MALICIOUS

Classifications: Ransomware

Threat Names: -

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe**
ID	#4177845
MD5	3d1cc4ef33bad0e39c757fce317ef82a
SHA1	f34e4b7080aa2ee5cfee2dac38ec0c306203b4ac
SHA256	e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60
File Size	3631.50 KB
Report Created	2022-04-23 19:53 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (13 rules, 116 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe renames multiple user files.			
4/5	Defense Evasion	Tries to disable antivirus software	1	-
	• (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe stops a service related to Windows Defender via ControlService (API).			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe tries to detect "wine" by calling GetProcAddress() on "wine_get_version".			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe tries to read sensitive data of ftp application "AbleFTP" by file.			
2/5	Discovery	Executes WMI query	1	-
	• (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe executes WMI query: SELECT * FROM Win32_ShadowCopy.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe tries to read sensitive data of mail application "Windows Mail" by file.			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe creates mutex with name "Global\EKANS".			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe enumerates running processes.			
1/5	System Modification	Modifies application directory	100	-

- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\hd5gp40xnzxs9ceg h.gif".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\ihz5wsezsjksxbd.gif".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i641033.hash".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\clicktorun\i640.hash".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\clicktorun\c2rheartbeatconfig.xml".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\clicktorun\officeupdateschedule.xml".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\clicktorun\servicewatcherschedule.xml".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppobjs-spp-plugin-manifest-signed.xrm-ms".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppobjs.dll".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppcext.dll".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppc.dll".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppsvc.exe".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppwmi.dll".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\officesoftwareprotectionplatform\osppwmi.mof".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\microsoft shared\stationery\desktop.ini".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\common files\ybi.jpg".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\internet explorer\signup\install.ins".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\reference assemblies\microsoft\framework\v3.0\winfxlist.xml".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\reference assemblies\microsoft\framework\v3.0\redistlist\frameworklist.xml".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\msbuild\microsoft\windows workflow foundation\v3.0\workflow.visualbasic.targets".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\msbuild\microsoft\windows workflow foundation\v3.0\workflow.targets".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\windows sidebar\settings.ini".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\windowspowershell\modules\powershellget\1.0.0.1\en-us\psget.resource.psd1".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.format.ps1xml".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\windowspowershell\modules\packagemanagement\1.0.0.1\packagemanagement.psd1".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\windowspowershell\modules\powershellget\1.0.0.1\powershellget.psd1".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\windowspowershell\modules\packagemanagement\1.0.0.1\packageproviderfunctions.psm1".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\windowspowershell\modules\powershellget\1.0.0.1\psget.format.ps1xml".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\windowspowershell\modules\powershellget\1.0.0.1\psget.resource.psd1".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\common files\microsoft shared\office16\liclua.exe".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files\windowspowershell\modules\powershellget\1.0.0.1\psmodule.psm1".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\common files\microsoft shared\officesoftwareprotectionplatform\osppc.dll".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\common files\designer\msaddndr.olb".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\common files\microsoft shared\office16\office setup controller\pkeyconfig-office.xrm-ms".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\common files\microsoft shared\officesoftwareprotectionplatform\osppcext.dll".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\common files\microsoft shared\stationery\desktop.ini".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\common files\microsoft shared\vsta\pipeline.v10.0\pipelinesegments.store".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\common files\microsoft shared\vsto\actionspane3.xsd".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\common files\microsoft shared\vsta\vstofiles.cat".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\common files\microsoft shared\source engine\ose.exe".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\common files\microsoft shared\vsta\appinfodocument\addins.store".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\microsoft office\filesystemmetadata.xml".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\internet explorer\signup\install.ins".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\microsoft office\appxmanifest.xml".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\microsoft office\office16\ospp.vbs".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe modifies "c:\program files (x86)\microsoft office\office16\ospp.htm".

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Changes folder appearance	5	-

- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe changes the appearance of folder "c:\program files\common files\microsoft shared\stationery".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe changes the appearance of folder "c:\program files (x86)\common files\microsoft shared\stationery".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe changes the appearance of folder "c:\program files (x86)\microsoft office\root\office16\1033\dataservices".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe changes the appearance of folder "c:\users\default\appdata\local\microsoft\windows mail\stationery".
- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe changes the appearance of folder "c:\users\keecfmwgj\appdata\local\microsoft\windows mail\stationery".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	1	-

- (Process #1) e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe resolves 58 API functions by name.

Mitre ATT&CK Matrix

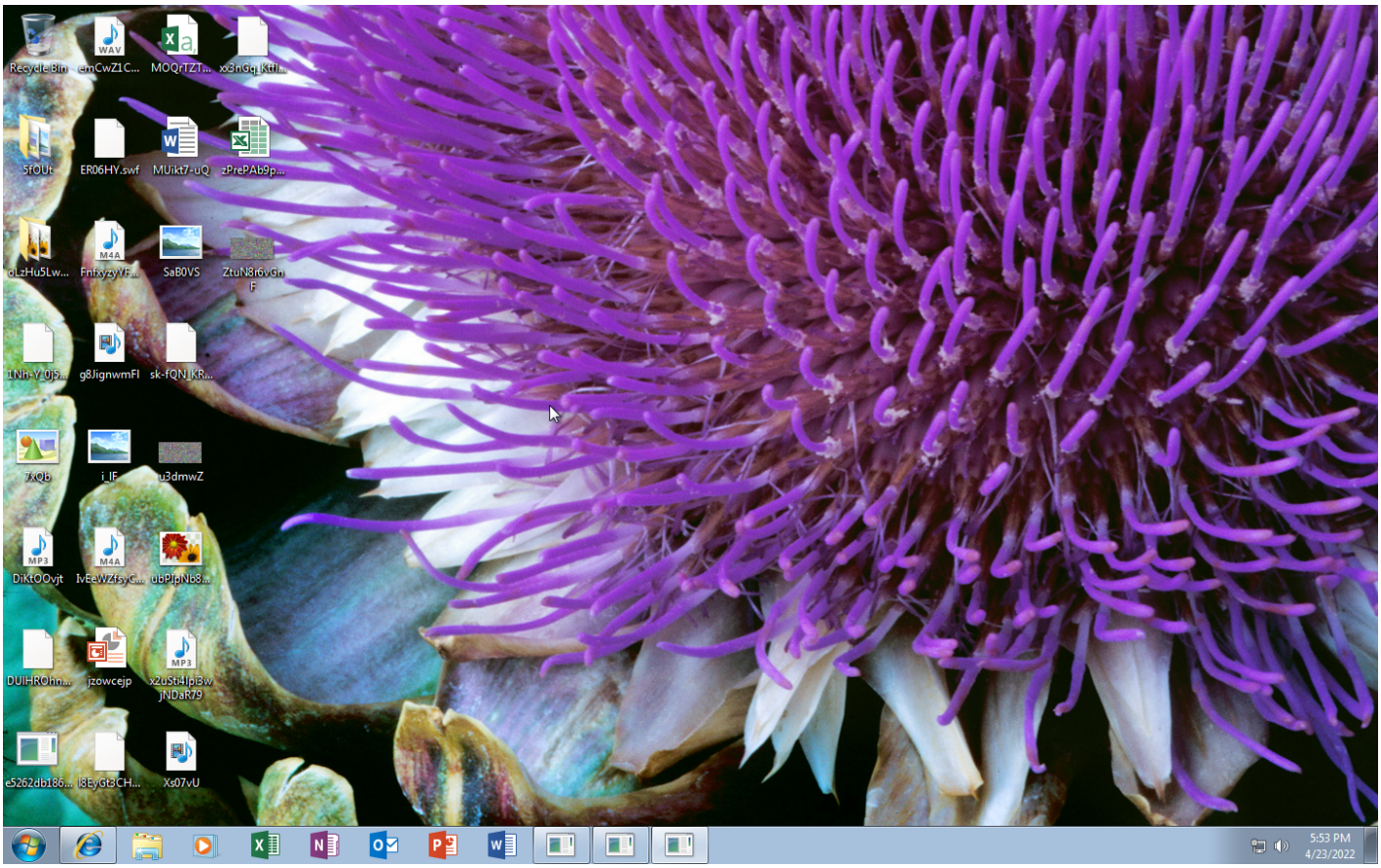
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1497 Virtualization/ Sandbox Evasion	#T1081 Credentials in Files	#T1497 Virtualization/ Sandbox Evasion		#T1119 Automated Collection			#T1489 Service Stop
				#T1089 Disabling Security Tools		#T1083 File and Directory Discovery		#T1005 Data from Local System			#T1486 Data Encrypted for Impact
				#T1036 Masquerading		#T1057 Process Discovery					
				#T1045 Software Packing							

