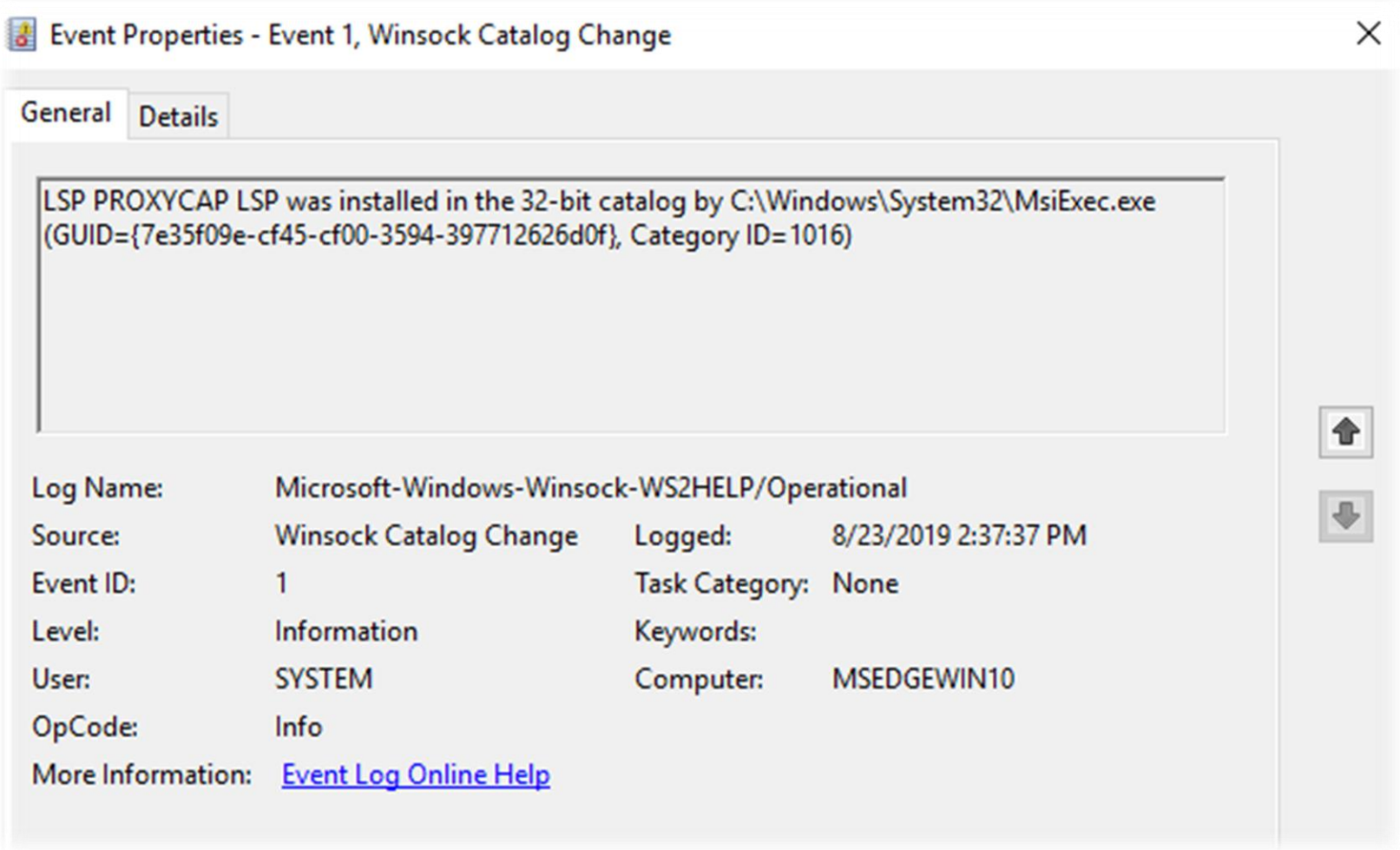
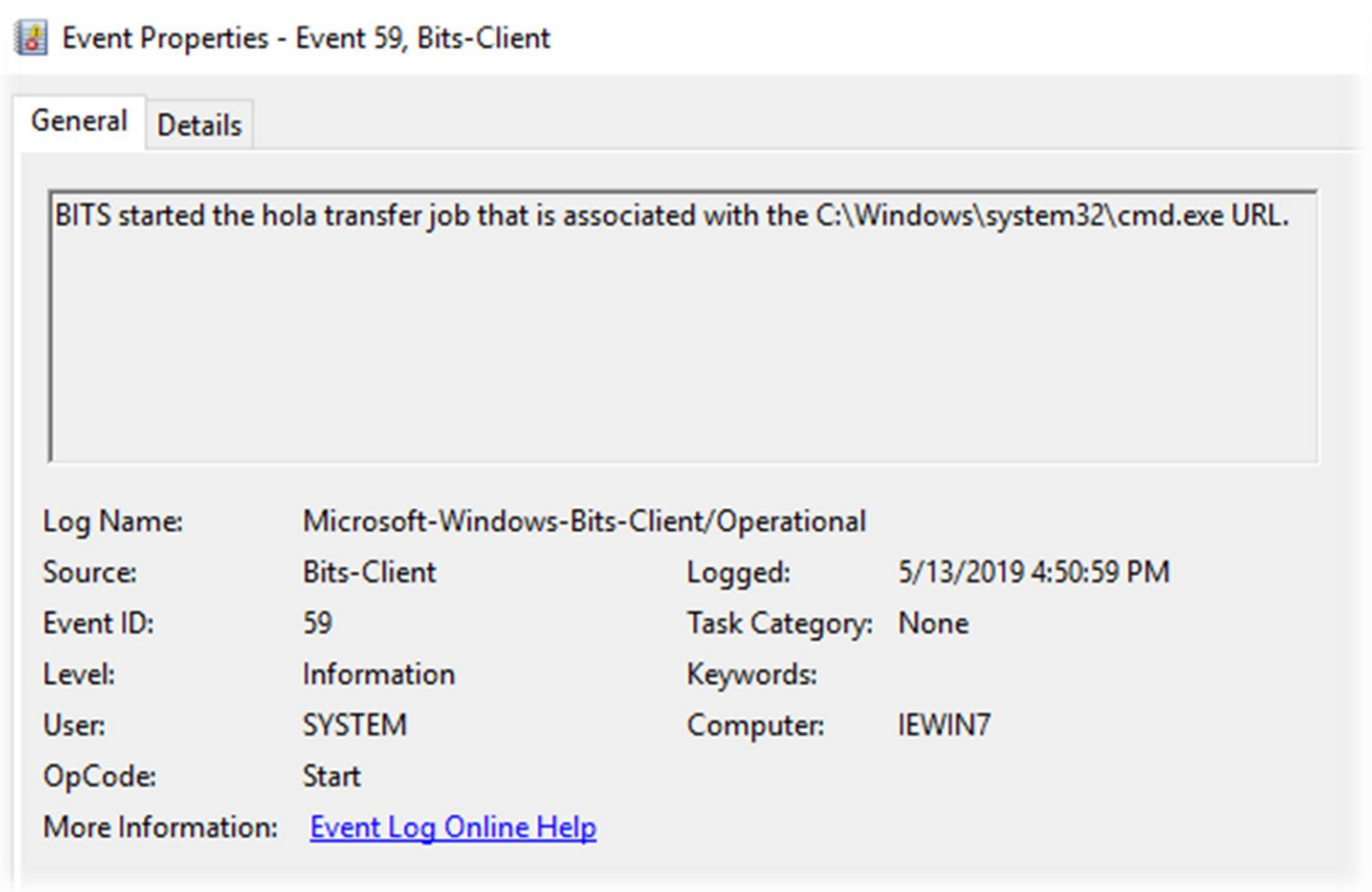
Author: @SBousseaden

