Report #13361

Creation Date: Aug. 20, 2021, 1:43 p.m.
Last Update: Aug. 20, 2021, 8:46 p.m.
File:
regedt32.exe
Results:

Binary

DLL	**False**
Size	10.00KB
trid	**61.7%** Win64 Executable **14.7%** Win32 Dynamic Link Library **10.0%** Win32 Executable **4.5%** OS/2 Executable **4.4%** Generic Win/DOS Executable
type	PE
wordsize	32
Subsystem	Windows GUI

Hashes

md5	49e9ea6f79338b350a8b23cea47d1a86
sha1	b51311eee2a58fdf80cd55616b5a15291a5ee951
crc32	0xb0958c77
sha224	f61dd09a256cddc97cc22aea4d2887e858a44156a93d84998e35de31
sha256	b9a0659a5f8173629c2cc702f9d786f699be2c1c1bd10ee354494df75c618954
sha384	0b7d872c1ae2c053ceccb83bea2a393105f573e60c5fd8bf6397627a2511151a91a474b7be855fb09d66b6da0244002b
sha512	a6f473794315e9a38c3d08f1777ba14d0de3f98f560e8db120f96ed6fb6ef2a14568f444783ae2520f958e872223a8d4cfaeb98718089e3bc5a3da35539c85e0
ssdeep	96:cT/8zwOtfZOWkcTLEp2TyIRoJIP3DGjsl3tTZFovnzeDJFMVWVEWlZhHWwB:cT8zwqrTaGRoTeTZFovnz0MWbxWG

Community

Google	False
HashLib	False

YARA

Matches	domain, HasRichSignature, contentis_base64, HasDebugData, IP, IsPE32, System_Tools, IsWindowsGUI
Suspicious	True

Imports

msvcrt.dll	__setusermatherr, _controlfp, ?terminate@@YAXXZ, _acmdln, _initterm, _ismbblead, __p__fmode, _cexit, _exit, exit, __set_app_type, __getmainargs, _amsg_exit, __p__commode, _XcptFilter, _except_handler4_common
SHELL32.dll	ShellExecuteA
KERNEL32.dll	GetModuleHandleA, GetCommandLineA, HeapSetInformation, GetWindowsDirectoryA, GetStartupInfoA, ExitProcess, GetSystemTimeAsFileTime, GetCurrentThreadId, GetCurrentProcessId, QueryPerformanceCounter, GetModuleHandleW, TerminateProcess, GetCurrentProcess, SetUnhandledExceptionFilter, UnhandledExceptionFilter, GetStartupInfoW, Sleep, GetTickCount
api-ms-win-core-shlwapi-legacy-l1-1-0.dll	PathAppendA

Strings

List

regedt32.pdb
regedt32.exe
regedt32.exe
regedit.exe
name="Microsoft.Windows.Regedt32"
api-ms-win-core-shlwapi-legacy-l1-1-0.dll
6 6%6G6M6T6Y6f6u6}6
<requestedPrivileges>
_acmdln
ExitProcess
TerminateProcess
ShellExecuteA
QueryPerformanceCounter
GetModuleHandleW
GetModuleHandleA

Registry Editor Utility

GetTickCount
Sleep
<description>Registry Editor Utility</description>
<requestedExecutionLevel
10.0.19041.1 (WinBuild.160101.0800)
version="1.0.0.0"
__p__commode
type="win32"
_initterm
__p__fmode
10.0.19041.1
_ismbblead
.CRT$XIAA
.CRT$XCAA
<assemblyIdentity
__setusermatherr
_controlfp
__set_app_type
_amsg_exit
__getmainargs
level="highestAvailable"
_XcptFilter
.rdata$brc
uiAccess="false"
?terminate@@YAXXZ
Microsoft
Microsoft Corporation
</assembly>
.CRT$XIY
CompanyName
ProductName
StringFileInfo
FileVersion
InternalName
OriginalFilename
VarFileInfo
FileDescription
Translation
`.data
_cexit
_exit
.gfids
@.rsrc
RichS
<security>
</security>
GCTL
RSDS
Windows
!This program cannot be run in DOS mode.
VS_VERSION_INFO
processorArchitecture="x86"
<!-- Copyright (c) Microsoft Corporation -->
_except_handler4_common
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
</requestedPrivileges>
LegalCopyright

