MALICIOUS

Classifications: Ransomware

Threat Names: Sodinokibi, CVE-2018-8453, Mal/Generic-S, Trojan.Brsecmon.1, Generic.Ransom.Sodinokibi.F8A01CC1

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**sodinokibi.exe**
ID	#694134
MD5	fb68a02333431394a9a0cdbff3717b24
SHA1	1399bf98a509adb07663476dee7f9fee571e09f3
SHA256	0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d
File Size	290.00 KB
Report Created	2021-07-03 20:09 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (18 rules, 124 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) sodinokibi.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #1) sodinokibi.exe renames multiple user files.			
5/5	YARA	Malicious content matched by YARA rules	1	-
	• Rule "Sodinokibi_CVE_2018_8453" from ruleset "Ransomware" has matched on a memory dump for (process #1) sodinokibi.exe.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 212 files by appending the extension ".06ak3t5y".			
5/5	User Data Modification	Modifies Windows automatic backups	2	-
	• (Process #1) sodinokibi.exe deletes Windows volume shadow copies. • (Process #2) cmd.exe deletes Windows volume shadow copies.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
4/5	Antivirus	Malicious content was detected by heuristic scan	3	-
	• Built-in AV detected the sample itself as "Trojan.Brsecmon.1". • Built-in AV detected a memory dump of (process #1) sodinokibi.exe as "Trojan.Brsecmon.1". • Built-in AV detected a memory dump of (process #1) sodinokibi.exe as "Generic.Ransom.Sodinokibi.F8A01CC1".			
3/5	System Modification	Disables a Windows system tool	1	-
	• (Process #1) sodinokibi.exe disables startup repair by executing ""C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures".			
3/5	User Data Modification	Possibly drops ransom note files	1	Ransomware
	• (Process #1) sodinokibi.exe possibly drops ransom note files (creates 52 instances of the file "06ak3t5y-readme.txt" in different locations).			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #1) sodinokibi.exe has a thread which sleeps more than 5 minutes.			
2/5	System Modification	Changes the desktop wallpaper	1	-
	• (Process #1) sodinokibi.exe sets the desktop wallpaper to the file "c:\users\keecfmwgj\appdata\local\temp\866s90pv.bmp".			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• (Process #1) sodinokibi.exe is possibly trying to detect a VM via rdtsc.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	5	-

Score	Category	Operation	Count	Classification
	• (Process #1) sodinokibi.exe makes a direct system call to "NtUserCallOneParam". • (Process #1) sodinokibi.exe makes a direct system call to "NtUserDefSetText". • (Process #1) sodinokibi.exe makes a direct system call to "NtUserSetWindowFNID". • (Process #1) sodinokibi.exe makes a direct system call to "NtUserThunkedMenuItemInfo". • (Process #1) sodinokibi.exe makes a direct system call to "NtUserInternalGetWindowText".			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) sodinokibi.exe creates mutex with name "Global\DAE678E1-967E-6A19-D564-F7FCA6E7AEBC".			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) sodinokibi.exe enumerates running processes.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) sodinokibi.exe starts (process #2) cmd.exe with a hidden window.			
1/5	System Modification	Modifies operating system directory	100	-

- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_hid-user.resources_31bf3856ad364e35_6.1.7600.16385_en-us_c19781a304e374a4.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_hid-user.resources_31bf3856ad364e35_6.1.7600.16385_en-us_c19781a304e374a4_hid.dll.mui_cccd5ae0" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_hid-user.resources_31bf3856ad364e35_6.1.7600.16385_en-us_c19781a304e374a4_hidserv.dll.mui_561adfc8" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..ce-router.resources_31bf3856ad364e35_6.1.7600.16385_en-us_243862f6e4997dad.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..ce-router.resources_31bf3856ad364e35_6.1.7600.16385_en-us_243862f6e4997dad_activeds.dll.mui_67414db4" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..core-base.resources_31bf3856ad364e35_6.1.7600.16385_en-us_c620663a0d83d04f.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..core-base.resources_31bf3856ad364e35_6.1.7600.16385_en-us_c620663a0d83d04f_winmm.dll.mui_224f6445" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..ence-infrastructure_31bf3856ad364e35_6.1.7601.17514_none_3337092d63596104.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..ence-infrastructure_31bf3856ad364e35_6.1.7601.17514_none_3337092d63596104_aelupsvc.dll_f420497b" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..ence-infrastructure_31bf3856ad364e35_6.1.7601.17514_none_3337092d63596104_apphelp.dll_7ce69c4a" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..ence-infrastructure_31bf3856ad364e35_6.1.7601.17514_none_3337092d63596104_sdbinst.exe_8725e339" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..ence-infrastructure_31bf3856ad364e35_6.1.7601.17514_none_3337092d63596104_shimeng.dll_2036b947" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..es-interface-router_31bf3856ad364e35_6.1.7600.16385_none_b3eaf84f983a33ee.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..es-interface-router_31bf3856ad364e35_6.1.7600.16385_none_b3eaf84f983a33ee_activeds.dll_662643d7" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..es-interface-router_31bf3856ad364e35_6.1.7600.16385_none_b3eaf84f983a33ee_activeds.tlb_662648dd" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..llservice.resources_31bf3856ad364e35_6.1.7600.16385_en-us_b9c303c8bce24ecf.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..llservice.resources_31bf3856ad364e35_6.1.7600.16385_en-us_b9c303c8bce24ecf_axinstsv.dll.mui_be092a2d" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..llservice.resources_31bf3856ad364e35_6.1.7600.16385_en-us_b9c303c8bce24ecf_axinstui.exe.mui_aea34130" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..on-authui.resources_31bf3856ad364e35_6.1.7600.16385_en-us_e7718915b6ba8195.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..on-authui.resources_31bf3856ad364e35_6.1.7600.16385_en-us_e7718915b6ba8195_authui.dll.mui_19b92789" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..structure.resources_31bf3856ad364e35_6.1.7600.16385_en-us_541d3a4db051d913.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..structure.resources_31bf3856ad364e35_6.1.7600.16385_en-us_541d3a4db051d913_aelupsvc.dll.mui_5d6cb110" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..structure.resources_31bf3856ad364e35_6.1.7600.16385_en-us_541d3a4db051d913_apphelp.dll.mui_59096153" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-a..structure.resources_31bf3856ad364e35_6.1.7600.16385_en-us_541d3a4db051d913_sdbinst.exe.mui_258ad624" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-acledit.resources_31bf3856ad364e35_6.1.7600.16385_en-us_853b0789da5b1e2a.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-acledit.resources_31bf3856ad364e35_6.1.7600.16385_en-us_853b0789da5b1e2a_acledit.dll.mui_5f932ccb" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-acledit_31bf3856ad364e35_6.1.7600.16385_none_c3d671ef7642fced.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-acledit_31bf3856ad364e35_6.1.7600.16385_none_c3d671ef7642fced_acledit.dll_89da72d2" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-aclui.resources_31bf3856ad364e35_6.1.7600.16385_en-us_9dc6c5d5ca9cbc28.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-aclui.resources_31bf3856ad364e35_6.1.7600.16385_en-us_9dc6c5d5ca9cbc28_aclui.dll.mui_adadbfb7" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-aclui_31bf3856ad364e35_6.1.7600.16385_none_b0ff4fc4cd57c163.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-aclui_31bf3856ad364e35_6.1.7600.16385_none_b0ff4fc4cd57c163_aclui.dll_ebee9df6" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-acproxy_31bf3856ad364e35_6.1.7600.16385_none_520444733f7b8add.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-acproxy_31bf3856ad364e35_6.1.7600.16385_none_520444733f7b8add_acproxy.dll_5d65b262" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-activexcompat_31bf3856ad364e35_8.0.7601.17514_none_6f29eb5391300db2.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-activexproxy_31bf3856ad364e35_6.1.7601.17514_none_703438df00e9e0d7.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-activexproxy_31bf3856ad364e35_6.1.7601.17514_none_703438df00e9e0d7_actxprxy.dll_82133921" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-advapi32.resources_31bf3856ad364e35_6.1.7600.16385_en-us_747e69daca85f63e.manifest" in the OS directory.
- (Process #1) sodinokibi.exe modifies file "c:\windows\winsxs\backup\amd64_microsoft-windows-advapi32.resources_31bf3856ad364e35_6.1.7600.16385_en-us_747e69daca85f63e_advapi32.dll.mui_28c7718f" in the OS directory.

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

• (Process #1) sodinokibi.exe resolves 103 API functions by name.

Mitre ATT&CK Matrix

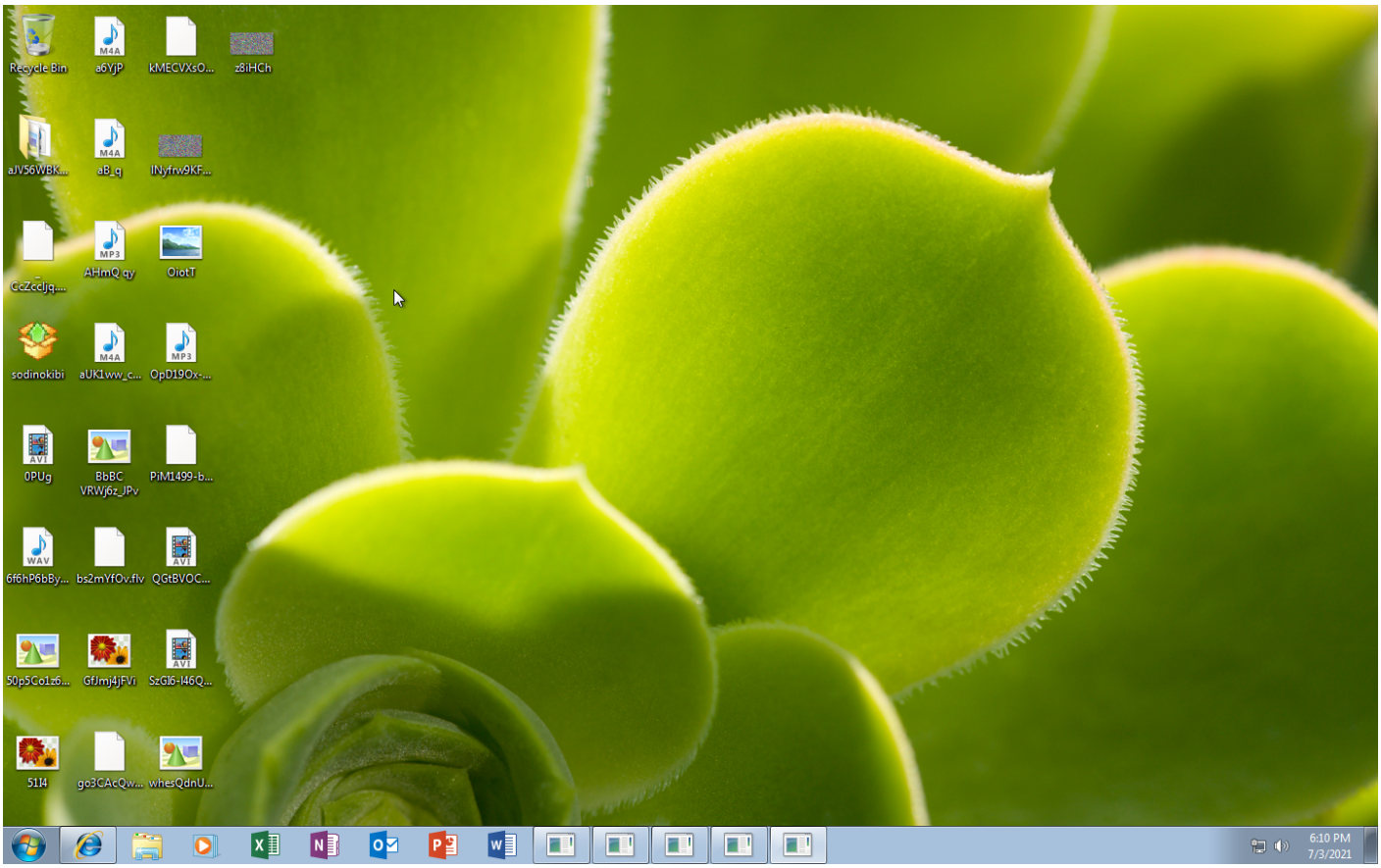
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window		#T1057 Process Discovery					#T1490 Inhibit System Recovery
				#T1497 Virtualization/ Sandbox Evasion		#T1497 Virtualization/ Sandbox Evasion					#T1486 Data Encrypted for Impact
				#T1045 Software Packing		#T1124 System Time Discovery					#T1491 Defacement

