LEGACY SEARCH PROCESSING LANGUAGE (SPL) SPLUNK FORMAT:

Execution Of Whoami

- FileName=whoami.exe

Netcat

- FileName=netcat.exe OR FileName=ncat.exe OR CommandLine="*nc*"

Bloodhound Activity

- event_simpleName=NetworkConnect* RemotePort_decimal=445 AND FileName=ntoskrnl.exe AND FileName=*

- FileTimestampsModified=sessions.csv OR FileTimestampsModified=acls.csv OR FileTimestampsModified=group_membership.csv OR FileTimestampsModified=local_admins.csv OR FileTimestampsModified=computer_props.csv OR FileTimestampsModified=user.props.csv
  | table _time FileTimestampsModified TargetFileName

Malicious Office Documents

- (ParentBaseFileName=excel.exe OR ParentBaseFileName=winword.exe OR ParentBaseFileName=outlook.exe) AND FileName=csc.exe

- event_simpleName=ProcessRollup2 (FileName=powerpnt.exe OR FileName=excel.exe OR FileName=word.exe)
  | rename FileName as ParentFile
  | rename CommandLine as ParentCmd
  | table aid TargetProcessId_decimal ParentFile ParentCmd
  | join max=0 aid TargetProcessId_decimal
  [search event_simpleName=ProcessRollup2 FileName=cmd.exe OR FileName=powershell.exe OR FileName=cscript.exe OR FileName=wscript.exe
  | rename ParentProcessId_decimal as TargetProcessId_decimal
  | rename FilePath as ChildPath
  | dedup aid TargetProcessId_decimal MD5HashData
  | fields aid TargetProcessId_decimal FileName CommandLine]
  | table _time ParentFile ParentCmd FileName CommandLine aid

Payload Download or Creation

- event_simpleName=ProcessRollup2 (FileName=excel.exe OR FileName=winword.exe OR FileName=outlook.exe)
  | rename FileName as ParentFile
  | rename CommandLine as ParentCmd
  | table aid TargetProcessId_decimal ParentFile ParentCmd
  | join max=0 aid TargetProcessId_decimal
  [search event_simpleName=ProcessRollup2 FileName=csc.exe
  | rename ParentProcessId_decimal as TargetProcessId_decimal
  | rename FilePath as ChildPath
  | dedup aid TargetProcessId_decimal MD5HashData
  | fields aid TargetProcessId_decimal FileName CommandLine]
  | table _time ParentFile ParentCmd FileName CommandLine aid

- (ParentImageFileName=powershell.exe OR ParentImageFileName=cmd.exe OR ParentImageFileName=mshta.exe OR ParentImageFileName=explorer.exe OR ParentImageFileName=wmiprvse.exe) AND FileName=msbuild.exe

Execution/File Changes In C:\Perflogs

- (event_simpleName=ProcessRollup2 OR event_simpleName=SyntheticProcessRollup2) AND ImageFileName="*\\perflogs*"
  | regex ImageFileName=".*\\\\perflogs\\\\\w+\.exe"
  | table ComputerName UserName ImageFileName FileName SHA256HashData

Execution In C:\Temp

- (event_simpleName=ProcessRollup2 OR event_simpleName=SyntheticProcessRollup2) AND ImageFileName="*\\temp*"
  | regex ImageFileName=".*\\\\temp\\\\\w+\.exe"
  | table ComputerName UserName ImageFileName FileName SHA256HashData

- (event_simpleName=ProcessRollup2 OR event_simpleName=SyntheticProcessRollup2) AND ImageFileName="*\\windows\\temp*"
  | regex ImageFileName=".*\\\\windows\\\\temp\\\\\w+\.exe"
  | table ComputerName UserName ImageFileName FileName SHA256HashData

Execution Of Scheduled Task Exe's

- event_simpleName=ScheduledTask*

- FileName=at.exe OR (FileName=schtasks.exe AND CommandLine=*create)

Webshell Activity

- ParentImageFileName=php.exe (FileName=cmd.exe OR FileName=powershell.exe)

