



Reverse Engineering (REV3)

UE 04 – Dynamische Analyse – Protokoll

Jakob Mayr

WS 2023/2024

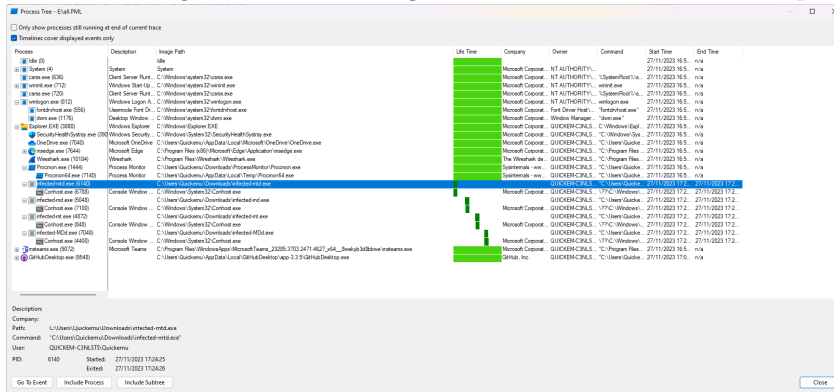
Aufgabe 1 - Dynamische Analyse Windows

Note

Die Analyse wurde in einer Windows 11 VM unter qemu durchgeführt.

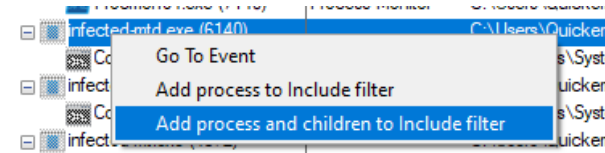
Process Tree

Prozessbäume geben immer einen guten ersten Überblick, was alles passiert (ist):



Filtern auf Prozess und Kind-Prozesse

Anschließend kann auf einen Prozess und dessen Kind-Prozesse gefiltert werden:

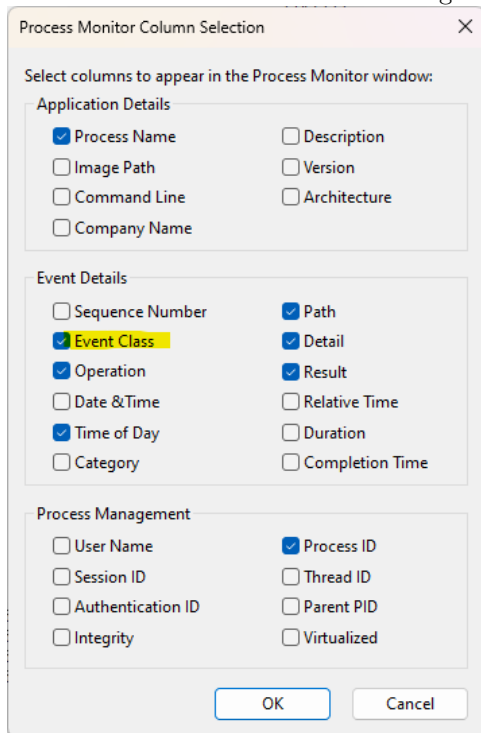


Folglich der Filter:

Column	Relation	Value	Action
<input checked="" type="checkbox"/> PID	is	6140	Include
<input checked="" type="checkbox"/> PID	is	6788	Include

Filtern auf Event-Klassen

In ProcMon kann auf Event-Klassen gefilter werden:

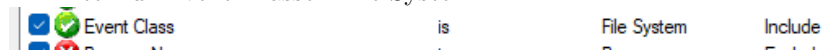


Folgende Event-Klassen mit den jeweiligen Event-Typen konnten auf dem System (allgemein) gefunden werden:

File System	Registry	Network	Process	Thread
CreateFile	QueryValue	TCP Connect	Process Create	Thread Create
CloseFile	SetValue	UDP Receive	Process Exit	Thread Exit
ReadFile	CreateKey	TCP Disconnect	Load Image	
WriteFile	EnumValue	UDP Send	Unload Image	
DeleteFile	QueryKey			
QueryInformationFile				
SetInformationFile				
RenameFile				
QueryDirectory				
QueryEaFile				
SetEaFile				
QuerySecurityFile				
SetSecurityFile				
CreateFileMapping				

