

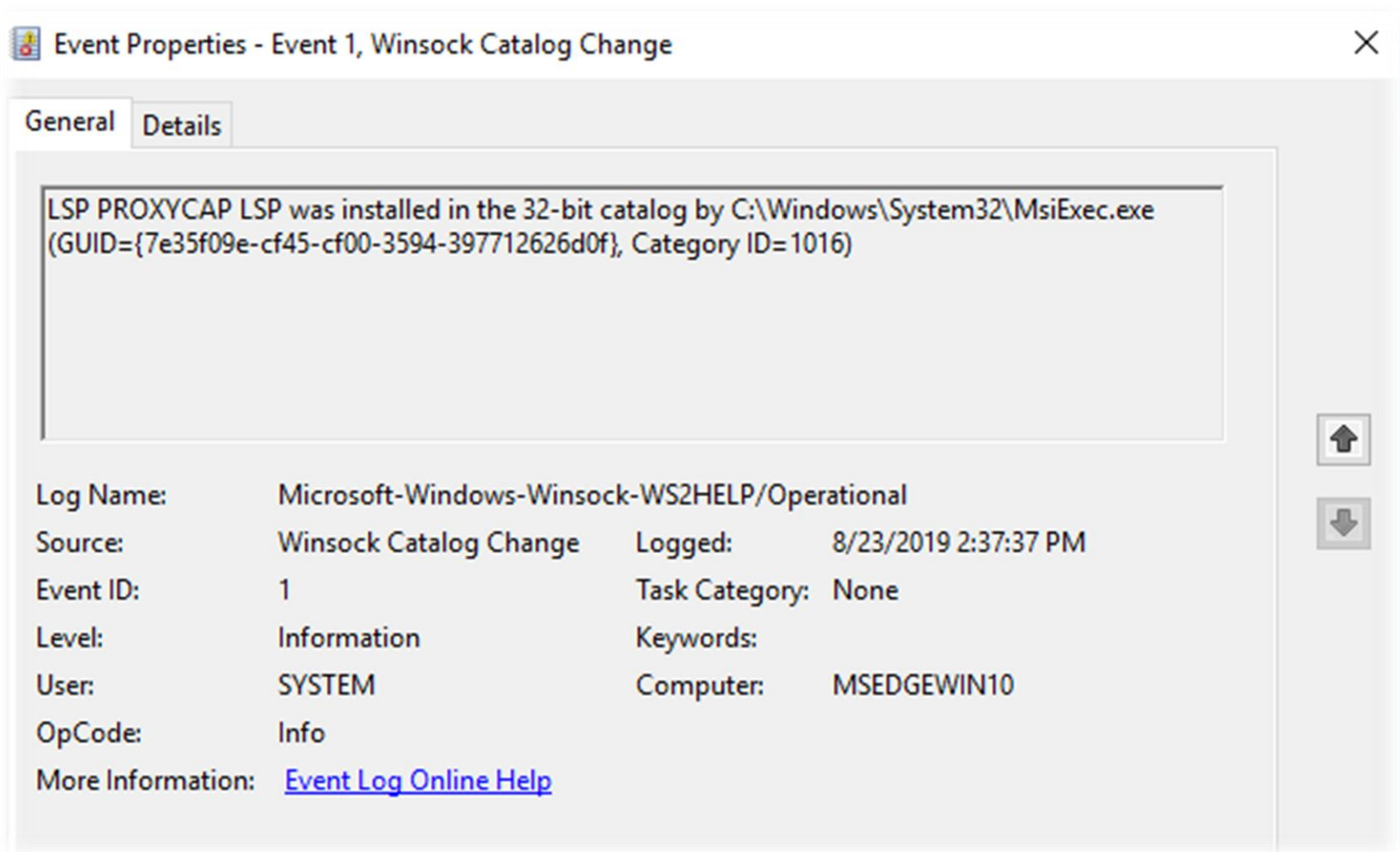


Author: @SBousseaden

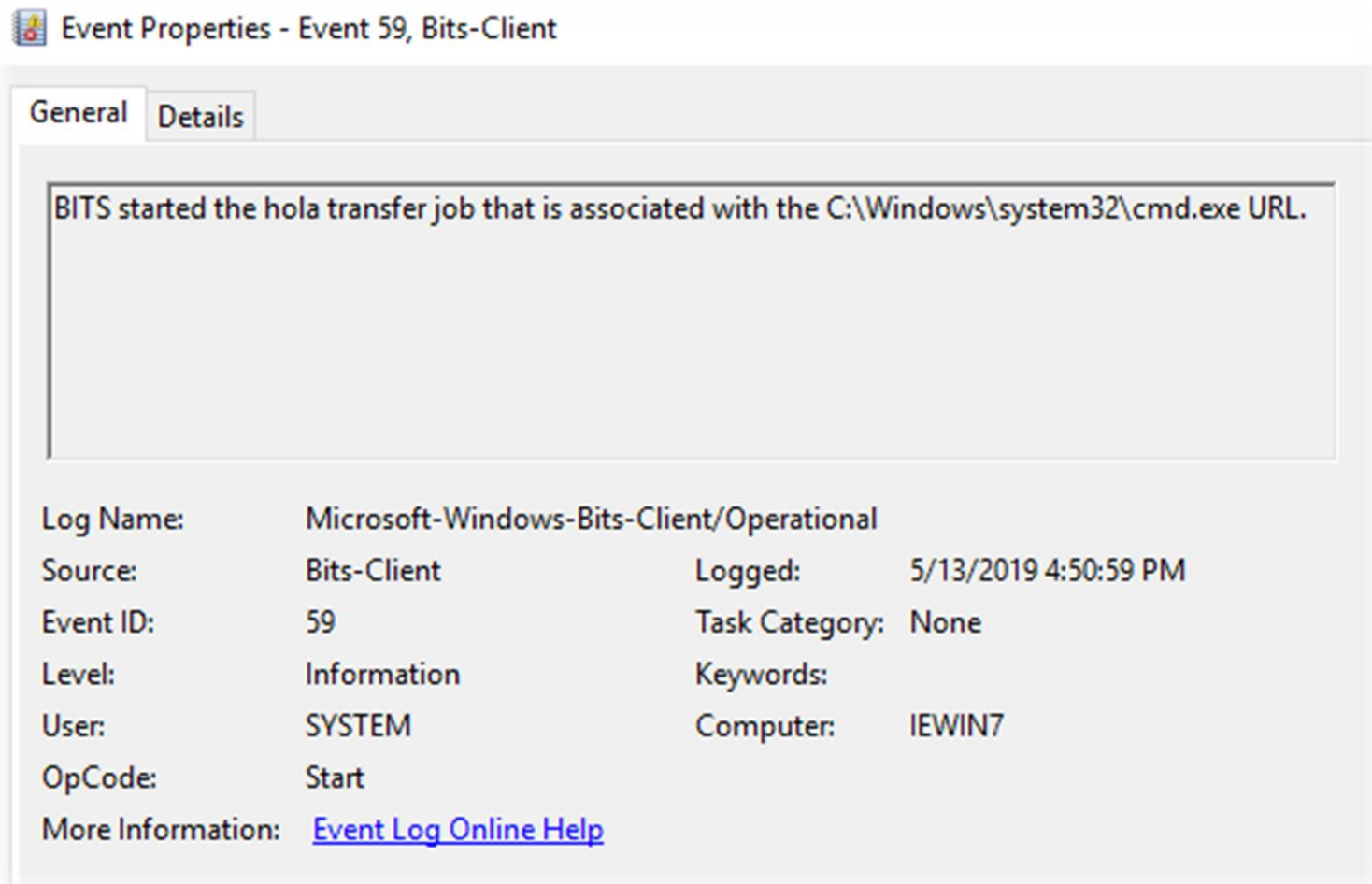
# The Power of Windows EVT

#DFIR – Collection of Events useful for  
Forensics

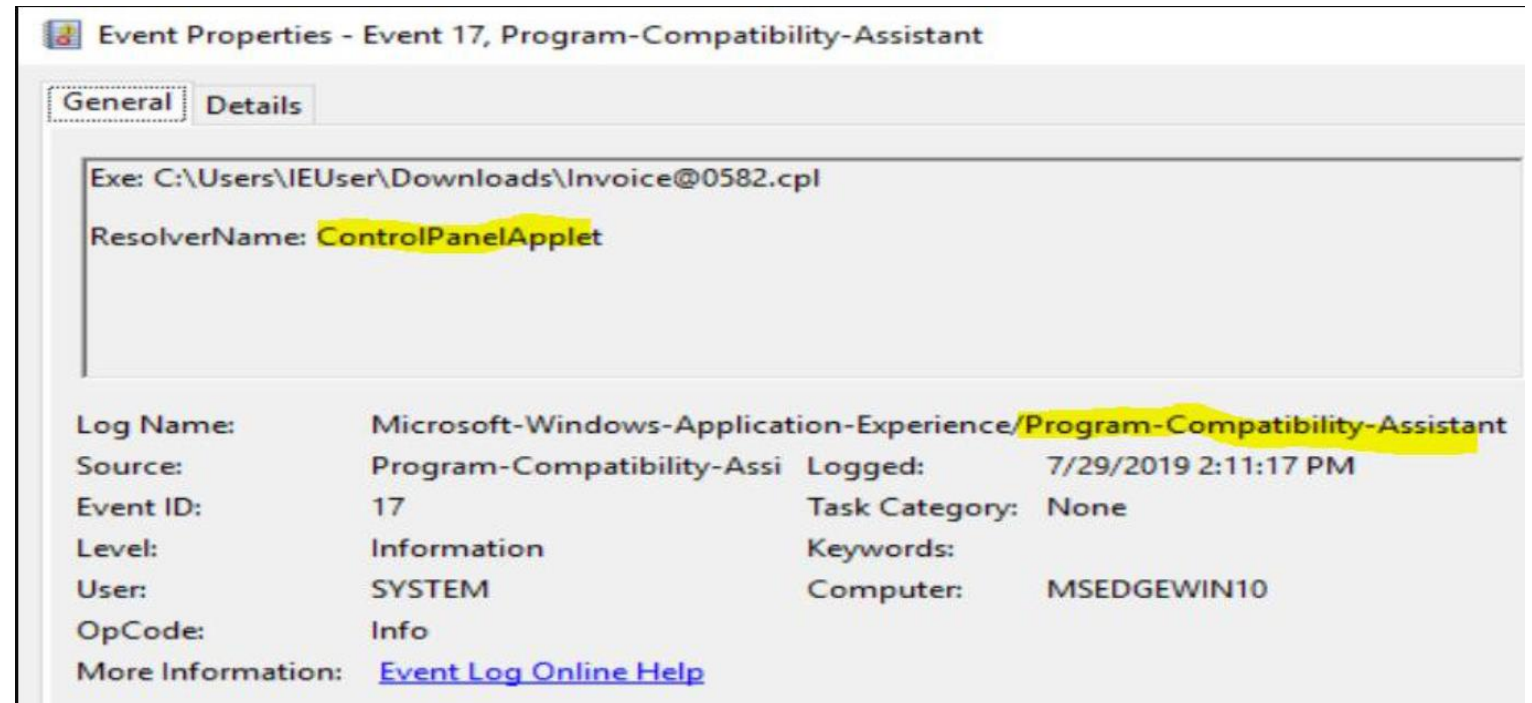