- ParentImageFileName=w3wp.exe (FileName=cmd.exe OR FileName=powershell.exe)

- ParentImageFileName=httpd.exe (FileName=cmd.exe OR FileName=powershell.exe)

- ParentImageFileName=w3wp.exe AND (FileName=cmd.exe OR FileName=powershell.exe OR FileName=whoami.exe OR FileName=netstat.exe OR FileName=ipconfig.exe)

WMI Process Creation & Activity

- FileName=wmic.exe AND CommandLine=*create*

- CommandLine="*wmic /node:*"

Cobalt Strike

- "*\\windows\\syswow64\\ntmarta\.dll" AND FileName=svchost.exe

- ("*\\iertutil.dll" OR "*\\ntmarta.dll") AND FileName=rundll32.exe

Suspicious Powershell

- FileName=powershell.exe AND (CommandLine="*-NoP" OR CommandLine="*-NoProfile")

- FileName=powershell.exe AND event_simpleName=NetworkConnect*

- FileName=powershell.exe AND (CommandLine="*-enc" OR CommandLine="*-EncodedCommand" OR CommandLine="*-E")

- FileName=powershell.exe AND CommandLine=*hidden)

- FileName=powershell.exe AND CommandLine=*iex

- ParentImageFileName=wsmprovhost.exe AND FileName=*
  | stats count
  | where count > 1

- event_simpleName=NetworkConnect* ParentImageFileName=wsmprovhost.exe AND FileName=*
  | stats count
  | where count > 1

- event_simpleName=ProcessRollup2 FileName=powershell.exe (CommandLine=*-enc* OR CommandLine=*encoded*)

Mimikatz

- FileTimestampsModified=advapi32.dll AND FileTimestampsModified=crypt32.dll AND FileTimestampsModified=cryptdll.dll AND
  FileTimestampsModified=gdi32.dll AND FileTimestampsModified=imm32.dll AND FileTimestampsModified=kernel32.dll AND
  FileTimestampsModified=KernelBase.dll AND FileTimestampsModified=msasn1.dll AND FileTimestampsModified=msvcrt.dll
  AND FileTimestampsModified=ntdll.dll AND FileTimestampsModified=rpcrt4.dll AND FileTimestampsModified=rsaenh.dll
  AND FileTimestampsModified=samlib.dll AND FileTimestampsModified=sechost.dll AND FileTimestampsModified=secur32.dll
  AND FileTimestampsModified=shell32.dll AND FileTimestampsModified=shlwapi.dll
  AND FileTimestampsModified=sspicli.dll AND FileTimestampsModified=user32.dll AND FileTimestampsModified=vaultcli.dll

- FileName=mimikatz.exe

- "gentilkiwi (Benjamin DELPY)"

- FileName=lsass.exe AND "*mimilsa.log"

Modifications To Files In C:\Windows\System32

- FileTimestampsModified="*system32*"
  | dedup FileName
  | stats values(FileName)

Files of Interest Making Connections

- event_simpleName=NetworkConnect* AND (FileName=cmd.exe OR FileName=powershell.exe OR FileName=wmic.exe OR FileName=msbuild.exe OR FileName=mshta.exe
  OR FileName=wscrpit.exe OR FileName=cscript.exe OR FileName=installutil.exe OR FileName=rundll32.exe OR FileName=regsvr32.exe OR FileName=msxsl.exe OR FileName=regasm.exe)

Use Of Meterpreter Default Port

- event_simpleName=NetworkConnect* AND "4444"

Search For Remote Access Programs

- FileName=dameware* OR FileName=vnc* OR FileName=teamv* OR FileName=screenc* OR FileName=remcom* OR FileName=logmein*

Data Exfiltration

- FileName=ssh.exe OR FileName=ftp* OR FileName=sftp* OR FileName=winscp* OR FileName=filezilla*