Table 1: ProcMon Event Classes and Types

Filter für Event-Klasse "File System":



Filter für Event-Klasse "Registry":



Filter für Event-Klasse "Network":



Interpretation der Ergebnisse der erzeugten Windows-Executables

Dateizugriffe:

- dll's:
Auffällig ist, dass die mit "md" und "mdd" kompilierten Files mehr Datei-Operationen durchgeführt haben. Die Operationen betreffen bei beiden die "vcruntime140.dll" und die "ucrtbased.dll" bei "mdd".
- Prefetch:
Alle Varianten bis auf "mtd" beinhalten Datei-Operationen mit dem Pfad "C:\Windows\Prefetchch\...". Dieser Pfad beschleunigt unter Windows 11 das ausführen von Dateien durch vorgeladenene Inhalte, welche in diesem Verzeichnis liegen.
- Conhost.exe:
Die Dateizugriffe vom Kind-Prozess "Conhost.exe" sind bei allen Executables gleich.

Allgemein anzumerken ist, dass unter Windows 7 mehr Events zu sehen sind, da das Laden von dlls anders funktioniert. Die **api-ms-win-*.dlls** tauchen unter Windows 11 nicht auf. Die genauen Gründe für die Unterschiede zwischen Win7 und Win10 konnten nicht recherchiert werden.

Windows 7 Beispiel-Screenshot (md-Variante):