# Persistence – WinSock



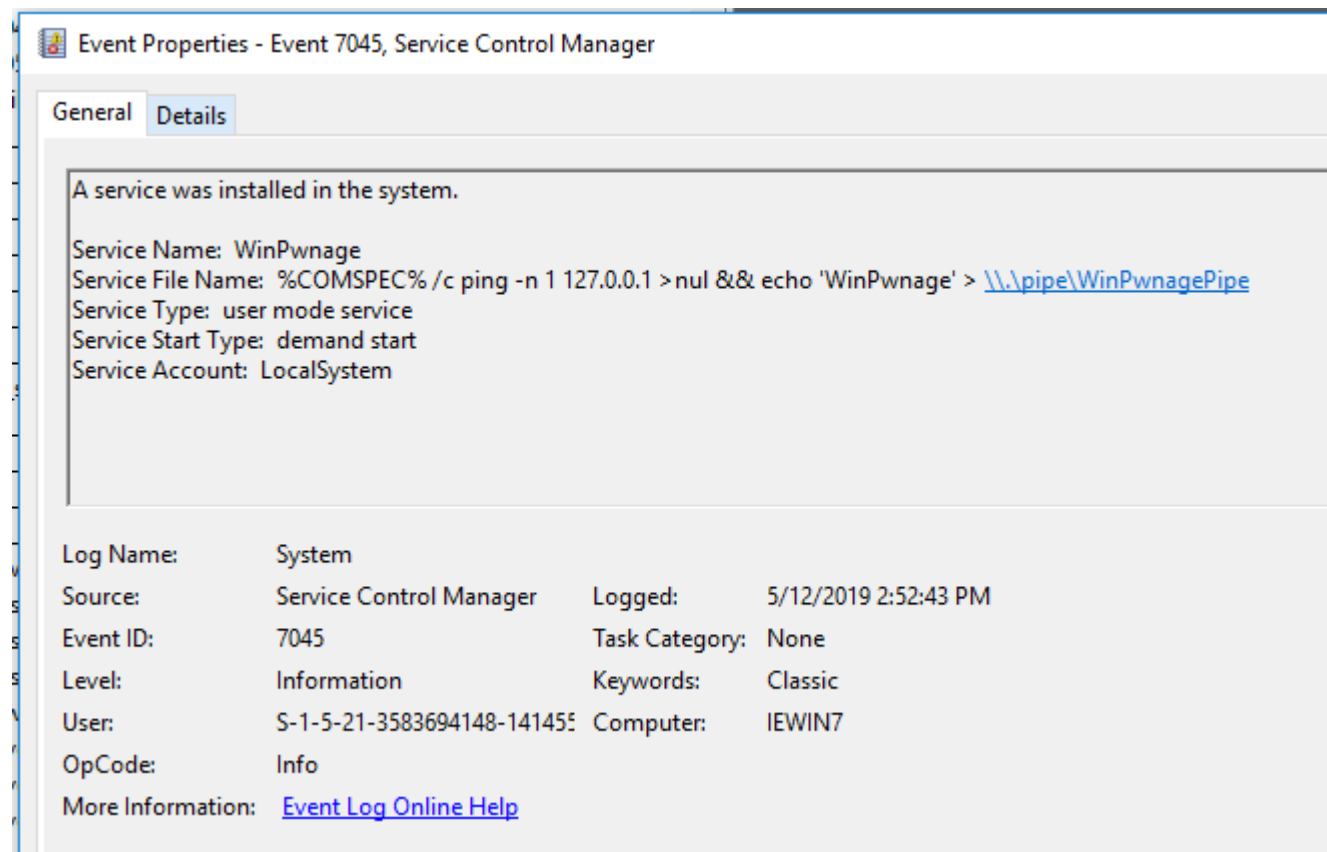
# Persistence – BITS



# Execution - Control Panel



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



# Persistence: Applnit\_DLLs

Event Properties - Event 11, Winit

General Details

Custom dynamic link libraries are being loaded for every application. The system administrator should review the list of libraries to ensure they are related to trusted applications. Please visit <http://support.microsoft.com/kb/197571> for more information.