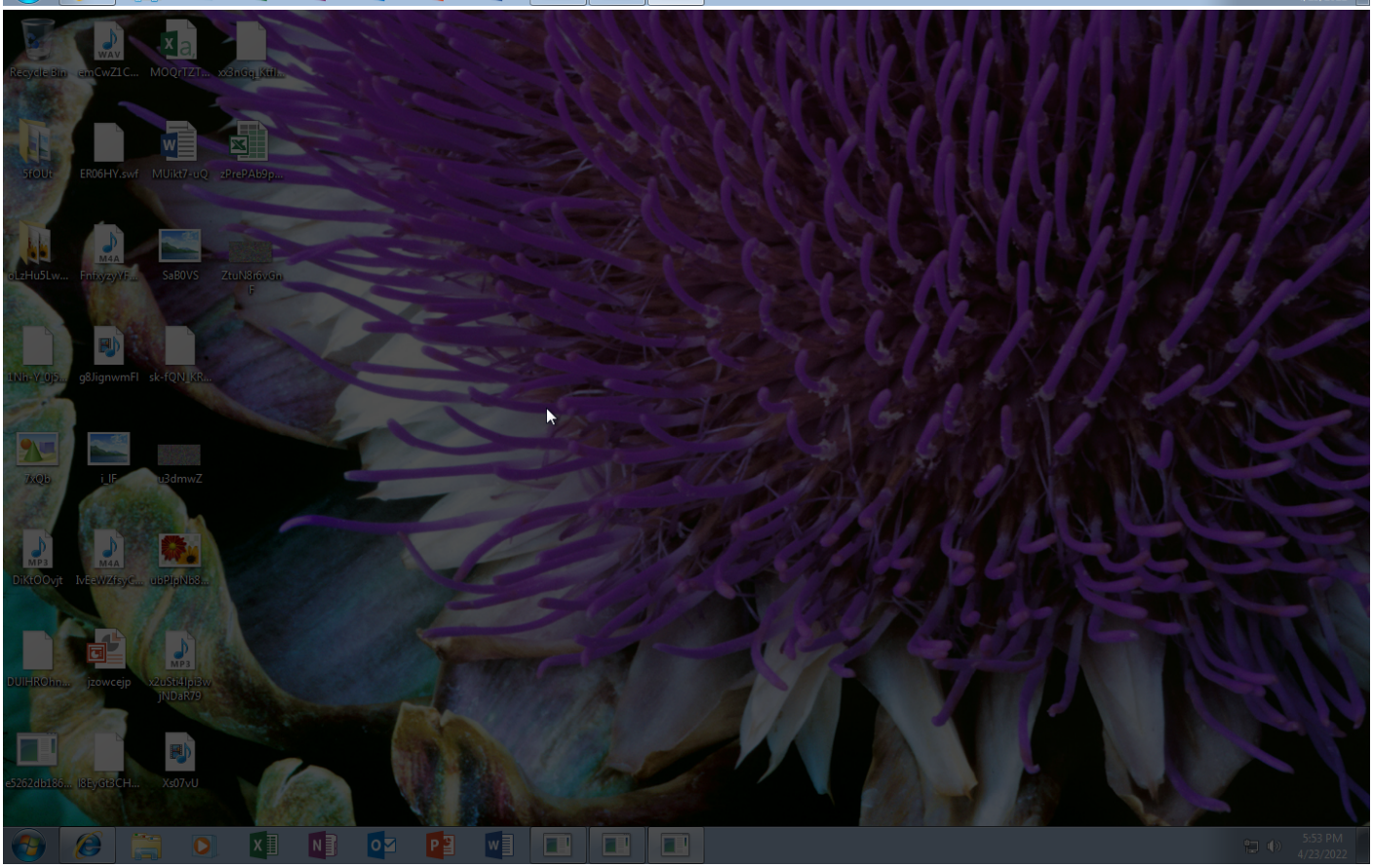
Sample Information

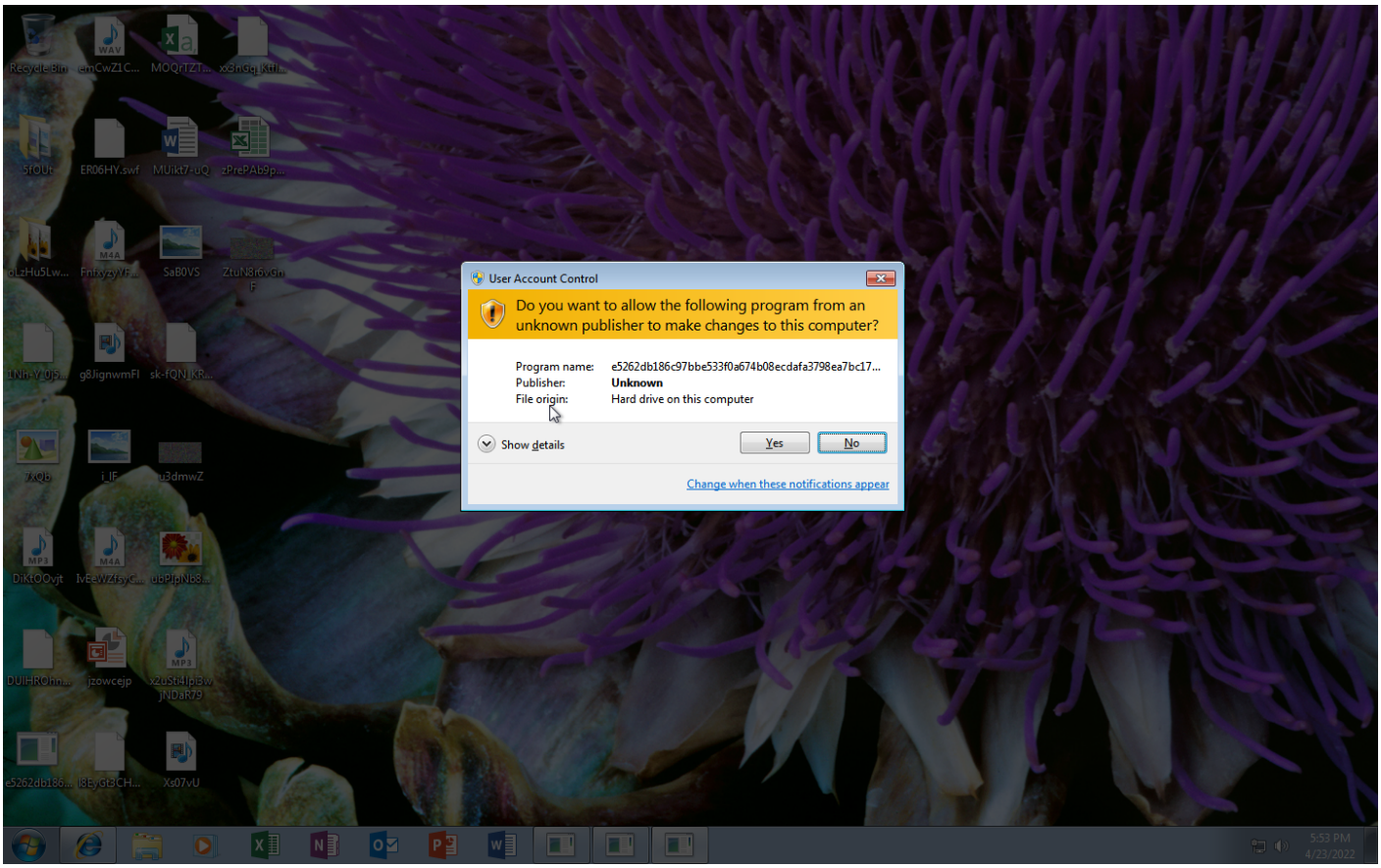
ID	#4177845
MD5	3d1cc4ef33bad0e39c757fce317ef82a
SHA1	f34e4b7080aa2ee5cfee2dac38ec0c306203b4ac
SHA256	e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60
SSDeep	49152:QAdGB73ejP3+EMfRdASVaAvrC5Xh602+:QAgR3epMjASHch
ImpHash	96c44fa1eee2c4e9b9e77d7bf42d59e6
File Name	e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe
File Size	3631.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

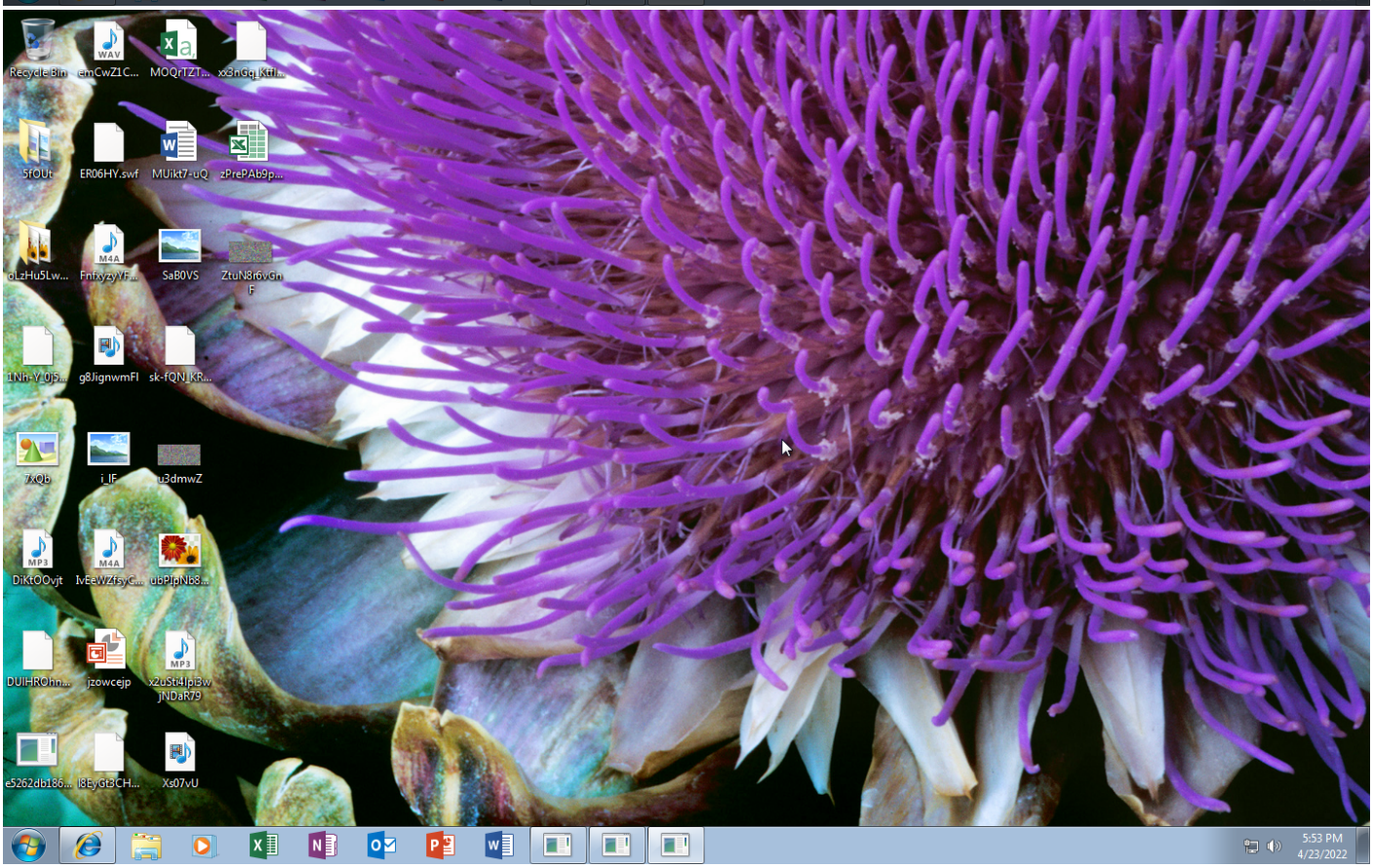
Analysis Information

Creation Time	2022-04-23 19:53 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	4
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
emCwZ1C...
MOQrTZT...
xc6nGq.KtH...
5fOUt
ER06HY.swf
MUikt7-uQ
zPrePAb9p...
oLzHu5Lw...
FnrxyzyYF...
SaB0VS
ZtuN8r6vGn
F
1NhY_0j5...
g8JignwmFI
sk-fQN_KR...
7xQb
i_IF
u3dmwZ
DiktOOvjt
IvEeWZfsyC...
ubPIpNb8...
DUIHROhn...
jzowcejp
x2uSt4JpBw
jNDaR79
e5262db186...
l8EyGt3CH...
Xs07vU
5:53 PM
4/23/2022


Recycle Bin
emCwZ1C...
MOQrTZT...
xc6nGq.KtH...
5fOUt
ER06HY.swf
MUikt7-uQ
zPrePAb9p...
oLzHu5Lw...
FnrxyzyYF...
SaB0VS
ZtuN8r6vGn
F
1NhY_0j5...
g8JignwmFI
sk-fQN_KR...
7xQb
i_IF
u3dmwZ
DiktOOvjt
IvEeWZfsyC...
ubPIpNb8...
DUIHROhn...
jzowcejp
x2uSt4JpBw
jNDaR79
e5262db186...
l8EyGt3CH...
Xs07vU
5:53 PM
4/23/2022





Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph

Process #1: e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 39764, Reason: Analysis Target
Unmonitor End Time	End Time: 261939, Reason: Terminated
Monitor duration	222.18s
Return Code	0
PID	3660
Parent PID	1928
Bitness	32 Bit

