Information:	Event Log Online Help		

Persistence – BITS

Event Properties - Event 59, Bits-Client

General | Details

BITS started the hola transfer job that is associated with the C:\Windows\system32\cmd.exe URL.

Log Name:	Microsoft-Windows-Bits-Client/Operational		
Source:	Bits-Client	Logged:	5/13/2019 4:50:59 PM
Event ID:	59	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	IEWIN7
OpCode:	Start		
More Information:	Event Log Online Help		

Execution – Control Panel

Traces of PrivEsc (np's privileged client token imperson)

Event Properties - Event 7045, Service Control Manager

General | Details

A service was installed in the system.

Service Name: WinPwnage
Service File Name: %COMSPEC% /c ping -n 1 127.0.0.1 >nul && echo 'WinPwnage' > \\.\pipe\WinPwnagePipe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Log Name:	System		
Source:	Service Control Manager	Logged:	5/12/2019 2:52:43 PM
Event ID:	7045	Task Category:	None
Level:	Information	Keywords:	Classic
User:	S-1-5-21-3583694148-141455	Computer:	IEWIN7
OpCode:	Info		
More Information:	Event Log Online Help		

Persistence: AppInit_DLLs

Traces of Persistence / Accessibility Backdoor via Shim AppPatch

Event Properties - Event 500, Application-Experience

General | Details

Compatibility fix applied to C:\Windows\system32\utilman.exe.
Fix information: CorrectFilePaths, {8a23a24a-9a8d-44b6-a6d4-556c53a289b5}, 0x10205.

Log Name:	Microsoft-Windows-Application-Experience/Program-Telemetry		
Source:	Application-Experience	Logged:	3/19/2019 9:58:31 PM
Event ID:	500	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	PC01.example.corp
OpCode:	Info		
More Information:	Event Log Online Help		

Traces of BlueKeep Scan Traces on Win10 "ms_t120 chan"

Event Properties - Event 148, RemoteDesktopServices-RdpCoreTS

General | Details

Channel ms_t120 has been closed between the server and the client on transport tunnel: 0.

Log Name:	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational		
Source:	RemoteDesktopServices-Rdp	Logged:	8/28/2019 4:52:55 PM
Event ID:	148	Task Category:	RemoteFX module
Level:	Information	Keywords:	
User:	NETWORK SERVICE	Computer:	MSEDGEWIN10
OpCode:	CloseConnection		
More Information:	Event Log Online Help		

Traces of RDP Tunneling

Event Properties - Event 4624, Microsoft Windows security auditing.

General | Details

An account was successfully logged on.

Subject:
    Security ID: SYSTEM
    Account Name: PC02$
    Account Domain: EXAMPLE
    Logon ID: 0x3E7

Logon Type: 10

New Logon:
    Security ID: S-1-5-21-3583694148-1414552638-2922671848-1000
    Account Name: IEUser
    Account Domain: PC02
    Logon ID: 0x45120
    Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
    Process ID: 0x658
    Process Name: C:\Windows\System32\winlogon.exe

Network Information:
    Workstation Name: PC02
    Source Network Address: 127.0.0.1
    Source Port: 49164