Time	Process Name	PID	Operation	Path	Result	Detail
5.18.0	infected-md.exe	992	Process Start		SUCCESS	Parent PID: 1292, ...
5.18.0	infected-md.exe	992	Thread Create		SUCCESS	Thread ID: 1444
5.18.0	infected-md.exe	992	Load Image	C:\Users\User\Documents\infected_ue02tmp\infected-md.exe	SUCCESS	Image Base: 0x13...
5.18.0	infected-md.exe	992	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77c...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\Prefetch\INFECTED-MD_EXE-EF4ED578.pf	NAME NOT FOUND	Desired Access: G...
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	Desired Access: G...
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Di...	NAME NOT FOUND	Length: 1,024
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R...
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\CWDIllegalDLLSearch	NAME NOT FOUND	Length: 1,024
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	SUCCESS	
5.18.0	infected-md.exe	992	CreateFile	C:\Users\User\Documents\infected_ue02tmp	SUCCESS	Desired Access: E...
5.18.0	infected-md.exe	992	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x77a...
5.18.0	infected-md.exe	992	Load Image	C:\Windows\System32\kernelbase.dll	SUCCESS	Image Base: 0x77e...
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Q...
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Q...
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\System\CurrentControlSet\Control\Ssp\GPI/DLL	REPARSE	Desired Access: R...
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\System\CurrentControlSet\Control\Ssp\GPI/DLL	NAME NOT FOUND	Desired Access: R...
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\SafelyCodeIdentifiers	SUCCESS	Desired Access: Q...
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\SafelyCodeIdentifiers\TransparentEnabled	NAME NOT FOUND	Length: 80
5.18.0	infected-md.exe	992	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\SafelyCodeIdentifiers	SUCCESS	
5.18.0	infected-md.exe	992	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\SafelyCodeIdentifiers	NAME NOT FOUND	Desired Access: Q...
5.18.0	infected-md.exe	992	CreateFile	C:\Users\User\Documents\infected_ue02tmp\VCRUNTIME140.dll	NAME NOT FOUND	Desired Access: R...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\vcruntime140.dll	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	QueryBasicInfo	C:\Windows\System32\vcruntime140.dll	SUCCESS	CreationTime: 3/8/...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\vcruntime140.dll	SUCCESS	
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\vcruntime140.dll	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	CreateFileMap	C:\Windows\System32\vcruntime140.dll	FILE LOCKED WI...	SyncType: SyncTy...
5.18.0	infected-md.exe	992	CreateFileMap	C:\Windows\System32\vcruntime140.dll	SUCCESS	SyncType: SyncTy...
5.18.0	infected-md.exe	992	Load Image	C:\Windows\System32\vcruntime140.dll	SUCCESS	Image Base: 0x77e...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\vcruntime140.dll	SUCCESS	
5.18.0	infected-md.exe	992	CreateFile	C:\Users\User\Documents\infected_ue02tmp\api-ms-win-crt-runtime-h1-1-0.dll	NAME NOT FOUND	Desired Access: R...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-crt-runtime-h1-1-0.dll	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	QueryBasicInfo	C:\Windows\System32\api-ms-win-crt-runtime-h1-1-0.dll	SUCCESS	CreationTime: 11/5...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-crt-runtime-h1-1-0.dll	SUCCESS	
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-crt-runtime-h1-1-0.dll	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	CreateFileMap	C:\Windows\System32\api-ms-win-crt-runtime-h1-1-0.dll	FILE LOCKED WI...	SyncType: SyncTy...
5.18.0	infected-md.exe	992	CreateFileMap	C:\Windows\System32\api-ms-win-crt-runtime-h1-1-0.dll	SUCCESS	SyncType: SyncTy...
5.18.0	infected-md.exe	992	Load Image	C:\Windows\System32\api-ms-win-crt-runtime-h1-1-0.dll	SUCCESS	Image Base: 0x77e...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-crt-runtime-h1-1-0.dll	SUCCESS	
5.18.0	infected-md.exe	992	CreateFile	C:\Users\User\Documents\infected_ue02tmp\ucrtbased.DLL	NAME NOT FOUND	Desired Access: R...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\ucrtbased.dll	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	QueryBasicInfo	C:\Windows\System32\ucrtbased.dll	SUCCESS	CreationTime: 11/5...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\ucrtbased.dll	SUCCESS	
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\ucrtbased.dll	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	CreateFileMap	C:\Windows\System32\ucrtbased.dll	FILE LOCKED WI...	SyncType: SyncTy...
5.18.0	infected-md.exe	992	CreateFileMap	C:\Windows\System32\ucrtbased.dll	SUCCESS	SyncType: SyncTy...
5.18.0	infected-md.exe	992	Load Image	C:\Windows\System32\ucrtbased.dll	SUCCESS	Image Base: 0x77e...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\ucrtbased.dll	SUCCESS	
5.18.0	infected-md.exe	992	CreateFile	C:\Users\User\Documents\infected_ue02tmp\api-ms-win-core-timezone-h1-1-0.dll	NAME NOT FOUND	Desired Access: R...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-timezone-h1-1-0.dll	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	QueryBasicInfo	C:\Windows\System32\api-ms-win-core-timezone-h1-1-0.dll	SUCCESS	CreationTime: 11/5...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-timezone-h1-1-0.dll	SUCCESS	
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-timezone-h1-1-0.dll	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	CreateFileMap	C:\Windows\System32\api-ms-win-core-timezone-h1-1-0.dll	FILE LOCKED WI...	SyncType: SyncTy...
5.18.0	infected-md.exe	992	CreateFileMap	C:\Windows\System32\api-ms-win-core-timezone-h1-1-0.dll	SUCCESS	SyncType: SyncTy...
5.18.0	infected-md.exe	992	Load Image	C:\Windows\System32\api-ms-win-core-timezone-h1-1-0.dll	SUCCESS	Image Base: 0x77e...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-timezone-h1-1-0.dll	SUCCESS	
5.18.0	infected-md.exe	992	CreateFile	C:\Users\User\Documents\infected_ue02tmp\api-ms-win-core-file-h1-1-0.dll	NAME NOT FOUND	Desired Access: R...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-file-h1-1-0.dll	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	QueryBasicInfo	C:\Windows\System32\api-ms-win-core-file-h1-1-0.dll	SUCCESS	CreationTime: 11/5...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-file-h1-1-0.dll	SUCCESS	
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-file-h1-1-0.dll	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	CreateFileMap	C:\Windows\System32\api-ms-win-core-file-h1-1-0.dll	FILE LOCKED WI...	SyncType: SyncTy...
5.18.0	infected-md.exe	992	CreateFileMap	C:\Windows\System32\api-ms-win-core-file-h1-1-0.dll	SUCCESS	SyncType: SyncTy...
5.18.0	infected-md.exe	992	Load Image	C:\Windows\System32\api-ms-win-core-file-h1-1-0.dll	SUCCESS	Image Base: 0x77e...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-file-h1-1-0.dll	SUCCESS	
5.18.0	infected-md.exe	992	CreateFile	C:\Users\User\Documents\infected_ue02tmp\api-ms-win-core-localization-h1-2-0.dll	NAME NOT FOUND	Desired Access: R...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-localization-h1-2-0.dll	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	QueryBasicInfo	C:\Windows\System32\api-ms-win-core-localization-h1-2-0.dll	SUCCESS	CreationTime: 11/5...
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-localization-h1-2-0.dll	SUCCESS	
5.18.0	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-localization-h1-2-0.dll	SUCCESS	Desired Access: R...
5.18.0	infected-md.exe	992	CreateFileMap	C:\Windows\System32\api-ms-win-core-localization-h1-2-0.dll	FILE LOCKED WI...	SyncType: SyncTy...
5.18.0	infected-md.exe	992	CreateFileMap	C:\Windows\System32\api-ms-win-core-localization-h1-2-0.dll	SUCCESS	SyncType: SyncTy...

