



sumo logic

# Hunting Malicious Office Macros

Defcon 30 BTV

By Anton Ovrutsky | 2022

sumo logic

Threat Labs



# Talk Materials

<https://github.com/Antonlovesdnb/BTV30>

# About Me

- Current: Sumo Logic Threat Research
- Previous: Lares
- Purple Teaming / Hunting / Logs / Queries
- Twitter : @Antonlovesdnb

# Agenda

Why focus on Macros

Baselining

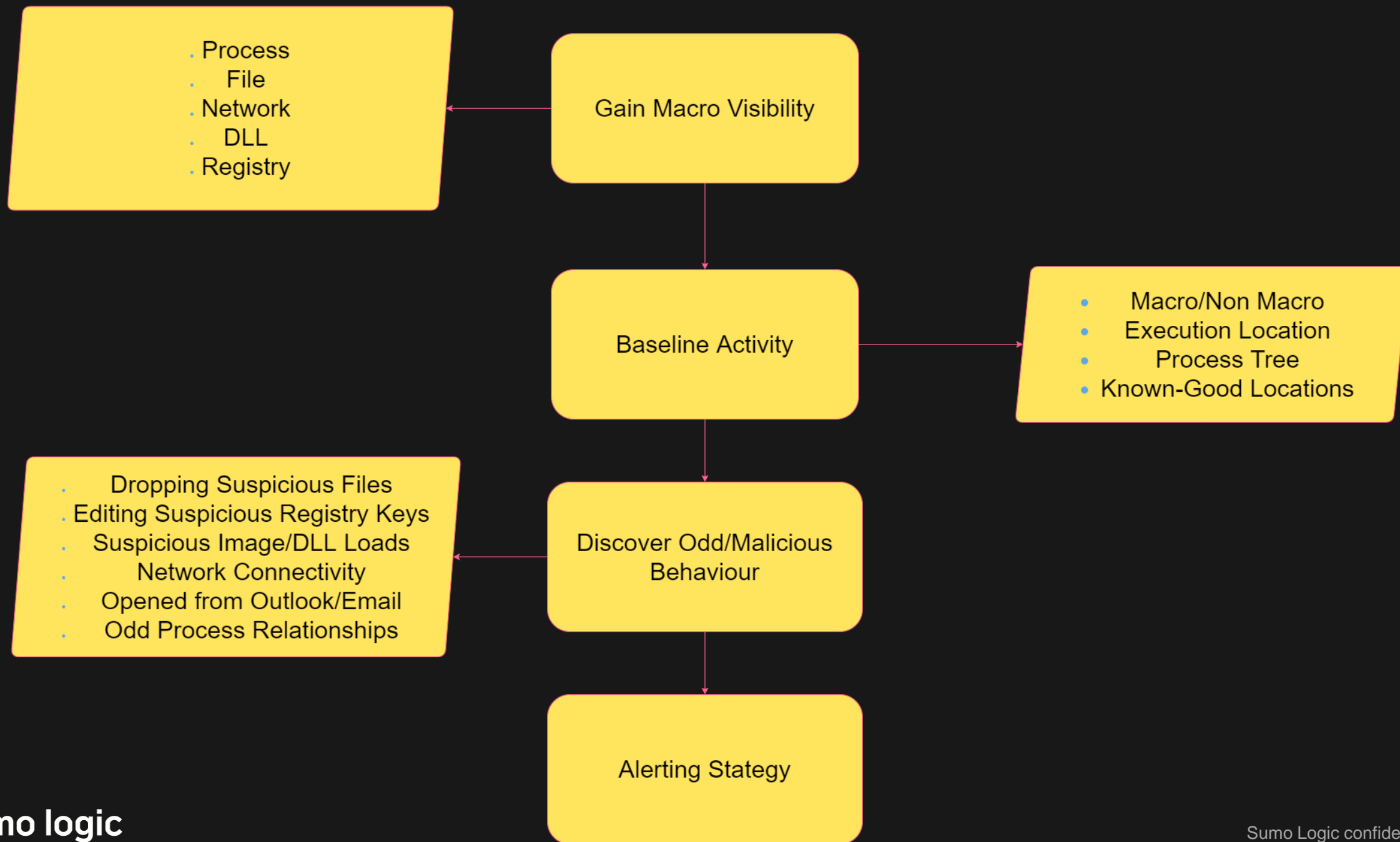
Hunting

# Why Macros ?

- Out of 122 Groups tracked by ATT&CK 59 utilize T1024.002
- Google: macros site:<https://thedfirreport.com/>

While Microsoft announced earlier this year that it would block VBA macros on downloaded documents by default, Redmond said on Thursday that it will roll back this change based on "feedback" until further notice.