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

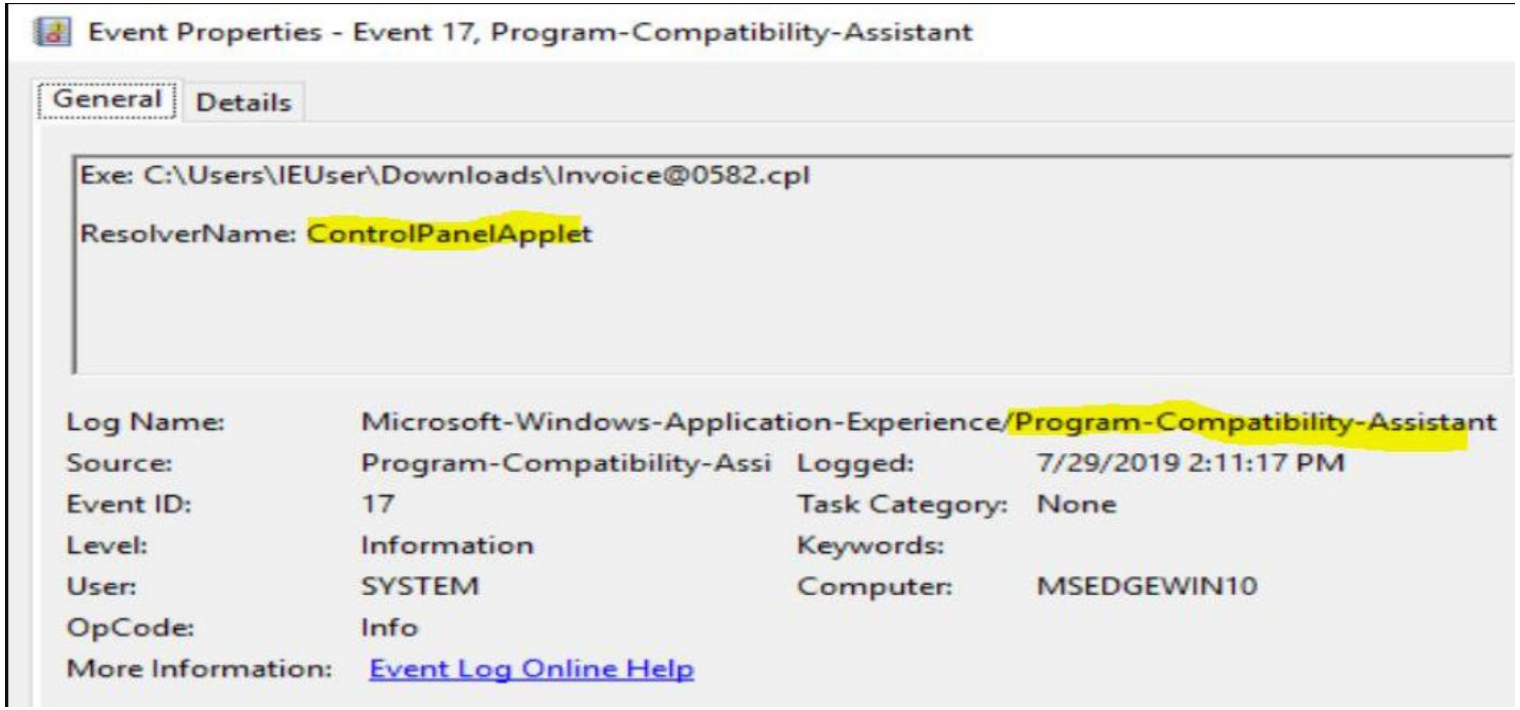
# Persistence – WinSock



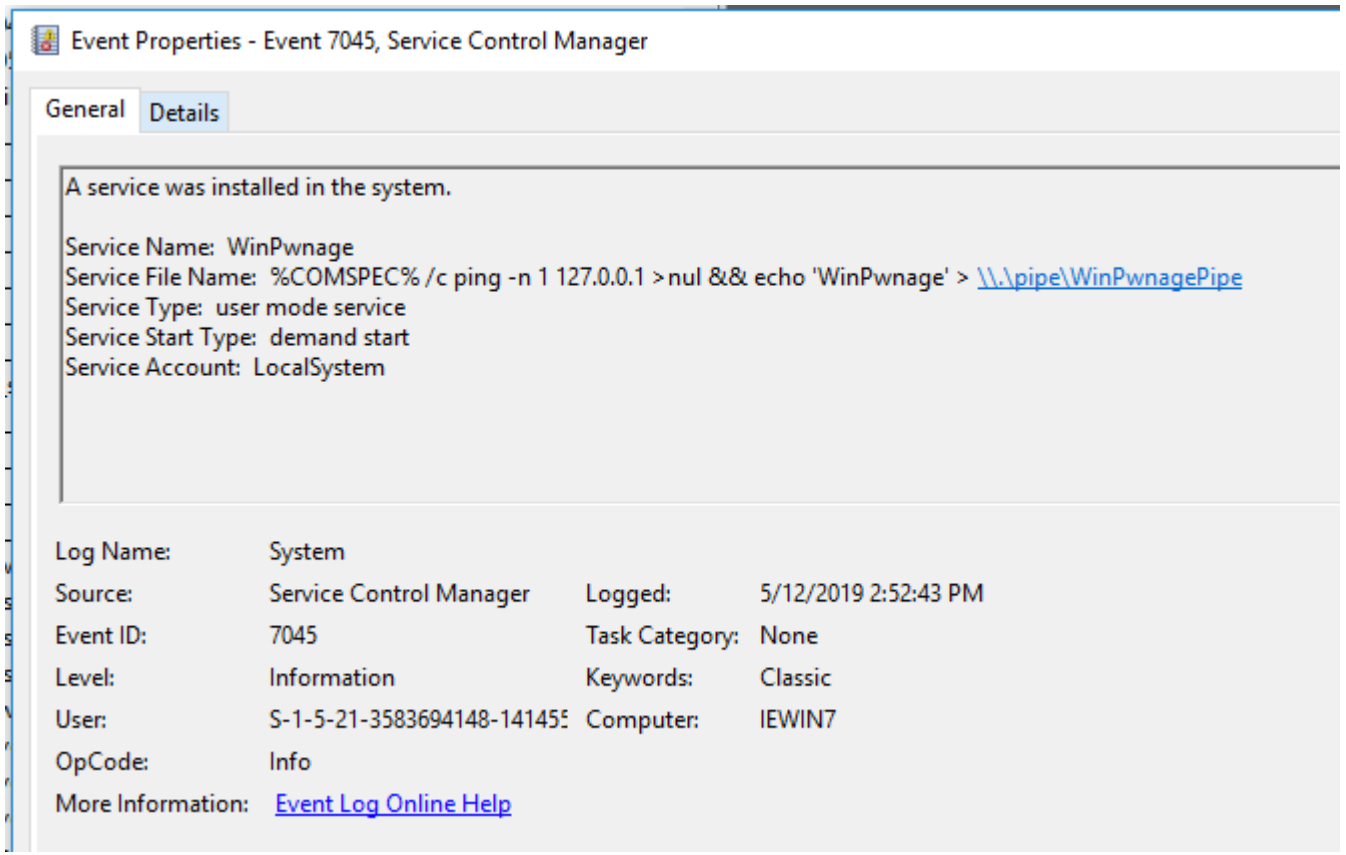
