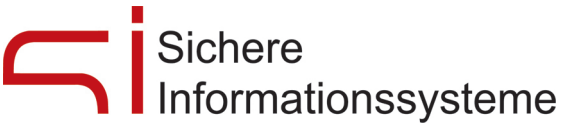


Reverse Engineering (REV3)

UE 04 – Dynamische Analyse – Protokoll

Jakob Mayr

WS 2023/2024

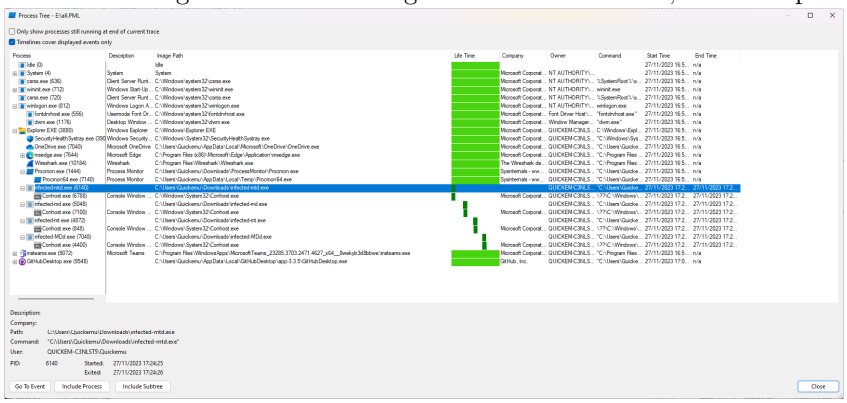
Aufgabe 1 - Dynamische Analyse Windows

Note

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

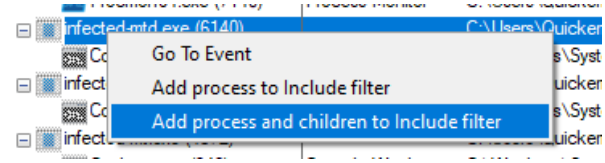
Process Tree

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

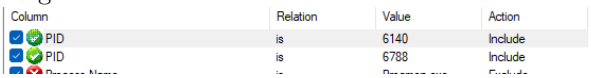


Filtern auf Prozess und Kind-Prozesse

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



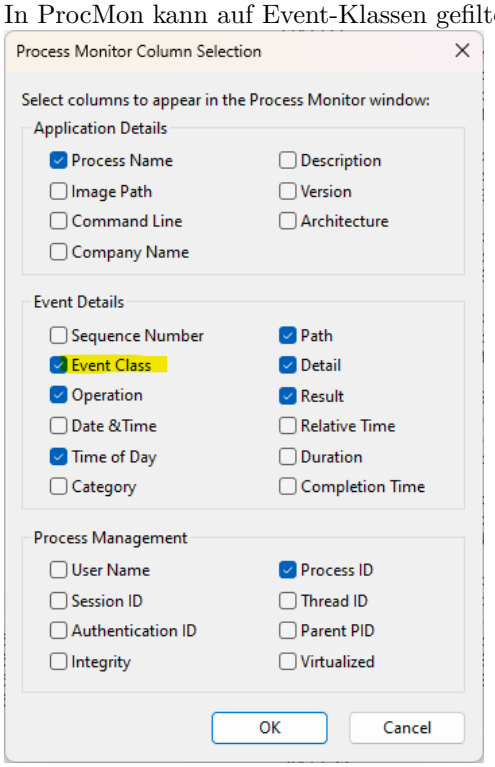
Folglich der Filter:



Column	Relation	Value	Action
PID	is	6140	Include
PID	is	6788	Include

Filtern auf Event-Klassen

In ProcMon kann auf Event-Klassen gefilter werden:

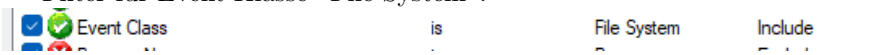


Folgende Event-Klassen mit den jeweiligen Event-Typen konnten auf dem System (allgemein) gefunden werden:

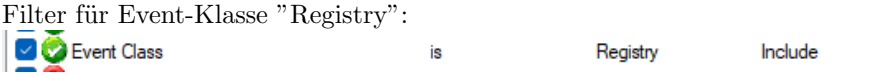
File System	**Registry**	**Network**	**Process**	**Thread**
CreateFile	QueryValue	TCP Connect	Process Create	Thread Create
CloseFile	SetValue	UDP Receive	Process Exit	Thread Exit
ReadFile	CreateKey	TCP Disconnect	Load Image	
WriteFile	EnumValue	UDP Send	Unload Image	
DeleteFile	QueryKey			
QueryInformationFile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