[Microsoft rolls back decision to block Office macros by default \(bleepingcomputer.com\)](https://bleepingcomputer.com/news/microsoft-rolls-back-office-macro-block/)



# Baselining Toolbox



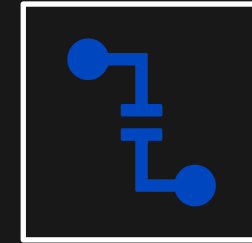
## OfficeWatch.xml

Utilize to see all Office activity that can be captured via Sysmon



## OfficeShush.xml

Filter out the noise that Office applications make, compare to events seen with OfficeWatch.xml



## OfficeSus.xml

Add suspicious events to this config for testing, then add to main Sysmon config

Image loaded:  
RuleName: Image Load-Include  
UtcTime: 2022-07-08 13:59:42.600  
ProcessGuid: {26d732db-384a-62c8-2d10-000000007e00}  
ProcessId: 9564  
Image: C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE  
ImageLoaded: C:\Program Files\Microsoft Office\root\vfs\ProgramFilesCommonX64\Microsoft Shared\VBA\VBA7.  
\1033\VBETINTL.DLL  
FileVersion: 7.01.1091  
Description: Visual Basic Environ  
Product: Visual Basic Environment  
Company: Microsoft Corporation  
OriginalFileName: -  
Hashes: MD5=CDA3EA478C604783B76964  
Signed: true  
Signature: Microsoft Corporation  
SignatureStatus: Valid  
User: SUMOTR1\Administrator

Loading of VBE/VBA  
DLLs

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon  
Event ID: 7  
Level: Information  
User: SYSTEM  
OpCode: Info  
More Information: [Event Log Online Help](#)

Copy

- > TerminalServices-ClientActiveX
- > TerminalServices-ClientUSBDev
- > TerminalServices-LocalSessionI
- > TerminalServices-PnPDevices
- > TerminalServices-Printers
- > TerminalServices-RemoteConn
- > TerminalServices-ServerUSBDev
- > Time-Service
- > Time-Service-PTP-Provider
- > Troubleshooting-Recommende
- > TZSync

General Details

Process accessed:  
RuleName: function\_name=InternalCreateProcessWCommand  
UtcTime: 2022-07-08 13:59:42.678  
SourceProcessGUID: {26d732db-384a-62c8-2d10-000000007e00}  
SourceProcessId: 9564  
SourceThreadId: 6004  
SourceImage: C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE  
TargetProcessGUID: {26d732db-384e-62c8-2f10-000000007e00}  
TargetProcessId: 6228  
TargetImage: C:\Windows\System32\notepad.exe  
GrantedAccess: 0x1FFFFFFF  
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+9e834|C:\Windows\SYSTEM32\KERNELBASE.dll+71a6|C:\Windows\System32\USER32.dll+10000|C:\Program Files\Microsoft Office\Root\Office16\AppDataVsvSubsystems64.dll+d9437|C:\Program Files\Microsoft Office\Root\Office16\AppDataVsvSubsystems64.dll+d848f|C:\Program Files\Microsoft Office\Root\Office16\AppDataVsvSubsystems64.dll+d8ef8|C:\Program Files\Microsoft Office\Root\Office16\AppDataVsvSubsystems64.dll+d192e|C:\Program Files\Microsoft Office\Root\Office16\AppDataVsvSubsystems64.dll+d24c7|C:\Windows\SYSTEM32\windows.storage.dll+19fbb9|C:\Windows\SYSTEM32\windows.storage.dll+bc39c|C:\Windows\SYSTEM32\windows.storage.dll+b5acd|C:\Windows\SYSTEM32\windows.storage.dll+b58f3|C:\Windows\SYSTEM32\windows.storage.dll+b55fd|C:\Windows\SYSTEM32\windows.storage.dll+1d9a00|C:\Windows\SYSTEM32\windows.storage.dll+b543b|C:\Windows\SYSTEM32\windows.storage.dll+bb3b7|C:\Windows\System32\SHELL32.dll+a456d|C:\Windows\System32\SHELL32.dll+6e159|C:\Windows\System32\SHELL32.dll+59f0d|C:\Windows\System32\SHCORE.dll+2bf69|C:\Windows\System32\USER32.dll+17034|C:\Windows\SYSTEM32\ntdll.dll+52651  
SourceUser: SUMOTR1\Administrator