Dropped Files (267)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Temp\ygMWDLG1.docx	60.70 KB	46eb1da33355ad44115624c5298022441ffc7817930dc7d1fbf475b258492f0c	✗
C:\Users\kEecfMwgj\AppData\Roaming\l6oQCklppOV.docx	49.42 KB	e0a105c8add41178eac0179ddfe8ab7f2961bd44902d0b1bc402e5cde87af2e4	✗
C:\Users\kEecfMwgj\Desktop\MUikt7-uQ.docx	64.64 KB	d5a0fae9bfd67b94ec200abc38e842bb3bfe9f30ae20303a64466f444c6c2e87	✗
C:\Users\kEecfMwgj\Documents\56ixAATbHJkDzbE.docx	88.17 KB	881d96f01c78f5cd967d611e86ca81ebbf01f45b94fe629a0d8c94a267f90a9c	✗
C:\Users\kEecfMwgj\AppData\Roaming\hABtzl81jau7GXG.docx	88.05 KB	3e68041f92d84b6f6043d81e531561d0d9726368bea0e315be1eb222de5cf357	✗
C:\Users\kEecfMwgj\Documents\bspGlPMk4_an1.docx	78.56 KB	11a05f9bf9955cea10757fc7a6fb04a0c623e6b24ce98b3288f4a22325b72909	✗
C:\Users\kEecfMwgj\Documents\5Z2lDBjIfl7blTzL-.docx	71.72 KB	c22b05262cc804ccf992c04620bc9a45f5d9c8456f050d87b8ffa9cba58514e6	✗
C:\Users\kEecfMwgj\Documents\djjdzoNAgImR2tzKl.docx	22.68 KB	ca0fcb722d9cb68a7cf40ce887e6cf9358e09b5035590b0d586229aecefe0475	✗
C:\Users\kEecfMwgj\Documents\8YVRCgZcMH3Llujoyf4g.docx	59.06 KB	653da690f068e9db72540d5e9e609eceb6f50e814c0319cb4756f4f78d12c1c7	✗
C:\Users\kEecfMwgj\Documents\DPUHbDi_baXkj\b90Z dF_C.docx	73.51 KB	467554056480fa99fbbdfa98e31046d98da4e56fa8fa206ba603bb8249485b63	✗
C:\Users\kEecfMwgj\Documents\lpmQl9lE7gPmac-Inw.docx	66.53 KB	d37561da95f0794265a871216afaf375e28f00c9df98ebaad303e82a44c11d90	✗
C:\Users\kEecfMwgj\Documents\xLwfr oEb7Mm.docx	84.74 KB	dba304459651e3a306acf599be94c13ce7296ae8c1b96138152ed25d569cd959	✗
C:\Boot\BOOTSTAT.DAT	64.38 KB	b4c49d77bd118755f5325a12c3d895da9becbcdd543c8866bb9affe2606486be	✗
C:\Program Files\Common Files\hD5gp40XNzXS9cEg h.gif	36.97 KB	aed340981c65c2ebe0d63a294537c0dacc49521ffbc43ab6f8199f5c3e5c16d9	✗
C:\Program Files\Common Files\lhz5WseZSjkSxbd.gif	10.31 KB	bad6ae663875bb18dbdbc5b099306b6f2208319223039 39d46806b2696fabae8	✗
C:\Program Files\Common Files\Microsoft Shared\ClickToRun\C2RHeartbeatConfig.xml	4.48 KB	59a77baaa208242b04f743dcc6d2c206af38e9335aa37b518b1bde24e9e77744	✗
C:\Program Files\Common Files\Microsoft Shared\ClickToRun\i640.hash	541 bytes	32ba7270296e16e61e0492e46561aa92386769a883e8b7b61ac3e830c9177cd8	✗
C:\Program Files\Common Files\Microsoft Shared\ClickToRun\i641033.hash	544 bytes	6903befb8d6ae785afe3f67f3a80f7be8cdfc5e2ff68e07d586d32c68083b4a1	✗

File Name	File Size	SHA256	YARA Match
C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeUpdateSchedule.xml	5.11 KB	6d448ef5f360f048fdf30f274d859a1992a0260a3b3a1234860219fb71ee2d2f	✗
C:\Program Files\Common Files\Microsoft Shared\ClickToRun\ServiceWatcherSchedule.xml	4.79 KB	dee2a25e4e5d12b9be3e99115430a3eb9aea0e0c8daf1743286c46f2004ede59	✗
C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPC.DLL	200.04 KB	ffa4169dbf07971ddb5b5499343253251833ece734ccf5e85c876434ffe0b348	✗
C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPCEXT.DLL	1791.04 KB	4ae9f77e6615778ee2101ad27438bec1ab311b32fde339a333fc7e053bb5663d	✗
C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\osppobjs-spp-plugin-manifest-signed.xrm-ms	9.66 KB	e370082f83f6c7bf47b4274ae062f9ad64ea2669b4825c2bb437184aeeb20319	✗
C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPOBJS.DLL	2178.54 KB	205478ba9bde5d1ccee0da3bfcd9d3527ebf180dd857fa8a3168570bcaa7d012	✗
C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE	5013.04 KB	bce7204e9a0db9e919994a7b0557ef65c9fd34b566947df750b0afb979aed595	✗
C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPWMI.DLL	144.04 KB	e37e8acb042fb39ef6aaaf87343450467723a64581c8bdc96f845fd89e453489	✗
C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPWMI.MOF	47.40 KB	13b4d471d65c6027758bf2e554bcf1e32a7d132f4cc195eae3ed95d033046d2d	✗
C:\Program Files\Common Files\Microsoft Shared\Stationery\Desktop.ini	1.06 KB	122df3d628042b3cc40d51abadb4c913d0b2de373bafa0f5ad3b9cd6283e2861	✗
C:\Program Files\Common Files\ybi.jpg	71.10 KB	afe6ce6c17e47111798e72e783fd0319c2447d4aec829457cd870fdbe8c31d9b	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\CLASSIC2.WMF	2.64 KB	a5b5d80ba2bbe63e8fd087c76dc7f8ab96f2df353daece342e0f6a6c7e68b31d	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\CLIP.WMF	2.64 KB	27f19f12127bd08c8616d5d5974be6e6c57a94da308723d57e37166f02c02b92	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\CMNTY_01.MID	7.24 KB	0de1f6e54ffe8e947705b0be17d739ec4669fa8de1ef11a2d3aaad2567af8b08	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\CRANE.WMF	5.58 KB	250ee3f16d79b4343f32ff104bf347a344feb508d1f33a0e35279ebe1986228b	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\CRANINST.WMF	48.82 KB	4cbf79fa55efcd487206c5a64f9f0026bfc19f0bf7d61abb450828ccd5a5e7be	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\CUP.WMF	3.33 KB	b94610cc87bd2382b057b92142dd7ceb353d565304c0c7a7dd548f565ba5ff4c	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\CUPINST.WMF	10.52 KB	dc826d94defdf82cae55304fee47299ea1b7d445d3e21c2a0e63a079d07fff49	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00117_.WMF	30.83 KB	6ee08b6773ea1e9f4d0d4469e9c1ac8b0a6c110d38bda28a303f9091096eaff3	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00121_.WMF	8.50 KB	5b9b32bce97956f8474247dd6ec9dcee31654c3aabc473c1fd2e6722958d9f96	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00255_.WMF	3.06 KB	b822baa316b87a2bd16c4fe1e6a2c142291982fd4c56389131e3058b7082ea01	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00234_.WMF	29.37 KB	37272d8aef6493340be2f60df8dc79d52d1f610f6ef6f29f17c9c4417417365f	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00256_.WMF	3.20 KB	03a95c67b87e3bb2d0f2fb8d0678a7183efc02a7cdc7dd7fa2ae7b59ea207990	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00261_.WMF	37.52 KB	728d3702babb57f3b7bd0c721b82fe8ea83cc8898a0fd08e906fa928ff77ad70	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00297_.WMF	39.53 KB	4bd7775d7007fddd51f7034e56f305ef0684ac1039582bcc0bb54e0ab21925a4	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00372_.WMF	1.21 KB	0401746c00423ca479ace61a0374c135cb905eca2c0be99cfe56fbe0bb5c4c35	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00405_.WMF	17.61 KB	5f02de460b36a919fd6207cc585307e5398f72e16f6c77c9710ba49b28db097e	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00407_.WMF	8.08 KB	b2f879f0c0178aa0bb8cfe88eb43d6e946b0612691bb83209647123127fe636c	✗

File Name	File Size	SHA256	YARA Match
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00413_.WMF	42.42 KB	54fe2aff2f1b3bc7c667186ac707e338b62a33c3fe9077dc18c4d497279eedf0	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00414_.WMF	42.34 KB	65326be6b8901235df18ddf9ca82b1d14344ac4403e5cc0f09ced099c01a7ab6	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00419_.WMF	1.13 KB	25cf456031b26a05b7d302e4824856f73a04512c57dc47db709394c6f124737d	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00448_.WMF	3.32 KB	d0a518d6402f9bcc3e0532affffd191c064bc7ba8922a49446f29d07098e2b7c	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00437_.WMF	2.32 KB	59b7fa7403392caf206f7e204b94c6428f439ff4e7180171963903324ff6844a	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00449_.WMF	10.19 KB	89fffad868ee1b02c011c98c78702b88534410d0809ab6725540b8d9bdab12e3	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00687_.WMF	20.73 KB	30b986c075eafeef03da701d4aceee0eff6df58a896c800d775ad01642ade788	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD00705_.WMF	24.45 KB	1880741e8548c31d9958b1a388c2dae014989917489c83b67b42cfb9d3230c3c	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01015_.WMF	2.61 KB	c5e9e67491eba953d6ea48634f13dac7af936da6ccadcdba77ef93808e16a2ff	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01039_.WMF	14.91 KB	ecfc1adc51154ced042b87bec5551b78210f7ace41ddbee01e83083e0c696897	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01138_.WMF	4.04 KB	9dd55ef2c28487181bb3bf36a01107a35cb75eacca6a949eca76997cdc36e2aa	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01139_.WMF	3.98 KB	8e16826f0e4cd958ba4cd5f9fd03744607b7fb03f2bd855d03e1ce0dfa7bcfcc	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01140_.WMF	3.97 KB	ea63a28766ec4be76eda4d2c4367372124c93fb418d044fb6982bd1599c54eda	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01143_.WMF	2.53 KB	a9e31d9b7a169017ae7882cecb2fa4f906e9280939093284c7ec19432cf2fa80	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01145_.WMF	3.15 KB	60733e86e13a80fb0d6ec6ff604d314be730f484827639967565d2855c1bb2a0	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01151_.WMF	3.33 KB	947d6d0560546824b5b8c81cc06f61f1e2a832236382625a1e71b6506df79933	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01146_.WMF	3.17 KB	a17a2734faf5716b5fbe0659fd729a351369b2a1bc92b5bfc294c5a3bb6829df	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01152_.WMF	3.33 KB	accaacc38abff157fae3c465c2878ab2848ccb912d6f52207e445255eb0b4699	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01157_.WMF	3.94 KB	511bf5b29fd1a29d35665450e0fb119aab1b49ce4746ea06c26043becdd91a63	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01160_.WMF	2.61 KB	8e50565ffd7c809a6dea44d54181d62f906f1ac6c444174c18daabe097306a3f	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01162_.WMF	2.68 KB	d63c01d3936062634516b517d3ed901c3508a5a1c54319fe0428d93021a21ad3	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01163_.WMF	2.68 KB	27b366ac143767216a93c820a9a01350cefe603e2f6063fe5a155c7efcbc71ae	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01166_.WMF	2.47 KB	ee36d84e8041ef81ca5183b5b50cfcaffb4f735a1d76950d919161e8771b17dc	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01167_.WMF	2.47 KB	963dd974543ad8ad320279bbe5958e42c60dcde199fe6d9423f8e18ebb6daf65	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01168_.WMF	2.39 KB	c0ab4e2f4f4f5071b2518a87e47af109cafafaa4be014e34db52e4482183318c	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01169_.WMF	2.41 KB	cc2094c1ebb83e1566ab6afd84983909e3a145874ae0d32e3207024fc93c2a29	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01170_.WMF	2.78 KB	c06ffa02d4e307545a30625941d7f15a2597cef2d543192982f27fe7812f675a	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01171_.WMF	2.44 KB	2628d1d64fea3d67ba6024c097bce3aefd5530037cd7102021331714b722dd6b	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01172_.WMF	2.62 KB	cd5a1207fba3ad6ca2b67e83df7448f6736a680306b0bb4ab66ff65f3049f531	✗