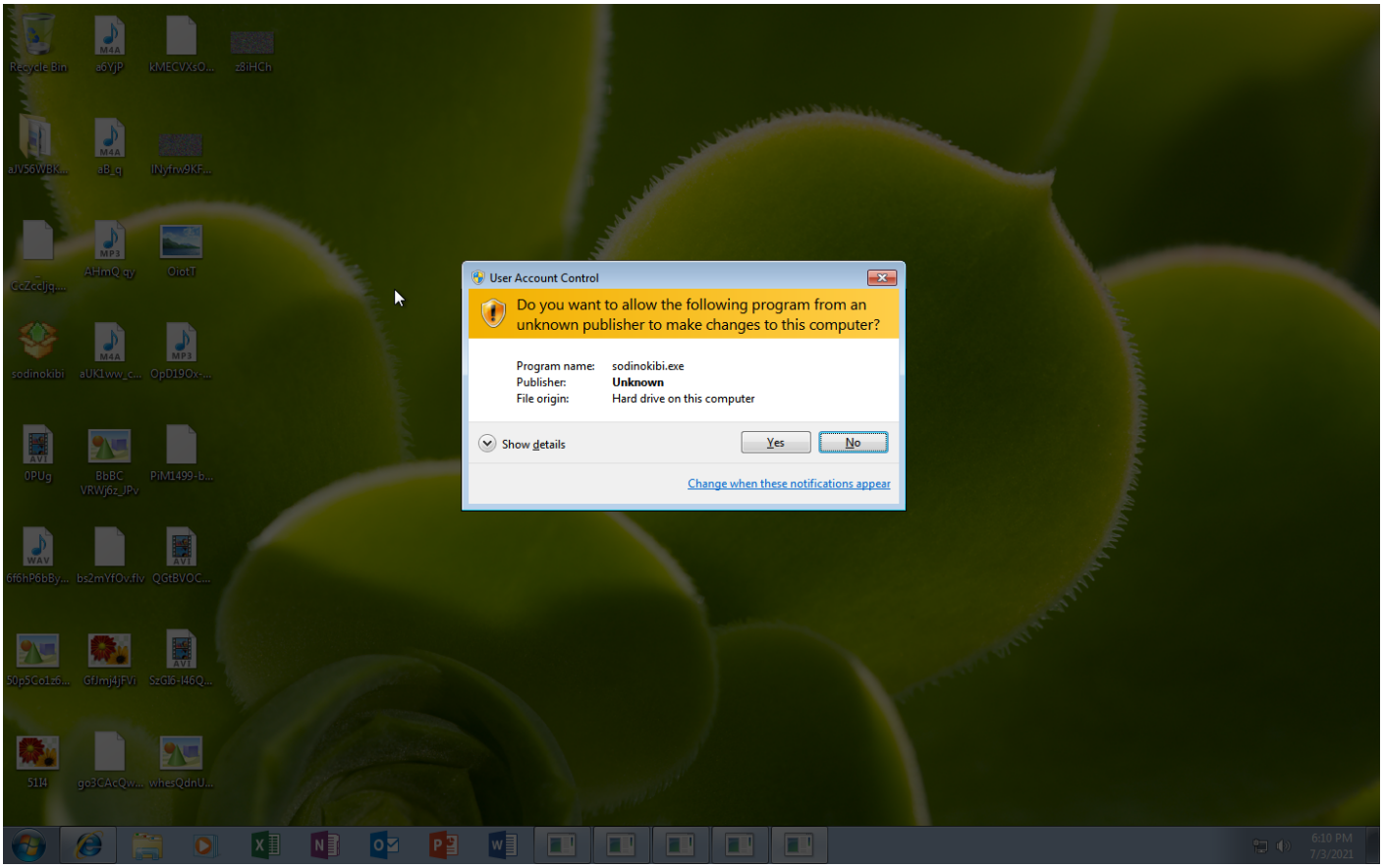
Sample Information

ID	#694134
MD5	fb68a02333431394a9a0cdbff3717b24
SHA1	1399bf98a509adb07663476dee7f9fee571e09f3
SHA256	0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d
SSDeep	6144:cGZamLIoveyefyOrA80qE1lHJv3loPHVb6:cEsomyef5k8k3Sb
ImpHash	672b84df309666b9d7d2bc8cc058e4c2
File Name	sodinokibi.exe
File Size	290.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-07-03 20:09 (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	15
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	17




User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: sodinokibi.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

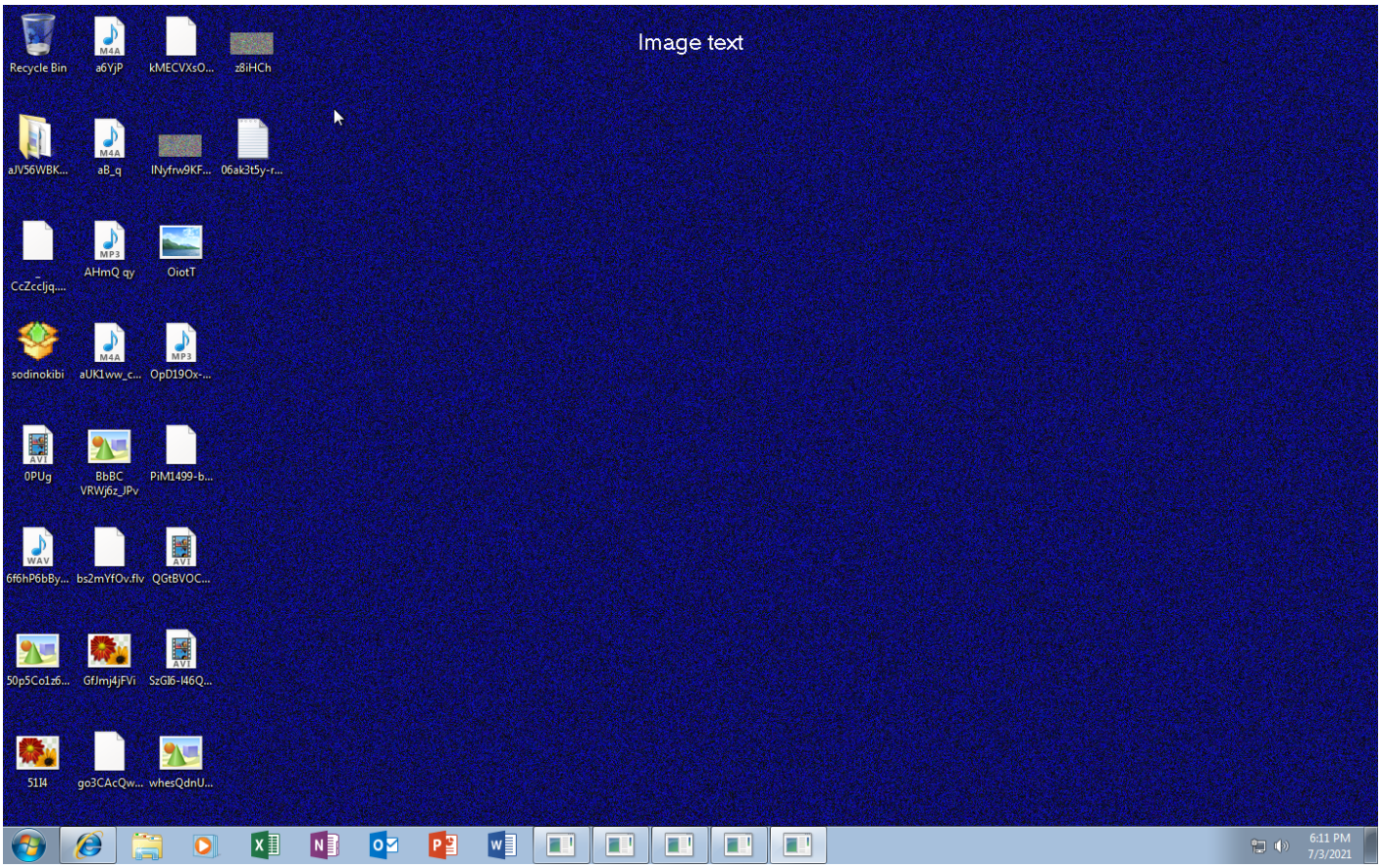


Image text
Recycle Bin
a6YjP
kMECVXsO...
z8iHCh
aJV56WBK...
aB_q
INyfrw9KF...
06ak3t5y-r...
CcZcCjq....
AHmQ qy
OiotT
sodinokibi
aUK1ww_c...
OpD19Ox-...
0PUg
BbBC VRWj6z_JPv
PiM1499-b...
6f6hP6bBy...
bs2mYfOv.flv
QGtBVOC...
50p5Co1z6...
GfJmj4jFVi
5zGl6-l46Q...
51l4
go3CAcQw...
whesQdnU...
6:11 PM
7/3/2021

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

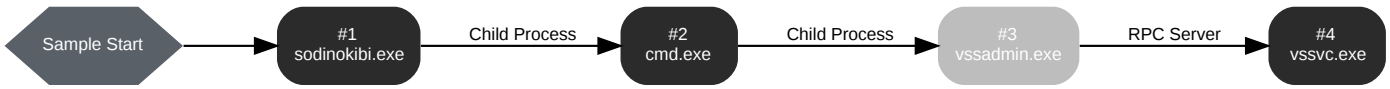
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: sodinokibi.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\sodinokibi.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\sodinokibi.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 35041, Reason: Analysis Target
Unmonitor End Time	End Time: 135527, Reason: Terminated
Monitor duration	100.49s
Return Code	0
PID	3784
Parent PID	1124
Bitness	32 Bit

Dropped Files (215)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
\\?\C:\Users\kEecfMwgj\06ak3t5y-readme.txt	3.60 KB	978133eb603107a6b404bb409ff5e5190ae23678ffd8ad4b91b72aec2263c162	✗
\\?\C:\Users\kEecfMwgj\Contacts\Administrator.contact	67.00 KB	89dc6f889bd8d16fe7562fd0d9b2c42caf80c8835c0932f74959dc4132e86731	✗
\\?\C:\Users\kEecfMwgj\Desktop\0PUg.avi	21.62 KB	fa22be6448fa9af677426ff1b993f141b457bed095934bdddece0c29dddf5065	✗
\\?\C:\Users\kEecfMwgj\Desktop\50p5Co1z6EVm.gif	21.99 KB	75bdc7ad65b2d5182a73a83d697a42ef3514c42745058f4797bf05ee33919357	✗
\\?\C:\Users\kEecfMwgj\Desktop\51I4.png	40.19 KB	ded808c753bdc011e544448fd752540f159d5dd4ae8cdb6caf0d80ff9231c03d	✗
\\?\C:\Users\kEecfMwgj\Desktop\6f6hP6bBydZ1otviYKm.wav	20.77 KB	3daf7ba6a50ed5d7904c9a99ccdeba3eb4e857c5429b8fe1cfa0192af345927f	✗
\\?\C:\Users\kEecfMwgj\Desktop\a6YjP.m4a	6.15 KB	a9ae78d44b6d5cb07241d14d45a419c14758fda9a2bf44e7df18940755e5579a	✗
\\?\C:\Users\kEecfMwgj\Desktop\aB_q.m4a	39.29 KB	dfe6ae0d47795a1a97ff464271676e90775a6860ee75caf8759df0a203ec08f5	✗
\\?\C:\Users\kEecfMwgj\Desktop\AHmQ qy.mp3	91.68 KB	84b0aa45562e23918ccc11ead690bf4f8c89d79b8f27cbdd803182364e4731f9	✗
\\?\C:\Users\kEecfMwgj\Desktop\aUK1ww_cNSEBhOhvD.m4a	79.32 KB	f5fbd8a63a79caeced35a81e9d8c0565d57305b72a65124e6efafd2d96b7f4b2	✗
\\?\C:\Users\kEecfMwgj\Desktop\BbBC VRWj6z_JPv.gif	69.17 KB	049305a7938d9602e9a2ce09d232c0682ae21272336e5ee6875291879ff2e4b5	✗
\\?\C:\Users\kEecfMwgj\Desktop\bs2mYfOv.flv	27.72 KB	ce4f0b8a4bb5bd8907ac76f283d460a84e561cc66e58fbdd678db8a39a0ddbac	✗
\\?\C:\Users\kEecfMwgj\Desktop\GfJmj4jFVi.png	30.93 KB	966777c0d898e3f5a3d3fe287706530ee097e110ae023c05f12027a4c579bf71	✗
\\?\C:\Users\kEecfMwgj\Desktop\go3CAcQwWoE5uapCI.mkv	25.74 KB	ccad8c864a6117a0450e275674fd37a9f9e9984b6c7a87ba74870be57d0c7006	✗
\\?\C:\Users\kEecfMwgj\Desktop\kMECVXsOvLSDJDAOA.ots	40.97 KB	114fb052aa94b083c63d06c7f4d5b9ff19c72248a75b66d8f347373951ea4880	✗
\\?\C:\Users\kEecfMwgj\Desktop\lNyfrw9KFObcc0Vbb.bmp	52.77 KB	4d15e542eae2f2df819ee8b289d7c005b4c3e5c0075b90b914d3992918bfc099	✗
\\?\C:\Users\kEecfMwgj\Desktop\OiotT.jpg	73.92 KB	d65b504669022c0cdc92860694125cc8fc7b9d0467da51d39b0bec093e4c1145	✗