SHELL32.dll
Operating System
</trustInfo>
GetCurrentProcess
GetCurrentProcessId
GetCurrentThreadId
GetCommandLineA
@.reloc
5 5(5.5;5C5I5a5f5l5q5v5{5
GetSystemTimeAsFileTime
HeapSetInformation
GetStartupInfoW
GetStartupInfoA
PathAppendA
ProductVersion
msvcrt.dll
/>
8"898B8M8T8f8l8r8x8~8
.rdata
.idata
.data
exit
t#hl#@
.idata$5
.idata$6
.idata$2

Foremost

Matches 0.exe, 10 KB

Suspicious True

Heuristics

IPs
hasIPs: False
Allowed
Suspicious
hasAllowed: False
hasSuspicious: False

URLs
Allowed
hasURLs: False
Suspicious
hasAllowed: False
hasSuspicious: False

Files
Allowed: api-ms-win-core-shlwapi-legacy-l1-1-0.dll, SHELL32.dll, KERNEL32.dll, msvcrt.dll
hasFiles: True
Suspicious
hasAllowed: True

hasSuspicious: False

Binary

Sizes

RVA
RVA: 16
Suspicious: False
Code
Size: 6144
Suspicious: False
Image
Address: 4194304
Suspicious: False
Stack
Stack: 8192
Suspicious: False
Headers
Headers: 1024
Suspicious: False
Suspicious: False

Symbols

Number
Number: 0
Suspicious: True
Pointer
Pointer: 0
Suspicious: True
Directories
Number: 16
Suspicious: False

Checksum

Value: 30681
Suspicous: False

Sections

Allowed: .text, .data, .idata, .rsrc, .reloc
Suspicious
hasAllowed: True
hasSections: True
hasSuspicious: False

Versions

OS
Version: 10
Suspicious: False
Image
Version: False
Suspicious: 10
Linker
Version: 14.20
Suspicious: False
Subsystem
Version: 10.0
Suspicious: False
Suspicious: False

EntryPoint	**Address**: 5536 **Suspicious**: False
Anomalies	**Anomalies** **hasAnomalies**: False
Libraries	**Allowed**: api-ms-win-core-shlwapi-legacy-l1-1-0.dll, shell32.dll, kernel32.dll, msvcrt.dll **hasLibs**: True **Suspicious** **hasAllowed**: True **hasSuspicious**: False
Timestamp	**Past**: True **Valid**: True **Value**: 1991-09-04 08:18:33 **Future**: False
Compilation	**Packed**: False **Missing**: False **Packers** **Compiled**: True **Compilers**: Microsoft Visual C++ 8
Obfuscation	**XOR**: False **Fuzzing**: False

PEDetector

Matches	None
Suspicious	False

Disassembly

hasTricks	True
Tricks	
pushret	**.text**: 1
garbagebytes	**.text**: 1

programcontrolflowchange **.text**: 1

cpuinstructionsresultscomparison **.rsrc**: 2

AVclass

File

Trace

20/8/2021 - 19:45:43 .481	Unknown	4		C:\Users\Behemot\Desktop\desktop.ini	
20/8/2021 - 19:45:43 .481	Unknown	4		C:\Windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf	CONHOST.EXE-1F3E9D7E.pf
20/8/2021 - 19:45:45 .497	Write	4		C:\Windows	
20/8/2021 - 19:45:47 .856	Open	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	
20/8/2021 - 19:45:47 .856	Unknown	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe
20/8/2021 - 19:45:47 .856	Open	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	
20/8/2021 - 19:45:47 .856	Unknown	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe
20/8/2021 - 19:45:47 .856	Open	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	
20/8/2021 - 19:45:47	Unkn	29	C:\Windows\System32\	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Us