Windows 11 Beispiel-Screenshot (md-Variante):

Registryzugriffe

1. Operationstypen:

Die einzigen Operationen in allen 4 Varianten sind "RegOpenKey", "RegQueryValue" und "RegCloseKey".

2. Pfade:

Die Pfade sind großteils in allen 4 Varianten gleich. Die einzigen Unterschiede sind die Anzahl der Events und der Pfad "HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode" welcher in den "mt"- und "mtd"-Varianten nicht vorkommt.

Time of Day	Process Name	PID	Operation	Path	Result	Detail	Event Class
17:24:28.7744839	infected-md.exe	5048	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode	NAME NOT FOUND	Length: 16	Registry

3. Conhost.exe:

Die Registryzugriffe vom Kind-Prozess "Conhost.exe" sind bei allen Executables gleich.

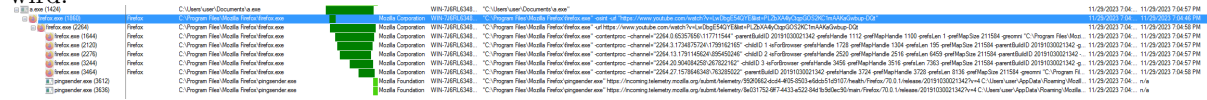
Netzwerkcommunication

Filtert man in **Process Monitor** auf die Event-Klasse "Network" so findet man in allen 4 Varianten keine Ergebnisse. Die Executables erstellen keine Sockets und somit gibt es auch keine Netzwerkcommunication.