File Name	File Size	SHA256	YARA Match
\\?\C:\Users\kEecfMwgj\Desktop\OpD19Ox-5GJ.mp3	4.38 KB	2234f94fd105f98b96d5f08b2fea369a3f8d729dd172eefb542a627299d10b82	✗
\\?\C:\Users\kEecfMwgj\Desktop\PiM1499-bCIJI-DrwX.flv	73.29 KB	c15e2a57a0b33f3fe5284b64e55f455b45861d2e406431f15360953007f4592e	✗
\\?\C:\Users\kEecfMwgj\Desktop\QGtBVOCQPa2FltB11SX3.avi	61.69 KB	0e58b2a75522c549aa7915e560373d573445ca435e1900635859e55ae89507a9	✗
\\?\C:\Users\kEecfMwgj\Desktop\SzGI6-l46QfkV6r.avi	86.02 KB	4a55b33aa5210fc0778129368be3175cfedc41c8a75ac62107e94e24179e5c3f	✗
\\?\C:\Users\kEecfMwgj\Desktop\whesQdnUMwd_xm-th3g0.gif	4.49 KB	9c321d080086217ddba8c6376da46121f547f2ffbb0b86bb2045c3ff7ad664d3	✗
\\?\C:\Users\kEecfMwgj\Desktop\z8iHCh.bmp	94.11 KB	d3bdd294315d1edc806edb694f5092546d632b8b3a963ff4238f82968cc86b01	✗
\\?\C:\Users\kEecfMwgj\Desktop_CcZcclJq.mkv	26.32 KB	5c51daf77a6f0ad108391ff535032e7eed3980b5894c3e1a9af428af15461c48	✗
\\?\C:\Users\kEecfMwgj\Documents\-5MKPFwyZwdE.docx	54.98 KB	e2f643d4ab1b4b63b3728283e3108a119296ae2b328e35dfdce0951f38aba9e1	✗
\\?\C:\Users\kEecfMwgj\Documents\07Y-vNHiW6TBEU.odp	17.27 KB	67a2801a874ec6627b9fcebb582dc091e0c1eabe34c72b5c2c88708b4b87a695	✗
\\?\C:\Users\kEecfMwgj\Documents\0ZUqqrgO.ppt	49.14 KB	afc454f98cb609fdf26a340532f9a781febc92b9ce2bcad8eae449894ac9ff57	✗
\\?\C:\Users\kEecfMwgj\Documents\3ozabK9D.pptx	43.97 KB	ccfb2030ecfa6955db63884ac6ecebf752514155477ec759bb403f03b747f94a	✗
\\?\C:\Users\kEecfMwgj\Documents\4cdMBjwoKg.odt	50.20 KB	67116f814d18e40cf7afeba930cc778c108fb5ed64859dfbe8ab9341fe8dfebc	✗
\\?\C:\Users\kEecfMwgj\Documents\5hmdrIDHtVpR.ots	52.16 KB	17e857252a8b03c0aafd43ead0b38390a9d323feae244781ae5ff2ba4c199a50	✗
\\?\C:\Users\kEecfMwgj\Documents\6cY9G.xlsx	18.44 KB	a0c71926e2e36c47c0a5c3272f1c88c74aa341861d0df09e4c2f11d159905c18	✗
\\?\C:\Users\kEecfMwgj\Documents\6Lo4VggeyxcF04AJM4nt.pptx	54.55 KB	2a2cc91e24690da714b2fd58e9b27cf82cb4f4dd675081e289f82fad53cae762	✗
\\?\C:\Users\kEecfMwgj\Documents\9WPMG5w3nojWcs51.docx	82.19 KB	26def8331dd758cd6b6881065ef017ad766b8fbbf770a9e473b3b3e4ba56f8b8	✗
\\?\C:\Users\kEecfMwgj\Documents\AIEvT4Qz7Bv01ypgZ.pdf	76.63 KB	d5c3fbb4cb2517505046642 90e55558d4d5462180f26d6bde9295b66f4bd38cc	✗
\\?\C:\Users\kEecfMwgj\Documents\aORICMsiaM.doc	8.31 KB	da8461e90e9fd505e83fcfa255fd3c31ff8305d15f5c1d7ff9d95e00473a4637	✗
\\?\C:\Users\kEecfMwgj\Documents\bOkgUz6.odp	4.40 KB	a05635cc1b72fd4ed4c99f2f96b0182e33fa359109ffbaa9cb2e141fcab7c07c	✗
\\?\C:\Users\kEecfMwgj\Documents\B_IKnAuj4tm9 PtH.pptx	77.17 KB	3a839350d67589a6fe8ed62a8b63c8f43d2217a92cc895c3d7ff90891ede6508	✗
\\?\C:\Users\kEecfMwgj\Documents\c0s1YUWcSTEroJdKuB.docx	8.61 KB	98b977f2ce9777984986a2c8656562b98ead6277229f47bc9af2192477df4ab5	✗
\\?\C:\Users\kEecfMwgj\Documents\chQiNux5apW.csv	55.37 KB	c59e883f7537c3c7bdbf3d7a97a0bb69b9fb936e57747d09ca253763beb9c087	✗
\\?\C:\Users\kEecfMwgj\Documents\D2B5.csv	49.13 KB	693554545968deba792686622d2416d52937bb45769f60ef64454f30f0af363f	✗
\\?\C:\Users\kEecfMwgj\Documents\Da8Oppcqp90t.docx	77.94 KB	559d22242652fbca6144e304acaf43d5597c987763cb5a7962451ffa4b68fb21	✗
\\?\C:\Users\kEecfMwgj\Documents\eB 95K8MWD.xlsx	77.92 KB	b23c88ad3c51a2a19458ad52685b9a299ff8492cd823b5999200cf720eae3304	✗
\\?\C:\Users\kEecfMwgj\Documents\fDhfuRyygxzvH.ods	28.92 KB	25e22dc970a2f921e590b0aec0052146a95dcf8bfe76b5c7a62a0240ddc36615	✗
\\?\C:\Users\kEecfMwgj\Documents\fWYCUggo7eiu Mez.odt	89.35 KB	c96eb09aef523df5f4e65ddc310fbf3f4f3ad0a9e1b171509b4ebb54129778d5	✗
\\?\C:\Users\kEecfMwgj\Documents\GMmGBk5gIcrjM.doc	39.84 KB	f820c012cc0a9553665d3ea2f58a2095c9709d6d66f496af793a52231d0c1f32	✗
\\?\C:\Users\kEecfMwgj\Documents\Jm6CiFV.pptx	61.31 KB	91041301aa177ced57d970f8999b310776feed3271f1b6a0c6899c8cd0125513	✗

File Name	File Size	SHA256	YARA Match
\\?\C:\Users\kEecfMwgj\Documents\JM7eM8laWBfHyX5ed.odt	75.48 KB	3cc5a519c1588053d677b78f3f1631049f20cfa7f41a420b096cccf2347c65c4	✗
\\?\C:\Users\kEecfMwgj\Documents\keforvhV3MOW.docx	19.12 KB	e91ca935445a1b80b03b6dbfa083ecfe0f32524262ea8c59ed5f4d24ebaa746b	✗
\\?\C:\Users\kEecfMwgj\Documents\LjI6.ods	10.36 KB	23bc0802a7b8048fd15af94d8f6af1fd88b1be119115215fd32a5e5e91be1bbf	✗
\\?\C:\Users\kEecfMwgj\Documents\N6MTn7qEK2nADv.odt	10.94 KB	dfe596012ce08c38bf6c54b6ff64004e408ab0b9e154fd19657fc92737a92efa	✗
\\?\C:\Users\kEecfMwgj\Documents\N8CPfO-zjsOqif.xls	5.14 KB	8da5870e4dbdc4252e43ea6587d4228d886dad3edff6bb3969dc7fbe89421011	✗
\\?\C:\Users\kEecfMwgj\Documents\NpJmmrQh0nwG7_pUv.csv	99.47 KB	5d00990e24380255a0834943f13e8df5ee7c9198dc144eb87521f16131ad66ab	✗
\\?\C:\Users\kEecfMwgj\Documents\OOXxuWoBXn.docx	58.24 KB	0744db06634e50d150c875037004f4fe2408ba9d685e39540acef1aa3453e25d	✗
\\?\C:\Users\kEecfMwgj\Documents\othZzWJti-TuFa-zMAO.odp	52.08 KB	847cdb262cff2df8326a99bac1a8a1a75d4e89a51a709a56e4e7e3006f52aca4	✗
\\?\C:\Users\kEecfMwgj\Documents\pU7xrszOnuj.pptx	75.78 KB	80b297ed424ba8446b99ad1ed65f1d70c8b842da44e543004627da3b77aba9d7	✗
\\?\C:\Users\kEecfMwgj\Documents\PuoJ2S5Mug.odp	19.03 KB	d5fa4631f9936887c2ab53c9a07e81570806c52b1e4627f409fc2292fe0e6e03	✗
\\?\C:\Users\kEecfMwgj\Documents\PWIkIR.odp	93.59 KB	abb9a94104f074a9013828deee02beb1b4e4532062165b625fab4588d8dde843	✗
\\?\C:\Users\kEecfMwgj\Documents\QhYEo-WKA63tNNVSpa.docx	28.23 KB	cc93759c8c4d2c975542e96695dcfb4aaa7a89448334f5e7022c3e7eb3e8d63c	✗
\\?\C:\Users\kEecfMwgj\Documents\RYu7G-GPCGAN4l7O.odp	63.56 KB	884f39f9094866f1610f36d06081013cefb6746cd0ca4765b5b3c10d65a3145e	✗
\\?\C:\Users\kEecfMwgj\Documents\SGiE0.pptx	85.54 KB	5b2ce592c5f43b390c2112761123843e0a372154935a3996f98aaf6728963591	✗
\\?\C:\Users\kEecfMwgj\Documents\t4hmzP4sxl.doc	70.76 KB	efa55880734e60be91415520272c5838ef7ccf589641d7025c06dadd3e9cd304	✗
\\?\C:\Users\kEecfMwgj\Documents\TkZtgo9eUgYlcNaPSWIL.xlsx	18.07 KB	c6f5d37780df8becf6132d742a626902f38f4a7424b2a78b63513ac97e73f6c1	✗
\\?\C:\Users\kEecfMwgj\Documents\TQAB2NjEL6JO02B_.xlsx	2.18 KB	82438b27e593b8148e57a0c73b8a8c8f26bc7f9d08557d58aae93eb8e83ae9ec	✗
\\?\C:\Users\kEecfMwgj\Documents\TtXfXxvP2sv01dTtReh.docx	95.07 KB	fd0df9466a4ab5ea7f7acb65247f5326b6ee1dfbc2a4bfacd9f8117b97e208c5	✗
\\?\C:\Users\kEecfMwgj\Documents\U5KwAzHQh Ydz8ltp H.ppt	76.90 KB	6b3e4991ade17151184f911bedd5277406365720a4524d1a755c4fda8fe28bcb	✗
\\?\C:\Users\kEecfMwgj\Documents\uEWQ Dy-Fw0wiatk6.docx	91.94 KB	34f45c25fc4e08325ec83c4813d50164cb19c510d6521a431ea6af5245b47fee	✗
\\?\C:\Users\kEecfMwgj\Documents\Xhy8G8l_DiYgdEinCs86.pptx	55.02 KB	12cb190c25d44d6dd47bd28b3c64fbfca1c4e2a0c00dd09c433e849b0f88f5b6	✗
\\?\C:\Users\kEecfMwgj\Documents\y1Uz_.odt	1.52 KB	2af17b25bb50352fa7905b91ac334379447f88cee030f513c06715d742bf5f70	✗
\\?\C:\Users\kEecfMwgj\Documents\yJSmVxafx.pdf	88.43 KB	9a67bda257debfac08e7eb4734417ebf498b43109ebf36bd22203e93805df17b	✗
\\?\C:\Users\kEecfMwgj\Documents\yruBBVRJKY.pptx	53.73 KB	8f0b11937ebb495f5e085cf273a88816003bb9c30b9f590e60babf220a2940ec	✗
\\?\C:\Users\kEecfMwgj\Documents\Z t_Z1agjCu.xlsx	71.10 KB	079a332087e3c3c725bd6ef41c4af2e5d7e6557e3fcc5cd63764144eaca78414	✗
\\?\C:\Users\kEecfMwgj\Music\3MXvqj-GZEArJKONkb_.mp3	10.66 KB	776d586767532b6c1816d15bba3fea7cc259ad1647ec49f5aad26affa74fdeaa	✗
\\?\C:\Users\kEecfMwgj\Music\69r Y8_shB.mp3	6.93 KB	a1536a2a7e83b32c0830253ce17669df2ae6fe6c20a43d39cba83e80ad1ba7d0	✗
\\?\C:\Users\kEecfMwgj\Music\biDq-D.m4a	35.76 KB	c947ef16fa45dbab14f6310027c9cb7b9210a1bbb98ffa5e8aede741498bb834	✗
\\?\C:\Users\kEecfMwgj\Music\dCyh_q8 rpkVYgZLK m.wav	29.57 KB	97233f9a38f58332c2fa313e3911dcbe5a3a3d921249872a71298b7445512612	✗