# Persistence – BITS



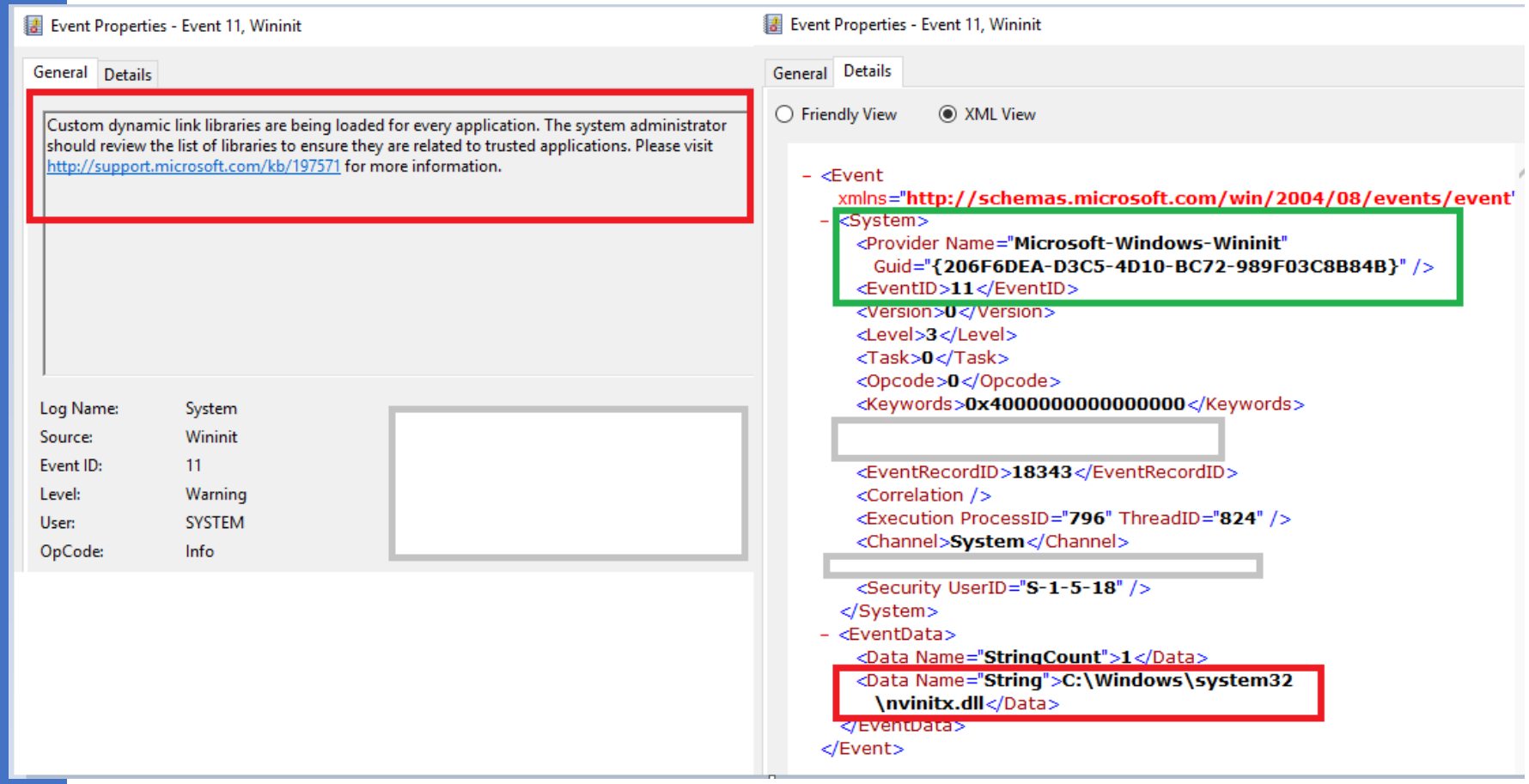
# Execution - Control Panel



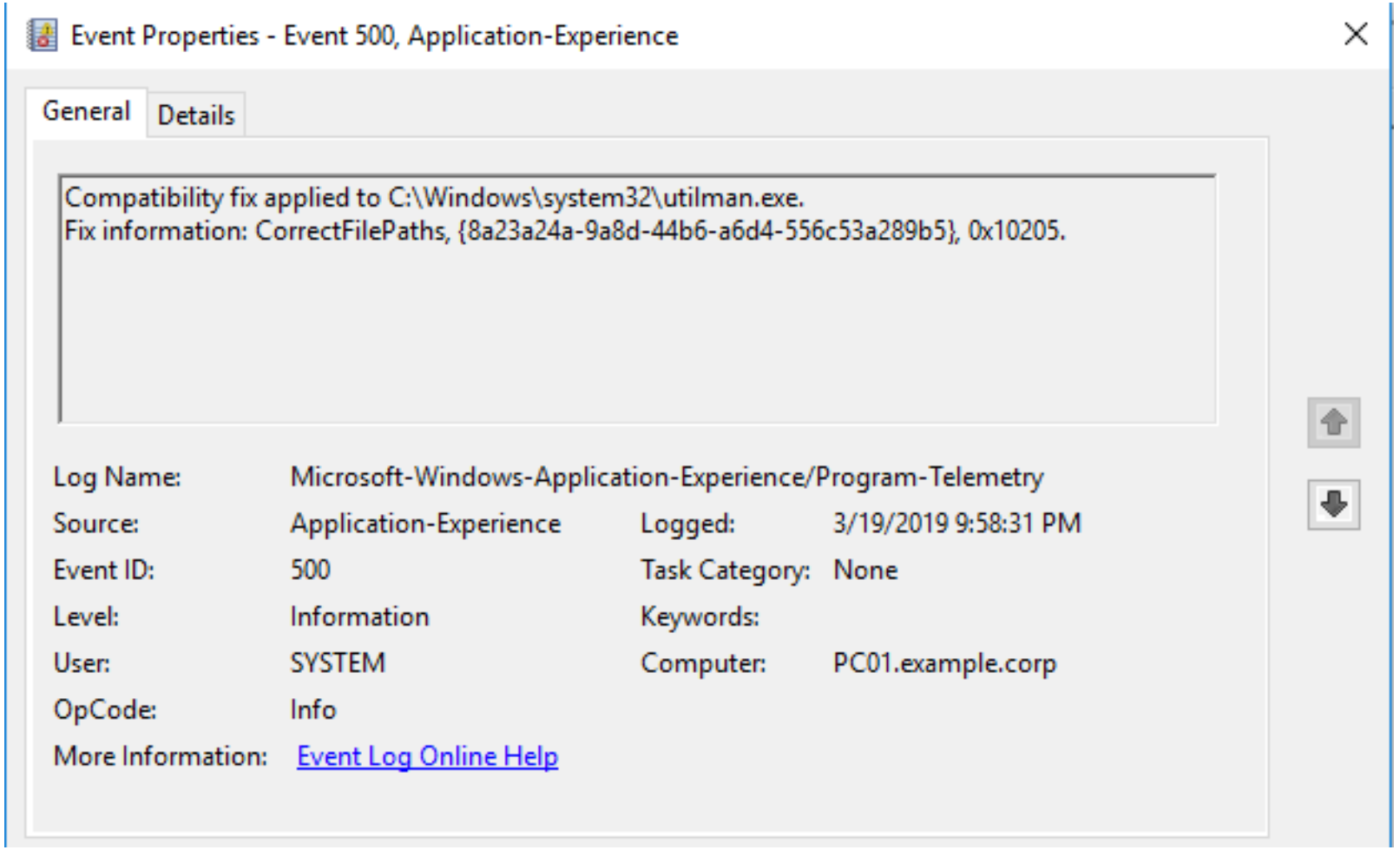
# Traces of PrivEsc (np's privileged client token imperson)