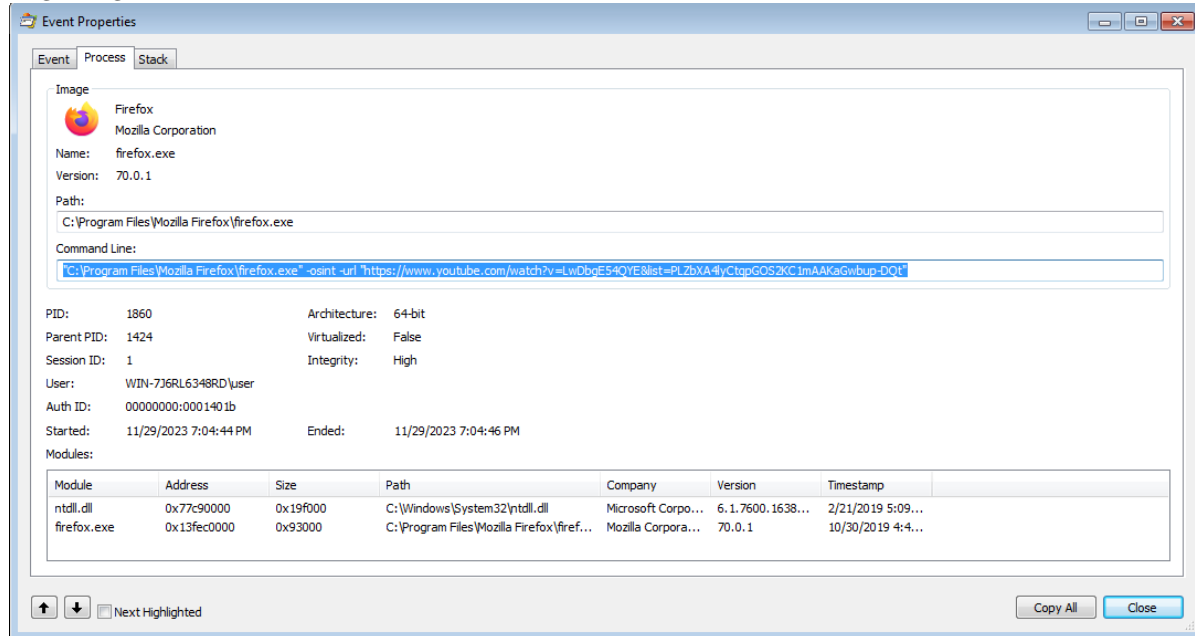
Note

Die .pml-Dateien (Process Monitor) der 4 Varianten sind im zip-Archiv unterschiedlich gefiltert hinterlegt.

Bei der Betrachtung der Prozesserstellungen ist beispielsweise auffällig, wie die "firefox.exe" aufgerufen wird:



Zugehörige CommandLine:



Dateizugriffe

Da nach dem Filtern auf "Process Name is a" und "Event Class is File System" immernoch weit über 1000 Events bleiben, kann das Tool "File Summary" im "Process Monitor" hilfreich sein:

Extension	File Time	Total Events	Opens	Closes	Reads	Writes	Read B.	Write B.	Get ACL	Set ACL	Other
(*) 18337_none_41e355142b5705d	0.0000554	15	6	6	0	0	0	0	0	0	3
(*) chrome>	0.0000395	382	118	101	13	17	13,736	72,743	26	0	107
(*) IE5	0.0004398	38	14	9	0	0	0	0	0	0	15
(*) IE5	0.0000145	6	2	2	0	0	0	0	0	0	2
(*) Local	0.0000229	3	3	0	0	0	0	0	0	0	0
(*) Manifest	0.0000167	7	1	1	0	0	0	0	0	0	5
(*) db	0.0000172	6	1	1	0	0	0	0	0	0	4
(*) dat	0.0000371	12	2	2	1	0	60	0	0	0	7
(*) dll	0.2010694	804	149	125	250	0	5,377,536	0	1	0	279
(*) exe	0.0004524	22	4	4	1	0	16,384	0	2	0	11
(*) C:\Program Files\Mozilla Firefox\firefox.exe	0.0004134	20	4	4	1	0	16,384	0	2	0	9
(*) C:\Users\user\Documents\ia.exe	0.0000390	2	0	0	0	0	0	0	0	0	2
(*) exe	0.0004210	26	3	3	4	13	85,636	85,636	0	0	3
(*) C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\EOV9M\achare.informationssysteme\11.htm	0.0000710	35	3	3	4	13	85,636	85,636	0	0	3
(*) htm	0.0002770	4	1	1	0	2	0	85,636	0	0	0
(*) C:\Users\user\Documents\101.htm	0.0002770	4	1	1	0	2	0	85,636	0	0	0
(*) mul	0.0010526	16	3	3	1	0	32,768	0	0	0	9
(*) mls	0.0000139	5	1	1	0	0	0	0	0	0	3
(*) pf	0.0000155	1	1	0	0	0	0	0	0	0	0
(*) C:\Windows\Prefetch\A.EXE-BC54C29A.pf	0.0000155	1	1	0	0	0	0	0	0	0	0
(*) tmp	0.0008999	49	10	9	17	7	242,681	242,438	0	0	6

Neben den "normal" interessanten Informationen, wie importierte Funktionen/geladenen Libraries, findet man über die File Summary sehr schnell, dass die firefox.exe verwendet wird und dass mit einem File "sib.html" gearbeitet wird. Anzumerken ist, dass hier nur das File "a" gezeigt wird (mit Kind-Prozessen mehr Information).