File Name	File Size	SHA256	YARA Match
\\?\C:\Users\kEecfMwgj\Music\FrpwP6s.wav	93.63 KB	8c85246dcc4f1f3cae4cc0ec5be00b67544ca0648ef39018b88d264de1da0064	✗
\\?\C:\Users\kEecfMwgj\Music\fSf1idQOVtocKEOHiEU.m4a	42.10 KB	375c6b01ba4560f68ee5dcc150fed492dde282e6b0367e431bc783c0abe9406a	✗
\\?\C:\Users\kEecfMwgj\Music\ht6mcbD4xY51MFFx.mp3	49.08 KB	a77f2bf4919945fc24e0bc97fc4441e878d569f7a1209996db8cfa82d4632725	✗
\\?\C:\Users\kEecfMwgj\Music\qsI-.m4a	96.68 KB	bd8671df408a3b6a027fa9fa6967a31dca0b07810e0acb6f000d8714f9f6a1ae	✗
\\?\C:\Users\kEecfMwgj\Music\tCh9inH.mp3	7.17 KB	119f9f916a2f92e43fb232864f883191fb4e9f6124973d105d435bdf56ac096a	✗
\\?\C:\Users\kEecfMwgj\Music\tzURC8_Z HJox8cSSbC.wav	17.52 KB	b42a5d4086d6ff22ea2896c02505da010f1474cfb40f0a5e2512932ebe7cdccd	✗
\\?\C:\Users\kEecfMwgj\Music\XUfUzf.mp3	3.68 KB	d5a6be05bcaa380a36952334ae756ca14746dd4e5de2769277a231d522cf7115	✗
\\?\C:\Users\kEecfMwgj\Music\zYUG2.m4a	97.03 KB	ff958cf37cb724773b117c5642a2e49585655cb60d2b6f2130c51220c92dd0d9	✗
\\?\C:\Users\kEecfMwgj\Pictures\4ldTijNb5enuQ.bmp	8.53 KB	d23a21a44f27d9204b4807c3189927f446f13bc4479e511dc5e5ead4564dcfa2	✗
\\?\C:\Users\kEecfMwgj\Pictures\h1WR8r.bmp	4.80 KB	58777a3de0532dd9a98768fbe5a5b75cbf02615777f0f438f6846d0b36c8857b	✗
\\?\C:\Users\kEecfMwgj\Pictures\hreakSGbo7iehUMhp.jpg	91.64 KB	0b0ba7bf5e967803b37fe794252bfb2ab4a2c15824954912ef83827f49ab8383	✗
\\?\C:\Users\kEecfMwgj\Videos\7oacghL0FgM.mp4	31.23 KB	dbc161813070b579ef67264575b053ec1ccc75e47e42eededd0119fbbe2c4db8	✗
\\?\C:\Users\kEecfMwgj\Videos\DdzxhrbP8S7OSzK7gvx-.avi	19.27 KB	65a34920b26ab7c6c911f3e308bc557ad263a6c0f6883c81d7a8db40a31f7104	✗
\\?\C:\Users\kEecfMwgj\Videos\OGP0BLXkOZqfcLE5 r.avi	35.13 KB	35196e0258e02feddd4e07105ba7440c35a9a1b1bac6bfe11f92f239b75b0273	✗
\\?\C:\Users\kEecfMwgj\Videos\PNp9VEShM5vJa6UfKU.mkv	49.06 KB	13b5cce9f0e2230a4c1fe1d67f805709475db14fb7e503cb1e0d9fbf03e49836	✗
\\?\C:\Users\Public\Libraries\RecordedTV.library-ms	1.07 KB	9fe6ef3e23ec8015220a1255b0ee54ebeb7625e42cbc3a3a3e4f50b5cbda951a	✗
\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\5PlGlZaCV4jqbsV7K0Fu.mp3	86.70 KB	507dce298eda77dff66efd0a6d121d88ec0362093f4482338b40c6f7ab4521cb	✗
\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\divc1VvDFB.mkv	60.29 KB	3647ff08d1bc14989c2d2dc72f1d97cb69b8cfa62a6e9af30902aef5db8af074	✗
\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\qWumTA_.mp4	8.08 KB	5c16605dbb18c7b7650cf69ec033e60286fc9c65f0cf3b322845b2c7f66fa7ab	✗
\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\x4 v.gif	27.31 KB	b50970e523bf2f5e8ad208377805815c052bd77c4ab5a765648178190d727590	✗
\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\ZAR5gyQrXI.gif	65.87 KB	569d157fab1086e7d1d4ff9923e864299eff1acc8ab696c778317c8fcc01d3ba	✗
\\?\C:\Users\kEecfMwgj\Documents\Outlook Files\franc@gdllo.de.pst	265.22 KB	1e2fc688461453c0ba73a686518d65aef8921c29f6f0d202996a99860c4ad7eb	✗
\\?\C:\Users\kEecfMwgj\Favorites\Links\Web Slice Gallery.url	450 bytes	873eef8c60e187e26bbb1199cbef7545d659e79f2a7e1a6f49e5ec97c45e08a4	✗
\\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE Add-on site.url	357 bytes	323a8e53450197db59b98dc67b2840eb630144885daea1bce4df552c8c4dc8e6	✗
\\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE site on Microsoft.com.url	357 bytes	d0b870d2a4ef1a8c6adfebabf4f30254f2241f7b2fc9d7a08f6d77ddfa1ec570	✗
\\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Home.url	357 bytes	af6ce02b553c1fda8ef7b062940f9a7c37c2a90d0197e0da9306635c3928bd48	✗
\\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Work.url	357 bytes	c3a004e0e1587eb1e6c7c8202a884d885b7cd831b6af4f0e81da4f75086a4fe5	✗
\\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url	358 bytes	4d838949c541c5b8f89852159531741d9d6e055f1e52f0ea0a8b67e96e17c07d	✗

File Name	File Size	SHA256	YARA Match
\\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Autos.url	357 bytes	3d0c834d5892d9da460aec5ad3c72e4d9d4240b6e15b7183dff017e860e7632d	✗
\\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Entertainment.url	357 bytes	f5a141c7a0c3e43de470dc6ce90a378aa8e1601ffcc1c00f6db316687cfd8082	✗
\\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url	357 bytes	82a283af24d3a3e14a5d3074b51bbd6fe37be324690fce897c28741a0d3faf06	✗
\\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Sports.url	357 bytes	346c19dc853ee699f841e4066ebed96638db26f349b797ad4dff958934eef6f9	✗
\\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN.url	357 bytes	b92db62a4199059f8745cb00b837bbb4b735cc68e723fdab2e6dbb4586ab6529	✗
\\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSNBC News.url	357 bytes	8c9796a7c3b8f1d5a9f4ae07e7181ed6098668ce98e24ab828fec01e22b61589	✗
\\?\C:\Users\kEecfMwgj\Favorites\Windows Live\Get Windows Live.url	357 bytes	81abfb706902258d02f519df2ea32420fddc12b8dc34ef2824b7057d5e292b27	✗
\\?\C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Gallery.url	357 bytes	9f32c4b6849a1b7ba27c6cea6a243b578385cab5d334a823794cf5862b517490	✗
\\?\C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Mail.url	357 bytes	a31eeba32c619c2495760e7c379027c4adb836138615f79c7efb363004105bc6	✗
\\?\C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Spaces.url	357 bytes	5735fbb5a0aacbcc90e188c848d01fa7d0e62942322e136e0bc3da0536851c84	✗
\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\bjOydzw.mp3	100.10 KB	653c72e1fb39e3c85382f5560a2b443b4f034bbaadc92c19f66f209146bae9d2	✗
\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\oCfLlu3p.mp3	70.34 KB	09a42b146f9b888342fd537d2485ed57980ff6e19b3c92979a9df1ab6b91d917	✗
\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\rPi6ROENBl.mp3	80.94 KB	ab85e3f0d997d2c3e9764075bbec433c15465480ed76d36be47980824391215d	✗
\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\SsOycCq2y.wav	79.01 KB	ec49b63cae866b86170cef02b93ee41ebf4a88423fa288eb293de4657806950a	✗
\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\z-ZcHxTcO3xPAhZK.wav	5.91 KB	c83feba1964a55cbdac6af54e1a2b4296718b1791780f517cac21f6a905d0dc0	✗
\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\zZYA2Sg.mp3	87.71 KB	6dc1b2348091effd32db93df8653cec9bcd77ccc26f65f566dadf9e64018ea62	✗
\\?\C:\Users\kEecfMwgj\Music\Rqx5DrLsWGq0fuHce-F\SdfXT.m4a	45.15 KB	68c380fa85a1ca8a4daf62aecf8ef285b58aded7413145b65c8c730b8c10fa66	✗
\\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou\-a8C ZzQY9ibDt.bmp	79.31 KB	a374b2eef2432d7feb048bd2c4fb8a784385dd559987fba439e4764a95a5fe5d	✗
\\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou\2pIHI6dW1Tj.png	75.47 KB	4954f950d5770ca570aad97634116a93aa13e02d48bbae20f1bc52e91a139d85	✗
\\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou\8kI9nfrKhl_-hQ6.gif	69.97 KB	fae7a8a48a1541d60a63f0d7fa96f32986eeac5e4904482299d09e6abda37db6	✗
\\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou\vuFOrfu.png	2.68 KB	cf6178222beb895985078fe746218077d754ff29a99028e144d598869a07e090	✗
\\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou_hY-b8CF6iv.png	42.09 KB	6a496af44bbf0ad53b46deb9c15b2602ef7c2d1c10d22793b3467556d12908e5	✗
\\?\C:\Users\kEecfMwgj\Videos\e xYTCaRLnxwOjYPkpp\BCVRhXmdcBbj0.avi	68.35 KB	6f93fd7b1f7335bb4ea41049103a99aaca6d2e3bc2cb3b546e25b72367aaddd3	✗
\\?\C:\Users\kEecfMwgj\Videos\e xYTCaRLnxwOjYPkpp\d_wE.flv	38.54 KB	6b8b6bb2a62bfc3099b2dc6fdc5360fa1dded4ac8936d75f3264574f6d6d4f2e	✗
\\?\C:\Users\kEecfMwgj\Videos\e xYTCaRLnxwOjYPkpp\VG-ilm5P4w8rjZV.mp4	54.15 KB	004775241a242fabeabbf80a9ad326a3eaf4a013061d9ad98acca4cf551bbff6	✗
\\?\C:\Users\kEecfMwgj\Videos\e xYTCaRLnxwOjYPkpp\X9RHt4PkF8UQ.flv	24.92 KB	4ea4ad06839108e98e47bae0df182a2726bedf024c8baeffae19c70049a33b75	✗
\\?\C:\Users\kEecfMwgj\Videos\e xYTCaRLnxwOjYPkpp\YjACMF.flv	46.94 KB	b43e8d4e5f720ff0f8aaed940341128a4dbd0cfd3aad35bfe9440dd73e69f0ed	✗
\\?\C:\Users\Public\Music\Sample Music\Kalimba.mp3	8217.45 KB	690614eb882fcbc2e29a419d65d7ad1fa07e1025c69ad21d8dd85aa3a4dfaeaa	✗