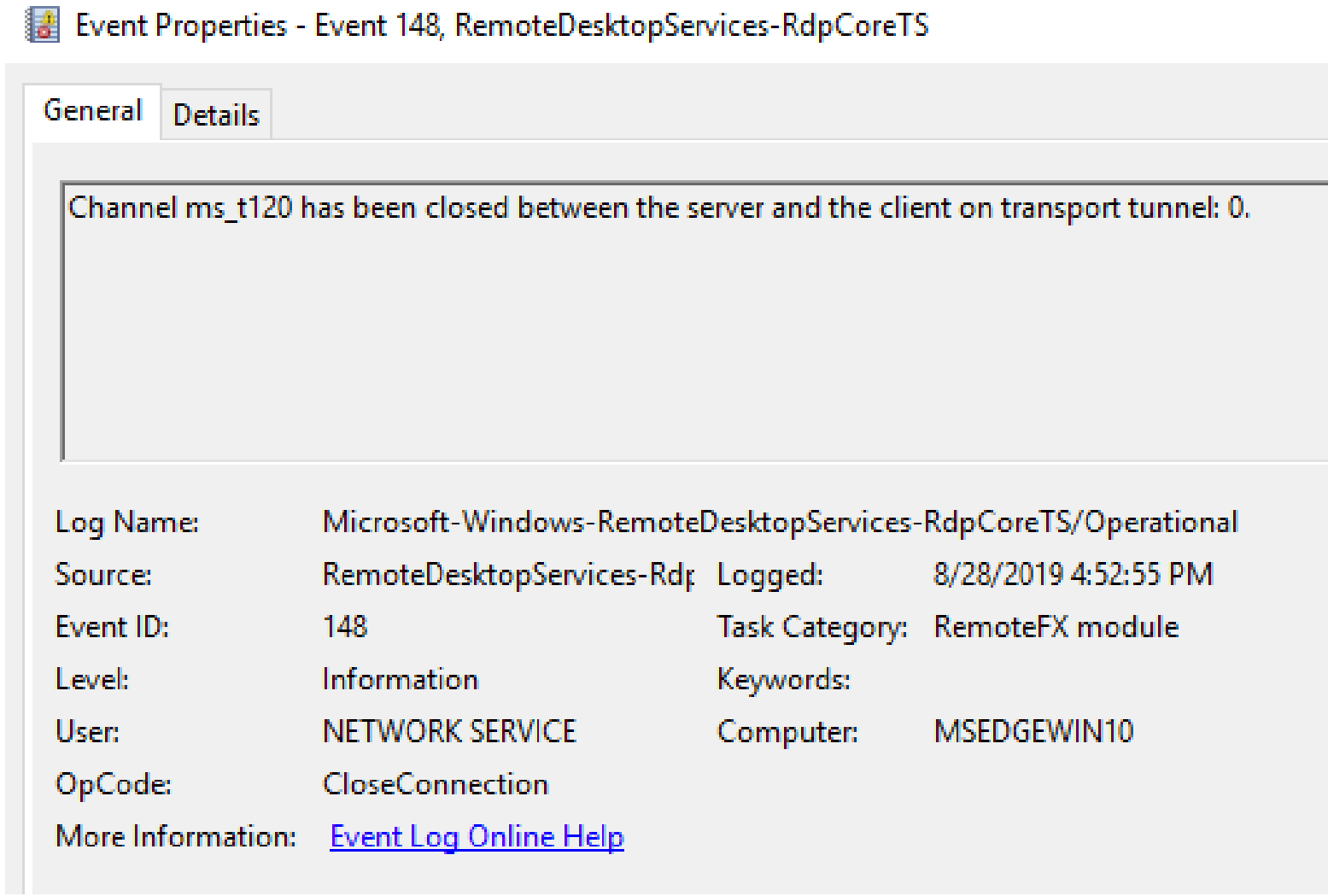
# Persistence: AppInit_DLLs



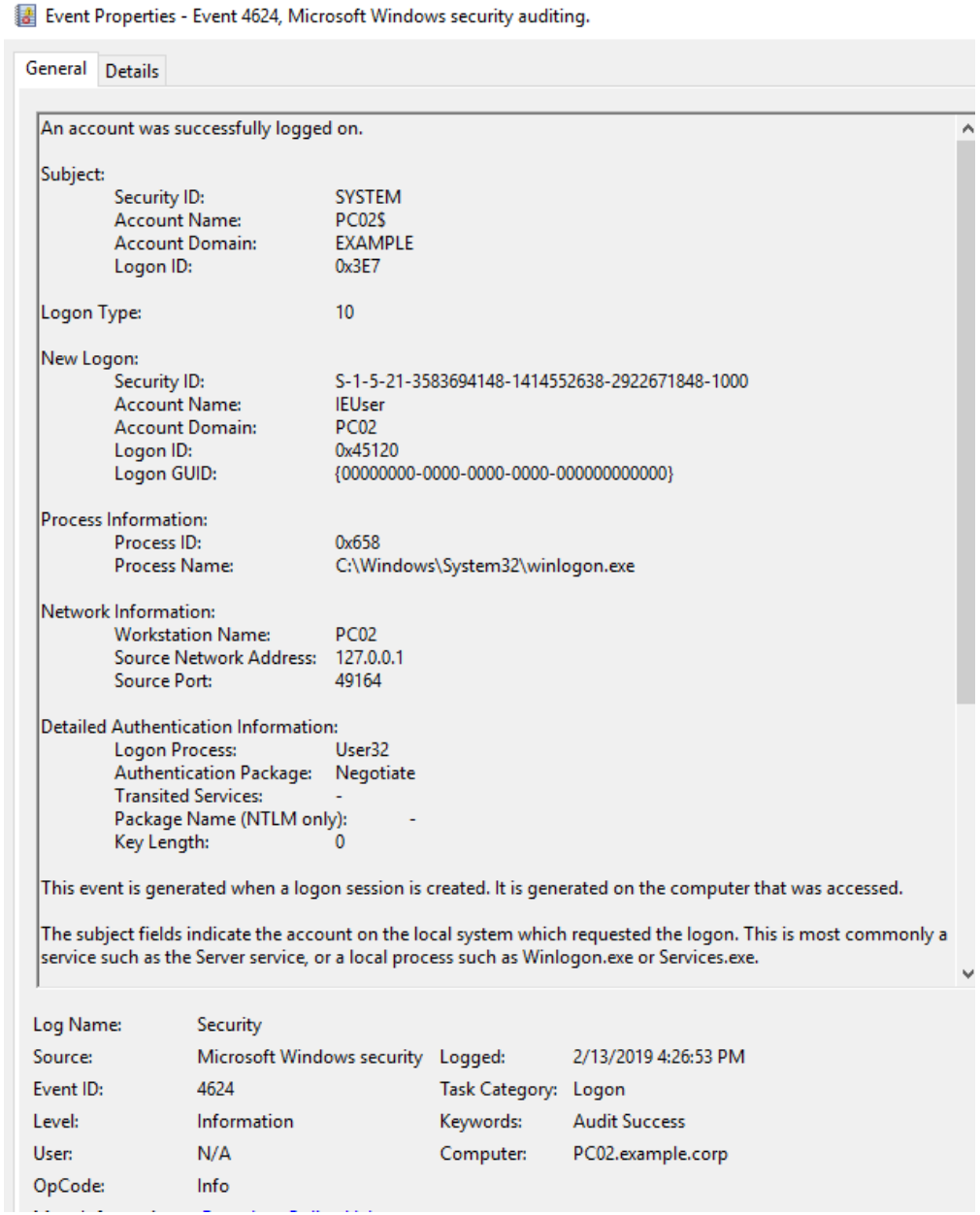
# Traces of Persistence / Accessibility Backdoor via Shim AppPatch



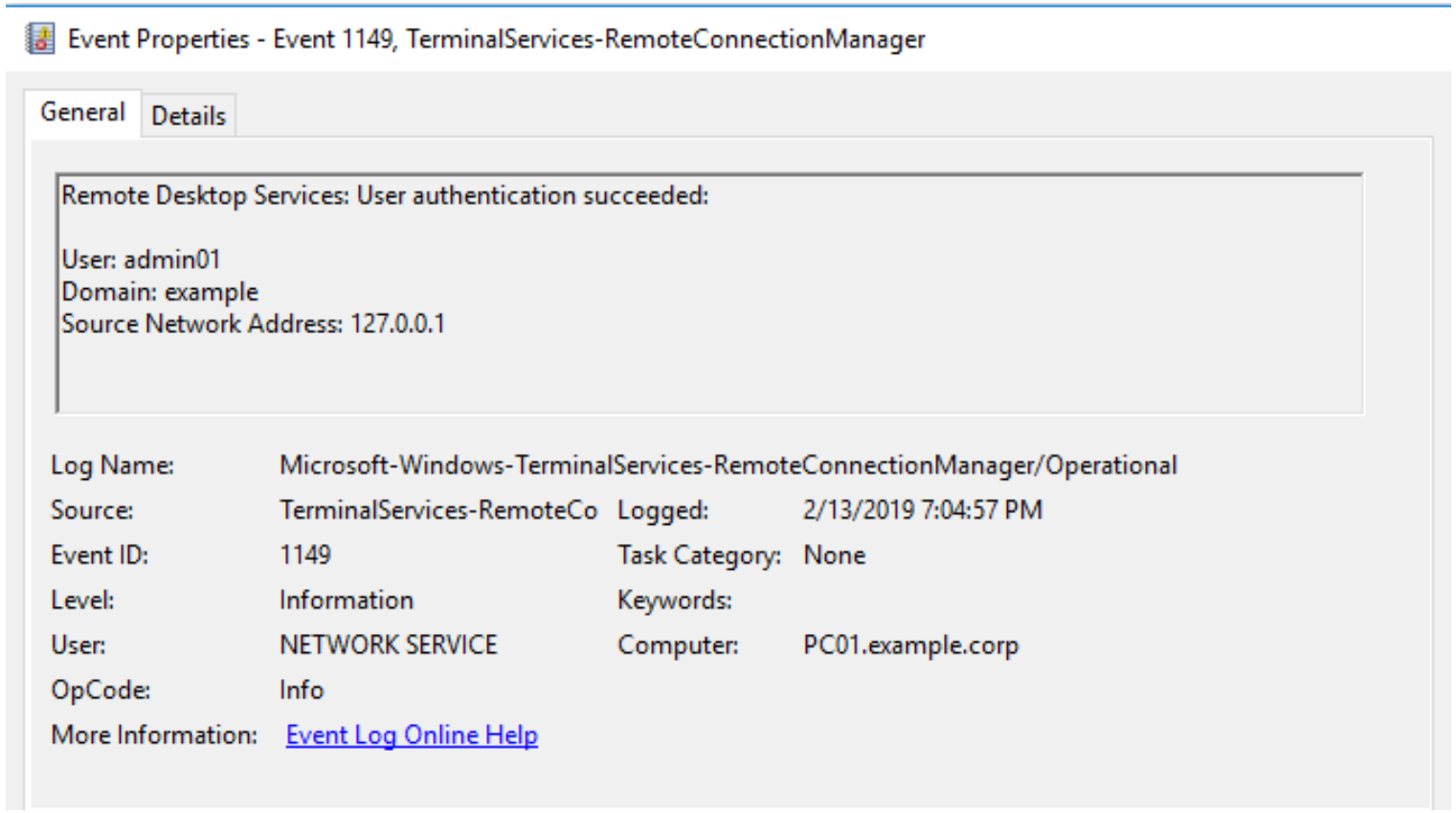
# Traces of BlueKeep Scan Traces on Win10 “ms_t120 chan”