Suspicious  
Function Calls  
and Memory  
Access

Event Properties - Event 13, Sysmon

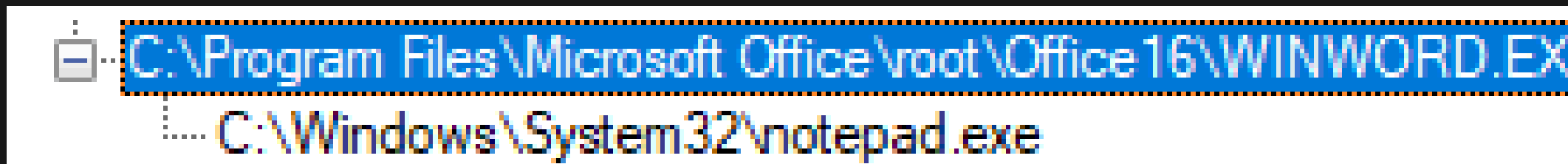
General Details

Registry value set:  
RuleName: RegKey-Include  
EventType: SetValue  
UtcTime: 2022-07-08 13:59:42.694  
ProcessGuid: {26d732db-384a-62c8-2d10-000000007e00}  
ProcessId: 9564  
Image: C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE  
TargetObject: HKU\S-1-5-21-178214487-144134600-1088407481-500\SOFTWARE\Microsoft\Office\16.0\Word\Security\Trusted Documents\TrustRecords\%USERPROFILE%\Desktop\Tests\calc\_vba.doc  
Details: Binary Data  
User: SUMOTR1\Administrator

Trust Record Modification



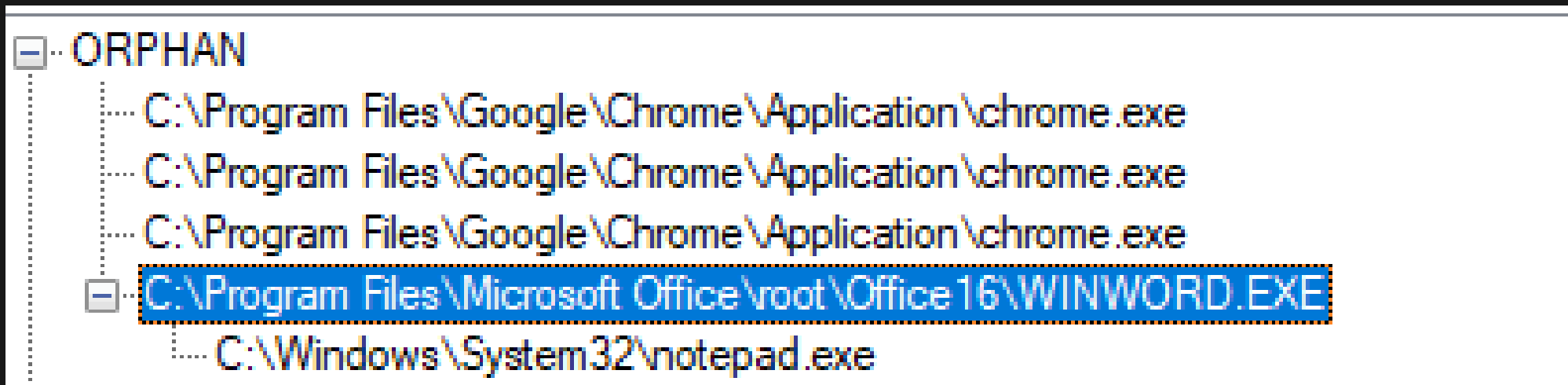
# Behavior – Macro Opened from File Share



<https://raw.githubusercontent.com/gtworek/PSBits/master/DFIR/Get-SysmonTree.ps1>

Grzegorz Tworek (@0gtweet) / Twitter

# Behavior – Macro Opened From Browser



# Behavior – Macro Opened As Attachment

## [-] ORPHAN

.... C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE

[-] C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE

.... C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

[-] C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE

.... C:\Windows\System32\notepad.exe

# Behavior – Encrypted Zip From Browser

Process Create:  
RuleName: -  
UtcTime: 2022-07-08 14:42:29.777  
ProcessGuid: {26d732db-4255-62c8-df11-000000007e00}  
ProcessId: 9776  
Image: C:\Program Files\Google\Chrome\Application\chrome.exe  
FileVersion: 103.0.5060.114  
Description: Google Chrome  
Product: Google Chrome  
Company: Google LLC  
OriginalFileName: chrome.exe  
CommandLine: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=quarantine.mojom.Quarantine --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=5108 --field-trial-handle=1832.i.16457764096035246145.468202325036307774.131072 /prefetch:8  
CurrentDirectory: C:\Program Files\Google\Chrome\Application\103.0.5060.114\  
User: SUMOTR1\Administrator  
LogonGuid: {26d732db-36ec-62c8-01af-ba0000000000}  
LogonId: 0xBAAF01  
TerminalSessionId: 1  
IntegrityLevel: High  
Hashes: SHA1=AF8A6E7216F67CA5D220084D07E1ED922AC72817,MD5=D3E37D1F3304A87EDAA2E4D3AC183980,SHA256=AA395EE3B33142BD96382709C515F321D122E249F773A457868C8666C9177A2,IMPHASH=6B4443349D1BF3B7F64F196803E28222  
ParentProcessGuid: {26d732db-3fa8-62c8-6011-000000007e00}  
ParentProcessId: 6624  
ParentImage: C:\Program Files\Google\Chrome\Application\chrome.exe  
ParentCommandLine: "C:\Program Files\Google\Chrome\Application\chrome.exe"  
ParentUser: SUMOTR1\Administrator