Ntds.Dit Theft

- FileName=esentutl.exe OR FileName=ntdsutil.exe OR FileName=wbadmin.exe

Net Activity

- FileName=net*.exe AND CommandLine="*user /add*"
- FileName=net*.exe AND CommandLine="*localgroup*"
- FileName=net*.exe AND CommandLine="*group*"
- FileName=net* AND CommandLine="*active*"
- FileName=net* AND CommandLine="*add*"

Common Recon Tools

- event_simpleName=ProcessRollup2 (FileName=net.exe OR FileName=ipconfig.exe OR FileName=whoami.exe OR FileName=quser.exe OR FileName=ping.exe OR FileName=netstat.exe OR FileName=tasklist.exe OR FileName=Hostname.exe OR FileName=at.exe)

Execution From Recycle Bin

- ImageFileName=*$Recycle.Bin* event_simpleName=ProcessRollup2 | stats values(name) values(MD5HashData) values(ComputerName) values(ImageFileName) count by aid

Svchost Running Outside Of System32

- event_simpleName=ServiceStarted ImageFileName="*\\svchost.exe" ImageFileName!="*\\System32*" | table aid ServiceDisplayName ImageFileName CommandLine ClientComputerName RemoteAddressIP4 RemoteAddressIP6

Lsass Running Outside System32

- ImageFileName!="*\\Windows\\System32\\lsass.exe" AND "*lsass.exe"

NEW LogScale CROWDSTRIKE QUERY LANGUAGE (CQL) FORMAT:

Execution Of Whoami

- #event_simpleName=ProcessRollup2

  | FileName = whoami.exe

  | rename(field="@timestamp", as="Time")

  | Time:=formatTime(format="%F %T", field="Time")

  | table([Time, ComputerName, UserName, FileName, FilePath])

Netcat

- #event_simpleName=ProcessRollup2

  | FileName = netcat.exe OR FileName = ncat.exe

  | rename(field="@timestamp", as="Time")

  | Time:=formatTime(format="%F %T", field="Time")

  | table([Time, ComputerName, UserName, FileName, FilePath, CommandLine])

Bloodhound Activity

- #event_simpleName=NetworkConnect*

  | RPort=445 AND FileName = ntoskrnl.exe

  | rename(field="@timestamp", as="Time")

  | Time:=formatTime(format="%F %T", field="Time")

  | table([Time, ComputerName, UserName, FileName, FilePath, CommandLine, RPort])

- FileTimestampsModified = sessions.csv OR FileTimestampsModified = acls.csv OR FileTimestampsModified = group_membership.csv OR FileTimestampsModified = local_admins.csv OR FileTimestampsModified = computer_props.csv OR FileTimestampsModified = user.props.csv
  | rename(field="_time", as="Time")
  | Time:=formatTime(format="%F %T", field="Time")
  | select [Time, FileTimestampsModified, TargetFileName]

Malicious Office Documents

- #event_simpleName=ProcessRollup2
  | ParentBaseFileName=winword.exe or ParentBaseFileName=excel.exe or ParentBaseFileName=outlook.exe
  | FileName = csc.exe
  | rename(field="@timestamp", as="Time")
  | Time:=formatTime(format="%F %T", field="Time")
  | table([Time, ComputerName, UserName,ParentBaseFileName, FileName, FilePath, CommandLine])

- #event_simpleName=ProcessRollup2
  | ParentBaseFileName=word.exe or ParentBaseFileName=excel.exe or ParentBaseFileName=powerpnt.exe
  | FileName = cscript.exe or FileName=powershell.exe or FileName=cmd.exe or FileName=wscript.exe
  | rename(field="@timestamp", as="Time")
  | Time:=formatTime(format="%F %T", field="Time")
  | table([Time, ComputerName, UserName,ParentBaseFileName, FileName, FilePath, CommandLine])

Payload Download or Creation

- #event_simpleName=ProcessRollup2
  | ParentBaseFileName=word.exe or ParentBaseFileName=excel.exe or ParentBaseFileName=outlook.exe
  | FileName = csc.exe
  | rename(field="@timestamp", as="Time")
  | Time:=formatTime(format="%F %T", field="Time")
  | table([Time, ComputerName, UserName,ParentBaseFileName, FileName, FilePath, CommandLine])