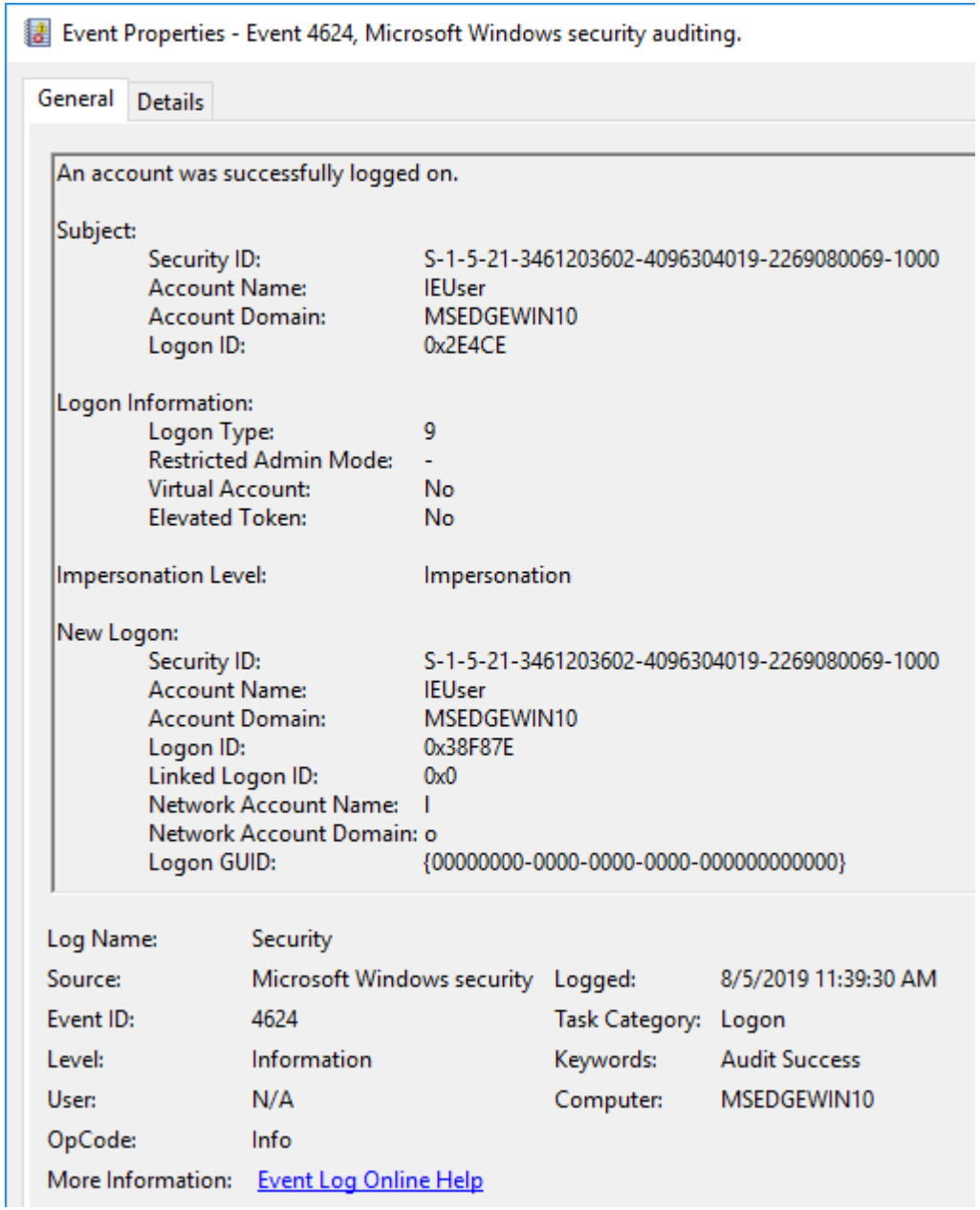
# Traces of RDP Tunneling



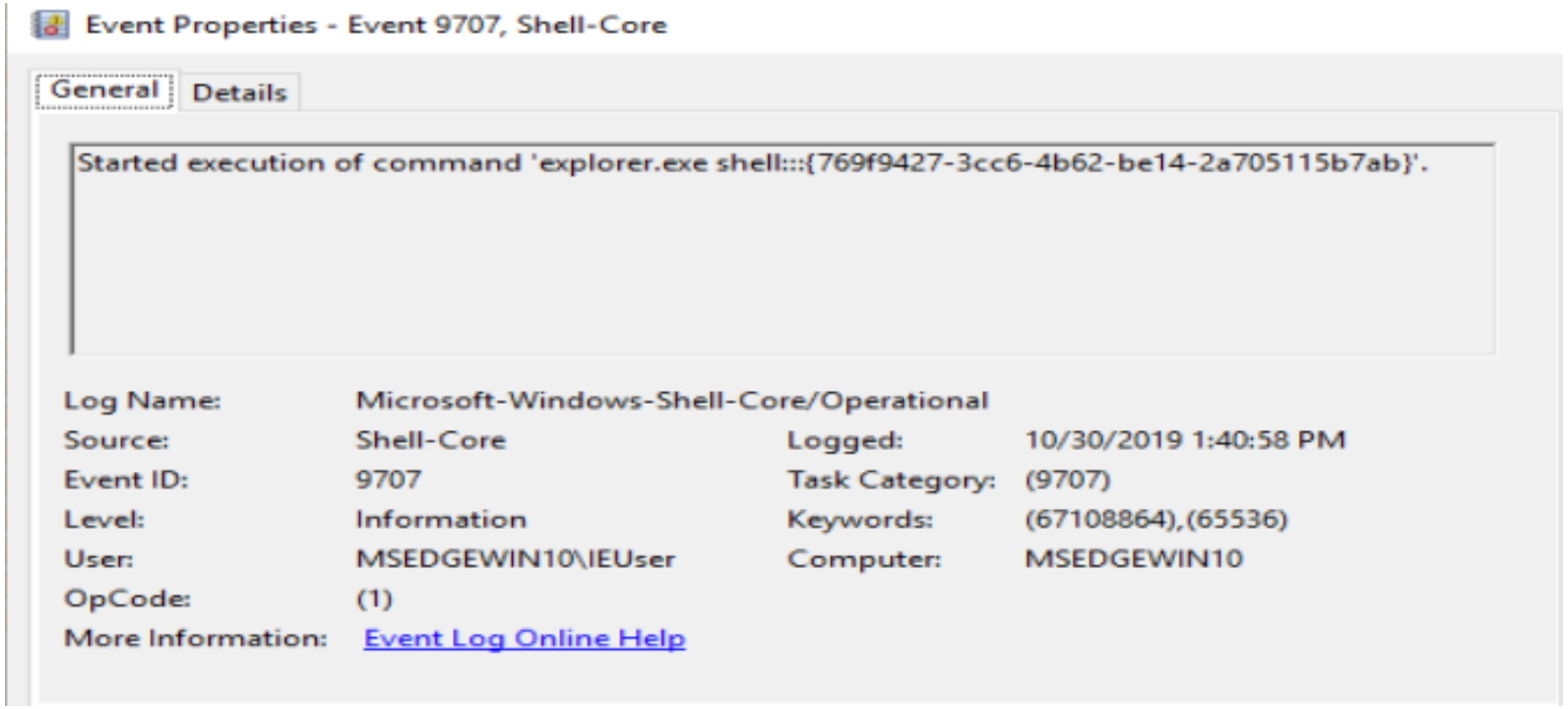
# Traces of RDP Tunneling



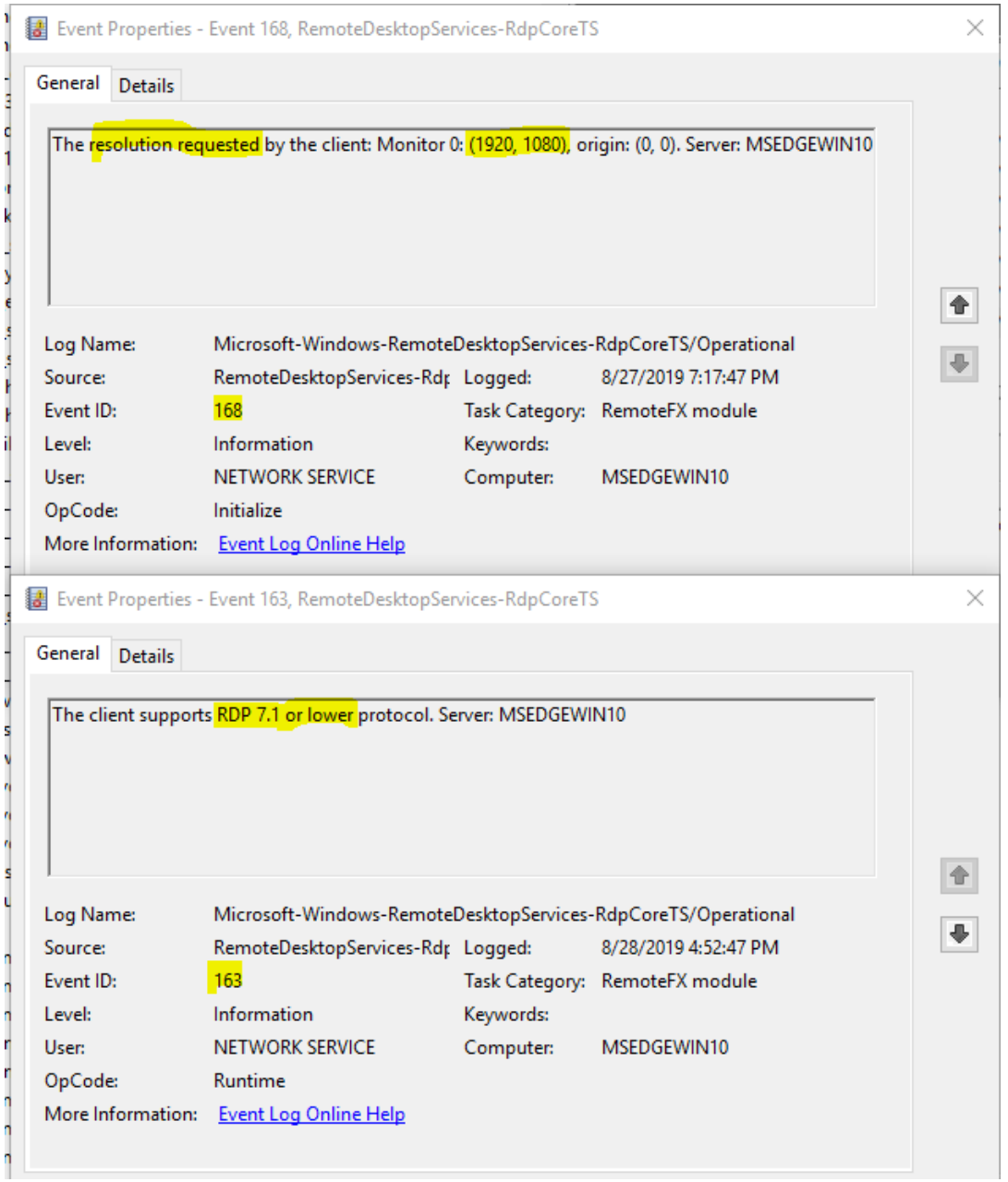