Table 1: ProcMon Event Classes and Types

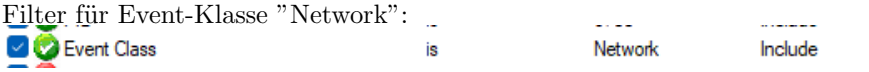
Filter für Event-Klasse "File System":



Filter für Event-Klasse "Registry":



Filter für Event-Klasse "Network":



Interpretation der Egebnisse der erzeugten Windows-Executables

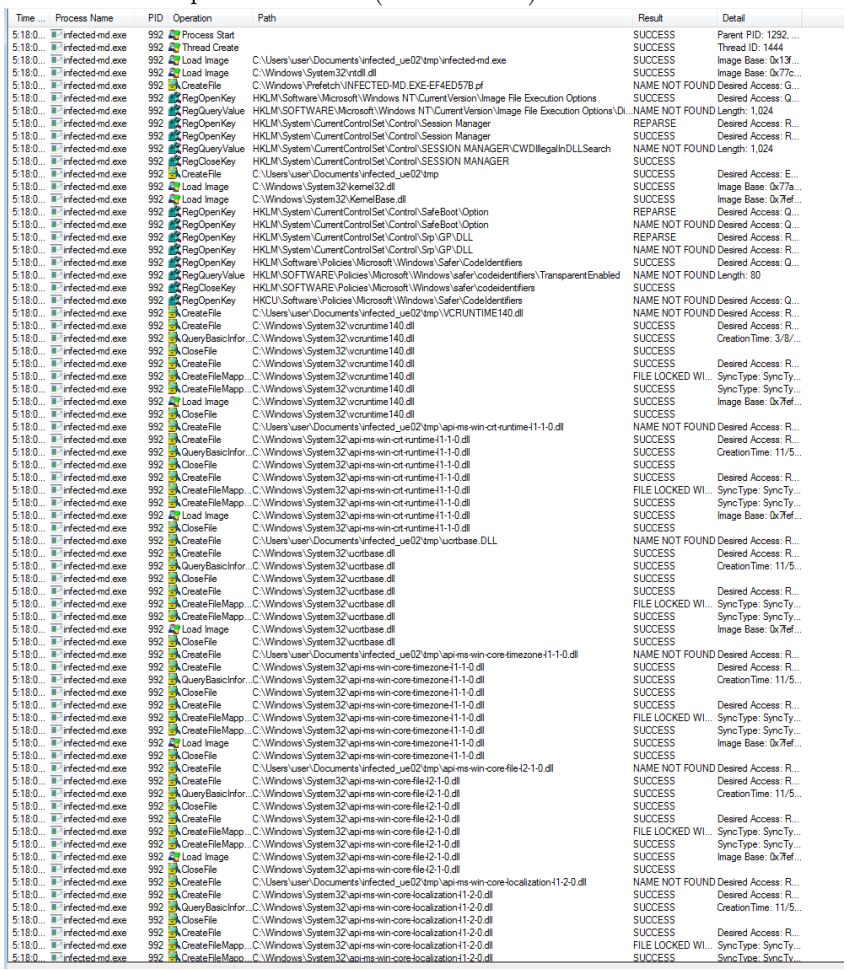
Dateizugriffe:

1. 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".

2. Prefetch:
   Alle Varianten bis auf "mtd" beinhalten Datei-Operationen mit dem Pfad "C:\Windows\Prefetch\...". Dieser Pfad beschleunigt unter Windows 11 das ausführen von Dateien durch vorgeladenene Inhalte, welche in diesem Verzeichnis liegen.

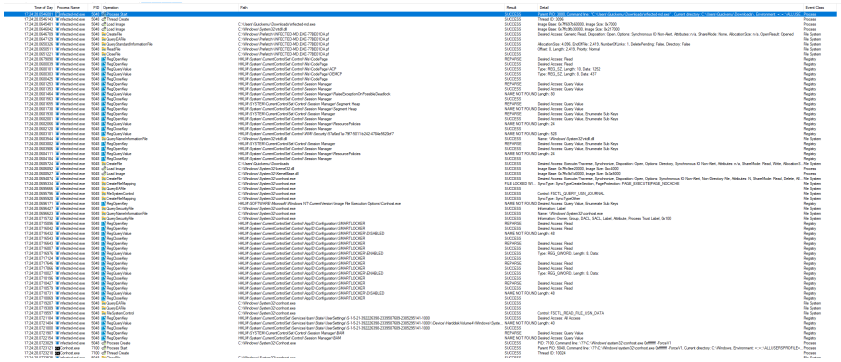
3. Conhost.exe:
   Die Dateizugriffe vom Kind-Prozess "Conhost.exe" sind bei allen Executables gleich.