Log Name: System  
Source: Winit  
Event ID: 11  
Level: Warning  
User: SYSTEM  
OpCode: Info

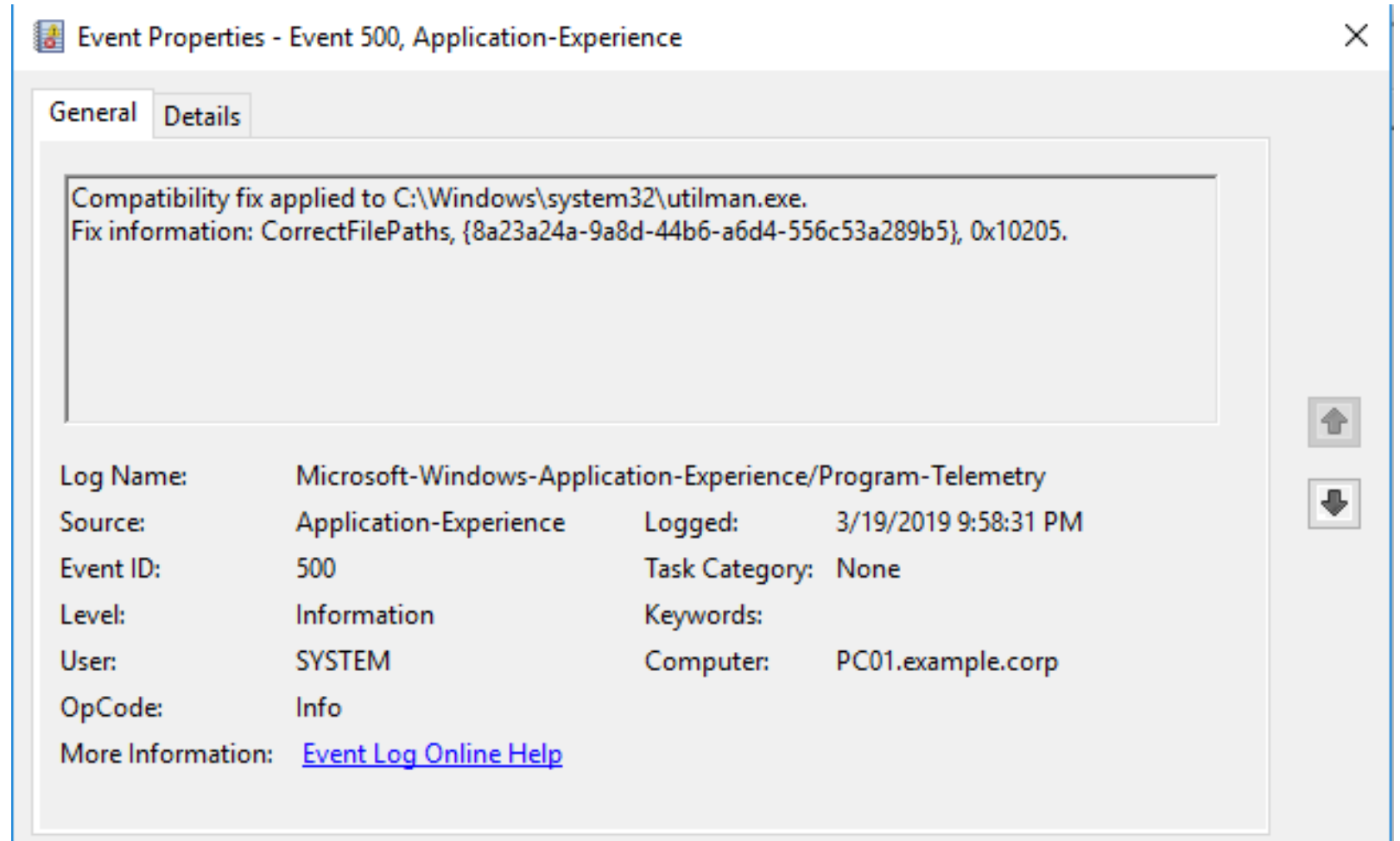
Event Properties - Event 11, Winit

General Details

☐ Friendly View ☒ XML View

```
- <Event
  xmlns="http://schemas.microsoft.com/win/2004/08/events/event"
- <System>
  <Provider Name="Microsoft-Windows-Winit"
    Guid="{206F6DEA-D3C5-4D10-BC72-989F03C8B84B}" />
  <EventID>11</EventID>
  <Version>0</Version>
  <Level>3</Level>
  <Task>0</Task>
  <Opcode>0</Opcode>
  <Keywords>0x4000000000000000</Keywords>
  <EventRecordID>18343</EventRecordID>
  <Correlation />
  <Execution ProcessID="796" ThreadID="824" />
  <Channel>System</Channel>
  <Security UserID="S-1-5-18" />
</System>
- <EventData>
  <Data Name="StringCount">1</Data>
  <Data Name="String">C:\Windows\system32\nvinitx.dll</Data>
</EventData>
</Event>
```