File Name	File Size	SHA256	YARA Match
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01173_.WMF	2.20 KB	ae788f78194963a8357cebf2cf437d87bfe1612ab3400179c9e9da5bad6ff7e6	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01176_.WMF	2.28 KB	fe7137e4a1b254cbb0f8b8f72221464c4fff49198791989222b6948c040fd12b	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01178_.WMF	4.14 KB	cbd9d59255b55fad355f75e5f189fbe5d85ff6cb00fd90b6ad3ed43277564611	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01179_.WMF	2.41 KB	ad52bcfe6628e23f68755a89d2651f32009aacf0f6a37f6fc310b4235bbabd87	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01180_.WMF	2.47 KB	435ea0dd68d6876c7ab562a29cd7e46af2b7d8826dab841e0646a407c3a106de	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01181_.WMF	1.85 KB	0fdcd57812951fd2eafea3566228c2708e11ee1c969a8d0dcedff10f35524254	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01182_.WMF	3.36 KB	09ce08efc35613e1d6d7f3866318673e493ca0e53a26c6cb88ff1bdd08f0d043	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01186_.WMF	8.80 KB	ff3d3e4f0bfade062b44ccf7f86842a002699e9ca39f983d997d2c28a505d0ad	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01183_.WMF	2.68 KB	d26782967662447657 46f0fcec92c9c6aab18acf0b7d5eb82fef18024e2e6080	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01366_.WMF	2.16 KB	cc630189b18678c2049b68c2315ddb4b9ab11cac253da5de2cbdb2f332cac855	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01434_.WMF	1.31 KB	59d76571a66509520bf0eba666e7b5cff7364ed2bb35aa2cd005e5b94553a83c	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01585_.WMF	2.90 KB	e8bf664e2cdd22467b3cd3f3713100a66568dd63a1c555243482ae0c44153a00	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01586_.WMF	2.71 KB	84d07390fdd8bb6fa54d849dca3e2f1f1eac2b5fdc743e1d580b56e71e327855	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01628_.WMF	19.06 KB	d13e11876b9996b5b8109b5f274f3fb20a7548ec73620694dfe324e6d8df0f39	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01629_.WMF	1.00 KB	e84117b3b7149a30541b9d718089e88d08d5a5bed1a8fa921b33df3d008a17f8	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01630_.WMF	742 bytes	6bac34d28480f82dd013927032a31d3aa75d7927ddd9a6e8ef2e29d8e3d23a47	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01761_.WMF	4.49 KB	37c5e8e3c6b091a6989816102140042eed79c2f0fb99460de0bfb9f2585b01f3	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01631_.WMF	998 bytes	c6390dfb4fa660ff1fa92a546cf20a3173b50680ffb452e56d66ae5f12f6b61a	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01772_.WMF	2.68 KB	b0345805221676a7e3112392cd553a803dca181d233db3b4e84040c7a7752c4c	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\DD01793_.WMF	3.61 KB	86331bfc40fbb695f096d969fdce9b420dc6de6b9e142b089109fa7e1ebbb62d	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\EAST_01.MID	6.46 KB	7381bfe40514b57cddc5ea91226b5eb6da0c5e1e6f91c60f3d0810c3da1efb24	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\ED00010_.WMF	1.79 KB	d9080ce7563e6a04082b449e8f356468b7781d8a8308b27f1e7e2eaf26193945	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\ED00019_.WMF	13.17 KB	5afb7b069fc4b327e063310e93b29ea528a709d3a1604f432038c0503e227da4	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\ED00172_.WMF	3.07 KB	e9a20c2ee8a22ccc1b1ee1dfcc4b6f3d329b9a5f1b596fa5f82cab568063e154	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\ED00184_.WMF	7.23 KB	32712bde87e24140ed9512209ee97a787a09c7e9bf2cc2bef79477b49280e266	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\EN00006_.WMF	14.04 KB	c28499a21aaefd8fc74a037c0bee7ba96d693b5f0bf349503b002c91159bd1a8	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\EN00202_.WMF	7.21 KB	a11df18dd677816e9da3013503f12551640773c57f0aa00178ba61fb10c25565	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\EN00222_.WMF	12.50 KB	fcb398dffe8eabcba96da34334a4eaefaf7682a06cd26200092e153bbee88430	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\EN00242_.WMF	7.06 KB	6876a136ab3615a9b2a2c3d49d259bdf2b12a9c42e3d5dbc2b58d665e99de418	✗

File Name	File Size	SHA256	YARA Match
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\EN00319_.WMF	2.66 KB	a56a3d20e3d96bbb29faf088337420acbbedb5a35ac562659f1f6d9afcd4c578	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\EN00320_.WMF	1.15 KB	19ad8fd854ce97dc4c4bd8cd05b8f8e8d6348dd5872681c1066f3c1e93c5d0ac	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\EN00397_.WMF	17.34 KB	ba973cb6be2db8a1d8c22cfc0f1c76d37029a3509266de77c7e5ce177a0a1e9c	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\EN00902_.WMF	8.19 KB	59558a0272bfa1455edb3c3ad0ee653d9d29a6f98d31a1e04e90fffd746e876d	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\EXPLR_01.MID	10.75 KB	5855b05a83fd529c290ddf26f2b81df7e7e8aba2446abf056b4f96953a782d5b	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FALL_01.MID	5.17 KB	d7c017b6f8e5b66e0e181e37299a95575f01ea9ccd31a2daa142434f78b98b6a	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00074_.WMF	17.87 KB	8d6720176e8cb11e0667a0fc7ed4639bfe7b3dcd6b5bc2ab9fc6bf2bc75a72e1	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00076_.WMF	12.15 KB	6634b77df7f6914889594cbf28ff8488f6d962879c0c74325d5b14943154efe5	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00077_.WMF	29.97 KB	cd4a0f0ce6c887b78cc53f7faa27a413f1fa100169af6599aa59023af5bea240	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00086_.WMF	28.96 KB	4da7f3d59ece132851f9806bc16bcd6bfe27f1ac2ee31f05ab686b2c729c3abc	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00090_.WMF	14.30 KB	91cf4d1d62ed625e8ca030b14527d2dc201bcad5f9e62d3b1fffce7085df6c0b	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00096_.WMF	36.95 KB	a16217d0db885a72e27bb47e389279b755193083356c8a5711749a434b42b9e1	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00296_.WMF	15.92 KB	0805dc34bb1d6a82f4a9fd23a6b98804fdc893ec24ae1384124cce06c4d5dfb6	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00297_.WMF	18.20 KB	22b7c91079038029bec149a3e1173474633c5551b6b4973b085102d1f98a3bc2	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00336_.WMF	6.36 KB	11a3b4814a33a11f1d1824b1e618d91a248b526c9fe274cb369ace8c8a740a3a	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00306_.WMF	46.15 KB	6d0da61c5e7a65e6193a0515687333a206550d2587a055057876ef56de570cf2	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00361_.WMF	4.41 KB	2371795829af6f1170510937bf557a6e2c54ba8cc2defa3816eb6ceafa4d93ce	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00369_.WMF	8.79 KB	afef8851b47899e2965aafed2c9b16bee14126a484a63c6cee7ddc5b6f5abd43	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00382_.WMF	8.66 KB	e4a191014df435860f5246c222d7b45e412f4861b10c53772106c86d34e923aa	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00397_.WMF	11.00 KB	ccfa490621ca68b77be12632dce73df1251126da06eb898bb0609f5c6797edc1	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00403_.WMF	8.13 KB	9bc06ddda02417693123ca05a7011350015fc543e727a53bca3c14786ce51690	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00414_.WMF	11.18 KB	9334d099c0c41fd17330019e50e7ecc1f9483698f2247c66c20861be5633f762	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00419_.WMF	16.45 KB	1f46049b4d0ca9f905105c4c722e53229ee51c3dcf2da4e2e82e7caff30b42fa	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00428_.WMF	5.12 KB	e85504145750363 51fd1544dcb8afc1c46495637359e7ab7fc162378aa448624	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00435_.WMF	2.49 KB	705486f1960357cb51da27278fc8ac79df24c7e7d86f129c0674bd013ab93aa5	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00438_.WMF	5.41 KB	40e4ae2db0f24db1cca054a5cd6a8d5d5d42daf25f0aa4bf86ae0cdccc50b647	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00455_.WMF	9.15 KB	0bc8580bc75b7deb51b1bdc20d49acfee30451005ea022fdcac105f0c0c3af0a	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00459_.WMF	17.43 KB	5c0d9e5de8d377622edff8a45ee61b15179c55e9deba5e5d984fddc587f7db9a	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00543_.WMF	1.87 KB	1e92e8645dc9197b1b25edb7450eaf07c7b69b9318889c8ada09ef667f677840	✗