## Chrome Starts

Process Create:  
RuleName: technique\_id=T1137,technique\_name=Office Application Startup  
UtcTime: 2022-07-08 14:42:49.360  
ProcessGuid: {26d732db-4269-62c8-e911-000000007e00}  
ProcessId: 5696  
Image: C:\Windows\System32\notepad.exe  
FileVersion: 10.0.19041.1741 (WinBuild.160101.0800)  
Description: Notepad  
Product: Microsoft® Windows® Operating System  
Company: Microsoft Corporation  
OriginalFileName: NOTEPAD.EXE  
CommandLine: "C:\Windows\System32\notepad.exe"  
CurrentDirectory: C:\Users\ADMINI~1\AppData\Local\Temp\7zO4913AF14\  
User: SUMOTR1\Administrator  
LogonGuid: {26d732db-36ec-62c8-01af-ba0000000000}  
LogonId: 0xBAAF01  
TerminalSessionId: 1  
IntegrityLevel: High  
Hashes: SHA1=ECFCAC0CC27FA48D0AE0B55FD3E0073E0F3B99C4,MD5=58CDBC205E6D83A83D9C8E7D5E2AD8B1,SHA256=0D54DA710565A3820860BE8DF519DF62458E9A997BED3C6925665268ECC1086F,IMPHASH=320FAF01086570930EFF84A436797927  
ParentProcessGuid: {26d732db-4263-62c8-e311-000000007e00}  
ParentProcessId: 9560  
ParentImage: C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE  
ParentCommandLine: "C:\Program Files\Microsoft Office\root\Office16\WINWORD.EXE" /n "C:\Users\ADMINI~1\AppData\Local\Temp\7zO4913AF14\calc\_vba.doc" /o ""  
ParentUser: SUMOTR1\Administrator

## Macro Opens in Word from temporary 7zip Directory

Process Create:  
RuleName: -  
UtcTime: 2022-07-08 14:42:38.869  
ProcessGuid: {26d732db-425e-62c8-e211-000000007e00}  
ProcessId: 8596  
Image: C:\Program Files\7-Zip\7zFM.exe  
FileVersion: 22.00  
Description: 7-Zip File Manager  
Product: 7-Zip  
Company: Igor Pavlov  
OriginalFileName: 7zFM.exe  
CommandLine: "C:\Program Files\7-Zip\7zFM.exe" "C:\Users\administrator\Downloads\calc\_vba.7z"  
CurrentDirectory: C:\Users\administrator\Downloads\  
User: SUMOTR1\Administrator  
LogonGuid: {26d732db-36ec-62c8-01af-ba0000000000}  
LogonId: 0xBAAF01  
TerminalSessionId: 1  
IntegrityLevel: High  
Hashes: SHA1=7C10676E4FC3F8823486DB298BD5C6EE8C1A2040,MD5=AA660881ACF368692EC48E6274A477E4,SHA256=BDFFAD682DB0CB0C11D36E850DD9E920097753E1BB1A6A6577C6316E410269C1,IMPHASH=3B2AD7C424FBD96489E02FA44B3D6025  
ParentProcessGuid: {26d732db-3fa8-62c8-6011-000000007e00}  
ParentProcessId: 6624  
ParentImage: C:\Program Files\Google\Chrome\Application\chrome.exe  
ParentCommandLine: "C:\Program Files\Google\Chrome\Application\chrome.exe"  
ParentUser: SUMOTR1\Administrator

## Chrome Opens 7zip

# Bonus: EID 15!

File stream created:

RuleName: technique\_id=T1089,technique\_name=Drive-by Compromise

UtcTime: 2022-07-08 14:42:29.958

ProcessGuid: {26d732db-4255-62c8-df11-000000007e00}

ProcessId: 9776

Image: C:\Program Files\Google\Chrome\Application\chrome.exe

TargetFilename: C:\Users\administrator\Downloads\calc\_vba.7z:Zone.Identifier

CreationUtcTime: 2022-07-08 14:40:17.455

Hash: SHA1=A7983B30D63F8DED807B3B34B2A86F965E131CAE,MD5

=F348A5F7942953CAF1FAFD9723B5BD42,SHA256

=A72EF26B66745E0884F51FF580BD81895B284F6D22498386367ECF96DD8B71A6,IMP

HASH=00000000000000000000000000000000

Contents: [ZoneTransfer] Zoneld=3 ReferrerUrl=https://9fbe-

46.ngrok.io/ HostUrl=https://9fbe-.ngrok.io/calc\_vba.7z

User: SUMOTR1\Administrator

# Bonus2: MOTW Removal

File stream created:  
RuleName: technique\_id=T1089,technique\_name=Drive-by Compromise  
UtcTime: 2022-07-08 15:55:05.361  
ProcessGuid: {26d732db-5359-62c8-2313-000000007e00}  
ProcessId: 1516  
Image: C:\Program Files\Google\Chrome\Application\chrome.exe  
TargetFilename: C:\Users\administrator\Downloads\calc\_vba.7z:Zone.Identifier  
CreationUtcTime: 2022-07-08 15:51:26.028  
Hash: MD5=22EEF009355DCE8AC0C558F95C702894  
Contents: [ZoneTransfer] Zoneld=3 ReferrerUrl=https://[REDACTED]  
46.ngrok.io/  
User: SUMOTR1\Administrator

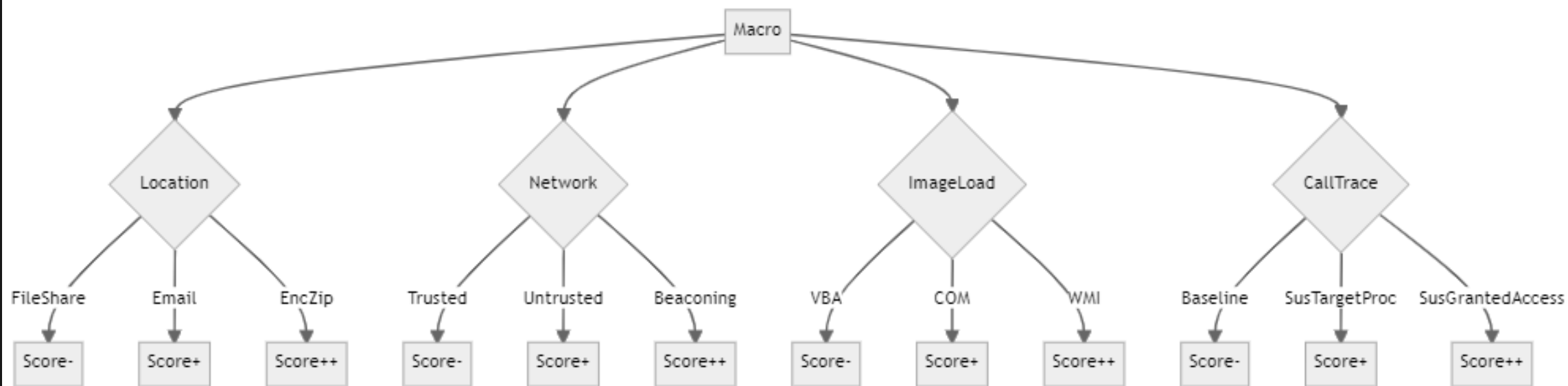
File Stream Created  
AKA MOTW Applied

Log Name: Microsoft-Windows-Sysmon/Operational  
Source: Sysmon Logged: 7/8/2022 11:55:05 AM  
Event ID: 15 Task Category: File stream created (rule: FileCreateStreamHash)  
Level: Information Keywords:  
User: SYSTEM Computer: WIN10-0.sumotr1.labs  
OpCode: Info  
More Information: [Event Log Online Help](#)

Process accessed:  
RuleName: MOTW Removed From File  
UtcTime: 2022-07-08 15:55:11.042  
SourceProcessGUID: {26d732db-50ea-62c8-f212-000000007e00}  
SourceProcessId: 6348  
SourceThreadId: 8844  
SourceImage: C:\Windows\system32\ctfmon.exe  
TargetProcessGUID: {26d732db-49bf-62c8-5612-000000007e00}  
TargetProcessId: 8812  
TargetImage: C:\Windows\explorer.exe  
GrantedAccess: 0x1000  
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+9d404|C:\Windows\System32\KERNELBASE.dll+2c13e|C:\Windows\SYSTEM32\TextInputFramework.dll+2a926|C:\Windows\SYSTEM32\TextInputFramework.dll+2915c|C:\Windows\SYSTEM32\TextInputFramework.dll+28fb2|C:\Windows\SYSTEM32\TextInputFramework.dll+2a55a|C:\Windows\SYSTEM32\TextInputFramework.dll+29c98|C:\Windows\System32\MSCTF.dll+32f3f|C:\Windows\System32\MSCTF.dll+306ce|C:\Windows\System32\USER32.dll+2624c|C:\Windows\SYSTEM32\ntdll.dll+a0d74|UNKNOWN(FFFFF80175BE54C5)|UNKNOWN(FFFF9D3C93B7E12B)|UNKNOWN(FFFF9D3C93B7DE62)|UNKNOWN(FFFF9D3C93BA25C8)|UNKNOWN(FFFF9D3C93BA3838)|UNKNOWN(FFFF9D3C93B07411)|UNKNOWN(FFFF9D3C93B064B8)|UNKNOWN(FFFF9D3C947D71AD)|UNKNOWN(FFFFF80175A098B8)|C:\Windows\System32\win32u.dll+1064|C:\Windows\System32\USER32.dll+a5c3|C:\Windows\System32\USER32.dll+a523|C:\Windows\system32\CoreMessaging.dll+15c04  
SourceUser: SUMOTR1\Administrator  
TargetUser: SUMOTR1\Administrator