Allgemein anzumerken ist, dass unter Windows 7 mehr Events zu sehen sind, da das Laden von dlls anders funktioniert. Die **api-ms-win-*.dll**s 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_ue02\tmp\infected-md.exe	SUCCESS	Image Base: 0x13f...
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-EF4ED57B.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: Q...
5:18:0...	infected-md.exe	992	RegQueryValue	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	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\CWDIllegalInDLLSearch	NAME NOT FOUND	Length: 1,024
5:18:0...	infected-md.exe	992	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	SUCCESS	
5:18:0...	infected-md.exe	992	CreateFile	C:\Users\user\Documents\infected_ue02\tmp	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: 0x7fef...
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\Srp\GP\DLL	REPARSE	Desired Access: R...
5:18:0...	infected-md.exe	992	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	NAME NOT FOUND	Desired Access: R...
5:18:0...	infected-md.exe	992	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Q...
5:18:0...	infected-md.exe	992	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled	NAME NOT FOUND	Length: 80
5:18:0...	infected-md.exe	992	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers	SUCCESS	
5:18:0...	infected-md.exe	992	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND	Desired Access: Q...
5:18:0...	infected-md.exe	992	CreateFile	C:\Users\user\Documents\infected_ue02\tmp\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	QueryBasicInfor...	C:\Windows\System32\vcruntime140.dll	SUCCESS	CreationTime: 3/8/...
5:18:0...	infected-md.exe	992	CloseFile	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	CreateFileMapp...	C:\Windows\System32\vcruntime140.dll	FILE LOCKED WI...	SyncType: SyncTy...
5:18:0...	infected-md.exe	992	CreateFileMapp...	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: 0x7fef...
5:18:0...	infected-md.exe	992	CloseFile	C:\Windows\System32\vcruntime140.dll	SUCCESS	
5:18:0...	infected-md.exe	992	CreateFile	C:\Users\user\Documents\infected_ue02\tmp\api-ms-win-crt-runtime-l1-1-0.dll	NAME NOT FOUND	Desired Access: R...
5:18:0...	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-crt-runtime-l1-1-0.dll	SUCCESS	Desired Access: R...
5:18:0...	infected-md.exe	992	QueryBasicInfor...	C:\Windows\System32\api-ms-win-crt-runtime-l1-1-0.dll	SUCCESS	CreationTime: 11/5...
5:18:0...	infected-md.exe	992	CloseFile	C:\Windows\System32\api-ms-win-crt-runtime-l1-1-0.dll	SUCCESS	
5:18:0...	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-crt-runtime-l1-1-0.dll	SUCCESS	Desired Access: R...
5:18:0...	infected-md.exe	992	CreateFileMapp...	C:\Windows\System32\api-ms-win-crt-runtime-l1-1-0.dll	FILE LOCKED WI...	SyncType: SyncTy...
5:18:0...	infected-md.exe	992	CreateFileMapp...	C:\Windows\System32\api-ms-win-crt-runtime-l1-1-0.dll	SUCCESS	SyncType: SyncTy...
5:18:0...	infected-md.exe	992	Load Image	C:\Windows\System32\api-ms-win-crt-runtime-l1-1-0.dll	SUCCESS	Image Base: 0x7fef...
5:18:0...	infected-md.exe	992	CloseFile	C:\Windows\System32\api-ms-win-crt-runtime-l1-1-0.dll	SUCCESS	
5:18:0...	infected-md.exe	992	CreateFile	C:\Users\user\Documents\infected_ue02\tmp\ucrtbase.DLL	NAME NOT FOUND	Desired Access: R...
5:18:0...	infected-md.exe	992	CreateFile	C:\Windows\System32\ucrtbase.dll	SUCCESS	Desired Access: R...
5:18:0...	infected-md.exe	992	QueryBasicInfor...	C:\Windows\System32\ucrtbase.dll	SUCCESS	CreationTime: 11/5...
5:18:0...	infected-md.exe	992	CloseFile	C:\Windows\System32\ucrtbase.dll	SUCCESS	