File Name	File Size	SHA256	YARA Match
\\?\C:\Users\Public\Music\Sample Music\Maid with the Flaxen Hair.mp3	4017.67 KB	69759b44c56199492594f1836158630225d2431f550c7e946b6d714844397f17	✗
\\?\C:\Users\Public\Music\Sample Music\Sleep Away.mp3	4729.31 KB	afcabea0b6130146713ae593a98096f15454d1f19c0421c590c2dd96a9ba47c8	✗
\\?\C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg	859.00 KB	9b428ee044eed278a37b7461e3039811ad2604502c6410e7bc3089dbf6b44991	✗
\\?\C:\Users\Public\Pictures\Sample Pictures\Desert.jpg	826.33 KB	37b89a8e3393ca1495ca9e19e744a371be19a1df81bff8a4089f85e9c5f7bf48	✗
\\?\C:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg	581.55 KB	079cb30e080b7430c51f1baf49b67a615de30db4fdd436e4adbfe377791ee4b6	✗
\\?\C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg	757.74 KB	a6f3a8150b83b5349b9e2683488e730c54f629028e59df122532232e8f3fc64a	✗
\\?\C:\Users\Public\Pictures\Sample Pictures\Koala.jpg	762.75 KB	95826142faa9e455deb455868ae5d60386c01469f66b7925c395fe940dca97e7	✗
\\?\C:\Users\Public\Pictures\Sample Pictures\Lighthouse.jpg	548.34 KB	4d1d5c2a3bfbeccaac161b60827e0e983eaf46a547ea0cb9ce76365574b40258	✗
\\?\C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg	759.82 KB	a55aaae0a42c050792245516c39df8a931331febb36a9e5a08fd7c2866f4ea29	✗
\\?\C:\Users\Public\Pictures\Sample Pictures\Tulips.jpg	606.55 KB	accaf758c7c8f80cd99f389497e9cb14891b9bb4eef1b173ae198849ff2ea2db	✗
\\?\C:\Users\Public\Recorded TV\Sample Media\win7_scenic-demoshort_raw.wtv	9472.22 KB	dae71252d063abe5737beb07878899ae1b943f0d470925bf8a057421e406fd1e	✗
\\?\C:\Users\Public\Videos\Sample Videos\Wildlife.wmv	10240.00 KB	8ba2db38de87b3b8c3592c06c7f0c7277643dcbee0965a519e1c45e5382cf9db	✗
\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\-9rGFqsYF62c2hsP.mp3	13.44 KB	2f79e518725d4ca4376642ad2af726b43fdfd5957ace971f2d8c98b4f0fee518	✗
\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\a48Mjh2i TKB2.mkv	16.51 KB	3888ede534a4ea8cde03157d5c11c19f866919207c3d794a4a0e566f95632298	✗
\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\pdbwVn-Lz4hgbH1S6sRs.bmp	65.56 KB	b4d4ff3c6e8c050afd1b5ad9c7b5dbe000d4f0cf718cac4933221ba9cb8c3081	✗
\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\WsOU.gif	56.01 KB	0f30f75d5f648c70402d2232bf10b7b29d60ad03ab3fa518f8469f41528bbe83	✗
\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\alGqygXdyMjy5o\aZ3qnO44VBmYATaQO.m4a	14.17 KB	fb3e045ef6fea3562a87f41ae15231f8dab25e76115e1cf8893baa2ee9a2825f	✗
\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\alGqygXdyMjy5o\C13Qxjjyorp.m4a	64.73 KB	e5a5a5a27886c24b8e6e55fcdf355dcf0ea1743b20e95d40e784c4225ba2f390	✗

Reduced dataset

Host Behavior

Type	Count
System	416
Module	281
File	1933
Environment	1
Mutex	1
Window	252
-	1
Process	282
User	1
Registry	40

Type	Count
Keyboard	4

Process #2: cmd.exe

ID	2
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 63417, Reason: Child Process
Unmonitor End Time	End Time: 78114, Reason: Terminated
Monitor duration	14.70s
Return Code	1
PID	3832
Parent PID	3784
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	14
Environment	8

Process #3: vssadmin.exe

ID	3
File Name	c:\windows\syswow64\vssadmin.exe
Command Line	vssadmin.exe Delete Shadows /All /Quiet
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 67413, Reason: Child Process
Unmonitor End Time	End Time: 76886, Reason: Terminated
Monitor duration	9.47s
Return Code	2
PID	3860
Parent PID	3832
Bitness	32 Bit

Process #4: vssvc.exe

ID	4
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: 74076, Reason: RPC Server
Unmonitor End Time	End Time: 275051, Reason: Terminated by Timeout
Monitor duration	200.97s
Return Code	Unknown
PID	3884
Parent PID	464
Bitness	64 Bit