MOTW  
Removed via  
Explorer

- Gotchas:
- Experimental
  - PID/GUID is different
  - Download and MOTW removal may occur minutes / hours apart
  - Difficult to correlate



# Hyper/Qualifier Queries

The screenshot displays the Sumo Logic web interface. At the top, the 'sumo logic' logo is on the left, and navigation icons (home, folders, notifications) are in the center. A dropdown menu shows 'qualifierquery\_macro' with a '+ New' button. The main area is a query editor with a line number column (23-38) and a code editor containing a Hyper/Qualifier query. The query starts with a transactionize statement and followed by a series of 'if' statements (q1-q13) that qualify events based on various criteria like ParentImage, ImageLoaded, CommandLine, TargetObject, GrantedAccess, Image, and TargetFilename. To the right of the editor is a search bar with '-15m' and a search icon, and a settings gear icon. Below the editor, a status bar shows the timestamp '07/12/2022 8:10:18 AM -0400', 'STATUS: Done', 'ELAPSED TIME: 00:00:00', 'RESULTS: None', 'SESSION: 692FBBF896658770', and 'LOAD:'. Below the status bar are tabs for 'Messages' and 'Aggregates'. The 'Messages' tab is active, showing a table with columns for time, source, and message. The table has 123 rows. At the bottom right, there are icons for 'Switch to Classic Table' and 'Add to Dashboard'.

```
23 | transactionize SourceProcessGUID,ProcessGuid as GUID
24 |
25 // Qualifiers
26 | if (ParentImage matches "*OUTLOOK.EXE*", "Outlook as Parent Process # score: 2", "") as q1
27 | if (ImageLoaded matches "*VBE*", "VBE DLL Loaded # score: 3", "") as q2
28 | if (ImageLoaded matches "*combase.dll*", "COM DLL Loaded # score: 4", "") as q3
29 | if (CommandLine matches "*MyFileShare*", "File Opened From Trusted Source # score: -6", "") as q4
30 | if (TargetObject matches "*Trusted Documents*", "Trust Record Modification # score: 3", "") as q5
31 | if (GrantedAccess matches "*0x1ffff*", "RWX Granted Access in CallTrace # score: 2", "") as q6
32 | if (Image matches "*powershell*", "PowerShell spawned from Office Product # score: 10", "") as q7
33 | if (Image matches "*cmd*", "Command Prompt spawned from Office Product # score: 10", "") as q8
34 | if (CommandLine matches "*\\c*", "Command Prompt with suspicious parameters spawned from Office Product # score: 15", "") as q9
35 | if (Image matches "*cscript.exe*", "Cscript spawned from Office Product # score: 10", "") as q10
36 | if (TargetFilename matches "*\\.jse*", "Suspicious JSE File Created # score: 10", "") as q11
37 | if (TargetFilename matches "*\\.vbs*", "Suspicious VBS File Created # score: 10", "") as q12
38 | if (RuleName matches "*ProviderExecMethod*", "Suspicious WMI Function # score: 10", "") as q13
```

07/12/2022 8:10:18 AM -0400 STATUS: Done ELAPSED TIME: 00:00:00 RESULTS: None SESSION: 692FBBF896658770 LOAD: 07/12/2022 8:25:18 AM -0400 Show

Messages Aggregates

Page: 1 of 123 Time Compare

Switch to Classic Table Add to Dashboard

[SIEM Hyper Queries: introduction, current detection methods \(part I/II\) | by Alex Teixeira | Medium](#)



# Baseline

Messages		Aggregates			
<< < Page: 1 of 1 > >>		Time Compare			
#	Time	qualifiers	score	event_codes	CommandLines
1	07/12/2022 8:20:00.000 AM -0400	File Opened From Trusted Source # score: -6 RWX Granted Access in CallTrace # score: 2 Suspicious WMI ImageLoad # score: 10 Trust Record Modification # score: 3 VBE DLL Loaded # score: 3	35	1 10 13 7	"C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n "\\dc\MyFileShare\Calc.doc" /o ""

# T1204.002 – Malicious File – Atomic Test 1

qualifiers	score	event_codes
Cscript spawned from Office Product # score: 10	48	1
RWX Granted Access in CallTrace # score: 2		10
Suspicious WMI ImageLoad # score: 10		7
VBE DLL Loaded # score: 3		