5:18:0...	infected-md.exe	992	CreateFile	C:\Windows\System32\ucrtbase.dll	SUCCESS	Desired Access: R...
5:18:0...	infected-md.exe	992	CreateFileMapp...	C:\Windows\System32\ucrtbase.dll	FILE LOCKED WI...	SyncType: SyncTy...
5:18:0...	infected-md.exe	992	CreateFileMapp...	C:\Windows\System32\ucrtbase.dll	SUCCESS	SyncType: SyncTy...
5:18:0...	infected-md.exe	992	Load Image	C:\Windows\System32\ucrtbase.dll	SUCCESS	Image Base: 0x7fef...
5:18:0...	infected-md.exe	992	CloseFile	C:\Windows\System32\ucrtbase.dll	SUCCESS	
5:18:0...	infected-md.exe	992	CreateFile	C:\Users\user\Documents\infected_ue02\tmp\api-ms-win-core-timezone-l1-1-0.dll	NAME NOT FOUND	Desired Access: R...
5:18:0...	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-timezone-l1-1-0.dll	SUCCESS	Desired Access: R...
5:18:0...	infected-md.exe	992	QueryBasicInfor...	C:\Windows\System32\api-ms-win-core-timezone-l1-1-0.dll	SUCCESS	CreationTime: 11/5...
5:18:0...	infected-md.exe	992	CloseFile	C:\Windows\System32\api-ms-win-core-timezone-l1-1-0.dll	SUCCESS	
5:18:0...	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-timezone-l1-1-0.dll	SUCCESS	Desired Access: R...
5:18:0...	infected-md.exe	992	CreateFileMapp...	C:\Windows\System32\api-ms-win-core-timezone-l1-1-0.dll	FILE LOCKED WI...	SyncType: SyncTy...
5:18:0...	infected-md.exe	992	CreateFileMapp...	C:\Windows\System32\api-ms-win-core-timezone-l1-1-0.dll	SUCCESS	SyncType: SyncTy...
5:18:0...	infected-md.exe	992	Load Image	C:\Windows\System32\api-ms-win-core-timezone-l1-1-0.dll	SUCCESS	Image Base: 0x7fef...
5:18:0...	infected-md.exe	992	CloseFile	C:\Windows\System32\api-ms-win-core-timezone-l1-1-0.dll	SUCCESS	
5:18:0...	infected-md.exe	992	CreateFile	C:\Users\user\Documents\infected_ue02\tmp\api-ms-win-core-file-l2-1-0.dll	NAME NOT FOUND	Desired Access: R...
5:18:0...	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-file-l2-1-0.dll	SUCCESS	Desired Access: R...
5:18:0...	infected-md.exe	992	QueryBasicInfor...	C:\Windows\System32\api-ms-win-core-file-l2-1-0.dll	SUCCESS	CreationTime: 11/5...
5:18:0...	infected-md.exe	992	CloseFile	C:\Windows\System32\api-ms-win-core-file-l2-1-0.dll	SUCCESS	
5:18:0...	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-file-l2-1-0.dll	SUCCESS	Desired Access: R...
5:18:0...	infected-md.exe	992	CreateFileMapp...	C:\Windows\System32\api-ms-win-core-file-l2-1-0.dll	FILE LOCKED WI...	SyncType: SyncTy...
5:18:0...	infected-md.exe	992	CreateFileMapp...	C:\Windows\System32\api-ms-win-core-file-l2-1-0.dll	SUCCESS	SyncType: SyncTy...
5:18:0...	infected-md.exe	992	Load Image	C:\Windows\System32\api-ms-win-core-file-l2-1-0.dll	SUCCESS	Image Base: 0x7fef...
5:18:0...	infected-md.exe	992	CloseFile	C:\Windows\System32\api-ms-win-core-file-l2-1-0.dll	SUCCESS	
5:18:0...	infected-md.exe	992	CreateFile	C:\Users\user\Documents\infected_ue02\tmp\api-ms-win-core-localization-l1-2-0.dll	NAME NOT FOUND	Desired Access: R...
5:18:0...	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-localization-l1-2-0.dll	SUCCESS	Desired Access: R...
5:18:0...	infected-md.exe	992	QueryBasicInfor...	C:\Windows\System32\api-ms-win-core-localization-l1-2-0.dll	SUCCESS	CreationTime: 11/5...
5:18:0...	infected-md.exe	992	CloseFile	C:\Windows\System32\api-ms-win-core-localization-l1-2-0.dll	SUCCESS	
5:18:0...	infected-md.exe	992	CreateFile	C:\Windows\System32\api-ms-win-core-localization-l1-2-0.dll	SUCCESS	Desired Access: R...
5:18:0...	infected-md.exe	992	CreateFileMapp...	C:\Windows\System32\api-ms-win-core-localization-l1-2-0.dll	FILE LOCKED WI...	SyncType: SyncTy...
5:18:0...	infected-md.exe	992	CreateFileMapp...	C:\Windows\System32\api-ms-win-core-localization-l1-2-0.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.