Detailed Authentication Information:
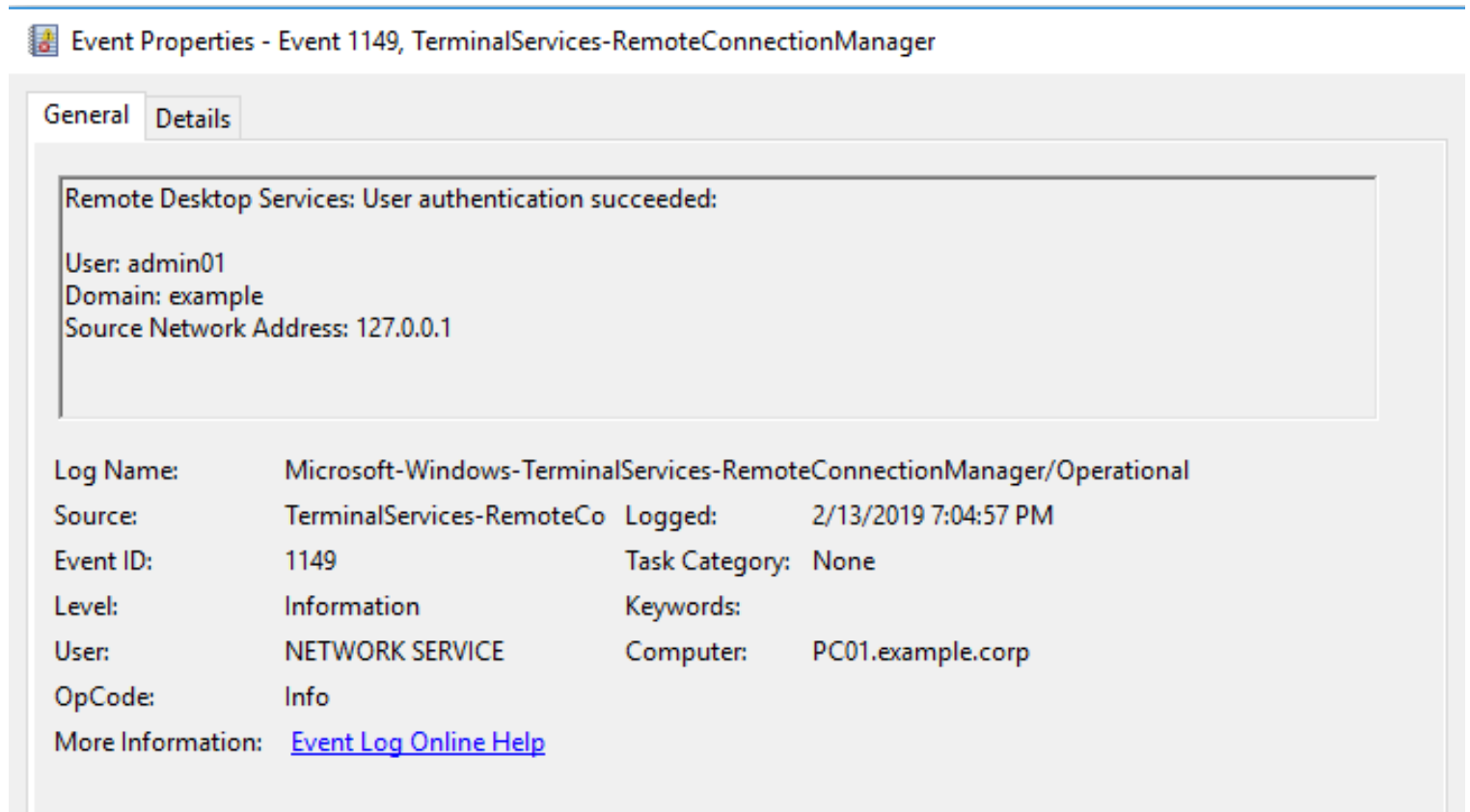   Logon Process: User32
    Authentication Package: Negotiate
    Transited Services: -
    Package Name (NTLM only):   -
    Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2/13/2019 4:26:53 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	PC02.example.corp
OpCode:	Info		

Traces of RDP Tunneling

Event Properties - Event 1149, TerminalServices-RemoteConnectionManager

General | Details

Remote Desktop Services: User authentication succeeded:

User: admin01
Domain: example
Source Network Address: 127.0.0.1

Log Name:	Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational		
Source:	TerminalServices-RemoteCo	Logged:	2/13/2019 7:04:57 PM
Event ID:	1149	Task Category:	None
Level:	Information	Keywords:	
User:	NETWORK SERVICE	Computer:	PC01.example.corp
OpCode:	Info		
More Information:	Event Log Online Help		

PrivEsc:
Traces of Invoke-ToeknDuplication — UAC Bypass hardcoded strings

Traces of Persistence via Run/RunOnce (9707, 9708)

Event Properties - Event 9707, Shell-Core

General | Details

Started execution of command 'explorer.exe shell:::{769f9427-3cc6-4b62-be14-2a705115b7ab}'.