Execution/File Changes In C:\Perflogs

- (#event_simpleName=ProcessRollup2 OR #event_simpleName=SyntheticProcessRollup2) AND ImageFileName="*\\perflogs*"
  | regex ImageFileName=".*\\\\perflogs\\\\\w+\.exe"
  | table([ComputerName, UserName, ImageFileName, FileName, SHA256HashData])

Execution In C:\Temp

- (#event_simpleName=ProcessRollup2 OR #event_simpleName=SyntheticProcessRollup2) AND ImageFileName="*\\temp*"
  | regex ImageFileName=".*\\\\temp\\\\\w+\.exe"
  | table([ComputerName, UserName, ImageFileName, FileName, SHA256HashData])

- (#event_simpleName=ProcessRollup2 OR #event_simpleName=SyntheticProcessRollup2) AND ImageFileName="*\\windows\\temp*"
  | regex ImageFileName=".*\\\\windows\\\\temp\\\\\w+\.exe"
  | table([ComputerName, UserName, ImageFileName, FileName, SHA256HashData])

Execution Of Scheduled Task Exe's

- #event_simpleName=ScheduledTask*
  | FileName=at.exe OR (FileName=schtasks.exe AND CommandLine=*create)
  | table([ComputerName, UserName, ImageFileName, FileName, SHA256HashData])

Webshell Activity

- ParentImageFileName=php.exe AND (FileName=cmd.exe OR FileName=powershell.exe)
  | table([ComputerName, UserName, ImageFileName, FileName, SHA256HashData])

- ParentImageFileName=w3wp.exe AND (FileName=cmd.exe OR FileName=powershell.exe)
  | table([ComputerName, UserName, ImageFileName, FileName, SHA256HashData])

- ParentImageFileName=httpd.exe AND (FileName=cmd.exe OR FileName=powershell.exe)
  | table([ComputerName, UserName, ImageFileName, FileName, SHA256HashData])

- ParentImageFileName=httpd.exe AND (FileName=cmd.exe OR FileName=powershell.exe)
  | table([ComputerName, UserName, ImageFileName, FileName, SHA256HashData])

- ParentImageFileName=w3wp.exe AND (FileName=cmd.exe OR FileName=powershell.exe OR FileName=whoami.exe OR FileName=netstat.exe OR FileName=ipconfig.exe)

WMI Process Creation & Activity

- FileName=wmic.exe AND CommandLine=*create*
  | table([ComputerName, UserName, ImageFileName, FileName, SHA256HashData])

Cobalt Strike

- "*\\windows\\syswow64\\ntmarta\.dll" AND FileName=svchost.exe
  | table([ComputerName, CommandLine, LocalAddressIP4, LocalPort_decimal, RemoteaddressIP4, RemotePort])

- ("*\\iertutil.dll" OR "*\\ntmarta.dll") AND FileName=rundll32.exe
  | select ComputerName, UserName, CommandLine

Suspicious Powershell

- FileName=powershell.exe AND (CommandLine="*-NoP" OR CommandLine="*-NoProfile")
  | table([ComputerName, CommandLine, UserName])

- FileName=powershell.exe AND #event_simpleName=NetworkConnect*
  | table([ComputerName, CommandLine, UserName])

- FileName=powershell.exe AND (CommandLine="*-enc" OR CommandLine="*-EncodedCommand" OR CommandLine="*-E")
  | table([ComputerName, CommandLine, UserName])

- CommandLine=*iex
  | table([ComputerName, CommandLine, UserName])

- #event_simpleName:"ProcessRollup2" AND process_name:"powershell.exe" AND (command_line:*-enc* OR command_line:*encoded*)
  | rename(field="@timestamp", as="Time")
  | Time:=formatTime(format="%F %T", field="Time")

| table([Time, ComputerName, UserName,ParentBaseFileName, FileName, FilePath, CommandLine])