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

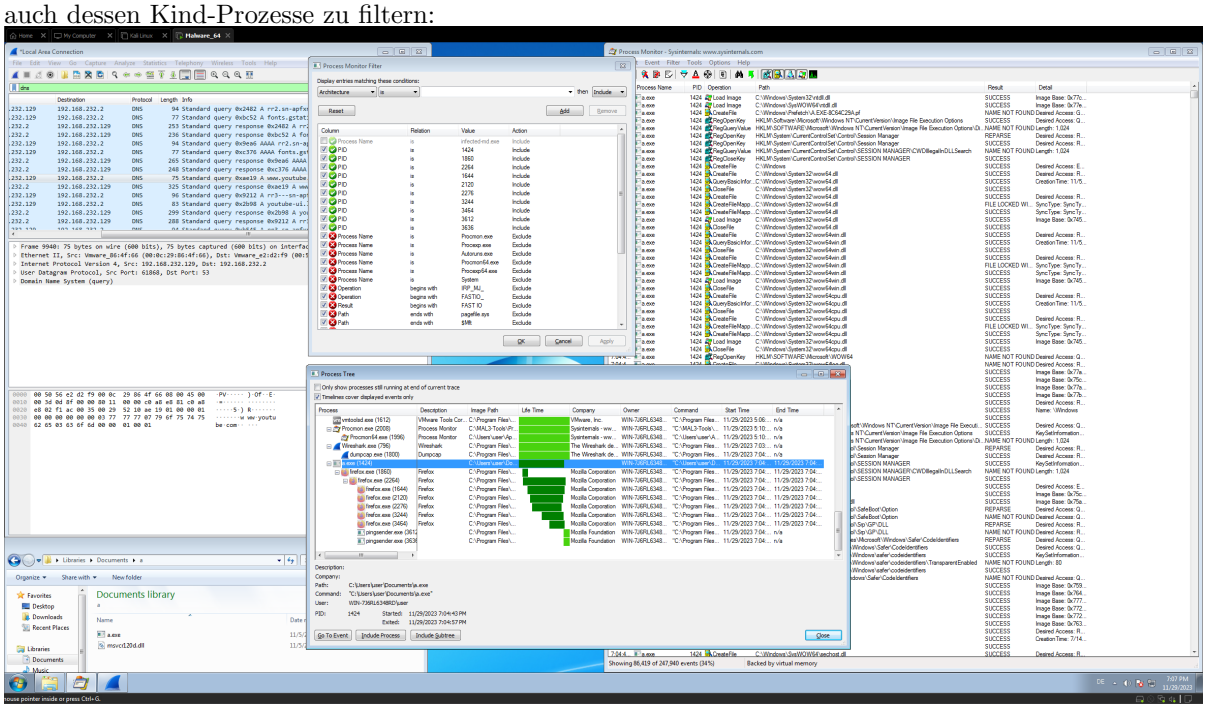
> **Note**
>
> Die .pml-Dateien (Process Monitor) der 4 Varianten sind im zip-Archiv unterschiedlich gefiltert hinterlegt.

Aufgabe 2 - Dynamische Analyse Windows (File: ”a”)