File Name	File Size	SHA256	YARA Match
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00544_.WMF	5.57 KB	452ee34abdb27d434c39bb0423b1a6733bc0e8ed4948afb57ad8d85e66c98cd6	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00564_.WMF	1.31 KB	b38256727edae2c96e4b7bc454aeb763994c33254871b3358ac68598b0057831	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00586_.WMF	1.17 KB	f654d9ae2bef79f9db15ec6670a9ac6dbb6a823a43426b0bd16c39716f2b7b1d	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00775_.WMF	11.33 KB	f233126b781dfbab258f7bf3b60334d45b7a07b55fdfbeb2d7d9d4a0a13de428	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00779_.WMF	9.23 KB	ccb5eee1eae2286dfa6be43fbcc4c719fda97dc1018e5b67b33cc1f60b922ec2	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00799_.WMF	14.08 KB	c5017318fb9d9ec2521f57f53730a515bd373923b401c8ab826b1c59663e6ba9	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00814_.WMF	42.14 KB	93d3f64ff10dcd37fd3a0f3f9b393fb7c277622bf1ed3b3642f7ced58260a928	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD00965_.WMF	15.24 KB	47ac74fec056955143e28816bed1c1b7efefb2c6c80dd4b56d9e745e6a8ea5b7	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD01074_.WMF	4.96 KB	cba24989485f279ea48d49960ba6fe0917ddb02f8f8a73074e98e8949872dde9	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD01084_.WMF	2.79 KB	ee6a83945eaac93b14df5c413df17d7e48623fe75b57e992e973b162597387ee	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD01176_.WMF	5.30 KB	178b7531e6ef234acbe58e4af1b22c213f3950ce9f2a9a711c83cf6535e77ad6	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD01191_.WMF	4.31 KB	ce76794b66e760daf7cecdfde8c81860a791c41f89bd2703591f0c9c6b84c413	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD01193_.WMF	1.57 KB	a8ba195f4c8de4a9e73da973ea20fdcbdf328ac420250ee37f3dfcdf28ce1488	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD01196_.WMF	2.71 KB	df37ed9c25f78d66476b27eff686ab0ea4c9b7599aaddf63a29fd0e84ca5d233	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD01548_.WMF	10.51 KB	505db7655be5ca42a1ec5fcc5f5d78da4c343638f52664824d7ede00159b2e10	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD01657_.WMF	30.14 KB	dd1306734356 23b64caed6d7f5ee0bc526a68b9c19f3a5f6680767d5ea0569e4	✗
C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\FD01658_.WMF	17.94 KB	29071c5b7c958a6242f2d7fca6adde3db9395f42dffc6a38bcd76d612d5f6e02	✗

Reduced dataset

Host Behavior

Type	Count
Module	80
System	4
Environment	5
-	11
File	50485
Mutex	1
-	33
Process	102
COM	8
Registry	5
-	1

Process #2: svchost.exe

ID	2
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 79745, Reason: RPC Server
Unmonitor End Time	End Time: 281000, Reason: Terminated by Timeout
Monitor duration	201.25s
Return Code	Unknown
PID	868
Parent PID	456
Bitness	64 Bit

Process #5: wmiprvse.exe

ID	5
File Name	c:\windows\syswow64\wbem\wmiprvse.exe
Command Line	C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 82692, Reason: RPC Server
Unmonitor End Time	End Time: 169111, Reason: Terminated
Monitor duration	86.42s
Return Code	0
PID	3772
Parent PID	584
Bitness	32 Bit

Process #6: vssvc.exe

ID	6
File Name	c:\windows\system32\vssvc.exe
Command Line	C:\Windows\system32\vssvc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 85257, Reason: RPC Server
Unmonitor End Time	End Time: 276939, Reason: Terminated
Monitor duration	191.68s
Return Code	0
PID	3804
Parent PID	456
Bitness	64 Bit