.856	own	28	svchost.exe		e.exe
20/8/2021 - 19:45:47 .856	Open	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	
20/8/2021 - 19:45:47 .856	Unknown	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe
20/8/2021 - 19:45:47 .856	Open	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	
20/8/2021 - 19:45:47 .856	Unknown	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe
20/8/2021 - 19:45:47 .856	Open	2928	C:\Windows\System32\svchost.exe	C:\Windows\Temp\TMP000000A2F27954F4B4C5FD26	
20/8/2021 - 19:45:47 .872	Unknown	2928	C:\Windows\System32\svchost.exe	C:\Windows\Temp\TMP000000A2F27954F4B4C5FD26	TMP000000A2F27954F4B4C5FD26
20/8/2021 - 19:45:47 .872	Open	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	
20/8/2021 - 19:45:47 .872	Open	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	
20/8/2021 - 19:45:47 .872	Read	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe
20/8/2021 - 19:45:47 .872	Read	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe
20/8/2021 - 19:45:47 .872	Read	292	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe

		8			
20/8/2021 - 19:45:47 .872	Read	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe
20/8/2021 - 19:45:47 .872	Open	2928	C:\Windows\System32\svchost.exe	C:\Windows\Temp\TMP000000A30415A103D3F52066	
20/8/2021 - 19:45:47 .872	Unknown	2928	C:\Windows\System32\svchost.exe	C:\Windows\Temp\TMP000000A30415A103D3F52066	TMP000000A30415A103D3F52066
20/8/2021 - 19:45:47 .872	Open	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe:Zone.Identifier	
20/8/2021 - 19:45:47 .872	Open	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe:Zone.Identifier	
20/8/2021 - 19:45:47 .872	Read	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe:Zone.Identifier	
20/8/2021 - 19:45:47 .872	Unknown	2928	C:\Windows\System32\svchost.exe	C:\Windows\Temp\TMP000000A30415A103D3F52066	TMP000000A30415A103D3F52066
20/8/2021 - 19:45:47 .872	Unknown	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe
20/8/2021 - 19:45:47 .872	Open	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	
20/8/2021 - 19:45:47 .872	Unknown	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe
20/8/2021 - 19:45:47 .872	Open	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	

20/8/2021 - 19:45:47 .872	Unknown	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe
20/8/2021 - 19:45:47 .872	Open	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	
20/8/2021 - 19:45:47 .872	Unknown	2928	C:\Windows\System32\svchost.exe	C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe
20/8/2021 - 19:45:47 .887	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:45:47 .918	Unknown	2928	C:\Windows\System32\svchost.exe	C:\Windows\Temp\TMP000000A2F27954F4B4C5FD26	TMP000000A2F27954F4B4C5FD26
20/8/2021 - 19:45:49 .481	Unknown	4		C:\Monitor\WKCD_Load_Use.exe	WKCD_Load_Use.exe
20/8/2021 - 19:45:49 .481	Write	4		C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:45:49 .481	Unknown	4		C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:45:52 .403	Open	796	C:\Windows\System32\svchost.exe	C:\Windows\Prefetch\WKCD_LOAD_USE.EXE-695C7827.pf	
20/8/2021 - 19:45:52 .403	Open	796	C:\Windows\System32\svchost.exe	C:\Windows\Prefetch\WKCD_LOAD_USE.EXE-695C7827.pf	
20/8/2021 - 19:45:52 .403	Write	796	C:\Windows\System32\svchost.exe	C:\Windows\Prefetch\WKCD_LOAD_USE.EXE-695C7827.pf	WKCD_LOAD_USE.EXE-695C7827.pf
20/8/2021 - 19:45:52 .403	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\Prefetch\WKCD_LOAD_USE.EXE-695C7827.pf	WKCD_LOAD_USE.EXE-695C7827.pf