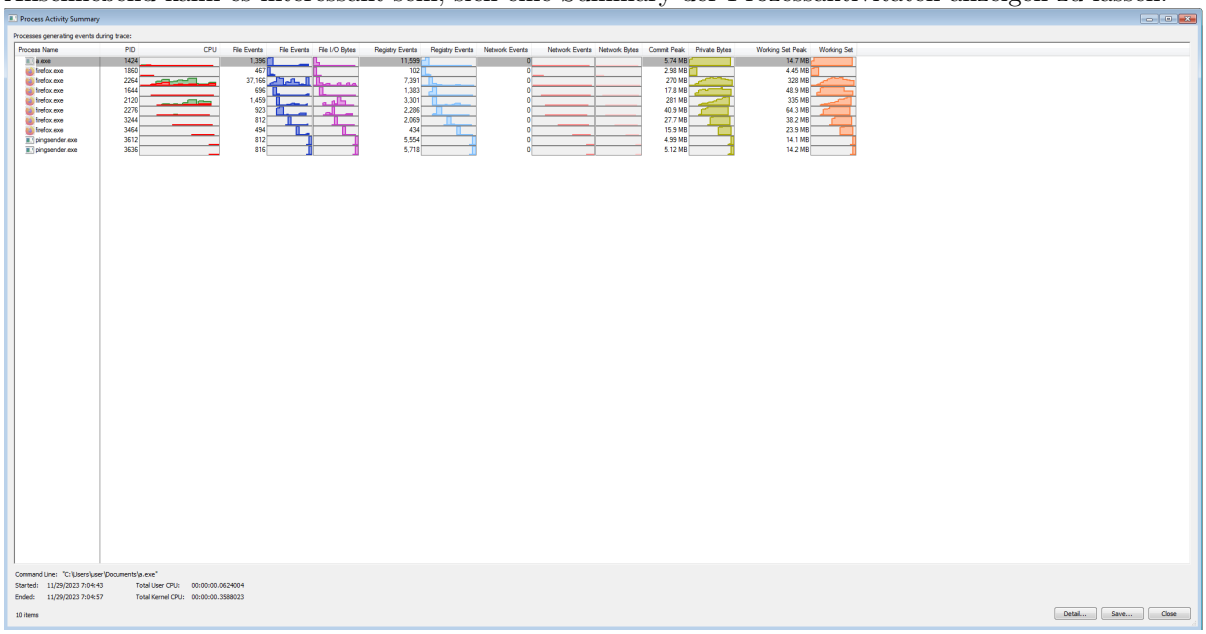
Note

Die Datei wurde in der zur Verfügung gestellten ”Malware VM” analysiert.

Zu Beginn ist es wieder hilfreich über den Prozessbaum auf den eigentlich zu analysierenden Prozess wie auch dessen Kind-Prozesse zu filtern:

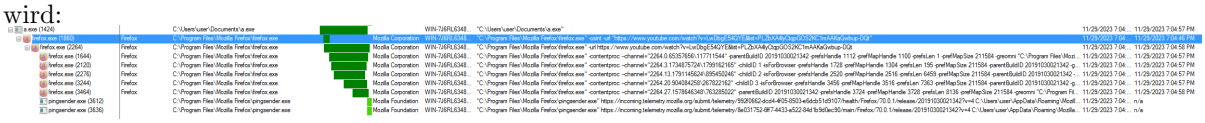


Anschließend kann es interessant sein, sich eine Summary der Prozessaktivitäten anzeigen zu lassen:

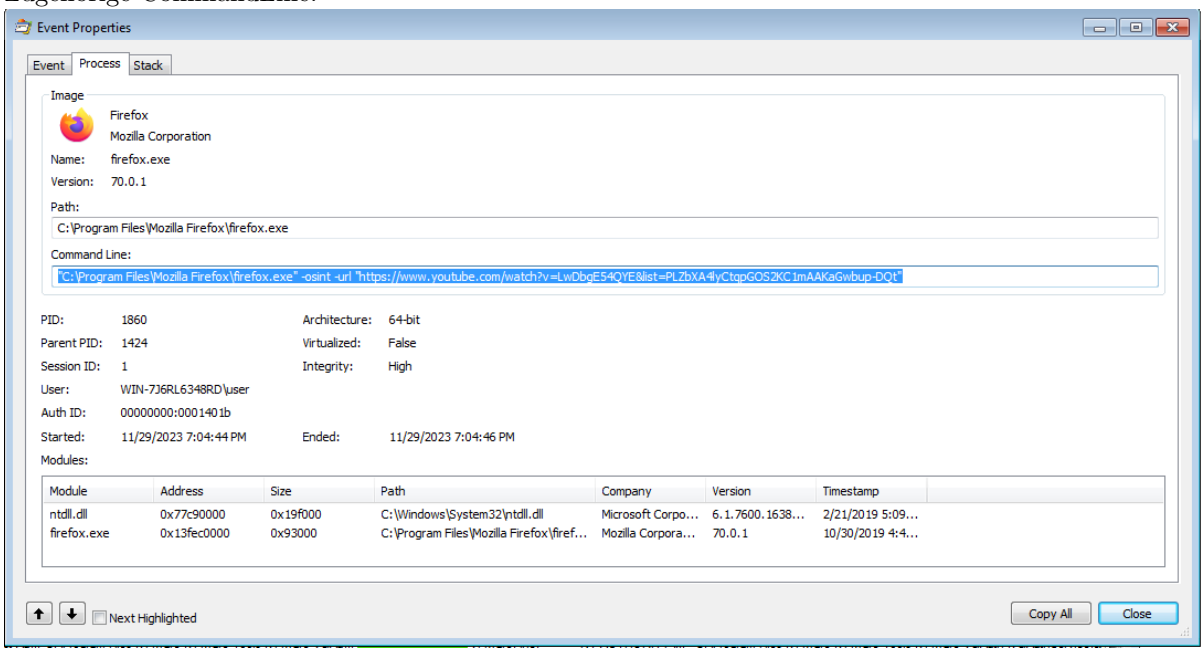


Dies verschafft bereits einen groben Überblick.