Registryzugriffe

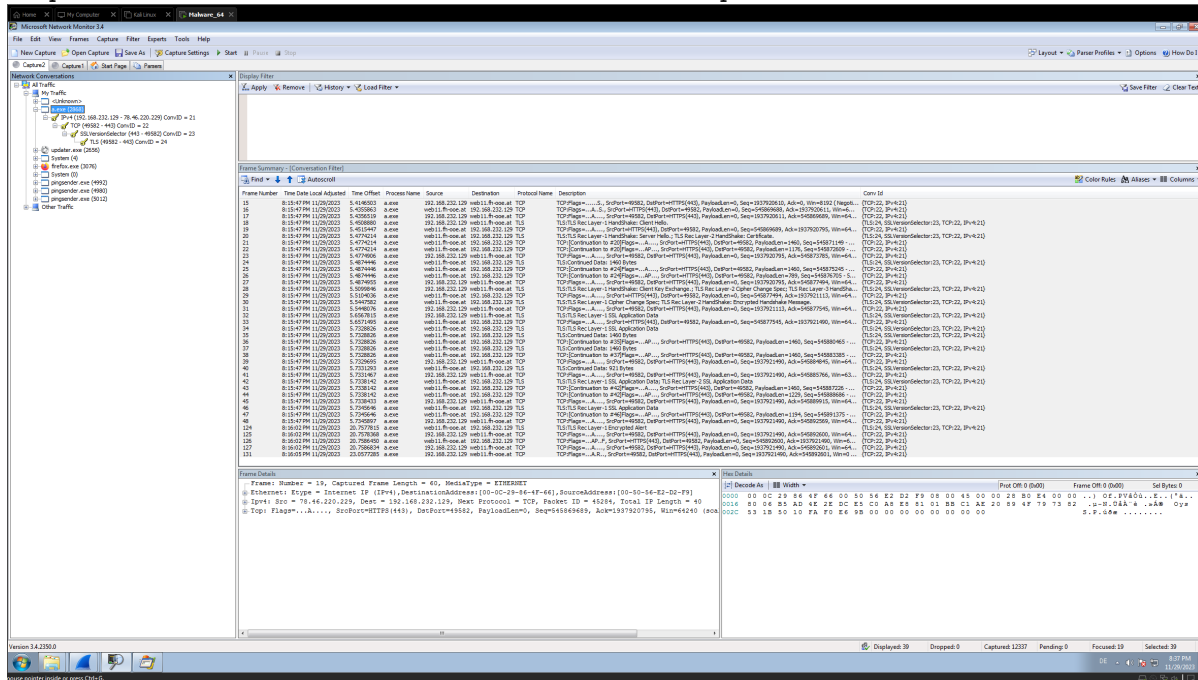
Da das "a"-File ebenfalls sehr viele Registryzugriffe hat, ist es am sinnvollsten die "Registry Summary" zu verwenden.