20/8/2021 - 19:45:52 .418	Open	796	C:\Windows\System32\svchost.exe	C:\Windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf	
20/8/2021 - 19:45:52 .418	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf	CONHOST.EXE-1F3E9D7E.pf
20/8/2021 - 19:45:52 .418	Open	796	C:\Windows\System32\svchost.exe	C:\Windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf	
20/8/2021 - 19:45:52 .418	Write	796	C:\Windows\System32\svchost.exe	C:\Windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf	CONHOST.EXE-1F3E9D7E.pf
20/8/2021 - 19:45:52 .418	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf	CONHOST.EXE-1F3E9D7E.pf
20/8/2021 - 19:45:52 .715	Write	4		C:\Monitor	
20/8/2021 - 19:45:52 .856	Open	2928	C:\Windows\System32\svchost.exe	C:\Windows\System32\conhost.exe	
20/8/2021 - 19:45:52 .856	Open	2928	C:\Windows\System32\svchost.exe	C:\Windows\System32\conhost.exe	
20/8/2021 - 19:45:52 .856	Open	2928	C:\Windows\System32\svchost.exe	C:\Windows\System32\conhost.exe	
20/8/2021 - 19:45:52 .856	Open	2928	C:\Windows\System32\svchost.exe	C:\Windows\System32\conhost.exe	
20/8/2021 - 19:45:52 .856	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:45:52 .856	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log	
20/8/2021					WKCD_LOAD_U

- 19:45:53.497	Write	4		C:\Windows\Prefetch\WKCD_LOAD_USE.EXE-695C7827.pf	SE.EXE-695C7827.pf
20/8/2021 - 19:45:53.497	Write	4		C:\Windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf	CONHOST.EXE-1F3E9D7E.pf
20/8/2021 - 19:45:53.497	Unknown	4		C:\Windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf	CONHOST.EXE-1F3E9D7E.pf
20/8/2021 - 19:45:53.497	Unknown	4		C:\Windows\Prefetch\CONHOST.EXE-1F3E9D7E.pf	CONHOST.EXE-1F3E9D7E.pf
20/8/2021 - 19:45:53.497	Write	4		C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:45:53.497	Unknown	4		C:\Windows\Prefetch\WKCD_LOAD_USE.EXE-695C7827.pf	WKCD_LOAD_USE.EXE-695C7827.pf
20/8/2021 - 19:45:53.497	Unknown	4		C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:46:9.481	Write	4		C:\Windows\Temp	
20/8/2021 - 19:46:17.481	Write	684	C:\Windows\System32\svchost.exe	C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat	
20/8/2021 - 19:46:18.262	Write	4		C:\Windows	
20/8/2021 - 19:46:19.497	Write	4		C:\Windows	
20/8/2021 - 19:46:27.418	Write	4		C:\Windows\System32\config\SYSTEM.LOG1	
20/8/2021 - 19:46:27.418	Write	4		C:\Windows\System32\config\SYSTEM.LOG1	

20/8/2021 - 19:46:27 .418	Write	4	C:\Windows\System32\config\SYSTEM.LOG1
20/8/2021 - 19:46:27 .418	Write	4	C:\Windows\System32\config\SYSTEM.LOG1
20/8/2021 - 19:46:27 .418	Write	4	C:\Windows\System32\config\SYSTEM
20/8/2021 - 19:46:27 .418	Write	4	C:\Windows\System32\config\SYSTEM
20/8/2021 - 19:46:27 .418	Write	4	C:\Windows\System32\config\SYSTEM
20/8/2021 - 19:46:27 .418	Write	4	C:\Windows\System32\config\SYSTEM
20/8/2021 - 19:46:32 .418	Write	4	C:\System Volume Information\Syscache.hve.LOG1
20/8/2021 - 19:46:32 .418	Write	4	C:\System Volume Information\Syscache.hve.LOG1
20/8/2021 - 19:46:32 .418	Write	4	C:\System Volume Information\Syscache.hve.LOG1
20/8/2021 - 19:46:32 .418	Write	4	C:\System Volume Information\Syscache.hve.LOG1
20/8/2021 - 19:46:32 .418	Write	4	C:\System Volume Information\Syscache.hve.LOG1
20/8/2021 - 19:46:32 .418	Write	4	C:\System Volume Information\Syscache.hve.LOG1
20/8/2021 - 19:46:32 .418	Write	4	C:\System Volume Information\Syscache.hve.LOG1
20/8/2021 - 19:46:32 .418	Write	4	C:\System Volume Information\Syscache.hve.LOG1