# T1204.002 – Malicious File – Atomic Test 3

qualifiers	score	event_codes
Command Prompt spawned from Office Product # score: 10	58	1
RWX Granted Access in CallTrace # score: 2Suspicious TargetImage CMD		10
# score: 10		7
Suspicious WMI ImageLoad # score: 10		
VBE DLL Loaded # score: 3		

# T1204.002 – Malicious File – Atomic Test 6

qualifiers	score	event_codes
RWX Granted Access in CallTrace # score: 2	60	1
Suspicious VBS File Created # score: 10		10
Suspicious WMI ImageLoad # score: 10		11
VBE DLL Loaded # score: 3		7

# Watch out for WMI

## Process Create:

RuleName: Process Creation-Include

UtcTime: 2022-07-12 12:56:28.322

ProcessGuid: {26d732db-6f7c-62cd-e90a-000000008000}

ProcessId: 620

Image: C:\Windows\System32\calc.exe **2**

FileVersion: 10.0.19041.1 (WinBuild.160101.0800)

Description: Windows Calculator

Product: Microsoft® Windows® Operating System

Company: Microsoft Corporation

OriginalFileName: CALC.EXE

CommandLine: calc

CurrentDirectory: C:\Windows\system32\

User: SUMOTR1\Administrator

LogonGuid: {26d732db-1fe2-62cc-fbb5-1b0000000000}

LogonId: 0x1BB5FB

TerminalSessionId: 1

IntegrityLevel: High

Hashes: MD5=5DA8C98136D98DFEC4716EDD79C7145F

ParentProcessGuid: {26d732db-1e20-62cc-6a00-000000008000}

ParentProcessId: 4900

ParentImage: C:\Windows\System32\wbem\WmiPrvSE.exe **1**

ParentCommandLine: C:\Windows\system32\wbem\wmiprvse.exe

ParentUser: NT AUTHORITY\NETWORK SERVICE

- ImageLoad
- CallTrace
- Functions

## Process accessed:

RuleName: technique id=T1047,technique name=Windows Management

Instrumentation, function\_name=ProviderExecMethod

UtcTime: 2022-07-12 13:06:49.230

SourceProcessGUID: {26d732db-1e20-62cc-6a00-000000008000}

SourceProcessId: 4900

SourceThreadId: 3832

SourceImage: C:\Windows\system32\wbem\wmiprvse.exe

TargetProcessGUID: {26d732db-71e9-62cd-1b0b-000000008000}

TargetProcessId: 9868

TargetImage: C:\Windows\system32\calc.exe

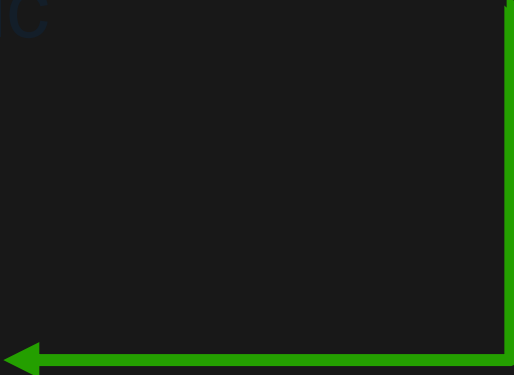
GrantedAccess: 0x1FFFFF

# PPID Spoofing

**Threat Actor goals:** Explorer → PowerShell

NOT WinWord → PowerShell → Calc

Process accessed:  
RuleName: function name=InternalCreateProcessWCommand  
UtcTime: 2022-07-12 13:11:00.133  
SourceProcessGUID: {26d732db-72e1-62cd-2c0b-000000008000}  
SourceProcessId: 116  
SourceThreadId: 11096  
SourceImage: C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE  
TargetProcessGUID: {26d732db-72e4-62cd-350b-000000008000}  
TargetProcessId: 1104  
TargetImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  
GrantedAccess: 0x1FFFFF



qualifiers	score	event_codes
RWX Granted Access in CallTrace #	score: 2	51 10
Suspicious TargetImage PowerShell #	score: 10	13
Suspicious WMI ImageLoad #	score: 10	7
Trust Record Modification #	score: 3	
VBE DLL Loaded #	score: 3	