Log Name:	Microsoft-Windows-Shell-Core/Operational		
Source:	Shell-Core	Logged:	10/30/2019 1:40:58 PM
Event ID:	9707	Task Category:	(9707)
Level:	Information	Keywords:	(67108864),(65536)
User:	MSEDGEWIN10\IEUser	Computer:	MSEDGEWIN10
OpCode:	(1)		
More Information:	Event Log Online Help		

Lateral Movement Obsolete RDC "RDP Client" Info (xfreerdp)

Event Properties - Event 168, RemoteDesktopServices-RdpCoreTS

General | Details

The resolution requested by the client: Monitor 0: (1920, 1080), origin: (0, 0). Server: MSEDGEWIN10

Log Name: Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
Source: RemoteDesktopServices-Rdp   Logged: 8/27/2019 7:17:47 PM
Event ID: 168   Task Category: RemoteFX module
Level: Information   Keywords:
User: NETWORK SERVICE   Computer: MSEDGEWIN10
OpCode: Initialize
More Information: Event Log Online Help

Event Properties - Event 163, RemoteDesktopServices-RdpCoreTS

General | Details

The client supports RDP 7.1 or lower protocol. Server: MSEDGEWIN10

Log Name: Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
Source: RemoteDesktopServices-Rdp   Logged: 8/28/2019 4:52:47 PM
Event ID: 163   Task Category: RemoteFX module
Level: Information   Keywords:
User: NETWORK SERVICE   Computer: MSEDGEWIN10
OpCode: Runtime
More Information: Event Log Online Help

Traces of previous "Lsa Notification Packages" [T1174: Password Filter] cleaned or corrupted entry - EventID 16953

Event Properties - Event 16953, Directory-Services-SAM

General | Details

The password notification DLL failed to load with error 87. Please verify that the notification DLL path defined in the registry, HKLM\System\CurrentControlSet\Control\Lsa\Notification Packages, refers to a correct and absolute path (<drive>:\<path>\<filename>.<ext>) and not a relative or invalid path. If the DLL path is correct, please validate that any supporting files are located in the same directory, and that the system account has read access to both the DLL path and any supporting files. Contact the provider of the notification DLL for additional support. Further details can be found on the web at http://go.microsoft.com/fwlink/?LinkId=245898.

Log Name:	System		
Source:	Directory-Services-SAM	Logged:	9/16/2019 10:33:54 PM
Event ID:	16953	Task Category:	None
Level:	Error	Keywords:	
User:	SYSTEM	Computer:	MSEDGEWIN10
OpCode:	Info		
More Information:	Event Log Online Help		

Execution - Traces of unsigned Drivers/Modules

Event Properties - Event 3001, CodeIntegrity

General | Details

Code Integrity determined an unsigned kernel module \Device\HarddiskVolume2\Windows\System32\drivers\A3E64E55_pr.sys is loaded into the system. Check with the publisher to see if a signed version of the kernel module is available.

Log Name:	Microsoft-Windows-CodeIntegrity/Operational		
Source:	CodeIntegrity	Logged:	10/6/2017 12:15:14 PM
Event ID:	3001	Task Category:	(1)
Level:	Warning	Keywords:	
User:	SYSTEM	Computer:	PC
OpCode:	(101)		
More Information:	Event Log Online Help		