# Traces of Persistence / Accessibility Backdoor via Shim AppPatch



# 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-RdpCoreTS	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:	<a href="#">Event Log Online Help</a>		



# 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:

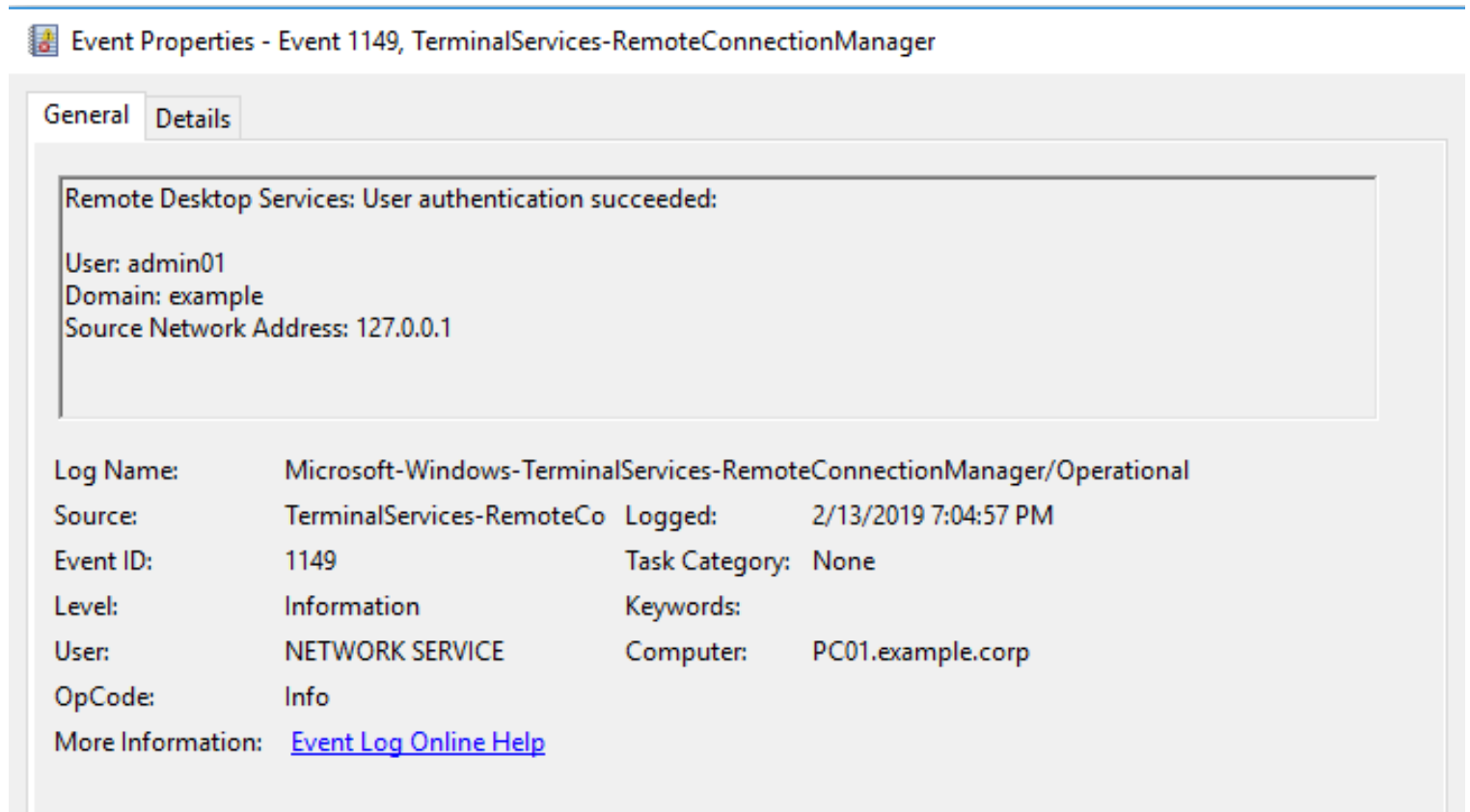
Logon Process:	User32
Authentication Package:	Negotiate
Transited Services:	-
Package Name (NTLM only):	-
Key Length:	0

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



# PrivEsc: Traces of Invoke- TokenDuplication – UAC Bypass hardcoded strings

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	S-1-5-21-3461203602-4096304019-2269080069-1000
Account Name:	IEUser
Account Domain:	MSEDGEWIN10
Logon ID:	0x2E4CE

Logon Information:

Logon Type:	9
Restricted Admin Mode:	-
Virtual Account:	No
Elevated Token:	No

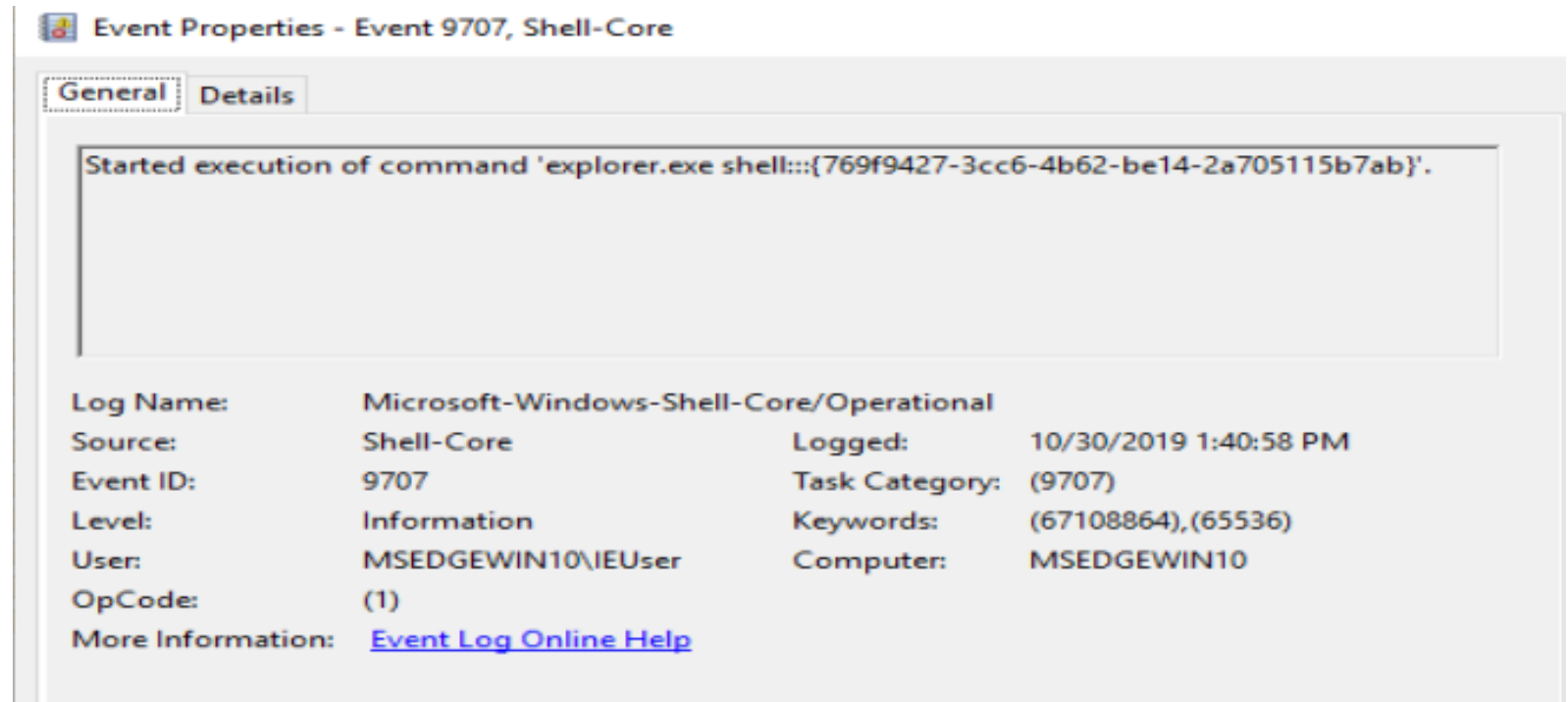
Impersonation Level: Impersonation

New Logon:

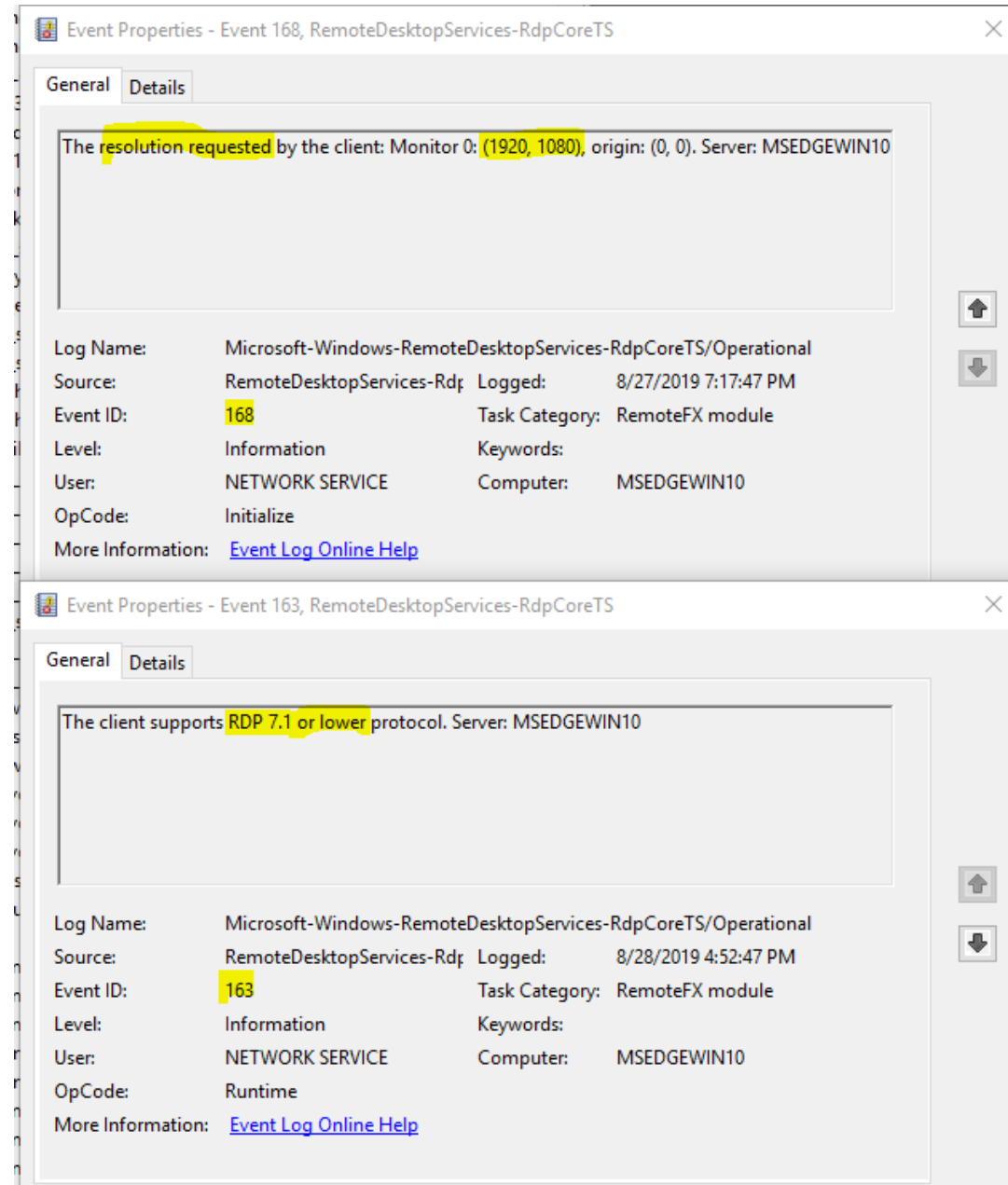
Security ID:	S-1-5-21-3461203602-4096304019-2269080069-1000
Account Name:	IEUser
Account Domain:	MSEDGEWIN10
Logon ID:	0x38F87E
Linked Logon ID:	0x0
Network Account Name:	I
Network Account Domain:	o
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/5/2019 11:39:30 AM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	MSEDGEWIN10
OpCode:	Info		
More Information:	<a href="#">Event Log Online Help</a>		

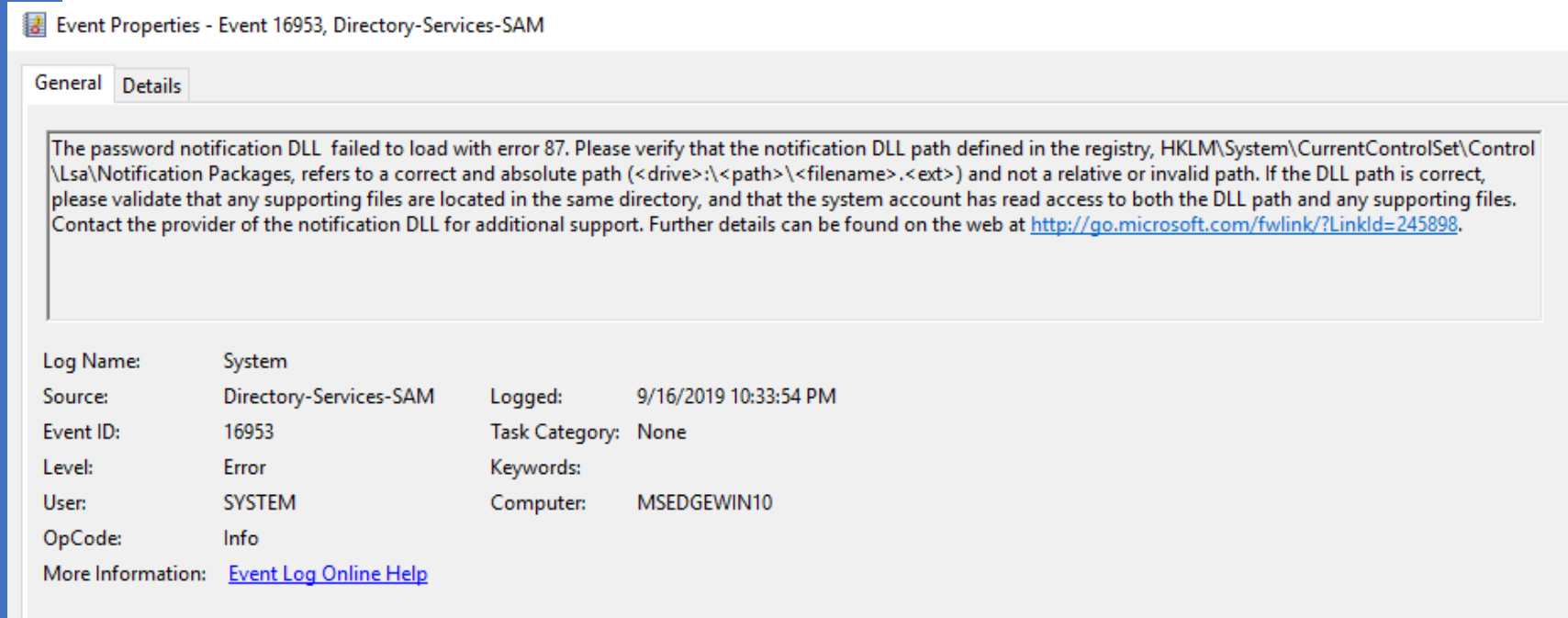
# Traces of Persistence via Run/RunOnce (9707, 9708)