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

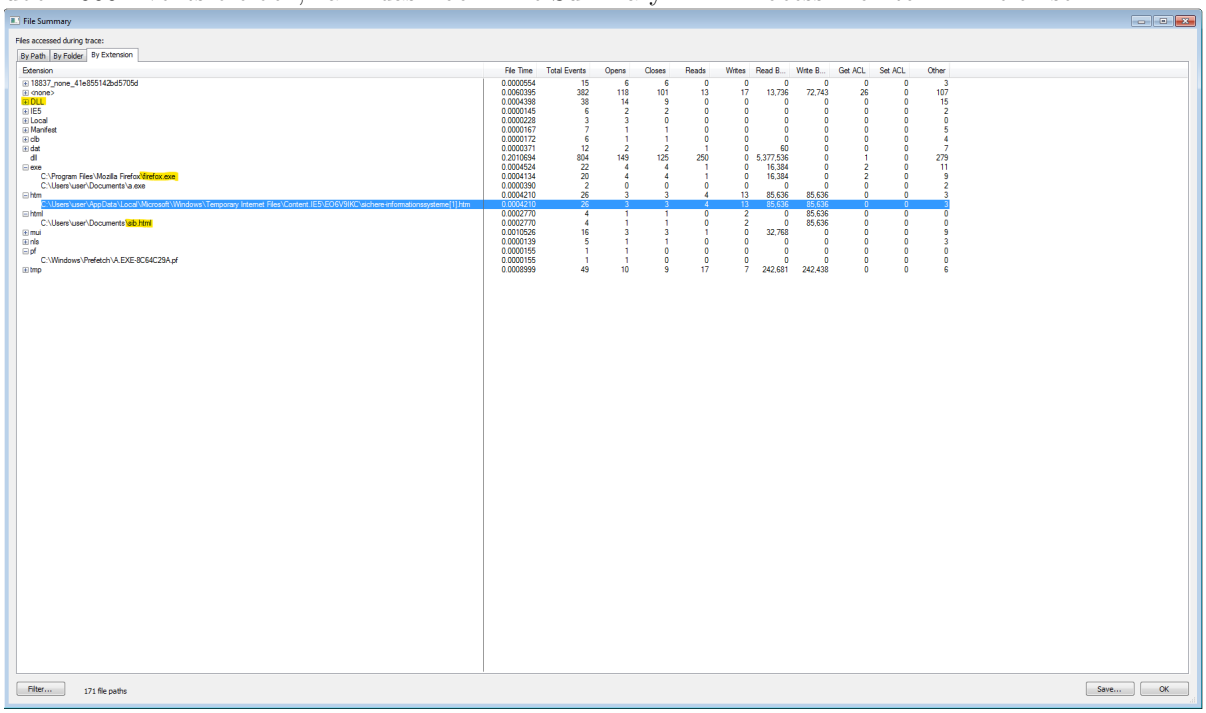


Zugehörige CommandLine:



Dateizugriffe

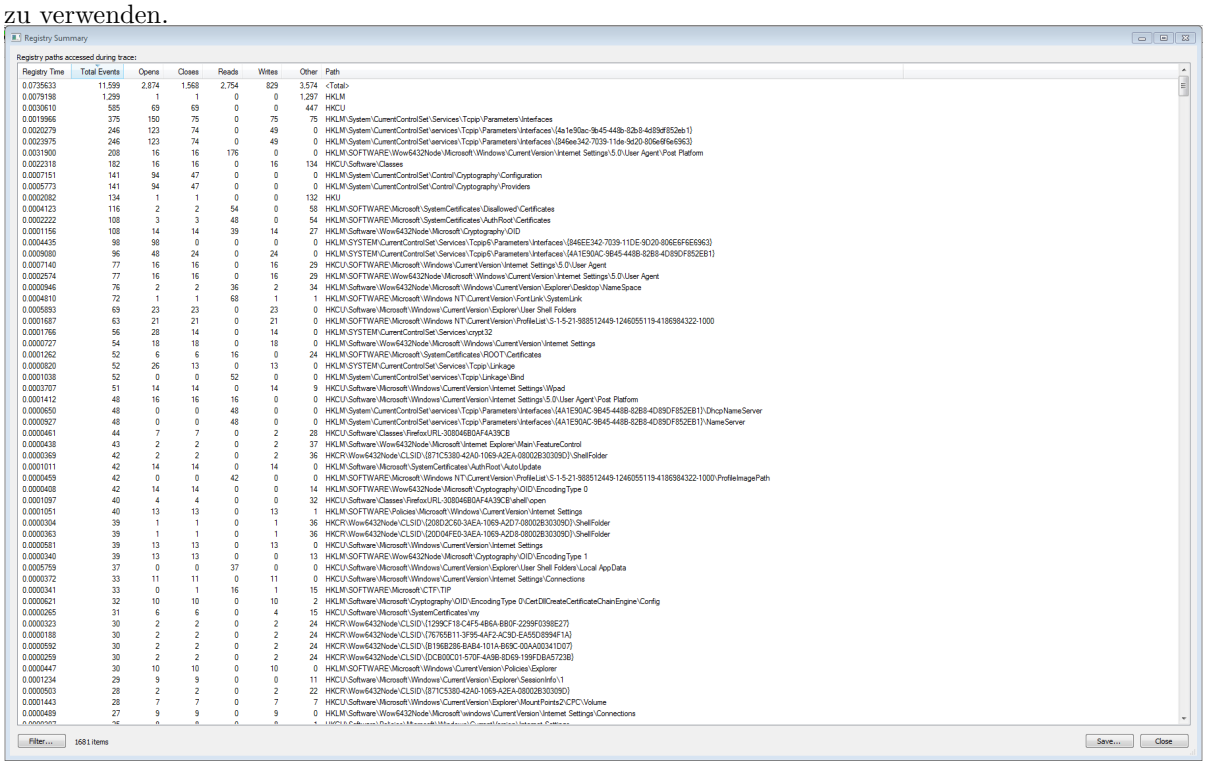
Da nach dem Filtern auf "`Process Name is a`" und "`Event Class is File System`" immernoch weit über 1000 Events bleiben, kann das Tool "File Summary" im "Process Monitor" hilfreich sein:



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

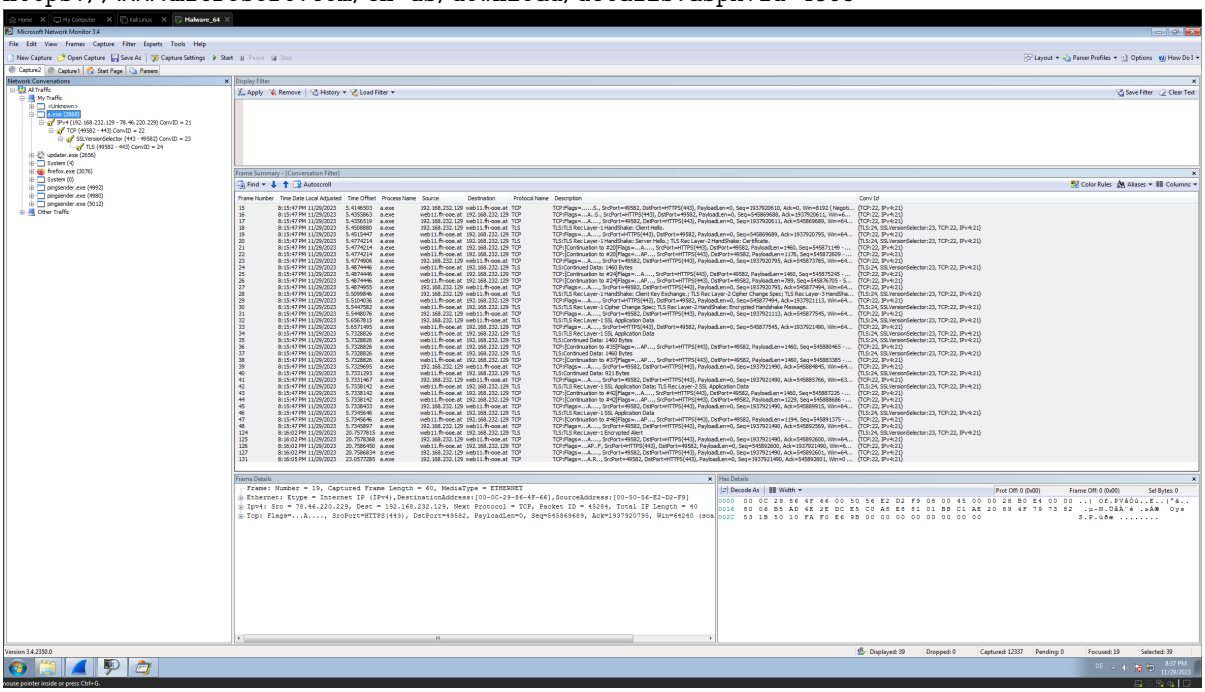
Da das "a"-File ebenfalls sehr viele Registryzugriffe hat, ist es am sinnvollsten die "Registry Summary" zu verwenden.



Besondere Auffälligkeiten konnte hier nicht gefunden werden.

Netzwerkkommunikation

Da die Analyse der Netzwerkkommunikation eines Prozesses unter Windows 7 mit dem "Process Monitor" nicht so gut funktioniert wie unter Windows 11, wurde eine zustätzliche 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