# .NET – Gadget2Jscript

qualifiers	score	ImagesLoaded	event_codes
DotNet Native Image Office Load # score: 10	139	C:\Program Files\Microsoft	13
DotNet Office Load # score: 10		Office\root\vfs\ProgramFilesCommonX64\Microsoft	7
Suspicious WMI ImageLoad # score: 10		Shared\VBA\VBA7.1\1033\VBE7INTL.DLL	
Trust Record Modification # score: 3		C:\Program Files\Microsoft	
VBE DLL Loaded # score: 3		Office\root\vfs\ProgramFilesCommonX64\Microsoft	
		Shared\VBA\VBA7.1\VBEUI.DLL	
		C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll	
		C:\Windows\System32\wbem\wbemprox.dll	
		C:\Windows\System32\wbem\wbemsvc.dll	
		C:\Windows\System32\wbemcomn.dll	
		C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\	
		45fd11ce5d29dfe9b51f09f3abc10a64\System.Configuration.ni.dll	
		C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\5a9aa981a	
		cfc11a81b346d71a68d228c\System.Core.ni.dll	
		C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\7e4d5a	
		4538b42f1efccd374d52c4bcb2\System.Drawing.ni.dll	
		C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Web\7f59c24f10	
		934a3f91fe4b88f9325e1d\System.Web.ni.dll	
		C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\	
		a3d508fae6a764d898ea5d194cf20fcc\System.Windows.Forms.ni.dll	
		C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Workca489553#\	
		13bd2685262ffd27cfd9c8a053bfd059\System.Workflow.ComponentModel.ni.d	
		ll	
		C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\589efcc3e0	
		6f6a5070740c035c6b6c41\System.Xml.ni.dll	
		C:\Windows\assembly\NativeImages_v4.0.30319_64\System\54c5a8ebfacb96	
		ef1f1af1d732b88f97\System.ni.dll	
		C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b8493bec853a	
		c702d2188091d76ccffa\mscorlib.ni.dll	

[med0x2e/GadgetToJScript: A tool for generating .NET serialized gadgets that can trigger .NET assembly load/execution when deserialized using BinaryFormatter from JS/VBS/VBA based scripts. \(github.com\)](#)

# .NET – VSTO

qualifiers 	score 	FilesCreated 	ImagesLoaded 	event_codes 
DotNet Native Image Office Load # score: 10 DotNet Office Load # score: 10 RWX Granted Access in CallTrace # score: 2  Suspicious File Created, Potential VSTO Plugin Execution # score: 10 Suspicious WMI ImageLoad # score: 10 VBE DLL Loaded # score: 3	430	C:\Users\administrator\AppData\Local\Temp\Deployment\C3ENLCL1.QX1	C:\Program Files\Microsoft Office\root\vfs\ProgramFilesCommonX64\Microsoft Shared\VBA\VBA7.1\1033\VBE7INTL.DLL C:\Program Files\Microsoft Office\root\vfs\ProgramFilesCommonX64\Microsoft Shared\VBA\VBA7.1\VBEUI.DLL C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll C:\Windows\System32\wbem\wbemprox.dll C:\Windows\System32\wbem\wbemsvc.dll C:\Windows\System32\wbemcomn.dll C:\Windows\assembly\NativeImages_v4.0.30319_64\Accessibility\4a236a5 dec505cd2e9d5ee7f38d214c5\Accessibility.ni.dll C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.02eb0cc9a#\ a2a34462fe777e0d6bd683a895479644\Microsoft.Office.Tools.v4.0.Framework rk.ni.dll C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.04a946565#\ 5132a29118c16b719fa4259a8c7871c1\Microsoft.Office.Tools.Common.Imple mentation.ni.dll C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.05949707a#\	10 11 7

[Make phishing great again. VSTO office files are the new macro nightmare? | by Daniel Schell | Medium](#)  
[VSTODetectionNotes.md \(github.com\)](#)

# 0Days

- Zero Day does not mean you are totally blind
- Keys to success:
  - Telemetry Generated
  - Telemetry Available
  - Telemetry flexibility
  - Baselined behavior
  - Alerting strategies

qualifiers	score	ImagesLoaded
Suspicious WMI ImageLoad # score: 10	930	C:\Windows\System32\PeerDist.dll
WARNING-Follina ImageLoad1 # score: 300		C:\Windows\System32\hlink.dll
WARNING-Follina ImageLoad2 # score: 300		C:\Windows\System32\ieframe.dll
WARNING-Follina ImageLoad3 # score: 300		C:\Windows\System32\wbem\wbemprox.dll
		C:\Windows\System32\wbem\wbemsvc.dll
		C:\Windows\System32\wbemcomn.dll

# More Alerting Ideas

- First-run macro for a user
- Office beaconing AND/OR Office making multiple network connections
- Office DNS Requests
- Office calling out to Azure (Blob, CDN, Azure Public IP)
- Macro downloaded from untrusted SharePoint / Google Drive
- SOAR Action → <https://github.com/decalage2/ViperMonkey>



# Wrapping Up

- Activities happen “before” and “after” a malicious macro execution
- Even if macros are disabled tomorrow, the visibility effort is worth it
- Go beyond process creation events
- Macro tradecraft runs deep, strongly consider hardening steps