Host Behavior

Type	Count
System	3

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0fa207940ea53e2b54a2b769d8ab033a6b2c5e08c78bf4d7dade79849960b54d	C:\Users\kEecfMwgj\Desktop\sodinokibi.exe	Sample File	290.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
978133eb603107a6b404bb409ff5e5190ae23678ffd8ad4b91b72aec2263c162	\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\n1idH_MUb\06ak3t5y-readme.txt, \\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLn... ...ontacts\06ak3t5y-readme.txt, \\?\C:\Users\kEecfMwgj\Searches\06ak3t5y-readme.txt, \\?\C:\Users\kEecfMwgj\Links\06ak3t5y-readme.txt	Dropped File	3.60 KB	application/octet-stream	Create, Write, Access	SUSPICIOUS
da26147148df62c4e9f8de75d9d6f68fd8bfdeb2257659f4c7ad47e6eeb76f6d	C:\Users\KEECFM~1\AppData\Local\Temp\866s90pv.bmp	Dropped File	5062.55 KB	application/octet-stream	Create, Write, Access	SUSPICIOUS
89dc6f889bd8d16fe7562fd0d9b2c42caf80c8835c0932f74959dc4132e86731	\\?\C:\Users\kEecfMwgj\Contacts\Administrator.contact, \\?\C:\Users\kEecfMwgj\Contacts\Administrator.contact.06ak3t5y	Modified File	67.00 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
fa22be6448fa9af677426ff1b993f141b457bed095934bddddce0c29dddf5065	\\?\C:\Users\kEecfMwgj\Desktop\0PUg.avi, \\?\C:\Users\kEecfMwgj\Desktop\0PUg.avi.06ak3t5y	Modified File	21.62 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
75bdc7ad65b2d5182a73a83d697a42ef3514c42745058f4797bf05ee33919357	\\?\C:\Users\kEecfMwgj\Desktop\50p5Co1z6EVm.gif.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\50p5Co1z6EVm.gif	Modified File	21.99 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
ded808c753bdc011e544448fd752540f159d5dd4ae8cdb6caf0d80ff9231c03d	\\?\C:\Users\kEecfMwgj\Desktop\51I4.png, \\?\C:\Users\kEecfMwgj\Desktop\51I4.png.06ak3t5y	Modified File	40.19 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
3daf7ba6a50ed5d7904c9a99ccdeba3eb4e857c5429b8fe1cfa0192af345927f	\\?\C:\Users\kEecfMwgj\Desktop\6f6hP6bBydZ1otviYKm.wav.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\6f6hP6bBydZ1otviYKm.wav	Modified File	20.77 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
a9ae78d44b6d5cb07241d14d45a419c14758fda9a2bf44e7df18940755e5579a	\\?\C:\Users\kEecfMwgj\Desktop\a6YjP.m4a.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\a6YjP.m4a	Modified File	6.15 KB	application/x-dosexec	Create, Delete, Read, Write, Access	CLEAN
dfe6ae0d47795a1a97ff464271676e90775a6860ee75caf8759df0a203ec08f5	\\?\C:\Users\kEecfMwgj\Desktop\aB_q.m4a.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\aB_q.m4a	Modified File	39.29 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
84b0aa45562e23918ccc11ead690bf4f8c89d79b8f27cbdd803182364e4731f9	\\?\C:\Users\kEecfMwgj\Desktop\AHmQqy.mp3, \\?\C:\Users\kEecfMwgj\Desktop\AHmQqy.mp3.06ak3t5y	Modified File	91.68 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
f5fbd8a63a79caeced35a81e9d8c0565d57305b72a65124e6efafd2d96b7f4b2	\\?\C:\Users\kEecfMwgj\Desktop\aUK1ww_cNSEBhOhvD.m4a, \\?\C:\Users\kEecfMwgj\Desktop\aUK1ww_cNSEBhOhvD.m4a.06ak3t5y	Modified File	79.32 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
049305a7938d9602e9a2ce09d232c0682ae21272336e5ee6875291879ff2e4b5	\\?\C:\Users\kEecfMwgj\Desktop\BbBCVRWj6z_JPv.gif, \\?\C:\Users\kEecfMwgj\Desktop\BbBCVRWj6z_JPv.gif.06ak3t5y	Modified File	69.17 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
ce4f0b8a4bb5bd8907ac76f283d460a84e561cc66e58fbdd678db8a39a0ddbac	\\?\C:\Users\kEecfMwgj\Desktop\bs2mYfOv.flv.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\bs2mYfOv.flv	Modified File	27.72 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
966777c0d898e3f5a3d3fe287706530ee097e110ae023c05f12027a4c579bf71	\\?\C:\Users\kEecfMwgj\Desktop\GfJmj4jFVi.png.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\GfJmj4jFVi.png	Modified File	30.93 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
ccad8c864a6117a0450e275674fd37a9f9e9984b6c7a87ba74870be57d0c7006	\\?\C:\Users\kEecfMwgj\Desktop\go3CAcQwWoE5uapCI.mkv, \\?\C:\Users\kEecfMwgj\Desktop\go3CAcQwWoE5uapCI.mkv.06ak3t5y	Modified File	25.74 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
114fb052aa94b083c63d06c7f4d5b9ff19c72248a75b66d8f347373951ea4880	\\?\C:\Users\kEecfMwgj\Desktop\kMECVXsOvLSDJDAOA.ots, \\?\C:\Users\kEecfMwgj\Desktop\kMECVXsOvLSDJDAOA.ots.06ak3t5y	Modified File	40.97 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
4d15e542eae2f2df819ee8b289d7c005b4c3e5c0075b90b914d3992918bfc099	\\?\C:\Users\kEecfMwgj\Desktop\INyfrw9KFObcc0Vbb.bmp.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\INyfrw9KFObcc0Vbb.bmp	Modified File	52.77 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
d65b504669022c0cdc92860694125cc8fc7b9d0467da51d39b0bec093e4c1145	\\?\C:\Users\kEecfMwgj\Desktop\OiotT.jpg, \\?\C:\Users\kEecfMwgj\Desktop\OiotT.jpg.06ak3t5y	Modified File	73.92 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
2234f94fd105f98b96d5f08b2fea369a3f8d729dd172eefb542a627299d10b82	\\?\C:\Users\kEecfMwgj\Desktop\OpD19Ox-5GJ.mp3.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\OpD19Ox-5GJ.mp3	Modified File	4.38 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
c15e2a57a0b33f3fe5284b64e55f455b45861d2e406431f15360953007f4592e	\\?\C:\Users\kEecfMwgj\Desktop\PiM1499-bCIJI-DrwX.flv.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\PiM1499-bCIJI-DrwX.flv	Modified File	73.29 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
0e58b2a75522c549aa7915e560373d573445ca435e1900635859e55ae89507a9	\\?\C:\Users\kEecfMwgj\Desktop\QGtBVOCQPa2FltB11SX3.avi.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\QGtBVOCQPa2FltB11SX3.avi	Modified File	61.69 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
4a55b33aa5210fc0778129368be3175cfedc41c8a75ac62107e94e24179e5c3f	\\?\C:\Users\kEecfMwgj\Desktop\SzGI6-l46QfkV6r.avi.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\SzGI6-l46QfkV6r.avi	Modified File	86.02 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
9c321d080086217ddba8c6376da46121f547f2ffbb0b86bb2045c3ff7ad664d3	\\?\C:\Users\kEecfMwgj\Desktop\whesQdnUMwd_xm-th3g0.gif, \\?\C:\Users\kEecfMwgj\Desktop\whesQdnUMwd_xm-th3g0.gif.06ak3t5y	Modified File	4.49 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
d3bdd294315d1edc806edb694f5092546d632b8b3a963ff4238f82968cc86b01	\\?\C:\Users\kEecfMwgj\Desktop\z8iHCh.bmp, \\?\C:\Users\kEecfMwgj\Desktop\z8iHCh.bmp.06ak3t5y	Modified File	94.11 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
5c51daf77a6f0ad108391ff535032e7eed3980b5894c3e1a9af428af15461c48	\\?\C:\Users\kEecfMwgj\Desktop_CcZccljq.mkv, \\?\C:\Users\kEecfMwgj\Desktop_CcZccljq.mkv.06ak3t5y	Modified File	26.32 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
e2f643d4ab1b4b63b3728283e3108a119296ae2b328e35dfdce0951f38aba9e1	\\?\C:\Users\kEecfMwgj\Documents\-5MKPFwyZwdE.docx, \\?\C:\Users\kEecfMwgj\Documents\-5MKPFwyZwdE.docx.06ak3t5y	Modified File	54.98 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
67a2801a874ec6627b9fcebb582dc091e0c1eabe34c72b5c2c88708b4b87a695	\\?\C:\Users\kEecfMwgj\Documents\07Y-vNHiW6TBEU.odp, \\?\C:\Users\kEecfMwgj\Documents\07Y-vNHiW6TBEU.odp.06ak3t5y	Modified File	17.27 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
afc454f98cb609fdf26a340532f9a781febc92b9ce2bcad8eae449894ac9ff57	\\?\C:\Users\kEecfMwgj\Documents\0ZUqqrgO.ppt.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\0ZUqqrgO.ppt	Modified File	49.14 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ccfb2030ecfa6955db63884ac6ecebf752514155477ec759bb403f03b747f94a	\\?\C:\Users\kEecfMwgj\Documents\3ozabK9D.pptx.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\3ozabK9D.pptx	Modified File	43.97 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
67116f814d18e40cf7afeba930cc778c108fb5ed64859dfbe8ab9341fe8dfebc	\\?\C:\Users\kEecfMwgj\Documents\4cdMBjwoKg.odt.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\4cdMBjwoKg.odt	Modified File	50.20 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
17e857252a8b03c0aafd43ead0b38390a9d323feae244781ae5ff2ba4c199a50	\\?\C:\Users\kEecfMwgj\Documents\5hmdrIDHtVpR.ots.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\5hmdrIDHtVpR.ots	Modified File	52.16 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
a0c71926e2e36c47c0a5c3272f1c88c74aa341861d0df09e4c2f11d159905c18	\\?\C:\Users\kEecfMwgj\Documents\6cY9G.xlsx.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\6cY9G.xlsx	Modified File	18.44 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
2a2cc91e24690da714b2fd58e9b27cf82cb4f4dd675081e289f82fad53cae762	\\?\C:\Users\kEecfMwgj\Documents\6Lo4VggeyxcF04AJM4nt.pptx.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\6Lo4VggeyxcF04AJM4nt.pptx	Modified File	54.55 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
26def8331dd758cd6b6881065ef017ad766b8fbbf770a9e473b3b3e4ba56f8b8	\\?\C:\Users\kEecfMwgj\Documents\9WPMG5w3nojWcs51.docx, \\?\C:\Users\kEecfMwgj\Documents\9WPMG5w3nojWcs51.docx.06ak3t5y	Modified File	82.19 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
d5c3fbb4cb25175050466429 0e55558d4d5462180f26d6bde9295b66f4bd38cc	\\?\C:\Users\kEecfMwgj\Documents\AIEvT4Qz7Bv01ypgZ.pdf.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\AIEvT4Qz7Bv01ypgZ.pdf	Modified File	76.63 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
da8461e90e9fd505e83fcfa255fd3c31ff8305d15f5c1d7ff9d95e00473a4637	\\?\C:\Users\kEecfMwgj\Documents\aORICMsiaM.doc.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\aORICMsiaM.doc	Modified File	8.31 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
a05635cc1b72fd4ed4c99f2f96b0182e33fa359109ffbaa9cb2e141fcab7c07c	\\?\C:\Users\kEecfMwgj\Documents\bOkgUz6.odp.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\bOkgUz6.odp	Modified File	4.40 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
3a839350d67589a6fe8ed62a8b63c8f43d2217a92cc895c3d7ff90891ede6508	\\?\C:\Users\kEecfMwgj\Documents\B_IKnAuj4tm9 PtH.pptx, \\?\C:\Users\kEecfMwgj\Documents\B_IKnAuj4tm9 PtH.pptx.06ak3t5y	Modified File	77.17 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
98b977f2ce9777984986a2c8656562b98ead6277229f47bc9af2192477df4ab5	\\?\C:\Users\kEecfMwgj\Documents\c0s1YUWcSTEroJdKuB.docx, \\?\C:\Users\kEecfMwgj\Documents\c0s1YUWcSTEroJdKuB.docx.06ak3t5y	Modified File	8.61 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
c59e883f7537c3c7bdbf3d7a97a0bb69b9fb936e57747d09ca253763beb9c087	\\?\C:\Users\kEecfMwgj\Documents\chQiNux5apW.csv.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\chQiNux5apW.csv	Modified File	55.37 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
693554545968deba792686622d2416d52937bb45769f60ef64454f30f0af363f	\\?\C:\Users\kEecfMwgj\Documents\D2B5.csv.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\D2B5.csv	Modified File	49.13 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
559d22242652fbca6144e304acaf43d5597c987763cb5a7962451ffa4b68fb21	\\?\C:\Users\kEecfMwgj\Documents\Da8Oppcqp90t.docx, \\?\C:\Users\kEecfMwgj\Documents\Da8Oppcqp90t.docx.06ak3t5y	Modified File	77.94 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
b23c88ad3c51a2a19458ad52685b9a299ff8492cd823b5999200cf720eae3304	\\?\C:\Users\kEecfMwgj\Documents\eB95K8MWD.xlsx, \\?\C:\Users\kEecfMwgj\Documents\eB95K8MWD.xlsx.06ak3t5y	Modified File	77.92 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
25e22dc970a2f921e590b0aec0052146a95dcf8bfe76b5c7a62a0240ddc36615	\\?\C:\Users\kEecfMwgj\Documents\fDhfuRyygxzvH.ods, \\?\C:\Users\kEecfMwgj\Documents\fDhfuRyygxzvH.ods.06ak3t5y	Modified File	28.92 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
c96eb09aef523df5f4e65ddc310fbf3f4f3ad0a9e1b171509b4ebb54129778d5	\\?\C:\Users\kEecfMwgj\Documents\fWYCUggo7eiu Mez.odt, \\?\C:\Users\kEecfMwgj\Documents\fWYCUggo7eiu Mez.odt.06ak3t5y	Modified File	89.35 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
f820c012cc0a9553665d3ea2f58a2095c9709d6d66f496af793a52231d0c1f32	\\?\C:\Users\kEecfMwgj\Documents\GMmGBk5gIcrjM.doc.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\GMmGBk5gIcrjM.doc	Modified File	39.84 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
91041301aa177ced57d970f8999b310776feed3271f1b6a0c6899c8cd0125513	\\?\C:\Users\kEecfMwgj\Documents\Jm6CiFV.pptx.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\Jm6CiFV.pptx	Modified File	61.31 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
3cc5a519c1588053d677b78f3f1631049f20cfa7f41a420b096cccf2347c65c4	\\?\C:\Users\kEecfMwgj\Documents\JM7eM8laWBfHyX5ed.odt.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\JM7eM8laWBfHyX5ed.odt	Modified File	75.48 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