Registry Time	Total Events	Opens	Closes	Reads	Writes	Other	Path
0.075633	11,599	2,874	1,568	2,754	829	3,574	<Total>
0.0079188	1,299	1	1	0	0	1,297	HKLM
0.0030510	595	69	69	0	0	447	HKCU
0.0019966	375	150	75	0	75	75	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
0.0020279	246	123	74	0	49	0	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{4a1e50ac-9b45-448b-82b8-4d89df852ab1}
0.0022975	246	123	74	0	49	0	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{34bee342-7039-11e6-8d20-806e9fae39c3}
0.0031900	208	16	16	176	0	0	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform
0.0022318	182	16	16	0	16	134	HKCU\Software\Classes
0.0007151	141	94	47	0	0	0	HKLM\System\CurrentControlSet\Control\Cryptography\Configuration
0.0005773	141	94	47	0	0	0	HKLM\System\CurrentControlSet\Control\Cryptography\Providers
0.0002082	134	1	1	0	0	132	HKU
0.0004123	116	2	2	54	0	58	HKLM\SOFTWARE\Microsoft\SystemCertificates\Disallowed\Certificates
0.0002222	108	3	3	48	0	54	HKLM\SOFTWARE\Microsoft\SystemCertificates\AutoRoot\Certificates
0.0001156	108	14	14	39	14	27	HKLM\Software\Wow6432Node\Microsoft\Cryptography\OID
0.0004435	98	98	0	0	0	0	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{246EE342-7039-11D6-9020-00E0FF8E963}
0.0009080	96	48	24	0	24	0	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{4A1E50AC-9B45-448B-82B8-4D89DF852AB1}
0.0007140	77	16	16	0	16	29	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent
0.0002574	77	16	16	0	16	29	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent
0.0000946	76	2	2	36	2	34	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace
0.0004810	72	1	1	68	1	1	HKLM\SOFTWARE\Microsoft\Windows\NT\CurrentVersion\FontLink\SystemLink
0.0005893	69	23	23	0	23	0	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
0.0001687	63	21	21	0	21	0	HKLM\SOFTWARE\Microsoft\Windows\NT\CurrentVersion\ProfileList\S-1-5-21-988512449-1246055119-4186994322-1000
0.0001766	56	28	14	0	14	0	HKLM\SYSTEM\CurrentControlSet\Services\crypt32
0.0000727	54	18	18	0	18	0	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings
0.0001262	52	6	6	16	0	24	HKLM\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates
0.0000820	52	26	13	0	13	0	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Linkage
0.0001038	52	0	0	52	0	0	HKLM\System\CurrentControlSet\Services\Tcpip\Linkage\Bld
0.0003707	51	14	14	0	14	9	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
0.0001412	48	16	16	16	0	0	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent\Post Platform
0.0000650	48	0	0	48	0	0	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{4A1E50AC-9B45-448B-82B8-4D89DF852AB1}\DhcpNameServer
0.0000927	48	0	0	48	0	0	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{4A1E50AC-9B45-448B-82B8-4D89DF852AB1}\NameServer
0.0000461	44	7	7	0	2	28	HKCU\Software\Classes\FrontURL\308D46B0AF4A39CB
0.0000438	43	2	2	0	2	37	HKLM\Software\Wow6432Node\Microsoft\Internet Explorer\Main\FeatureControl
0.0000369	42	2	2	0	2	36	HKCR\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B303090}\ShellFolder
0.0001011	42	14	14	0	14	0	HKLM\Software\Microsoft\SystemCertificates\AutoRoot\Auto Update
0.0000409	42	0	0	42	0	0	HKLM\SOFTWARE\Microsoft\Windows\NT\CurrentVersion\ProfileList\S-1-5-21-988512449-1246055119-4186994322-1000\ProfileImagePath
0.0000488	42	14	14	0	0	14	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 0
0.0001097	40	4	4	0	0	32	HKCU\Software\Classes\FrontURL\308D46B0AF4A39CB\shell\open
0.0001051	40	13	13	0	13	0	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
0.0000394	39	1	1	0	1	36	HKCR\Wow6432Node\CLSID\{20802C80-3A5A-1069-A2D7-08002B303090}\ShellFolder
0.0000363	39	1	1	0	1	36	HKCR\Wow6432Node\CLSID\{2004FED-3A5A-1069-A2D8-08002B303090}\ShellFolder
0.0000581	39	13	13	0	13	0	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings
0.0000240	39	13	13	0	0	13	HKLM\SOFTWARE\Wow6432Node\Microsoft\Cryptography\OID\EncodingType 1
0.0005759	37	0	0	37	0	0	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Local AppData
0.0000372	33	11	11	0	11	0	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
0.0000341	33	0	1	16	1	15	HKLM\SOFTWARE\Microsoft\CTF\TIP
0.0000621	32	10	10	0	10	2	HKLM\Software\Microsoft\Cryptography\OID\EncodingType 0\CertDistributedCertificateChainEngine\Config
0.0000265	31	6	6	0	4	15	HKCU\Software\Microsoft\SystemCertificates\my
0.0000323	30	2	2	0	2	24	HKCR\Wow6432Node\CLSID\{1299CF18-C4F5-486A-B80F-2299F038E277}
0.0000188	30	2	2	0	2	24	HKCR\Wow6432Node\CLSID\{16785811-3F85-44F2-2A2D-844502898F18}
0.0000592	30	2	2	0	2	24	HKCR\Wow6432Node\CLSID\{B1968286-8AB4-1D1A-B68C-00AA00341D07}
0.0000259	30	2	2	0	2	24	HKCR\Wow6432Node\CLSID\{DCB80021-570F-4A8B-8D69-199FD8A57238}
0.0000447	30	10	10	0	10	0	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer
0.0001234	29	9	9	0	0	11	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SeasonInfo\1
0.0000503	28	2	2	0	2	22	HKCR\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B303090}
0.0001443	28	7	7	0	7	7	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
0.0000489	27	9	9	0	9	0	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
0.0000000	16	8	8	0	8	0	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Besondere Auffälligkeiten konnte hier nicht gefunden werden.