# Lateral Movement Obsolete RDC “RDP Client” Info (xfreerdp)



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



# Execution - Traces of unsigned Drivers/Modules

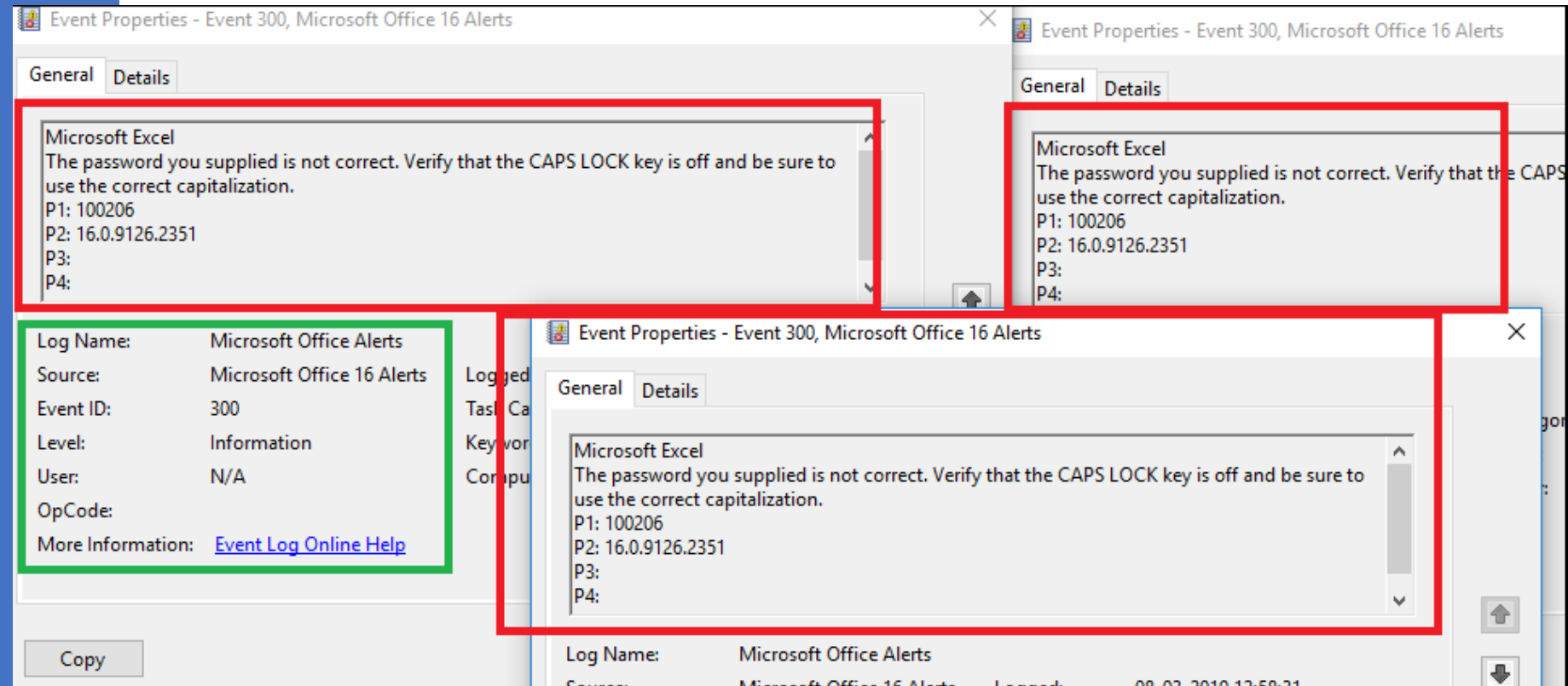
Event Properties - Event 3001, CodeIntegrity

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:	<a href="#">Event Log Online Help</a>		

# Traces of Brute forcing Protected Office File





# Traces of Phishing via DDE