Traces of Brute forcing Protected Office File
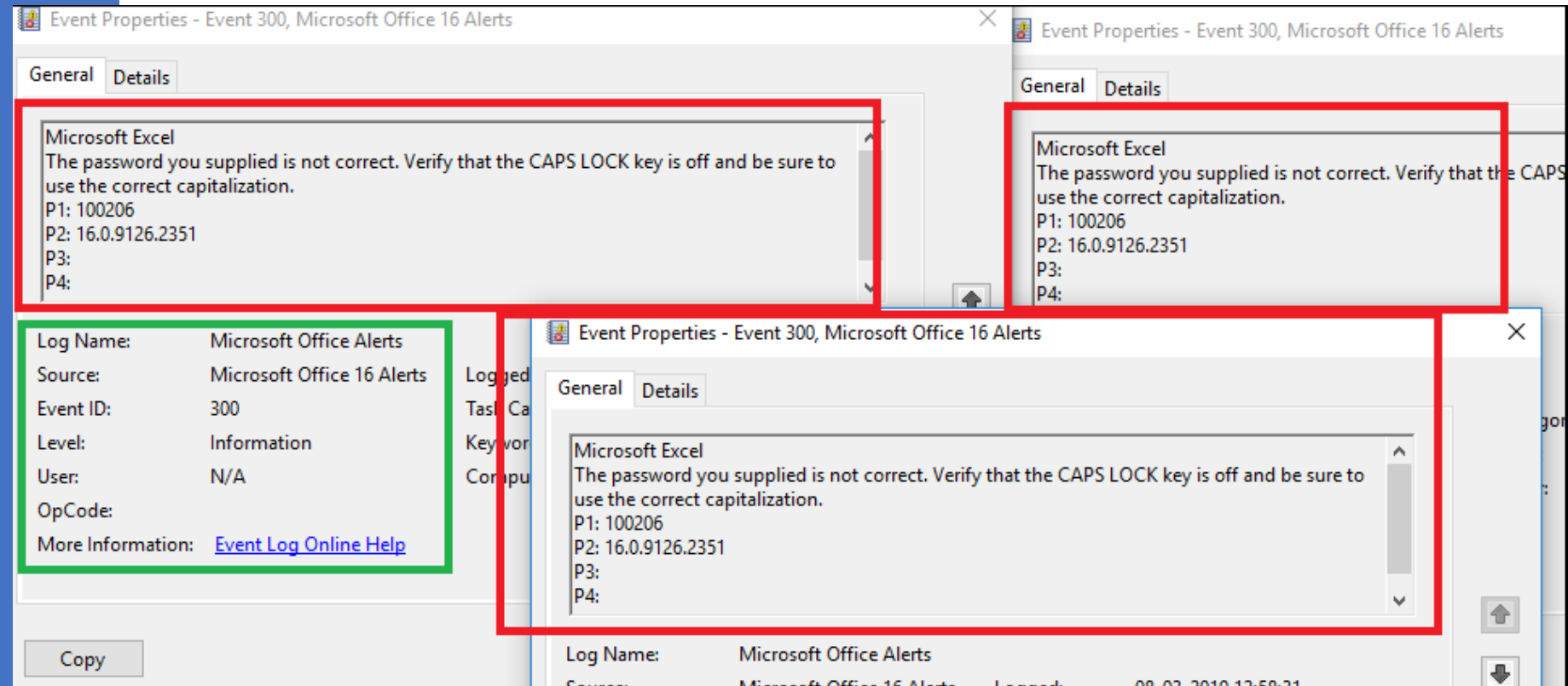
Initial Access: Traces of Phishing via DDE
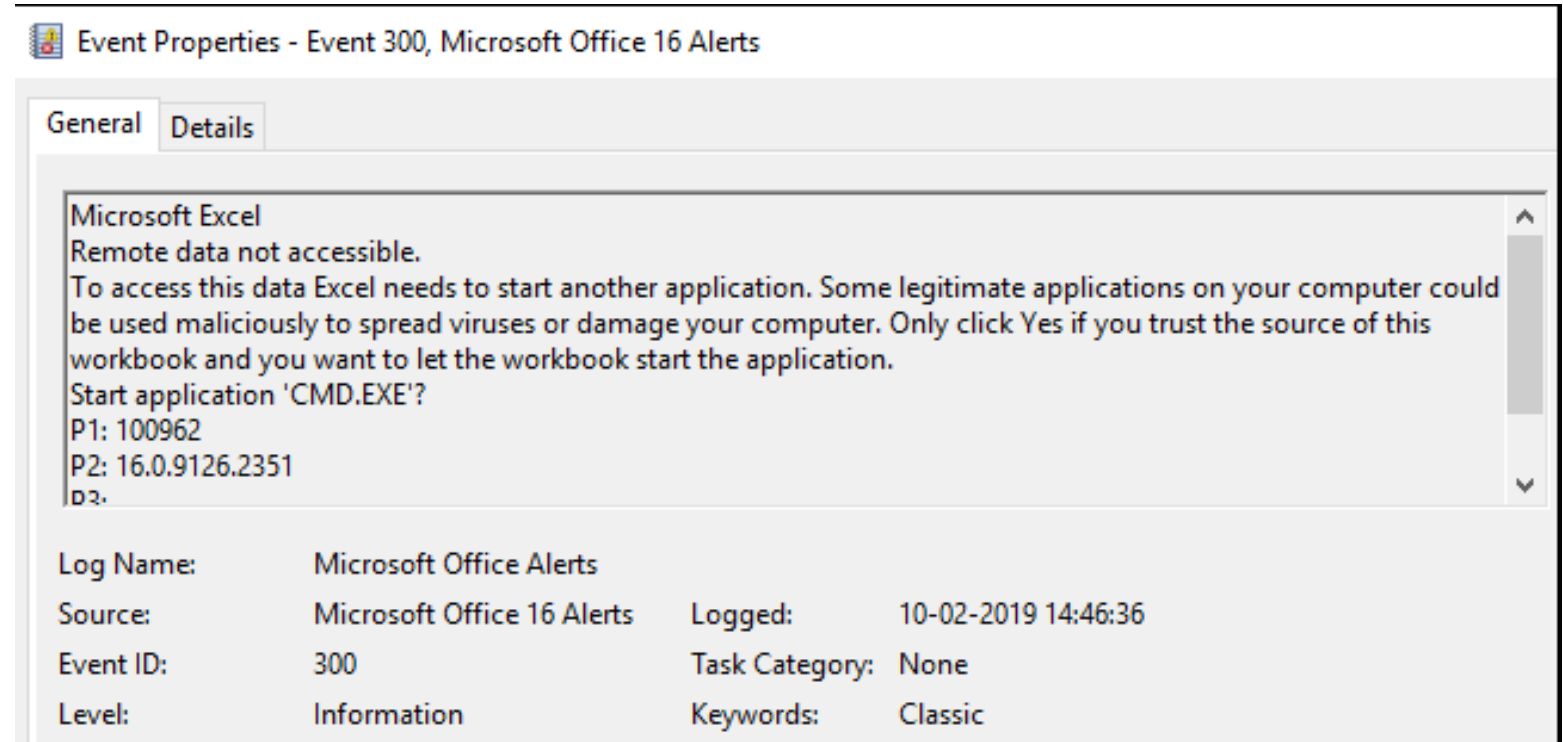