e91ca935445a1b80b03b6dbfa083ecfe0f32524262ea8c59ed5f4d24ebaa746b	\\?\C:\Users\kEecfMwgj\Documents\keforvhV3MOW.docx, \\?\C:\Users\kEecfMwgj\Documents\keforvhV3MOW.docx.06ak3t5y	Modified File	19.12 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
23bc0802a7b8048fd15af94d8f6af1fd88b1be119115215fd32a5e5e91be1bbf	\\?\C:\Users\kEecfMwgj\Documents\LjI6.ods, \\?\C:\Users\kEecfMwgj\Documents\LjI6.ods.06ak3t5y	Modified File	10.36 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
dfe596012ce08c38bf6c54b6ff64004e408ab0b9e154fd19657fc92737a92efa	\\?\C:\Users\kEecfMwgj\Documents\N6MTn7qEK2nADv.odt, \\?\C:\Users\kEecfMwgj\Documents\N6MTn7qEK2nADv.odt.06ak3t5y	Modified File	10.94 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
8da5870e4dbdc4252e43ea6587d4228d886dad3edff6bb3969dc7fbe89421011	\\?\C:\Users\kEecfMwgj\Documents\N8CPfO-zjsOqif.xls.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\N8CPfO-zjsOqif.xls	Modified File	5.14 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
5d00990e24380255a0834943f13e8df5ee7c9198dc144eb87521f16131ad66ab	\\?\C:\Users\kEecfMwgj\Documents\NpJmmrQh0nwG7_pUv.csv.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\NpJmmrQh0nwG7_pUv.csv	Modified File	99.47 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
0744db06634e50d150c875037004f4fe2408ba9d685e39540acef1aa3453e25d	\\?\C:\Users\kEecfMwgj\Documents\OOXxuWoBXn.docx, \\?\C:\Users\kEecfMwgj\Documents\OOXxuWoBXn.docx.06ak3t5y	Modified File	58.24 KB	application/x-dosexec	Create, Delete, Read, Write, Access	CLEAN
847cdb262cff2df8326a99bac1a8a1a75d4e89a51a709a56e4e7e3006f52aca4	\\?\C:\Users\kEecfMwgj\Documents\othZzWJti-TuFa-zMAO.odp.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\othZzWJti-TuFa-zMAO.odp	Modified File	52.08 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
80b297ed424ba8446b99ad1ed65f1d70c8b842da44e543004627da3b77aba9d7	\\?\C:\Users\kEecfMwgj\Documents\pU7xrszOnuj.pptx.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\pU7xrszOnuj.pptx	Modified File	75.78 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
d5fa4631f9936887c2ab53c9a07e81570806c52b1e4627f409fc2292fe0e6e03	\\?\C:\Users\kEecfMwgj\Documents\PuoJ2S5Mug.odp, \\?\C:\Users\kEecfMwgj\Documents\PuoJ2S5Mug.odp.06ak3t5y	Modified File	19.03 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
abb9a94104f074a9013828dee02beb1b4e4532062165b625fab4588d8dde843	\\?\C:\Users\kEecfMwgj\Documents\PWIklR.odp.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\PWIklR.odp	Modified File	93.59 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
cc93759c8c4d2c975542e96695dcfb4aaa7a89448334f5e7022c3e7eb3e8d63c	\\?\C:\Users\kEecfMwgj\Documents\QhYEo-WKA63tNNVSpa.docx.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\QhYEo-WKA63tNNVSpa.docx	Modified File	28.23 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
884f39f9094866f1610f36d06081013cefb6746cd0ca4765b5b3c10d65a3145e	\\?\C:\Users\kEecfMwgj\Documents\RYu7G-GPCGAN4l7O.odp, \\?\C:\Users\kEecfMwgj\Documents\RYu7G-GPCGAN4l7O.odp.06ak3t5y	Modified File	63.56 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
5b2ce592c5f43b390c2112761123843e0a372154935a3996f98aaf6728963591	\\?\C:\Users\kEecfMwgj\Documents\SGiE0.pptx.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\SGiE0.pptx	Modified File	85.54 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
efa55880734e60be91415520272c5838ef7ccf589641d7025c06dadd3e9cd304	\\?\C:\Users\kEecfMwgj\Documents\t4hmzP4sxl.doc.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\t4hmzP4sxl.doc	Modified File	70.76 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
c6f5d37780df8becf6132d742a626902f38f4a7424b2a78b63513ac97e73f6c1	\\?\C:\Users\kEecfMwgj\Documents\TkZtgo9eUgYlcNaPSWIL.xlsx, \\?\C:\Users\kEecfMwgj\Documents\TkZtgo9eUgYlcNaPSWIL.xlsx.06ak3t5y	Modified File	18.07 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
82438b27e593b8148e57a0c73b8a8c8f26bc7f9d08557d58aae93eb8e83ae9ec	\\?\C:\Users\kEecfMwgj\Documents\TQAB2NjEL6JO02B_.xlsx, \\?\C:\Users\kEecfMwgj\Documents\TQAB2NjEL6JO02B_.xlsx.06ak3t5y	Modified File	2.18 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
fd0df9466a4ab5ea7f7acb65247f5326b6ee1dfbc2a4bfacd9f8117b97e208c5	\\?\C:\Users\kEecfMwgj\Documents\TtXfXxvP2sv01dTtReh.docx, \\?\C:\Users\kEecfMwgj\Documents\TtXfXxvP2sv01dTtReh.docx.06ak3t5y	Modified File	95.07 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
6b3e4991ade17151184f911bedd5277406365720a4524d1a755c4fda8fe28bcb	\\?\C:\Users\kEecfMwgj\Documents\U5KwAzHQh Ydz8ltp H.ppt.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\U5KwAzHQh Ydz8ltp H.ppt	Modified File	76.90 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
34f45c25fc4e08325ec83c4813d50164cb19c510d6521a431ea6af5245b47fee	\\?\C:\Users\kEecfMwgj\Documents\uEWQDy-Fw0wiatk6.docx.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\uEWQDy-Fw0wiatk6.docx	Modified File	91.94 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
12cb190c25d44d6dd47bd28b3c64fbfca1c4e2a0c00dd09c433e849b0f88f5b6	\\?\C:\Users\kEecfMwgj\Documents\Xhy8G8l_DiYgdEinCs86.pptx.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\Xhy8G8l_DiYgdEinCs86.pptx	Modified File	55.02 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
2af17b25bb50352fa7905b91ac334379447f88cee030f513c06715d742bf5f70	\\?\C:\Users\kEecfMwgj\Documents\y1Uz_.odt.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\y1Uz_.odt	Modified File	1.52 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
9a67bda257debfac08e7eb4734417ebf498b43109ebf36bd22203e93805df17b	\\?\C:\Users\kEecfMwgj\Documents\yJSmVxafx.pdf, \\?\C:\Users\kEecfMwgj\Documents\yJSmVxafx.pdf.06ak3t5y	Modified File	88.43 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
8f0b11937ebb495f5e085cf273a88816003bb9c30b9f590e60babf220a2940ec	\\?\C:\Users\kEecfMwgj\Documents\yruBBVRJKY.pptx.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\yruBBVRJKY.pptx	Modified File	53.73 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
079a332087e3c3c725bd6ef41c4af2e5d7e6557e3fcc5cd63764144eaca78414	\\?\C:\Users\kEecfMwgj\Documents\Zt_Z1agjCu.xlsx, \\?\C:\Users\kEecfMwgj\Documents\Zt_Z1agjCu.xlsx.06ak3t5y	Modified File	71.10 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
776d586767532b6c1816d15bba3fea7cc259ad1647ec49f5aad26affa74fdeaa	\\?\C:\Users\kEecfMwgj\Music\3MXvqj-GZEArJKONkb_.mp3.06ak3t5y, \\?\C:\Users\kEecfMwgj\Music\3MXvqj-GZEArJKONkb_.mp3	Modified File	10.66 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a1536a2a7e83b32c0830253ce17669df2ae6fe6c20a43d39cba83e80ad1ba7d0	\\?\C:\Users\kEecfMwgj\Music\69rY8_shB.mp3, \\?\C:\Users\kEecfMwgj\Music\69rY8_shB.mp3.06ak3t5y	Modified File	6.93 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
c947ef16fa45dbab14f6310027c9cb7b9210a1bbb98ffa5e8aede741498bb834	\\?\C:\Users\kEecfMwgj\Music\biDq-D.m4a, \\?\C:\Users\kEecfMwgj\Music\biDq-D.m4a.06ak3t5y	Modified File	35.76 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
97233f9a38f58332c2fa313e3911dcbe5a3a3d921249872a71298b7445512612	\\?\C:\Users\kEecfMwgj\Music\dCyh_q8rpkVYgZLK m.wav, \\?\C:\Users\kEecfMwgj\Music\dCyh_q8rpkVYgZLK m.wav.06ak3t5y	Modified File	29.57 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
8c85246dcc4f1f3cae4cc0ec5be00b67544ca0648ef39018b88d264de1da0064	\\?\C:\Users\kEecfMwgj\Music\FrpwP6s.wav, \\?\C:\Users\kEecfMwgj\Music\FrpwP6s.wav.06ak3t5y	Modified File	93.63 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
375c6b01ba4560f68ee5dcc150fed492dde282e6b0367e431bc783c0abe9406a	\\?\C:\Users\kEecfMwgj\Music\fSf1idQOVtocKEOHiEU.m4a, \\?\C:\Users\kEecfMwgj\Music\fSf1idQOVtocKEOHiEU.m4a.06ak3t5y	Modified File	42.10 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
a77f2bf4919945fc24e0bc97fc4441e878d569f7a1209996db8cfa82d4632725	\\?\C:\Users\kEecfMwgj\Music\ht6mcbD4xY51MFFx.mp3, \\?\C:\Users\kEecfMwgj\Music\ht6mcbD4xY51MFFx.mp3.06ak3t5y	Modified File	49.08 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
bd8671df408a3b6a027fa9fa6967a31dca0b07810e0acb6f000d8714f9f6a1ae	\\?\C:\Users\kEecfMwgj\Music\qsI-.m4a, \\?\C:\Users\kEecfMwgj\Music\qsI-.m4a.06ak3t5y	Modified File	96.68 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
119f9f916a2f92e43fb232864f883191fb4e9f6124973d105d435bdf56ac096a	\\?\C:\Users\kEecfMwgj\Music\tCh9inH.mp3, \\?\C:\Users\kEecfMwgj\Music\tCh9inH.mp3.06ak3t5y	Modified File	7.17 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
b42a5d4086d6ff22ea2896c02505da010f1474cfb40f0a5e2512932ebe7cdccd	\\?\C:\Users\kEecfMwgj\Music\tzURC8_ZHJox8cSSbC.wav, \\?\C:\Users\kEecfMwgj\Music\tzURC8_ZHJox8cSSbC.wav.06ak3t5y	Modified File	17.52 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
d5a6be05bcaa380a36952334ae756ca14746dd4e5de2769277a231d522cf7115	\\?\C:\Users\kEecfMwgj\Music\XUfUzf.mp3, \\?\C:\Users\kEecfMwgj\Music\XUfUzf.mp3.06ak3t5y	Modified File	3.68 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
ff958cf37cb724773b117c5642a2e49585655cb60d2b6f2130c51220c92dd0d9	\\?\C:\Users\kEecfMwgj\Music\zYUG2.m4a, \\?\C:\Users\kEecfMwgj\Music\zYUG2.m4a.06ak3t5y	Modified File	97.03 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
d23a21a44f27d9204b4807c3189927f446f13bc4479e511dc5e5ead4564dcfa2	\\?\C:\Users\kEecfMwgj\Pictures\4ldTijNb5enuQ.bmp, \\?\C:\Users\kEecfMwgj\Pictures\4ldTijNb5enuQ.bmp.06ak3t5y	Modified File	8.53 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
58777a3de0532dd9a98768fbe5a5b75cbf02615777f0f438f6846d0b36c8857b	\\?\C:\Users\kEecfMwgj\Pictures\h1WR8r.bmp.06ak3t5y, \\?\C:\Users\kEecfMwgj\Pictures\h1WR8r.bmp	Modified File	4.80 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
0b0ba7bf5e967803b37fe794252bfb2ab4a2c15824954912ef83827f49ab8383	\\?\C:\Users\kEecfMwgj\Pictures\hreakSGbo7iehUMhp.jpg.06ak3t5y, \\?\C:\Users\kEecfMwgj\Pictures\hreakSGbo7iehUMhp.jpg	Modified File	91.64 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
dbc161813070b579ef67264575b053ec1ccc75e47e42eededd0119fbbe2c4db8	\\?\C:\Users\kEecfMwgj\Videos\7oacghL0FgM.mp4.06ak3t5y, \\?\C:\Users\kEecfMwgj\Videos\7oacghL0FgM.mp4	Modified File	31.23 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
65a34920b26ab7c6c911f3e308bc557ad263a6c0f6883c81d7a8db40a31f7104	\\?\C:\Users\kEecfMwgj\Videos\DdzxhrbP8S7OSzK7gvx-.avi.06ak3t5y, \\?\C:\Users\kEecfMwgj\Videos\DdzxhrbP8S7OSzK7gvx-.avi	Modified File	19.27 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
35196e0258e02feddd4e07105ba7440c35a9a1b1bac6bfe11f92f239b75b0273	\\?\C:\Users\kEecfMwgj\Videos\OGP0BLXkOZqfcLE5 r.avi.06ak3t5y, \\?\C:\Users\kEecfMwgj\Videos\OGP0BLXkOZqfcLE5 r.avi	Modified File	35.13 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
13b5cce9f0e2230a4c1fe1d67f805709475db14fb7e503cb1e0d9fbf03e49836	\\?\C:\Users\kEecfMwgj\Videos\PNp9VEShM5vJa6UfKU.mkv.06ak3t5y, \\?\C:\Users\kEecfMwgj\Videos\PNp9VEShM5vJa6UfKU.mkv	Modified File	49.06 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
9fe6ef3e23ec8015220a1255b0ee54ebeb7625e42cbc3a3a3e4f50b5cbda951a	\\?\C:\Users\Public\Libraries\RecordedTV.library-ms, \\?\C:\Users\Public\Libraries\RecordedTV.library-ms.06ak3t5y	Modified File	1.07 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
507dce298eda77dff66efd0a6d121d88ec0362093f4482338b40c6f7ab4521cb	\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\5PIGlZaCV4jqbsV7K0Fu.mp3, \\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\5PIGlZaCV4jqbsV7K0Fu.mp3.06ak3t5y	Modified File	86.70 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
3647ff08d1bc14989c2d2dc72f1d97cb69b8cfa62a6e9af30902aef5db8af074	\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\divc1VvDFB.mkv.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\divc1VvDFB.mkv	Modified File	60.29 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
5c16605dbb18c7b7650cf69ec033e60286fc9c65f0cf3b322845b2c7f66fa7ab	\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\qWum TA_.mp4, \\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\qWum TA_.mp4.06ak3t5y	Modified File	8.08 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
b50970e523bf2f5e8ad208377805815c052bd77c4ab5a765648178190d727590	\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\x4 v.gif.06ak3t5y, \\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\x4 v.gif	Modified File	27.31 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
569d157fab1086e7d1d4ff9923e864299eff1acc8ab696c778317c8fcc01d3ba	\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\ZAR5gyQrXl.gif, \\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\ZAR5gyQrXl.gif.06ak3t5y	Modified File	65.87 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
1e2fc688461453c0ba73a686518d65aef8921c29f6f0d202996a99860c4ad7eb	\\?\C:\Users\kEecfMwgj\Documents\Outlook Files\franc@gdllo.de.pst.06ak3t5y, \\?\C:\Users\kEecfMwgj\Documents\Outlook Files\franc@gdllo.de.pst	Modified File	265.22 KB	application/x-dosexec	Create, Delete, Read, Write, Access	CLEAN