20/8/2021 - 19:46:32 .418	Write	4		C:\System Volume Information\Syscache.hve.LOG1
20/8/2021 - 19:46:32 .418	Write	4		C:\System Volume Information\Syscache.hve.LOG1
20/8/2021 - 19:46:32 .418	Write	4		C:\System Volume Information\Syscache.hve
20/8/2021 - 19:46:32 .418	Write	4		C:\System Volume Information\Syscache.hve
20/8/2021 - 19:46:32 .418	Write	4		C:\System Volume Information\Syscache.hve
20/8/2021 - 19:46:32 .418	Write	4		C:\System Volume Information\Syscache.hve
20/8/2021 - 19:46:32 .418	Write	4		C:\System Volume Information\Syscache.hve
20/8/2021 - 19:46:32 .418	Write	4		C:\System Volume Information\Syscache.hve
20/8/2021 - 19:46:32 .418	Write	4		C:\System Volume Information\Syscache.hve
20/8/2021 - 19:46:32 .418	Write	4		C:\System Volume Information\Syscache.hve
20/8/2021 - 19:46:32 .418	Write	4		C:\System Volume Information\Syscache.hve
20/8/2021 - 19:46:32 .418	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log
20/8/2021 - 19:46:32 .512	Write	4		C:\System Volume Information\Syscache.hve
20/8/2021 - 19:46:35	Write	4		C:\Monitor\Files\Logs\File.log

.450				
20/8/2021 - 19:46:35 .450	Unknown	4		C:\Monitor\Files\Logs\File.log
20/8/2021 - 19:46:55 .965	Open	528	C:\Windows\System32\SearchIndexer.exe	C:\ProgramData\Microsoft\Search\Data
20/8/2021 - 19:46:55 .965	Unknown	528	C:\Windows\System32\SearchIndexer.exe	C:\ProgramData\Microsoft\Search\Data
20/8/2021 - 19:47:17 .497	Write	684	C:\Windows\System32\svchost.exe	C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive1.dat
20/8/2021 - 19:47:27 .559	Open	1864	C:\Windows\explorer.exe	C:\
20/8/2021 - 19:47:27 .559	Unknown	1864	C:\Windows\explorer.exe	C:\
20/8/2021 - 19:47:32 .809	Open	1864	C:\Windows\explorer.exe	C:\Users\Behemot
20/8/2021 - 19:47:32 .809	Open	1864	C:\Windows\explorer.exe	C:\Users\Behemot
20/8/2021 - 19:47:32 .809	Unknown	1864	C:\Windows\explorer.exe	C:\Users\Behemot
20/8/2021 - 19:47:32 .809	Open	1864	C:\Windows\explorer.exe	C:\Users\Behemot\AppData\Roaming
20/8/2021 - 19:47:32 .809	Open	1864	C:\Windows\explorer.exe	C:\Users\Behemot\AppData\Roaming
	Un	1		

20/8/2021 - 19:47:32 .809	known	864	C:\Windows\explorer.exe	C:\Users\Behemot\AppData\Roaming
20/8/2021 - 19:47:32 .809	Open	1864	C:\Windows\explorer.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\Themes
20/8/2021 - 19:47:32 .809	Open	1864	C:\Windows\explorer.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\Themes\slideshow.ini
20/8/2021 - 19:47:35 .856	Open	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:47:35 .856	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:47:35 .856	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:47:35 .856	Open	796	C:\Windows\System32\svchost.exe	\Device\Mup\.\.\
20/8/2021 - 19:47:35 .856	Open	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:47:35 .856	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:47:35 .856	Unknown	796	C:\Windows\System32\svchost.exe	\Device\Mup\.\.\
20/8/2021 - 19:47:35 .856	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:47:40 .825	Read	1232	C:\Program Files\Windows Media Player\wmpnetwk.exe	C:\Program Files\Windows Media Player\wmpnetwk.exe