Initial Access: Traces of Phishing via MSIEXEC – 1040/1042
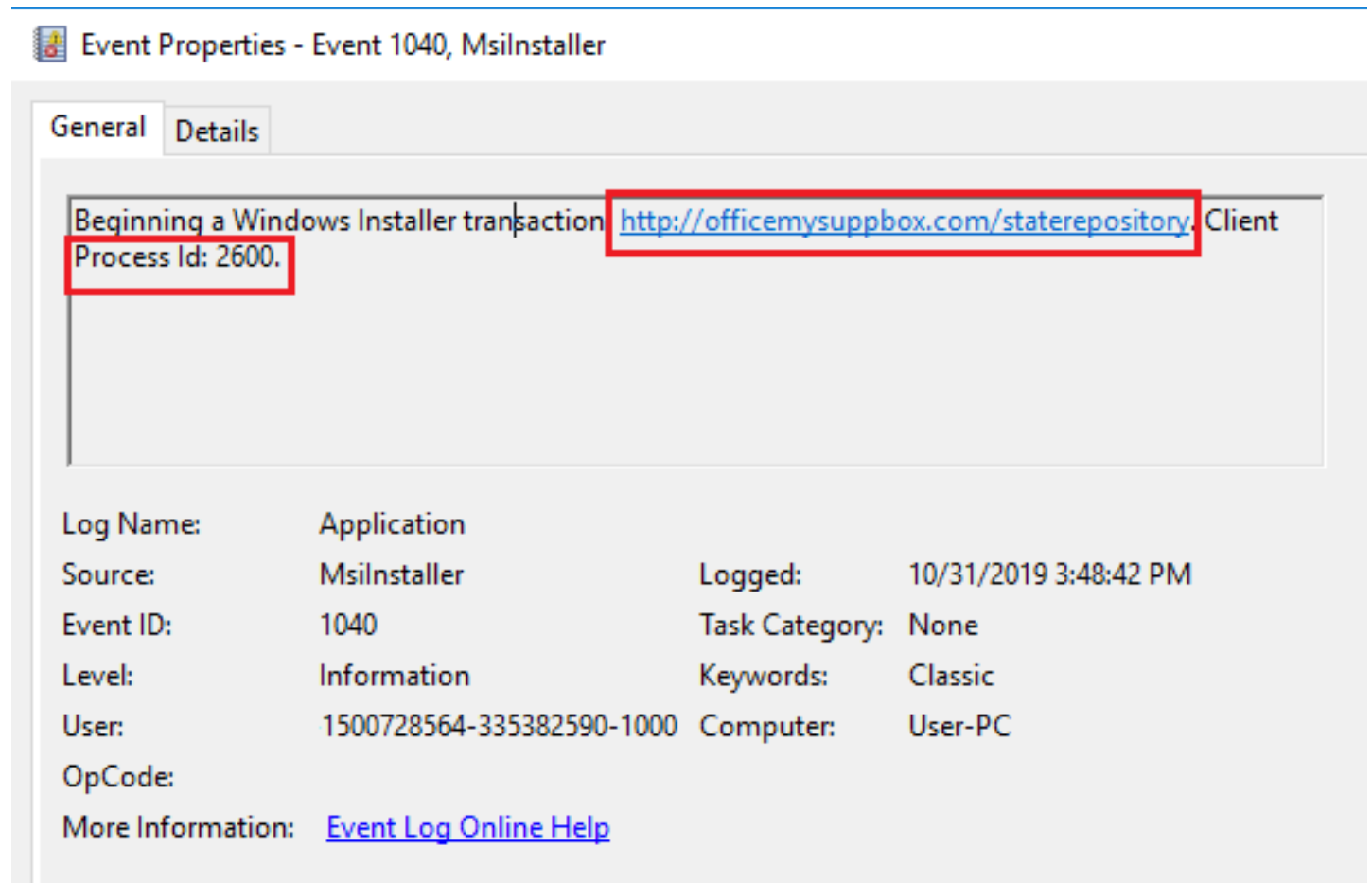
Defense Evasion: Traces of