# PrivEsc: Traces of Invoke-ToeknDuplication – UAC Bypass hardcoded strings



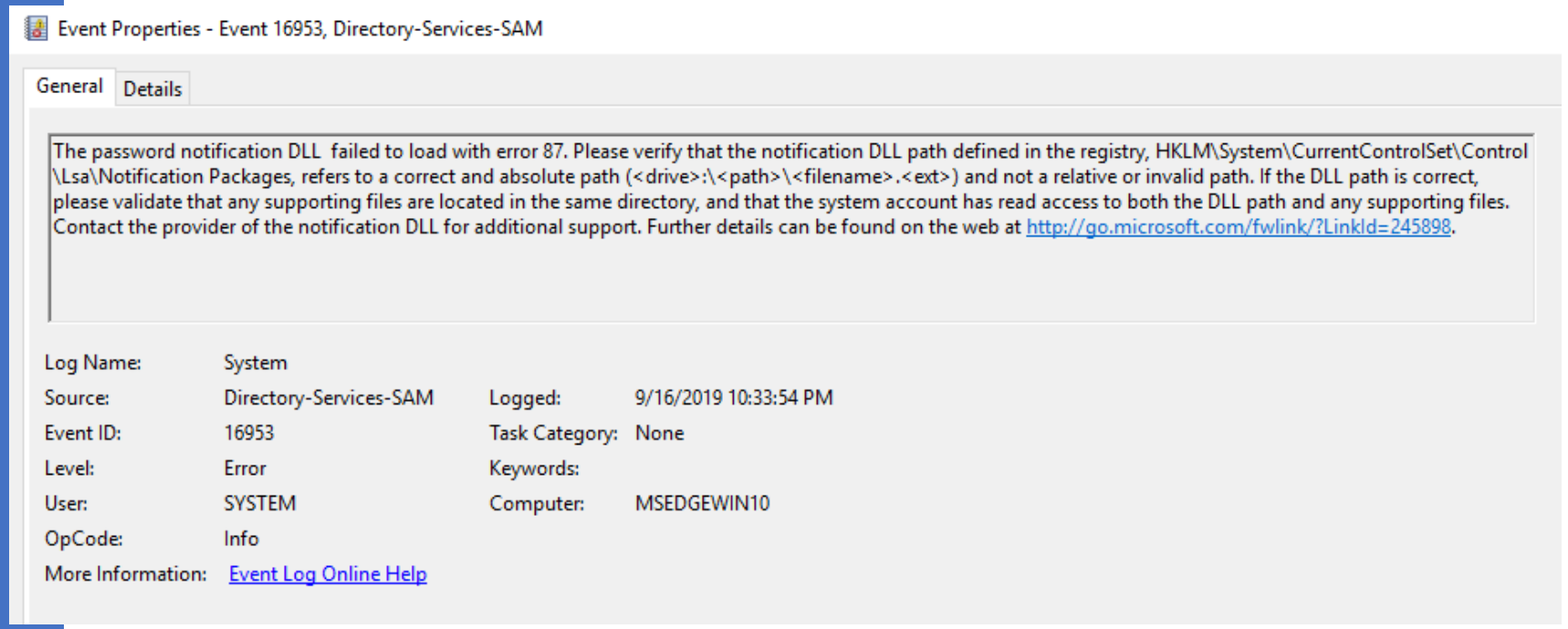
# Traces of Persistence via Run/RunOnce (9707, 9708)