20/8/2021 - 19:47:40 .825	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log
20/8/2021 - 19:47:40 .825	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log
20/8/2021 - 19:47:43 .825	Write	4		C:\Monitor\Files\Logs\File.log
20/8/2021 - 19:47:43 .825	Unknown	4		C:\Monitor\Files\Logs\File.log
20/8/2021 - 19:48:11 .309	Open	4		\Device\HarddiskVolume1\System Volume Information
20/8/2021 - 19:48:11 .309	Unknown	4		\Device\HarddiskVolume1\System Volume Information
20/8/2021 - 19:48:13 .59	Open	4		C:\System Volume Information
20/8/2021 - 19:48:13 .59	Open	4		C:\System Volume Information\{3808876b-c176-4e48-b7ae-04046e6cc752}
20/8/2021 - 19:48:13 .59	Open	4		C:\System Volume Information\{bcf7d7ec-4f18-11e8-8b8a-525400842a13}{3808876b-c176-4e48-b7ae-04046e6cc752}
20/8/2021 - 19:48:13 .59	Open	4		C:\System Volume Information\{bcf7d7f0-4f18-11e8-8b8a-525400842a13}{3808876b-c176-4e48-b7ae-04046e6cc752}
20/8/2021 - 19:48:13 .59	Unknown	4		C:\System Volume Information
20/8/2021 - 19:48:17 .481	Write	684	C:\Windows\System32\svchost.exe	C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat
20/8/2021 - 19:48:25 .872	Open	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace

20/8/2021 - 19:48:25 .872	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:48:25 .872	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:48:25 .872	Open	796	C:\Windows\System32\svchost.exe	\Device\Mup\.\.\
20/8/2021 - 19:48:25 .872	Open	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:48:25 .872	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:48:25 .872	Open	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:48:25 .872	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:48:25 .872	Unknown	796	C:\Windows\System32\svchost.exe	\Device\Mup\.\.\
20/8/2021 - 19:48:25 .872	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:48:25 .872	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:49:17 .465	Write	684	C:\Windows\System32\svchost.exe	C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive1.dat
20/8/2021 - 19:49:20 .715	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\container.dat

20/8/2021 - 19:49:20.715	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\container.dat	container.dat
20/8/2021 - 19:49:20.715	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\History\History.IE5\container.dat	
20/8/2021 - 19:49:20.715	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\History\History.IE5\container.dat	container.dat
20/8/2021 - 19:49:20.715	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Feeds Cache\container.dat	
20/8/2021 - 19:49:20.715	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Feeds Cache\container.dat	container.dat
20/8/2021 - 19:49:20.715	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\IECompatCache\container.dat	
20/8/2021 - 19:49:20.715	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\IECompatCache\container.dat	container.dat
20/8/2021 - 19:49:20.715	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\IECompatUACache\container.dat	
20/8/2021 - 19:49:20.715	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\IECompatUACache\container.dat	container.dat
20/8/2021 - 19:49:20.715	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\DNTException\container.dat	
20/8/2021 - 19:49:20.715	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\DNTException\container.dat	container.dat
		1			

20/8/2021 - 19:49:20.715	Open	7964	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\Cookies\container.dat	
20/8/2021 - 19:49:20.715	Unknown	7964	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\Cookies\container.dat	container.dat
20/8/2021 - 19:49:20.715	Open	7964	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Internet Explorer\EmieSiteList\container.dat	
20/8/2021 - 19:49:20.715	Unknown	7964	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Internet Explorer\EmieSiteList\container.dat	container.dat
20/8/2021 - 19:49:20.715	Open	7964	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Internet Explorer\EmieUserList\container.dat	
20/8/2021 - 19:49:20.715	Unknown	7964	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Internet Explorer\EmieUserList\container.dat	container.dat
20/8/2021 - 19:49:20.715	Open	7964	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Internet Explorer\DOMStore\container.dat	
20/8/2021 - 19:49:20.715	Unknown	7964	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Internet Explorer\DOMStore\container.dat	container.dat
20/8/2021 - 19:49:20.715	Open	7964	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018050320180504\container.dat	
20/8/2021 - 19:49:20.715	Unknown	7964	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012018050320180504\container.dat	container.dat
20/8/2021 - 19:49:20.715	Open	7964	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\container.dat	
20/8/2021	Un	1			