Host Behavior

Type	Count
System	3

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60	C:\Users\kEecfMwgj\Desktop\e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe	Sample File	3631.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
46eb1da33355ad44115624c5298022441ffc7817930dc7d1fbf475b258492f0c	C:\Users\kEecfMwgj\AppData\Local\Temp\ygMWDLG1.docxqiinU, C:\Users\kEecfMwgj\AppData\Local\Temp\ygMWDLG1.docx	Modified File	60.70 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
e0a105c8add41178eac0179ddfe8ab7f2961bd44902d0b1bc402e5cde87af2e4	C:\Users\kEecfMwgj\AppData\Roaming\I6oQCkIppOV.docxHxFKq, C:\Users\kEecfMwgj\AppData\Roaming\I6oQCkIppOV.docx	Modified File	49.42 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d5a0fae9bfd67b94ec200abc38e842bb3bfe9f30ae20303a64466f444c6c2e87	C:\Users\kEecfMwgj\Desktop\MUikt7-uQ.docx, C:\Users\kEecfMwgj\Desktop\MUikt7-uQ.docxoeWLy	Modified File	64.64 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
881d96f01c78f5cd967d611e86ca81ebbf01f45b94fe629a0d8c94a267f90a9c	C:\Users\kEecfMwgj\Documents\56ixAATbHJkDzbE.docx, C:\Users\kEecfMwgj\Documents\56ixAATbHJkDzbE.docxZMgAm	Modified File	88.17 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
11a05f9bf9955cea10757fc7a6fb04a0c623e6b24ce98b3288f4a22325b72909	C:\Users\kEecfMwgj\Documents\bspGlPMk4_an1.docx, C:\Users\kEecfMwgj\Documents\bspGlPMk4_an1.docxTSAyl	Modified File	78.56 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
c22b05262cc804ccf992c04620bc9a45f5d9c8456f050d87b8ffa9cba58514e6	C:\Users\kEecfMwgj\Documents\5Z2lDBjIfl7blTzL-.docxkjeVm, C:\Users\kEecfMwgj\Documents\5Z2lDBjIfl7blTzL-.docx	Modified File	71.72 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
ca0fcb722d9cb68a7cf40ce887e6cf9358e09b5035590b0d586229aecefe0475	C:\Users\kEecfMwgj\Documents\djjdzoNAgImR2tzKl.docx, C:\Users\kEecfMwgj\Documents\djjdzoNAgImR2tzKl.docxUQImp	Modified File	22.68 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
653da690f068e9db72540d5e9e609eceb6f50e814c0319cb4756f4f78d12c1c7	C:\Users\kEecfMwgj\Documents\8YVRCgZcMH3Llujoyf4g.docxiHpqT, C:\Users\kEecfMwgj\Documents\8YVRCgZcMH3Llujoyf4g.docx	Modified File	59.06 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
467554056480fa99fbbdfa98e31046d98da4e56fa8fa206ba603bb8249485b63	C:\Users\kEecfMwgj\Documents\DPUHbDi_baXkj\b90Z dF_C.docxNCFxW, C:\Users\kEecfMwgj\Documents\DPUHbDi_baXkj\b90Z dF_C.docx	Modified File	73.51 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d37561da95f0794265a871216afaf375e28f00c9df98ebaad303e82a44c11d90	C:\Users\kEecfMwgj\Documents\IpmQl9IE7gPmac-Inw.docxLzOqf, C:\Users\kEecfMwgj\Documents\IpmQl9IE7gPmac-Inw.docx	Modified File	66.53 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
dba304459651e3a306acf599be94c13ce7296ae8c1b96138152ed25d569cd959	C:\Users\kEecfMwgj\Documents\xLwfroEb7Mm.docxfdtZP, C:\Users\kEecfMwgj\Documents\xLwfroEb7Mm.docx	Modified File	84.74 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b4c49d77bd118755f5325a12c3d895da9becbcdd543c8866bb9affe2606486be	C:\Boot\BOOTSTAT.DAT, C:\Boot\BOOTSTAT.DATVVvcj	Modified File	64.38 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
aed340981c65c2ebe0d63a294537c0dacc49521ffbc43ab6f8199f5c3e5c16d9	C:\Program Files\Common Files\hD5gp40XNzXS9cEg h.gif, C:\Program Files\Common Files\hD5gp40XNzXS9cEg h.gifyGNgu	Modified File	36.97 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
bad6ae663875bb18dbdbc5b099306b6f220831922303939d46806b2696fabae8	C:\Program Files\Common Files\lhz5WseZSjkSxbd.gif, C:\Program Files\Common Files\lhz5WseZSjkSxbd.gifOIRmX	Modified File	10.31 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
59a77baaa208242b04f743dcc6d2c206af38e9335aa37b518b1bde24e9e77744	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\C2RHeartbeatConfig.xmlnzSrN, C:\Program Files\Common Files\Microsoft Shared\ClickToRun\C2RHeartbeatConfig.xml	Modified File	4.48 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
32ba7270296e16e61e0492e46561aa92386769a883e8b7b61ac3e830c9177cd8	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\i640.hasheopdz, C:\Program Files\Common Files\Microsoft Shared\ClickToRun\i640.hash	Modified File	541 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
6903befb8d6ae785afe3f67f3a80f7be8cdfc5e2ff68e07d586d32c68083b4a1	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\i641033.hash, C:\Program Files\Common Files\Microsoft Shared\ClickToRun\i641033.hashRvMtx	Modified File	544 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
6d448ef5f360f048fdf30f274d859a1992a0260a3b3a1234860219fb71ee2d2f	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeUpdateSchedule.xml, C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeUpdateSchedule.xmlTfqYQ	Modified File	5.11 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
dee2a25e4e5d12b9be3e99115430a3eb9aea0e0c8daf1743286c46f2004ede59	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\ServiceWatcherSchedule.xml, C:\Program Files\Common Files\Microsoft Shared\ClickToRun\ServiceWatcherSchedule.xmlpjxCW	Modified File	4.79 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
ffa4169dbf07971ddb5b5499343253251833ece734ccf5e85c876434ffe0b348	C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPC.DLLpJmKW, C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPC.DLL	Modified File	200.04 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
4ae9f77e6615778ee2101ad27438bec1ab311b32fde339a333fc7e053bb5663d	C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPCEXT.DLL, C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPCEXT.DLLGrjpa	Modified File	1791.04 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
e370082f83f6c7bf47b4274ae062f9ad64ea2669b4825c2bb437184aeeb20319	C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\osppobjs-spp-plugin-manifest-signed.xrm-ms, C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\osppobjs-spp-plugin-manifest-signed.xrm-msdjJGk	Modified File	9.66 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
205478ba9bde5d1ccee0da3bfcd9d3527ebf180dd857fa8a3168570bcaa7d012	C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPOBJS.DLL, C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPOBJS.DLLDQzOW	Modified File	2178.54 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
bce7204e9a0db9e919994a7b0557ef65c9fd34b566947df750b0afb979aed595	C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXEsxXRw, C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE	Modified File	5013.04 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
e37e8acb042fb39ef6aaaf87343450467723a64581c8bdc96f845fd89e453489	C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPWMI.DLL, C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPWMI.DLLDsFyL	Modified File	144.04 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
13b4d471d65c6027758bf2e554bcf1e32a7d132f4cc195eae3ed95d033046d2d	C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPWMI.MOFcXSsm, C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPWMI.MOF	Modified File	47.40 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
122df3d628042b3cc40d51abadb4c913d0b2de373bafa0f5ad3b9cd6283e2861	C:\Program Files\Common Files\Microsoft Shared\Stationery\Desktop.ini, C:\Program Files\Common Files\Microsoft Shared\Stationery\Desktop.inicAbSU	Modified File	1.06 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
afe6ce6c17e47111798e72e783fd0319c2447d4aec829457cd870fdbe8c31d9b	C:\Program Files\Common Files\ybi.jpg, C:\Program Files\Common Files\ybi.jpgabYwy	Modified File	71.10 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
f856a4ef6be364d3785a311a1c4aec74f15acab9572caadec790feaa1dbdcde5	C:\Program Files\Internet Explorer\SIGNUP\install.ins	Modified File	885 bytes	application/octet-stream	Write, Access, Read	CLEAN
0ac121c7c91e77c53451c82baa8995c844c0704d7ddecb845401efef40119466	C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList\FrameworkList.xml	Modified File	7.41 KB	application/octet-stream	Write, Access, Read	CLEAN
5f98e83b28b88053f18693f048cad7b06f5a2d4be22de825ae7150d0c25bb0a1	C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\WinFXList.xml	Modified File	2.96 KB	application/octet-stream	Write, Access, Read	CLEAN
dedef2566f13fa52db5ae53a045a2f6a8b66de7c2856a614e2f4200126c0782e	C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.Targets	Modified File	5.06 KB	application/octet-stream	Write, Access, Read	CLEAN
b950e3aeb168cb0101ef6436079fc22a956f944593ee96af66feba72056c4137	C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0\Workflow.VisualBasic.Targets	Modified File	5.52 KB	application/octet-stream	Write, Access, Read	CLEAN
9c991dafa0b62d46275dfbd2ac43fb0980dfe1573a3ffc4243178100c92ab6fd	C:\Program Files\Windows Sidebar\settings.ini	Modified File	497 bytes	application/octet-stream	Write, Access, Read	CLEAN
892d28fd4952ec685398ec9a120145d878144f4dbc132e9fdc4d3f09afd406cc	C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\PSGet.Resource.psd1	Modified File	74.04 KB	application/octet-stream	Write, Access, Read	CLEAN
f5a2bfd719e2aed22eee9e217c6b9c9b81b14ca4308ae798e8de4cd9aa9a0b89	C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.format.ps1xml	Modified File	16.55 KB	application/octet-stream	Write, Access, Read	CLEAN
7512943ecbaf18d26b367fd5864e4338509ac90adf61d24e541e63b6db9d8aad	C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Modified File	2.70 KB	application/octet-stream	Write, Access, Read	CLEAN
38529cf3947fe746fce3376e50fa387f59110d1b86e9100b0ca671437e8643af	C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageProviderFunctions.psm1	Modified File	10.86 KB	application/octet-stream	Write, Access, Read	CLEAN
4f37704f87a56cfd4c4b1cd218d21fdb968556627bc67692e57e2d72fbd6c4cd	C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Modified File	4.66 KB	application/octet-stream	Write, Access, Read	CLEAN
52a77bc1d382e98b03dad19f5246c35d4fb4f9e4da6806ef5448ad8948ca6b3f	C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Format.ps1xml	Modified File	8.50 KB	application/octet-stream	Write, Access, Read	CLEAN
b8f95630083a1df0bd099739a8910443dbe59909441e7b02ce8ca459cf0e5f45	C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Resource.psd1	Modified File	77.71 KB	application/octet-stream	Write, Access, Read	CLEAN
cebba80f628cf3705780eee975c5b1c722844860d4927f2932bf31210b252ffb	C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	Modified File	563.10 KB	application/octet-stream	Write, Access, Read	CLEAN
76c8115c3c42116d796faeeff09694d355a41154a3d2109d31ac436e238dd8ba	C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB	Modified File	16.03 KB	application/octet-stream	Write, Access, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9c5c967d97c41755a117276ea251309fdc712609102f45597f53dcc07af3cf00	C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE	Modified File	317.14 KB	application/octet-stream	Write, Access, Read	CLEAN
99514c172acd0e0fd739c42092156f3649861dad8c1253bb47417cc0bcc09a9b	C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\pkeyconfig-office.xrm-ms	Modified File	577.15 KB	application/octet-stream	Write, Access, Read	CLEAN
a2e9a46770e9ad8339d208ab6f2ab42cf5176bb183bcc276f3a3b446ced9eb52	C:\Program Files (x86)\Common Files\microsoft shared\OfficeSoftwareProtectionPlatform\OSPPC.DLL	Modified File	176.04 KB	application/octet-stream	Write, Access, Read	CLEAN
17543e6c42c3b80e01a0c6639702f3dd333c8639bb13917756330efbf49564ed	C:\Program Files (x86)\Common Files\microsoft shared\OfficeSoftwareProtectionPlatform\OSPPCEXT.DLL	Modified File	1615.04 KB	application/octet-stream	Write, Access, Read	CLEAN
81e76de00bfb633e26ac4ddcecbfa24fc32e95f696a91e845ed6c55774bc61a8	C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE	Modified File	200.01 KB	application/octet-stream	Write, Access, Read	CLEAN
c0b03e87c1696458203e0aa210491c784effd9f074fc784070eada6175f9b0c2	C:\Program Files (x86)\Common Files\microsoft shared\Stationery\Desktop.ini	Modified File	1.07 KB	application/octet-stream	Write, Access, Read	CLEAN
67077e3ee4f38e5a05701bd15bdbbb78890c09626e12033f9f39645337fef72d	C:\Program Files (x86)\Common Files\microsoft shared\VSTA\AppInfoDocument\AddIns.store	Modified File	9.88 KB	application/octet-stream	Write, Access, Read	CLEAN
5ebe66c67f1bcdb9f53f235c9521e193e628d2def355e2c0ed4027b13a4887e4	C:\Program Files (x86)\Common Files\microsoft shared\VSTA\Pipeline.v10.0\PipelineSegments.store	Modified File	127.89 KB	application/octet-stream	Write, Access, Read	CLEAN
57464ca7ff0ca22b2892fd779ecc9abd661d98b9504d49f60d64f83918c9c9e0	C:\Program Files (x86)\Common Files\microsoft shared\VSTA\VSTOFiles.cat	Modified File	89.38 KB	application/octet-stream	Write, Access, Read	CLEAN
38ff5ff11cd8d7b6d36ffb61cabddae92f6d331d5dbdf27c3fc8f2138fe3b8c5	C:\Program Files (x86)\Common Files\microsoft shared\VSTO\ActionsPane3.xsd	Modified File	581 bytes	application/octet-stream	Write, Access, Read	CLEAN
b6d4b66471e2d3888695e05daea6a93877e3821496ffd4d30476f1b739727ef7	C:\Program Files (x86)\Microsoft Office\AppXManifest.xml	Modified File	4818.43 KB	application/octet-stream	Write, Access, Read	CLEAN
b137f645ad30abc3c109a8db012b379091f1bf836cb57efa5503b1baae2188ef	C:\Program Files (x86)\Microsoft Office\FileSystemMetadata.xml	Modified File	715 bytes	application/octet-stream	Write, Access, Read	CLEAN
7d5d3877cd17b67446dfebc558185ebdb8c27bf2963d0ed4aac18ce1d91d24a5	C:\Program Files (x86)\Microsoft Office\Office16\OSPP.HTM	Modified File	170.86 KB	application/octet-stream	Write, Access, Read	CLEAN
0c70ca53ea72d5b004035d34905fcbe356e85964d1134c3071148b22678bc388	C:\Program Files (x86)\Internet Explorer\SIGNUP\install.ins	Modified File	891 bytes	application/octet-stream	Write, Access, Read	CLEAN
0288baf948b46fd067245c3e1a1a2774fd423380b5459c1189f5442fbdbce81b	C:\Program Files (x86)\Microsoft Office\Office16\OSPP.VBS	Modified File	92.67 KB	application/octet-stream	Write, Access, Read	CLEAN
41f63301179efe85fb593f73d41029fbdfd3fb258075f5ed81dd2367361505c3	C:\Program Files (x86)\Microsoft Office\Office16\OSPPREARM.EXE	Modified File	22.99 KB	application/octet-stream	Write, Access, Read	CLEAN