Netzwerkcommunication

Da die Analyse der Netzwerkcommunication eines Prozesses unter Windows 7 mit dem "Process Monitor" nicht so gut funktioniert wie unter Windows 11, wurde eine zusätzliche Software dafür verwendet: <https://www.microsoft.com/en-us/download/details.aspx?id=4865>



Die damit empfangenen Pakete können als .cap exportiert werden.

Folgende Tabelle zeigt oberflächlich die Netzwerk-kommunikation der "a"-Datei (siehe network.csv für mehr Details):

Note

Eine .cap-Datei (Netzwerk-capture-Datei) und die unterschiedlichen .pml-Dateien (Process Monitor) sind wiederum im .zip-Archiv angehängt.

Fame Number	Process Name	Source	Destination	Protocol Name
15	a.exe	192.168.232.129	web11.fh-ooe.at	TCP
16	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
17	a.exe	192.168.232.129	web11.fh-ooe.at	TCP
18	a.exe	192.168.232.129	web11.fh-ooe.at	TLS
19	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
20	a.exe	web11.fh-ooe.at	192.168.232.129	TLS
21	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
22	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
23	a.exe	192.168.232.129	web11.fh-ooe.at	TCP
24	a.exe	web11.fh-ooe.at	192.168.232.129	TLS
25	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
26	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
27	a.exe	192.168.232.129	web11.fh-ooe.at	TCP
28	a.exe	192.168.232.129	web11.fh-ooe.at	TLS
29	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
30	a.exe	web11.fh-ooe.at	192.168.232.129	TLS
31	a.exe	192.168.232.129	web11.fh-ooe.at	TCP
32	a.exe	192.168.232.129	web11.fh-ooe.at	TLS
33	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
34	a.exe	web11.fh-ooe.at	192.168.232.129	TLS
35	a.exe	web11.fh-ooe.at	192.168.232.129	TLS
36	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
37	a.exe	web11.fh-ooe.at	192.168.232.129	TLS
38	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
39	a.exe	192.168.232.129	web11.fh-ooe.at	TCP
40	a.exe	web11.fh-ooe.at	192.168.232.129	TLS
41	a.exe	192.168.232.129	web11.fh-ooe.at	TCP
42	a.exe	web11.fh-ooe.at	192.168.232.129	TLS
43	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
44	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
45	a.exe	192.168.232.129	web11.fh-ooe.at	TCP
46	a.exe	web11.fh-ooe.at	192.168.232.129	TLS
47	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
48	a.exe	192.168.232.129	web11.fh-ooe.at	TCP
124	a.exe	web11.fh-ooe.at	192.168.232.129	TLS
125	a.exe	192.168.232.129	web11.fh-ooe.at	TCP
126	a.exe	web11.fh-ooe.at	192.168.232.129	TCP
127	a.exe	192.168.232.129	web11.fh-ooe.at	TCP
131	a.exe	192.168.232.129	web11.fh-ooe.at	TCP

Table 2: a-File Netzwerkkommunikation