Injection via Process Doppleganging (NTFS transc)
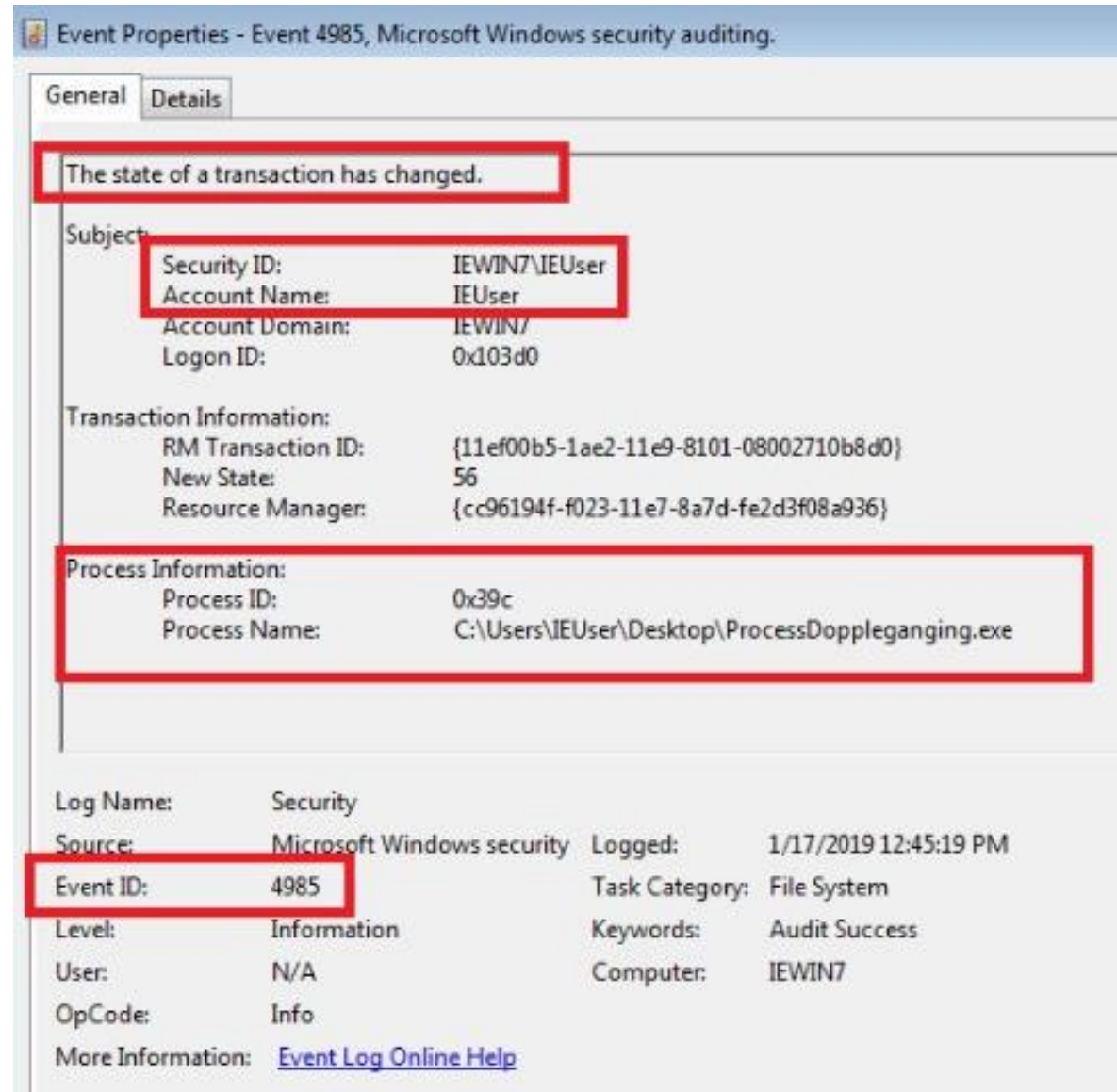
Lateral Movmt: Traces of Outbound DCOM LM activity (RPCSS SPN)