- 19:49:20.715	known	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\container.dat	container.dat
20/8/2021 - 19:49:20.715	Open	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\AppCache\B2419NGQ\container.dat	
20/8/2021 - 19:49:20.715	Unknown	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\AppCache\B2419NGQ\container.dat	container.dat
20/8/2021 - 19:49:20.715	Open	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache	
20/8/2021 - 19:49:20.715	Unknown	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache	
20/8/2021 - 19:49:20.715	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:49:20.715	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:49:20.762	Write	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021 - 19:49:20.762	Write	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021 - 19:49:20.856	Write	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021 - 19:49:20.856	Write	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021 - 19:49:20.950	Write	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021					

- 19:49:20.950	Write	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021 - 19:49:20.950	Write	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.log	
20/8/2021 - 19:49:20.950	Write	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.log	
20/8/2021 - 19:49:20.950	Read	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021 - 19:49:20.997	Write	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.log	
20/8/2021 - 19:49:20.997	Write	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.log	
20/8/2021 - 19:49:20.997	Write	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.log	
20/8/2021 - 19:49:20.997	Write	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.log	
20/8/2021 - 19:49:21.43	Write	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021 - 19:49:21.43	Write	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021 - 19:49:21.90	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\container.dat	
20/8/2021 - 19:49:21.90	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\container.dat	container.dat
20/8/2021		1			

- 19:49:21 .90	Open	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache	
20/8/2021 - 19:49:21 .90	Unknown	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache	
20/8/2021 - 19:49:21 .90	Open	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\container.dat	
20/8/2021 - 19:49:21 .90	Unknown	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\container.dat	container.dat
20/8/2021 - 19:49:21 .90	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:49:23 .731	Write	4		C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:49:23 .731	Unknown	4		C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:49:25 .887	Unknown	2360	C:\Windows\System32\audiodg.exe	C:\Windows	
20/8/2021 - 19:49:30 .762	Write	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021 - 19:49:30 .762	Write	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021 - 19:49:30 .809	Write	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021 - 19:49:30 .809	Write	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat	
20/8/2021		7			

- 19:49:30 .856	Open	96	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:49:30 .856	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:49:30 .856	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:49:30 .856	Open	796	C:\Windows\System32\svchost.exe	\Device\Mup\.\.\
20/8/2021 - 19:49:30 .856	Open	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:49:30 .856	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:49:30 .856	Unknown	796	C:\Windows\System32\svchost.exe	\Device\Mup\.\.\
20/8/2021 - 19:49:30 .856	Unknown	796	C:\Windows\System32\svchost.exe	C:\Windows\CSC\v2.0.6\namespace
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.chk
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.chk
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.chk
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.chk

20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.chk
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache
20/8/2021 - 19:49:30 .856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache
20/8/2021 - 19:49:30 .856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache
20/8/2021 - 19:49:30 .856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache
20/8/2021 - 19:49:30 .856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows

20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft
		1		

20/8/2021 - 19:49:30.856	Open	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local
20/8/2021		1		

- 19:49:30 .856	Open	796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local
20/8/2021 - 19:49:30 .856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local
20/8/2021 - 19:49:30 .856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData
20/8/2021 - 19:49:30 .856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData
20/8/2021 - 19:49:30 .856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData
20/8/2021 - 19:49:30 .856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData
20/8/2021 - 19:49:30 .856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData
20/8/2021 - 19:49:30	Op	17	C:\Windows\System32\t	C:\Users\Behemot\AppData

.856	en	96	askhost.exe	
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot
20/8/2021 - 19:49:30	Open	179	C:\Windows\System32\taskhost.exe	C:\Users

.856		6		
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users
20/8/2021 - 19:49:30.856	Open	1796	C:\Windows\System32\taskhost.exe	C:\Users
20/8/2021 - 19:49:30.856	Unknown	1796	C:\Windows\System32\taskhost.exe	C:\Users
20/8/2021 - 19:49:30.856	Write	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.chk
20/8/2021 - 19:49:30.856	Write	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.chk
20/8/2021 - 19:49:30.856	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log