7b5aac48f164d60fcd90a3f6910e8e99eab0b0b41663af6d201dfbb20ba9e3d1	C:\Program Files (x86)\Microsoft Office\Office16\SLERROR.XML	Modified File	35.91 KB	application/octet-stream	Write, Access, Read	CLEAN
dc7c673e7ad71806bcb62608a71e43d0d4e715dd25bfea7657158c4102a81e30	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0000-0000-0000000FF1CE.xml	Modified File	315.04 KB	application/octet-stream	Write, Access, Read	CLEAN
bac6c39a26961946618b41cacfa726fefb24ce3532041f394809ea42db182ad1	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0015-0409-0000-0000000FF1CE.xml	Modified File	1.97 KB	application/octet-stream	Write, Access, Read	CLEAN
c95069aa2405732574e1b904778e5137b68cc123daefc9c67787a896f4a2efb6	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0000-0000-0000000FF1CE.xml	Modified File	758.36 KB	application/octet-stream	Write, Access, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
cf43bdea8e5126c86bf6a59d00818ddeb3ae5b87aafbfe1885c0982a4ceb3da8	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0016-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
3028c331f9aa4d71f9a4f6c903563eb30443fa5a01739c1612e1613ec86e40d2	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0000-0000000FF1CE.xml	Modified File	453.58 KB	application/octet-stream	Write, Access, Read	CLEAN
0d078d244e992e0bf4431bb8651f087488a47462ded7bbe0ca588ef592e3f0f0	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0018-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
59f2b55a1661c94f26055e5e0c83f8343201e0b85e0fa34ec137ee8f4f884057	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0000-0000000FF1CE.xml	Modified File	248.24 KB	application/octet-stream	Write, Access, Read	CLEAN
54244b8d642aba646c0de1f1d3631b9e72c47d52e50f280bea8f4f56bb8d832d	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0019-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
0ed9707192acb00b82e72a6e76907391dac5b962314864f46287e204b772e87b	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0000-0000-0000000FF1CE.xml	Modified File	1099.05 KB	application/octet-stream	Write, Access, Read	CLEAN
d0c8fdedceb4371e5bde7421d7fd6cb5d2b17c72d19512bd5619dbd6f57d9c93	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001A-0409-0000-0000000FF1CE.xml	Modified File	19.47 KB	application/octet-stream	Write, Access, Read	CLEAN
5ae44937620891015683bea77c230db2c672170f04cad460f490a3abcb5e9120	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0000-0000-0000000FF1CE.xml	Modified File	721.06 KB	application/octet-stream	Write, Access, Read	CLEAN
2f17bbc00ce04a638613355bcfe3bfbe8f36240a08b1e7775115781cd9aa1faf	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001B-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
e7f1e33612a9ba6a0d8776a6743f64025f255cba80497891d38bd352d3ecf121	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
e8325394493a8b2b4f21ed54e914899d8f9fb41895cf68b1133c3a578de40fca	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-040C-0000-0000000FF1CE.xml	Modified File	2.57 KB	application/octet-stream	Write, Access, Read	CLEAN
affdceb226159cb8189df7b452b670fe28c4864ba7056ea4bc19ddc1f5993c07	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-001F-0C0A-0000-0000000FF1CE.xml	Modified File	2.57 KB	application/octet-stream	Write, Access, Read	CLEAN
7ead1eab29a69c2618baee68257b685b98656af0f66fcaac58a4d16e4d716810	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0000-1000-0000000FF1CE.xml	Modified File	34.35 KB	application/octet-stream	Write, Access, Read	CLEAN
3a2237d705d4d55c805f7fa6a251bd8a5739b3e94c56f644843f27f57495b694	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002A-0409-1000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
7768b1258767c955f2571ae04879488fb7ed56bbc4d586912b0c4315da4c9a4c	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-002C-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7487c68e03c189a085733fe891bbd09b87b2492124663cd33a904b0042bc7b4b	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-006E-0409-0000-0000000FF1CE.xml	Modified File	14.69 KB	application/octet-stream	Write, Access, Read	CLEAN
51efbe8209b59362b9360192217067d8d5dd7cc0c936015b9e955445122e1f65	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0000-0000-0000000FF1CE.xml	Modified File	349.41 KB	application/octet-stream	Write, Access, Read	CLEAN
2e1c2207d5b019418fb182e0e07538e249138d97526720ce94c56d1d52789b05	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0090-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
20c52f98a01a73cbae68f84e550849b7a7c9a6e66e9d46153dca40f8516f93b2	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0000-0000-0000000FF1CE.xml	Modified File	55.13 KB	application/octet-stream	Write, Access, Read	CLEAN
b64ec1bb91333fbd28469646b382c4b3c29c0d8c47e2b02708e1df471d89079d	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00A1-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
2ce6a5ac2cef60544990fc0d047611a9f7816e36b4a2cd4ddc08de8da7f821cc	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0000-0000-0000000FF1CE.xml	Modified File	9.47 KB	application/octet-stream	Write, Access, Read	CLEAN
76a0aef65a0a294d040eac63519d54e8112e05a50fd302687ff69a4c9aae0f8e	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00BA-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
cc3ce58e1fc1d546d7702548cc7d2ae92673554916fa3a23d6ab5949ddcf7c9a	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0000-0000-0000000FF1CE.xml	Modified File	1.89 KB	application/octet-stream	Write, Access, Read	CLEAN
0f46a98cfd954c6e79c16aeebdef6ec4b066522b1a422eb63bc4f4c2fdce8a47	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E1-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
7eba688c98be5b5e16efd75185d8619f2db3af4704226a95bae00b4796fa4bfe	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0000-0000-0000000FF1CE.xml	Modified File	4.14 KB	application/octet-stream	Write, Access, Read	CLEAN
cc84b3bd03168b28e14fbd89ababae37d4c8801b7dc66ee23a474b8d48305c1d	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-00E2-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
aabbc8813158a35a62731613e737865bdbe45a210ac1ccbb1afe821e9eda8532	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0115-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
e662fcff88d03770949001817 6c5ebec17281df795f95487e25d3b7ce2f6681d	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0116-0409-1000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
a701aceeedec643880db683265ac4cdb738e440f0336223c4d0ddcd23ccef6fb	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-0117-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
5b88b6661498a6a06e84338145ecdd8a2c983344af0f91a624fd3ad7aba2edc3	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012A-0000-0000-0000000FF1CE.xml	Modified File	516.75 KB	application/octet-stream	Write, Access, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7e658ff129afed23bd352549f113f36ee751aae60653e2462692ae2ead2d38fb	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-012B-0409-0000-0000000FF1CE.xml	Modified File	1.70 KB	application/octet-stream	Write, Access, Read	CLEAN
0907fa1e0e8b1c4d74e2de91559de1a0dc4fd2f84a611002ce7442add72009b0	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.90160000-3101-0000-0000-0000000FF1CE.xml	Modified File	3.77 KB	application/octet-stream	Write, Access, Read	CLEAN
85ec054b43b71c5bf8e45e65a71805631d489efee4bcd2e5049a260aa1900d4a	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifest.common.xml	Modified File	1951.43 KB	application/octet-stream	Write, Access, Read	CLEAN
bcb64073f1798cea926d21515c1dc2623085015ca101fe8368f12f952b8da99f	C:\Program Files (x86)\Microsoft Office\PackageManifests\AppXManifestLoc.en-us.xml	Modified File	10.04 KB	application/octet-stream	Write, Access, Read	CLEAN
ae2b0e0318088e148dac42faf3e100ed2479286be25d2422e6e81c6acbc78913	C:\Program Files (x86)\Microsoft Office\PackageManifests\AuthoredExtensions.xml	Modified File	824 bytes	application/octet-stream	Write, Access, Read	CLEAN
8a8689c47602d96fc26791a1f0a23f2b1570b3d9f9893424735e7f2cf09d7775	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00004_.GIF	Modified File	9.25 KB	application/octet-stream	Access, Read	CLEAN
68e127741ba5768714a175c6085e4446a2cd0be65b67e423ac08d853ad4d5ec3	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00011_.GIF	Modified File	7.48 KB	application/octet-stream	Write, Access, Read	CLEAN
ce2e3dda3ef6a7de74076ae6402ee0e469341ee9d48c26c8e803ace3356a4190	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00021_.GIF	Modified File	14.96 KB	application/octet-stream	Write, Access, Read	CLEAN
4ea349972fc226ef27b1f6ef225dd61e26f7a185c86c0ddc6ca8b2c2c5a7985a	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00037_.GIF	Modified File	6.96 KB	application/octet-stream	Write, Access, Read	CLEAN
1df002e1f86f701984c75e88964927da2afc0654f2f9f3788ad383721cf7d23f	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00038_.GIF	Modified File	3.61 KB	application/octet-stream	Write, Access, Read	CLEAN
63ae0e5ae3c8b18d8f115496a4399e0c922e248b31c03dc8b991ab99cb423b6c	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00040_.GIF	Modified File	8.34 KB	application/octet-stream	Access, Read	CLEAN
345c02aa27b18ccddda54ea92bf47d59fe89254e60a21885575d824e6329c125	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00057_.GIF	Modified File	12.05 KB	application/octet-stream	Access	CLEAN
15907c322df6416e84ba1494a6f9ea962ef0a772b63dbe2de0d0903b2c4b3f76	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00052_.GIF	Modified File	7.94 KB	application/octet-stream	Write, Access, Read	CLEAN
fc09801581a2789471dbadf3a8600202581e4e71359ccd4d430d911cb9236a32	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00090_.GIF	Modified File	963 bytes	application/octet-stream	Write, Access, Read	CLEAN
50d74f10be4b68d88a7cd4ad568083dfeee74428d4d99c44858cb2154d8801d4	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00103_.GIF	Modified File	12.84 KB	application/octet-stream	Write, Access, Read	CLEAN
09fc5736f7de76bf23e80385206d61df784dfa88f7299c66c33f198a3c824f6c	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00092_.GIF	Modified File	948 bytes	application/octet-stream	Access	CLEAN
3d6062fee18df5bd0f9a99fb7331ee7803c23ae019953e133a2be32b5917c638	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00120_.GIF	Modified File	3.84 KB	application/octet-stream	Access, Read	CLEAN
5c50e38c46ab0463fe59ac6c5b742f949f8bfe5d087102eeaf24e5c210630731	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00126_.GIF	Modified File	3.50 KB	application/octet-stream	Write, Access, Read	CLEAN
611460bce42788017a3534632c62967db098362e1fd55b0b1bd2f42955fa82f0	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00129_.GIF	Modified File	12.62 KB	application/octet-stream	Access, Read	CLEAN
8d22e6a2576336cd749f4c87ad08db2c511f6a30b398e99a52bd7498646de341	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00130_.GIF	Modified File	5.57 KB	application/octet-stream	Write, Access, Read	CLEAN
4ca5cd17290a25df0364d76364bd3892a1eb01d85ece7ee0eec63bee18dab1e1	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00135_.GIF	Modified File	2.97 KB	application/octet-stream	Write, Access, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
54c1edc0cda20ad061c1376999d92de4fbd306867eca9b04e84803014cb74658	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00139_.GIF	Modified File	10.79 KB	application/octet-stream	Access	CLEAN
0b9ded204819ee2195bc4719eea7efc62d2499edebf960feac02f32c7e1770d9	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00142_.GIF	Modified File	15.38 KB	application/octet-stream	Access	CLEAN
aad8b381de94545a1c458430d6fbcfaac517096acc2bc492ee4ebc35ff1ca30b	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00154_.GIF	Modified File	5.63 KB	application/octet-stream	Write, Access, Read	CLEAN
070068e74a9191225e787413e3f5d6f259c4ece5ecf54f25ab829bcacfb3e570	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00157_.GIF	Modified File	5.27 KB	application/octet-stream	Write, Access, Read	CLEAN
de9c32ee57560e69cf92e617e5f189e7bb2a201ec32b68e43be30e06c70871f1	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00158_.GIF	Modified File	5.35 KB	application/octet-stream	Write, Access, Read	CLEAN
e427cff0990ef12b197a1bb1708f4cbc795a80114ef4a8e1b65e720a0a0140f1	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00160_.GIF	Modified File	1.55 KB	application/octet-stream	Access	CLEAN
8d792add615b64bf688bf089c1f516221c5be64a6050de0b511fa450b8b3ee86	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00161_.GIF	Modified File	7.84 KB	application/octet-stream	Write, Access, Read	CLEAN
666a88751359c0a7e86f4c35ee2b56544a3b7a24c289c24e9f0d047e0e84527b	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00163_.GIF	Modified File	7.26 KB	application/octet-stream	Access	CLEAN
0c1091025caf023622233928e20e00e583722a4a293c37bcf6287e9b70f483bb	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00164_.GIF	Modified File	13.38 KB	application/octet-stream	Write, Access, Read	CLEAN
a18dceb1610280c970143c7089ee592ef61bc22bed2cd484c176164eb370e569	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00165_.GIF	Modified File	8.82 KB	application/octet-stream	Write, Access, Read	CLEAN
d8c9124aa1e74f4db748ced97938fa0cf359ded24328af4d867c1b8521b37433	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00169_.GIF	Modified File	5.68 KB	application/octet-stream	Write, Access, Read	CLEAN
f1e49cb19f0b80b30005c0e08ca913df8163982ca9d5c6153a1b5c5c7ac093f9	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00167_.GIF	Modified File	5.21 KB	application/octet-stream	Write, Access, Read	CLEAN
a575c001e30010a7d1d528c97388d1f055f7c8fe4253cc715c09b51f0d9a6b49	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00171_.GIF	Modified File	5.33 KB	application/octet-stream	Write, Access, Read	CLEAN
21cc09fedf4f78b1d20386ce6360d29a5ba2b61f8e8ddbe215f8d6c1c341aee1	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00170_.GIF	Modified File	9.47 KB	application/octet-stream	Write, Access, Read	CLEAN