Event Properties - Event 4648, Microsoft Windows security auditing.

General | Details

A logon was attempted using explicit credentials.

Subject:
    Security ID: S-1-5-21-1587066498-1489273250-1035260531-1106
    Account Name: user01
    Account Domain: EXAMPLE
    Logon ID: 0x18A7875
    Logon GUID: {3523b8be-1c1a-a740-a8c3-4cc91a5f3b14}

Account Whose Credentials Were Used:
    Account Name: administrator
    Account Domain: EXAMPLE.CORP
    Logon GUID: {50419e1a-1c62-023a-239e-78c43a7792ab}

Target Server:
    Target Server Name: WIN-77LTAPHIQ1R.example.corp
    Additional Information: RPCSS/WIN-77LTAPHIQ1R.example.corp

Process Information:
    Process ID: 0x304
    Process Name: C:\Windows\System32\svchost.exe

Network Information:
    Network Address: -
    Port: -

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	18-03-2019 12:27:23
Event ID:	4648	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	PC01.example.corp
OpCode:	Info		
More Information:	Event Log Online Help		

Lateral Movmt: Traces of Inbound RDP (ProcName winlogon + NetAddrs!="localhost or null or –")

Event Properties - Event 4648, Microsoft Windows security auditing.

General | Details

A logon was attempted using explicit credentials.