20/8/2021 - 19:49:30.856	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:49:30.856	Write	1796	C:\Windows\System32\taskhost.exe	C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.chk	
20/8/2021 - 19:49:30.856	Write	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.chk	
20/8/2021 - 19:49:30.856	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:49:30.872	Write	804	C:\Monitor\WKCD_Load_Use.exe	C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:49:31.465	Write	4		C:\Monitor\Files\Logs\File.log	
20/8/2021 - 19:49:31.465	Unknown	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.chk	
20/8/2021 - 19:49:31.465	Unknown	4		C:\Users\Behemot\AppData\Local\Microsoft\Windows\WebCache\V01.chk	
20/8/2021 - 19:49:31.559	Unknown	4		C:\Monitor\Files\Logs\File.log	

Process

Trace

20/8/2021 - 19:49:25.887	Terminate	684	C:\Windows\System32\svchost.exe	2360	C:\Windows\System32\audiodg.exe

Analysis

Reason Timeout

Status Sucessfully Executed

Results 1

Registry

Trace

20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\LruList	CurrentLru
20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\LruList\00000000000000ED	ObjectId
20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\LruList\00000000000000ED	ObjectLru
20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\ObjectTable\1E	_ObjectLru_
20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\LruList\00000000000000E8	ObjectId
20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\LruList\00000000000000E8	ObjectLru
20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\ObjectTable\3E	_ObjectLru_
20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\LruList\00000000000000EB	ObjectId
20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\LruList\00000000000000EB	ObjectLru
20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\ObjectTable\3F	_ObjectLru_
20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\LruList\00000000000000F0	ObjectId
20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\LruList\00000000000000F0	ObjectLru
20/8/2021 - 19:46:22.418	Write	4	\REGISTRY\A\{BCF7D7EA-4F18-11E8-8B8A-525400842A13}\DefaultObjectStore\ObjectTable\40	_ObjectLru_
20/8/2021 - 19:4	Wr	4	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nsi\{eb004a03-9b	

6:23.934	ite		1a-11d4-9123-0050047759bc}\22	
20/8/2021 - 19:46:23.934	Write	4	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24	ffffffffffffffffffffffffffffff00
20/8/2021 - 19:46:23.934	Write	4	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24	ffffffffffffffffffffffffffffff01
20/8/2021 - 19:46:23.934	Write	4	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24	ffffffffffffffffffffffffffffff02
20/8/2021 - 19:46:23.934	Write	4	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Nsi\{eb004a03-9b1a-11d4-9123-0050047759bc}\24	ffffffffffffffffffffffffffffff03

File Summary

Created **Identified**: True

Deleted **Identified**: False

Process Summary

Created **Identified**: False

Deleted **Identified**: True

Registry Summary

Proxy **Identified**: False

AutoRun **Identified**: False

Created **Identified**: True

Deleted **Identified**: False

Browsers **Identified**: False

Internet **Identified**: False

DNS

Query

Response

TCP

Info

UDP

Info

HTTP

Info

Summary

DNS	**False** ⊗
TCP	**False** ⊗
UDP	**False** ⊗
HTTP	**False** ⊗

Results

BINARY

NFS 2.0 (Threshold = 0.8)

confidence: 77.50%
suspicious: **False** ✗

NFS 3.0 (Threshold = 0.75)
confidence: 78.00%
suspicious: **True** ✓

Decision Tree (NFS-BRMalware)
confidence: 100.00%
suspicious: **True** ✓

MalConv (Ember: Raw Bytes, Threshold=0.5)
confidence: 93.56%
suspicious: **True** ✓

Random Forest (100 estimators, NFS-BRMalware)
confidence: 69.00%
suspicious: **False** ✗

Non-Negative MalConv (Ember: Raw Bytes, Threshold=0.35)
confidence: 81.93%
suspicious: **True** ✓

LightGDM (Ember: File Characteristics, Threshold=0.8336)
confidence: 100.00%
suspicious: **False** ✗