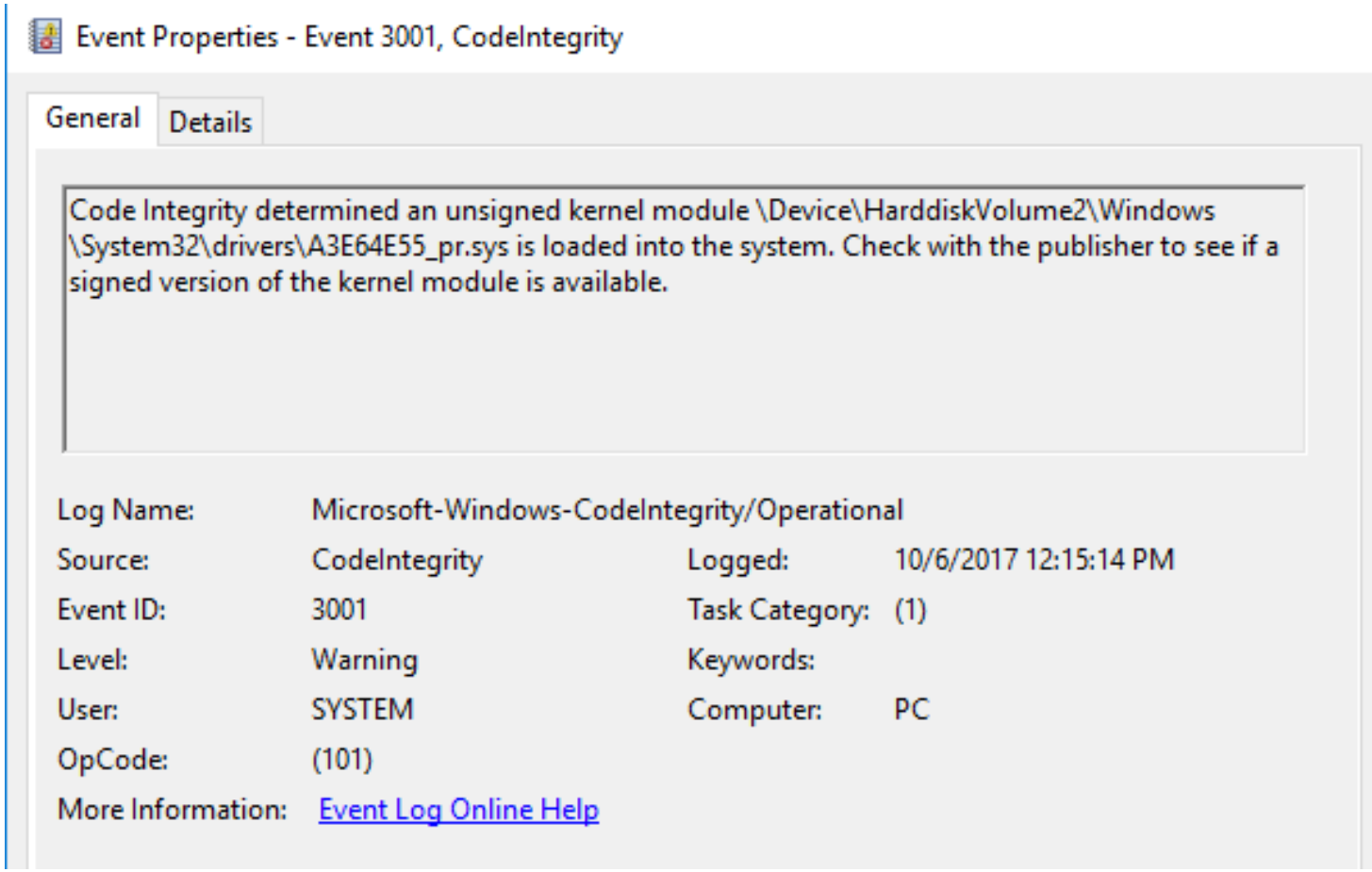
# Lateral Movement Obsolete RDC “RDP Client” Info (xfreerdp)



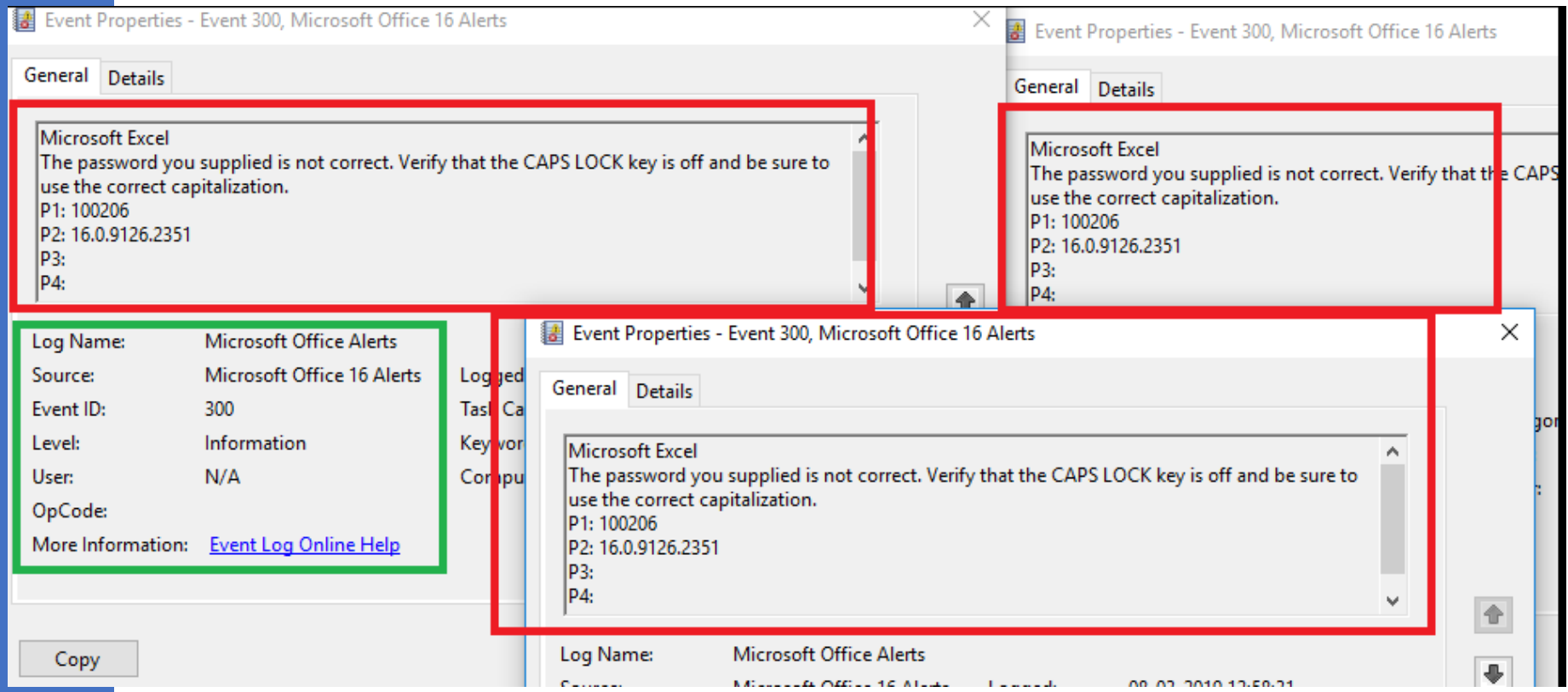
# Traces of previous "Lsa Notification Packages" [T1174: Password Filter] cleaned or corrupted entry - EventID 16953



# Execution - Traces of unsigned Drivers/Modules



# Traces of Brute forcing Protected Office File



# Traces of Phishing via DDE