4bd7d72262756070d9378f5bb9964db781c82628d1b8d9a9e82b6c7f82319e42	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00172_.GIF	Modified File	4.72 KB	application/octet-stream	Write, Access, Read	CLEAN
2bbf2fbebaaacde1f3a11298bcabd6330d6cb35b964d9be2ee3bb61c7bcb0052	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00174_.GIF	Modified File	4.31 KB	application/octet-stream	Access, Read	CLEAN
2d47a6267c35f9ea49475b4b8ad5af55b5cbfdb9fb38a2c1a4815f8f82c0e595	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00175_.GIF	Modified File	3.73 KB	application/octet-stream	Access, Read	CLEAN
610c623d1436c46a58caa6456b94999416b5f4778f5580ac3614e34dbafb9193	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AG00176_.GIF	Modified File	3.48 KB	application/octet-stream	Write, Access, Read	CLEAN
7885962a1aa05659e562c4501c5725eb5a5a43972865e199328ca06dc6541b4a	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00010_.WMF	Modified File	3.39 KB	application/octet-stream	Write, Access, Read	CLEAN
d970607e325d3a2bb7b324344072ae42ad8417982d73093203b66468d0118a06	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00015_.WMF	Modified File	5.06 KB	application/octet-stream	Write, Access, Read	CLEAN
fa1380b216bb2d78e4ca837d5ffbea0c5c53bce1fefbc85bd35c882cb267a505	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00790_.WMF	Modified File	5.99 KB	application/octet-stream	Write, Access, Read	CLEAN
30ecc2fdf4fd2d08f685d22ac8eb0697e2befda621b9740c9e2feb64250be633	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00853_.WMF	Modified File	20.53 KB	application/octet-stream	Write, Access, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a477a838d361b4e07de124e1115f96ae892032d390ddc6a46a51e8777e059fa5	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00914_.WMF	Modified File	11.01 KB	application/octet-stream	Write, Access, Read	CLEAN
7f4de62c59fe1307e90b631ffe2ba529f6f941fd7e5243b7a83d0d5467790310	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00932_.WMF	Modified File	14.53 KB	application/octet-stream	Write, Access, Read	CLEAN
5b88016ee8d7808ab141d04d6b6981e9d6599de1247515648f347c16fe9dfa32	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN00965_.WMF	Modified File	7.34 KB	application/octet-stream	Write, Access, Read	CLEAN
1a50d37e8023ef62a85e7094b780c2a9f377659abd706ca9d1eb140dc5de41e3	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01039_.WMF	Modified File	3.70 KB	application/octet-stream	Write, Access, Read	CLEAN
880bed632ca3427647054a77fbfa17db3fe552c6ec0254d29879ae98eccef0e8	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01044_.WMF	Modified File	1.99 KB	application/octet-stream	Write, Access, Read	CLEAN
01a984473a7a48f68d1b467bb2a4d16482b28f604733801f06231809e31d587b	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01060_.WMF	Modified File	8.22 KB	application/octet-stream	Access, Read	CLEAN
88d5b8d64b720445372004f7e1b8ad3382b41ade93b6be0ec0b2524c09d77d8c	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01084_.WMF	Modified File	2.22 KB	application/octet-stream	Write, Access, Read	CLEAN
84e51843d36c03fbb519287a1162fbc9dc587ab71d50df9377c0829ae8420c98	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01173_.WMF	Modified File	26.15 KB	application/octet-stream	Access, Read	CLEAN
3d6275142a25a9d8bf3c9b648676a9e1090cb38d68a1d77b59835d687375b192	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01184_.WMF	Modified File	4.09 KB	application/octet-stream	Access, Read	CLEAN
b7a22d06e1cb10253d7b8019911367154fc029f1a8841ea1eaac8d15548b36d0	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01174_.WMF	Modified File	27.64 KB	application/octet-stream	Access, Read	CLEAN
d8bf8a8c8b1a715ad34a19f45b7f775f61b3ff444d42911729299fb3593d8ce5	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01216_.WMF	Modified File	6.13 KB	application/octet-stream	Write, Access, Read	CLEAN
05922b719c18bc87d49a8ba2f592dbf25b1039f737d0a7d9b2eb534fa8b3e69f	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01218_.WMF	Modified File	3.38 KB	application/octet-stream	Write, Access, Read	CLEAN
dcb3013cfc3e93dd58b1a084caad58bf6244be433b329130fc530a96f68629de	C:\Program Files (x86)\Microsoft Office\root\CLIPART\PUB60COR\AN01545_.WMF	Modified File	7.63 KB	application/octet-stream	Write, Access, Read	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
C:\	Accessed File	Access	CLEAN
C:\$Recycle.Bin	Accessed File	Access	CLEAN
C:\$Recycle.Bin\S-1-5-21-4219442223-4223814209-3835049652-1000	Accessed File	Access	CLEAN
C:\Boot	Accessed File	Access	CLEAN
C:\Boot\cs-CZ	Accessed File	Access	CLEAN
C:\Boot\da-DK	Accessed File	Access	CLEAN
C:\Boot\de-DE	Accessed File	Access	CLEAN
C:\Boot\el-GR	Accessed File	Access	CLEAN
C:\Boot\en-US	Accessed File	Access	CLEAN
C:\Boot\es-ES	Accessed File	Access	CLEAN
C:\Boot\fi-FI	Accessed File	Access	CLEAN
C:\Boot\Fonts	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Boot\fr-FR	Accessed File	Access	CLEAN
C:\Boot\hu-HU	Accessed File	Access	CLEAN
C:\Boot\it-IT	Accessed File	Access	CLEAN
C:\Boot\ja-JP	Accessed File	Access	CLEAN
C:\Boot\ko-KR	Accessed File	Access	CLEAN
C:\Boot\nb-NO	Accessed File	Access	CLEAN
C:\Boot\nl-NL	Accessed File	Access	CLEAN
C:\Boot\pl-PL	Accessed File	Access	CLEAN
C:\Boot\pt-BR	Accessed File	Access	CLEAN
C:\Boot\pt-PT	Accessed File	Access	CLEAN
C:\Boot\ru-RU	Accessed File	Access	CLEAN
C:\Boot\sv-SE	Accessed File	Access	CLEAN
C:\Boot\tr-TR	Accessed File	Access	CLEAN
C:\Boot\zh-CN	Accessed File	Access	CLEAN
C:\Boot\zh-HK	Accessed File	Access	CLEAN
C:\Boot\zh-TW	Accessed File	Access	CLEAN
C:\PerfLogs	Accessed File	Access	CLEAN
C:\PerfLogs\Admin	Accessed File	Access	CLEAN
C:\Program Files	Accessed File	Access	CLEAN
C:\Program Files\Common Files	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ClickToRun	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\ar-SA	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\bg-BG	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\cs-CZ	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\da-DK	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\de-DE	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\el-GR	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\en-US	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\es-ES	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\et-EE	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\fi-FI	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\fr-FR	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\fsdefinitions	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Ink\fsdefinitions\auxpad	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\keypad	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\main	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\numbers	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskmenu	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\osknumpad	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\oskpred	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\symbols	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\fsdefinitions\web	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\he-IL	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\hr-HR	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\hu-HU	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\HWRCustomization	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\it-IT	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\ja-JP	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\ko-KR	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\lt-LT	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\lv-LV	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\nb-NO	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\nl-NL	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\pl-PL	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\pt-BR	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\pt-PT	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\ro-RO	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\ru-RU	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\sk-SK	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\sl-SI	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\sr-Latn-CS	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\sv-SE	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\th-TH	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\tr-TR	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\uk-UA	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\zh-CN	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\ink\zh-TW	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\MSInfo	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\Common Files\Microsoft Shared\MSInfo\en-US	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Stationery	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\TextConv	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\TextConv\en-US	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Triedit	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\Triedit\en-US	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\VC	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Microsoft Shared\VGX	Accessed File	Access	CLEAN
C:\Program Files\Common Files\Services	Accessed File	Access	CLEAN
C:\Program Files\Common Files\SpeechEngines	Accessed File	Access	CLEAN
C:\Program Files\Common Files\SpeechEngines\Microsoft	Accessed File	Access	CLEAN
C:\Program Files\Common Files\SpeechEngines\Microsoft\TTS20	Accessed File	Access	CLEAN
C:\Program Files\Common Files\SpeechEngines\Microsoft\TTS20\en-US	Accessed File	Access	CLEAN
C:\Program Files\Common Files\SpeechEngines\Microsoft\TTS20\en-US\enu-dsk	Accessed File	Access	CLEAN
C:\Program Files\Common Files\System	Accessed File	Access	CLEAN
C:\Program Files\Common Files\System\ado	Accessed File	Access	CLEAN
C:\Program Files\Common Files\System\ado\en-US	Accessed File	Access	CLEAN
C:\Program Files\Common Files\System\en-US	Accessed File	Access	CLEAN
C:\Program Files\Common Files\System\msadc	Accessed File	Access	CLEAN
C:\Program Files\Common Files\System\msadc\en-US	Accessed File	Access	CLEAN
C:\Program Files\Common Files\System\Ole DB	Accessed File	Access	CLEAN
C:\Program Files\Common Files\System\Ole DB\en-US	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\en-US	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\BabyBoy	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\BabyGirl	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\FlipPage	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\Full	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\HueCycle	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\LayeredTitles	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\Memories	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\OldAge	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\DVD Maker\Shared\DvdStyles\Performance	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\Pets	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\Push	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\Rectangles	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\ResizingPanels	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\Shatter	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\SpecialOccasion	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\Sports	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\Stacking	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\Travel	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\VideoWall	Accessed File	Access	CLEAN
C:\Program Files\DVD Maker\Shared\DvdStyles\Vignette	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer\en-US	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer\SIGNUP	Accessed File	Access	CLEAN
C:\Program Files\Microsoft Office 15	Accessed File	Access	CLEAN
C:\Program Files\Microsoft Office 15\ClientX64	Accessed File	Access	CLEAN
C:\Program Files\MSBuild	Accessed File	Access	CLEAN
C:\Program Files\MSBuild\Microsoft	Accessed File	Access	CLEAN
C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation	Accessed File	Access	CLEAN
C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.0	Accessed File	Access	CLEAN
C:\Program Files\MSBuild\Microsoft\Windows Workflow Foundation\v3.5	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\Microsoft	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\Microsoft\Framework	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\RedistList	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.5	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.5\RedistList	Accessed File	Access	CLEAN
C:\Program Files\Uninstall Information	Accessed File	Access	CLEAN
C:\Program Files\Windows Defender	Accessed File	Access	CLEAN
C:\Program Files\Windows Defender\en-US	Accessed File	Access	CLEAN
C:\Program Files\Windows Journal	Accessed File	Access	CLEAN

Reduced dataset

Mutex

Name	Operations	Parent Process Name	Verdict
Global\EKANS	access	e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	access, read	e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	access, read	e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe	CLEAN

Process

Process Name	Commandline	Verdict
e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe	"C:\Users\kEecfMwgj\Desktop\e5262db186c97bbe533f0a674b08ecdafa3798ea7bc17c705df526419c168b60.exe"	MALICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
wmiprvse.exe	C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding	CLEAN
vssvc.exe	C:\Windows\system32\vssvc.exe	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.4.1
Dynamic Engine Version	4.4.1 / 01/14/2022 05:06
Static Engine Version	4.4.1.0 / 2022-01-14 04:00:58
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.16 / 2022-03-11 16:16:43
Smart Memory Dumping Rules Version	4.4.1.6 / 2021-12-14 15:06:27
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.19 / 2022-03-31 10:55:59
YARA Built-in Ruleset Version	4.4.1.19

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp
System Root	C:\Windows