Subject:
    Security ID: S-1-5-18
    Account Name: PC02$
    Account Domain: EXAMPLE
    Logon ID: 0x3E7
    Logon GUID: {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
    Account Name: IEUser
    Account Domain: PC02
    Logon GUID: {00000000-0000-0000-0000-000000000000}

Target Server:
    Target Server Name: localhost
    Additional Information: localhost

Process Information:
    Process ID: 0xd94
    Process Name: C:\Windows\System32\winlogon.exe

Network Information:
    Network Address: 10.0.2.18
    Port: 49175

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	13-02-2019 13:53:04
Event ID:	4648	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	PC02.example.corp

Lateral Movmt: Traces of Outbound RDP (TERMSRV SPN)
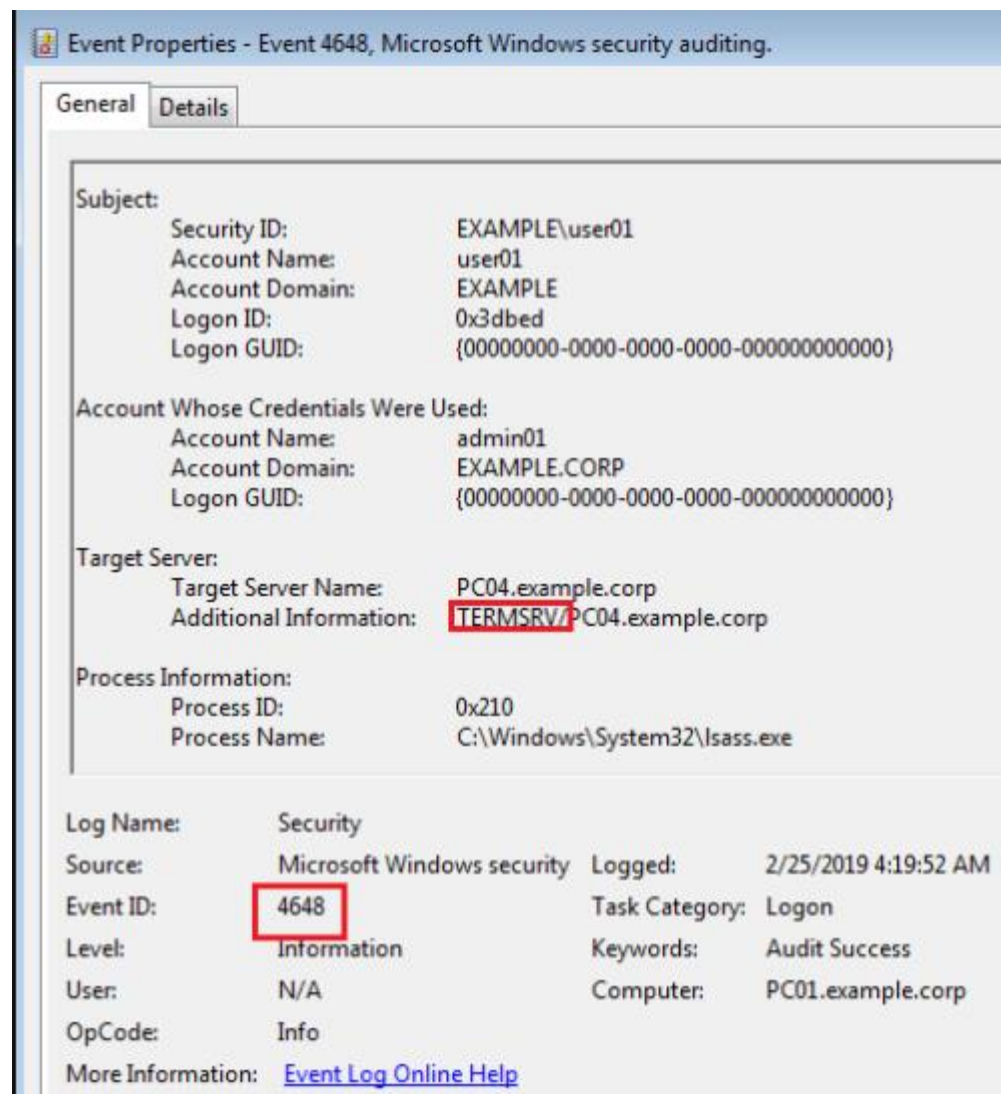
Lateral Movmt: Traces of Outbound SMB (ProcId=0x4 & TargetServName!=localhost)

Traces of usage of sc.exe for Lateral Movmt (same apply to other utilities like wmic when used with explicit creds)