Mimikatz

- CommandLine="*user" OR CommandLine="*pwd" OR CommandLine="*username" OR CommandLine="*password"
  | select ComputerName, UserName, CommandLine
  FileTimestampsModified=advapi32.dll AND FileTimestampsModified=crypt32.dll AND FileTimestampsModified=cryptdll.dll AND
  FileTimestampsModified=gdi32.dll AND FileTimestampsModified=imm32.dll AND
  FileTimestampsModified=kernel32.dll AND
  FileTimestampsModified=KernelBase.dllANDFileTimestampsModified=msasn1.dll AND
  FileTimestampsModified=msvcrt.dll AND
  FileTimestampsModified=ntdll.dll AND
  FileTimestampsModified=rpcrt4.dll AND FileTimestampsModified=rsaenh.dll
  AND FileTimestampsModified=samlib.dll AND FileTimestampsModified=sechost.dll AND FileTimestampsModified=secur32.dll
  AND FileTimestampsModified=shell32.dll AND FileTimestampsModified=shlwapi.dll
  AND FileTimestampsModified=sspicli.dll AND FileTimestampsModified=user32.dll AND FileTimestampsModified=vaultcli.dll
  | table ([ComputerName, CommandLine, UserName])

- | search "gentilkiwi (Benjamin DELPY)"

- FileName=lsass.exe AND "*mimilsa.log"

Modifications To Files In C:\Windows\System32

- FileTimestampsModified="*system32*"
  | dedup FileName
  | table([ComputerName, CommandLine, UserName])

Files of Interest Making Connections

- #event_simpleName=NetworkConnect* AND (FileName=cmd.exe OR FileName=powershell.exe OR FileName=wmic.exe OR FileName=msbuild.exe OR FileName=mshta.exe OR FileName=wscript.exe OR FileName=cscript.exe OR FileName=installutil.exe OR FileName=rundll32.exe OR FileName=regsvr32.exe OR FileName=msxsl.exe OR FileName=regasm.exe)

Use Of Meterpreter Default Port

- #event_simpleName=NetworkConnect*
  | RPort = 4444

Search For Remote Access Programs

- FileName=dameware* OR FileName=vnc* OR FileName=teamv* OR FileName=screenc* OR FileName=remcom* OR FileName=logmein*

Data Exfiltration

- FileName=ssh.exe OR FileName=ftp* OR FileName=sftp* OR FileName=winscp* OR FileName=filezilla*

Ntds.Dit Theft

- FileName=esentutl.exe OR FileName=ntdsutil.exe OR FileName=wbadmin.exe

Net Activity

- process_name:"net*.exe" AND command_line:"*user /add*"

Common Recon Tools

- event_simpleName:"ProcessRollup2" AND (process_name:"net.exe" OR process_name:"ipconfig.exe" OR process_name:"whoami.exe" OR process_name:"quser.exe" OR process_name:"ping.exe" OR process_name:"netstat.exe" OR process_name:"tasklist.exe")
  | rename(field="@timestamp", as="Time")
  | Time:=formatTime(format="%F %T", field="Time")
  | table([Time, ComputerName, UserName,ParentBaseFileName, FileName, FilePath, CommandLine])

Execution From Recycle Bin

- ImageFileName="*$Recycle.Bin*" AND event_simpleName="ProcessRollup2"
  | rename(field="@timestamp", as="Time")
  | Time:=formatTime(format="%F %T", field="Time")
  | table([Time, ComputerName, UserName,ParentBaseFileName, FileName, FilePath, CommandLine])

Svchost Running Outside Of System32

- event_simpleName="ServiceStarted" ImageFileName="*\\svchost.exe" NOT ImageFileName="*\\System32*"
  | rename(field="@timestamp", as="Time")
  | Time:=formatTime(format="%F %T", field="Time")
  | table([aid, ServiceDisplayName, ImageFileName, CommandLine, ClientComputerName, RemoteAddressIP4, RemoteAddressIP6])

Lsass Running Outside System32

- NOT ImageFileName="*\\Windows\\System32\\lsass.exe" AND ImageFileName="*lsass.exe"