873eef8c60e187e26bbb1199cbef7545d659e79f2a7e1a6f49e5ec97c45e08a4	\\?\C:\Users\kEecfMwgj\Favorites\Links\Web Slice Gallery.url.06ak3t5y, \\?\C:\Users\kEecfMwgj\Favorites\Links\Web Slice Gallery.url	Modified File	450 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
323a8e53450197db59b98dc67b2840eb630144885daea1bce4df552c8c4dc8e6	\\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE Add-on site.url.06ak3t5y, \\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE Add-on site.url	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
d0b870d2a4ef1a8c6adfebabf4f30254f2241f7b2fc9d7a08f6d77ddfa1ec570	\\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE site on Microsoft.com.url, \\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE site on Microsoft.com.url.06ak3t5y	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
af6ce02b553c1fda8ef7b062940f9a7c37c2a90d0197e0da9306635c3928bd48	\\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Home.url, \\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Home.url.06ak3t5y	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c3a004e0e1587eb1e6c7c8202a884d885b7cd831b6af4f0e81da4f75086a4fe5	\\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Work.url.06ak3t5y, \\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Work.url	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
4d838949c541c5b8f89852159531741d9d6e055f1e52f0ea0a8b67e96e17c07d	\\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url.06ak3t5y, \\?\C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url	Modified File	358 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
3d0c834d5892d9da460aec5ad3c72e4d9d4240b6e15b7183dff017e860e7632d	\\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Autos.url.06ak3t5y, \\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Autos.url	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
f5a141c7a0c3e43de470dc6ce90a378aa8e1601ffcc1c00f6db316687cfd8082	\\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Entertainment.url.06ak3t5y, \\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Entertainment.url	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
82a283af24d3a3e14a5d3074b51bbd6fe37be324690fce897c28741a0d3faf06	\\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url, \\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url.06ak3t5y	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
346c19dc853ee699f841e4066ebed96638db26f349b797ad4dff958934eef6f9	\\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Sports.url.06ak3t5y, \\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Sports.url	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
b92db62a4199059f8745cb00b837bbb4b735cc68e723fdab2e6dbb4586ab6529	\\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN.url, \\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN.url.06ak3t5y	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
8c9796a7c3b8f1d5a9f4ae07e7181ed6098668ce98e24ab828fec01e22b61589	\\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSNBC News.url.06ak3t5y, \\?\C:\Users\kEecfMwgj\Favorites\MSN Websites\MSNBC News.url	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
81abfb706902258d02f519df2ea32420fddc12b8dc34ef2824b7057d5e292b27	\\?\C:\Users\kEecfMwgj\Favorites\Windows Live\Get Windows Live.url, \\?\C:\Users\kEecfMwgj\Favorites\Windows Live\Get Windows Live.url.06ak3t5y	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
9f32c4b6849a1b7ba27c6cea6a243b578385cab5d334a823794cf5862b517490	\\?\C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Gallery.url.06ak3t5y, \\?\C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Gallery.url	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
a31eeba32c619c2495760e7c379027c4adb836138615f79c7efb363004105bc6	\\?\C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Mail.url.06ak3t5y, \\?\C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Mail.url	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
5735fbb5a0aacbcc90e188c848d01fa7d0e62942322e136e0bc3da0536851c84	\\?\C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Spaces.url.06ak3t5y, \\?\C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Spaces.url	Modified File	357 bytes	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
653c72e1fb39e3c85382f5560a2b443b4f034bbaadc92c19f66f209146bae9d2	\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\bjOydzw.mp3, \\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\bjOydzw.mp3.06ak3t5y	Modified File	100.10 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
09a42b146f9b888342fd537d2485ed57980ff6e19b3c92979a9df1ab6b91d917	\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\oCfLIu3p.mp3.06ak3t5y, \\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\oCfLIu3p.mp3	Modified File	70.34 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ab85e3f0d997d2c3e9764075bbec433c15465480ed76d36be47980824391215d	\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\rPi6ROENBl.mp3.06ak3t5y, \\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\rPi6ROENBl.mp3	Modified File	80.94 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
ec49b63cae866b86170cef02b93ee41ebf4a88423fa288eb293de4657806950a	\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\SsOycCq2y.wav.06ak3t5y, \\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\SsOycCq2y.wav	Modified File	79.01 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
c83feba1964a55cbdac6af54e1a2b4296718b1791780f517cac21f6a905d0dc0	\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\z-ZcHxTcO3xPAhZK.wav, \\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\z-ZcHxTcO3xPAhZK.wav.06ak3t5y	Modified File	5.91 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
6dc1b2348091effd32db93df8653cec9bcd77ccc26f65f566dadf9e64018ea62	\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\zZYA2Sg.mp3, \\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\zZYA2Sg.mp3.06ak3t5y	Modified File	87.71 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
68c380fa85a1ca8a4daf62aecf8ef285b58aded7413145b65c8c730b8c10fa66	\\?\C:\Users\kEecfMwgj\Music\Rqx5DrLsWGq0fuHce-F\SdfXT.m4a, \\?\C:\Users\kEecfMwgj\Music\Rqx5DrLsWGq0fuHce-F\SdfXT.m4a.06ak3t5y	Modified File	45.15 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
a374b2eef2432d7feb048bd2c4fb8a784385dd559987fba439e4764a95a5fe5d	\\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou\-a8C ZzQY9ibDt.bmp, \\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou\-a8C ZzQY9ibDt.bmp.06ak3t5y	Modified File	79.31 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
4954f950d5770ca570aad97634116a93aa13e02d48bbae20f1bc52e91a139d85	\\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou\2pIHI6dW1Tj.png, \\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou\2pIHI6dW1Tj.png.06ak3t5y	Modified File	75.47 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
fae7a8a48a1541d60a63f0d7fa96f32986eeac5e4904482299d09e6abda37db6	\\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou\8kI9nfrKhl_-hQ6.gif.06ak3t5y, \\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou\8kI9nfrKhl_-hQ6.gif	Modified File	69.97 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
cf6178222beb895985078fe746218077d754ff29a99028e144d598869a07e090	\\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou\vuFOrfu.png, \\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou\vuFOrfu.png.06ak3t5y	Modified File	2.68 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
6a496af44bbf0ad53b46deb9c15b2602ef7c2d1c10d22793b3467556d12908e5	\\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou_hY-b8CF6iv.png.06ak3t5y, \\?\C:\Users\kEecfMwgj\Pictures\BL2lkdvDBou_hY-b8CF6iv.png	Modified File	42.09 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
6f93fd7b1f7335bb4ea41049103a99aaca6d2e3bc2cb3b546e25b72367aaddd3	\\?\C:\Users\kEecfMwgj\Videos\exYTCaRLnxwOjYPkpp\BCVRhXmdcBbj0.avi.06ak3t5y, \\?\C:\Users\kEecfMwgj\Videos\exYTCaRLnxwOjYPkpp\BCVRhXmdcBbj0.avi	Modified File	68.35 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
6b8b6bb2a62bfc3099b2dc6fdc5360fa1dded4ac8936d75f3264574f6d6d4f2e	\\?\C:\Users\kEecfMwgj\Videos\exYTCaRLnxwOjYPkpp\d_wE.flv.06ak3t5y, \\?\C:\Users\kEecfMwgj\Videos\exYTCaRLnxwOjYPkpp\d_wE.flv	Modified File	38.54 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
004775241a242fabeabbf80a9ad326a3eaf4a013061d9ad98acca4cf551bbff6	\\?\C:\Users\kEecfMwgj\Videos\exYTCaRLnxwOjYPkpp\VG-iIm5P4w8rjZV.mp4.06ak3t5y, \\?\C:\Users\kEecfMwgj\Videos\exYTCaRLnxwOjYPkpp\VG-iIm5P4w8rjZV.mp4	Modified File	54.15 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
4ea4ad06839108e98e47bae0df182a2726bedf024c8baeffae19c70049a33b75	\\?\C:\Users\kEecfMwgj\Videos\exYTCaRLnxwOjYPkpp\X9RHt4PkF8UQ.flv.06ak3t5y, \\?\C:\Users\kEecfMwgj\Videos\exYTCaRLnxwOjYPkpp\X9RHt4PkF8UQ.flv	Modified File	24.92 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b43e8d4e5f720ff0f8aaed940341128a4dbd0cfd3aad35bfe9440dd73e69f0ed	\\?\C:\Users\kEecfMwgj\Videos\exYTCaRLnxwOjYPkpp\YjACMF.flv, \\?\C:\Users\kEecfMwgj\Videos\exYTCaRLnxwOjYPkpp\YjACMF.flv.06ak3t5y	Modified File	46.94 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
690614eb882fcbc2e29a419d65d7ad1fa07e1025c69ad21d8dd85aa3a4dfaeaa	\\?\C:\Users\Public\Music\Sample Music\Kalimba.mp3.06ak3t5y, \\?\C:\Users\Public\Music\Sample Music\Kalimba.mp3	Modified File	8217.45 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
69759b44c56199492594f1836158630225d2431f550c7e946b6d714844397f17	\\?\C:\Users\Public\Music\Sample Music\Maid with the Flaxen Hair.mp3.06ak3t5y, \\?\C:\Users\Public\Music\Sample Music\Maid with the Flaxen Hair.mp3	Modified File	4017.67 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
afcabea0b6130146713ae593a98096f15454d1f19c0421c590c2dd96a9ba47c8	\\?\C:\Users\Public\Music\Sample Music\Sleep Away.mp3.06ak3t5y, \\?\C:\Users\Public\Music\Sample Music\Sleep Away.mp3	Modified File	4729.31 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
9b428ee044eed278a37b7461e3039811ad2604502c6410e7bc3089dbf6b44991	\\?\C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg.06ak3t5y, \\?\C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg	Modified File	859.00 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
37b89a8e3393ca1495ca9e19e744a371be19a1df81bff8a4089f85e9c5f7bf48	\\?\C:\Users\Public\Pictures\Sample Pictures\Desert.jpg.06ak3t5y, \\?\C:\Users\Public\Pictures\Sample Pictures\Desert.jpg	Modified File	826.33 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
079cb30e080b7430c51f1baf49b67a615de30db4fdd436e4adbfe377791ee4b6	\\?\C:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg, \\?\C:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg.06ak3t5y	Modified File	581.55 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
a6f3a8150b83b5349b9e2683488e730c54f629028e59df122532232e8f3fc64a	\\?\C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg, \\?\C:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg.06ak3t5y	Modified File	757.74 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
95826142faa9e455deb455868ae5d60386c01469f66b7925c395fe940dca97e7	\\?\C:\Users\Public\Pictures\Sample Pictures\Koala.jpg, \\?\C:\Users\Public\Pictures\Sample Pictures\Koala.jpg.06ak3t5y	Modified File	762.75 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
4d1d5c2a3bfbeccaac161b60827e0e983eaf46a547ea0cb9ce76365574b40258	\\?\C:\Users\Public\Pictures\Sample Pictures\Lighthouse.jpg.06ak3t5y, \\?\C:\Users\Public\Pictures\Sample Pictures\Lighthouse.jpg	Modified File	548.34 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
a55aaae0a42c050792245516c39df8a931331febb36a9e5a08fd7c2866f4ea29	\\?\C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg, \\?\C:\Users\Public\Pictures\Sample Pictures\Penguins.jpg.06ak3t5y	Modified File	759.82 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
accaf758c7c8f80cd99f389497e9cb14891b9bb4eef1b173ae198849ff2ea2db	\\?\C:\Users\Public\Pictures\Sample Pictures\Tulips.jpg, \\?\C:\Users\Public\Pictures\Sample Pictures\Tulips.jpg.06ak3t5y	Modified File	606.55 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
dae71252d063abe5737beb07878899ae1b943f0d470925bf8a057421e406fd1e	\\?\C:\Users\Public\Recorded TV\Sample Media\win7_scenic-demoshort_raw.wtv.06ak3t5y, \\?\C:\Users\Public\Recorded TV\Sample Media\win7_scenic-demoshort_raw.wtv	Modified File	9472.22 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
8ba2db38de87b3b8c3592c06c7f0c7277643dcbee0965a519e1c45e5382cf9db	\\?\C:\Users\Public\Videos\Sample Videos\Wildlife.wmv, \\?\C:\Users\Public\Videos\Sample Videos\Wildlife.wmv.06ak3t5y	Modified File	10240.00 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
2f79e518725d4ca4376642ad2af726b43fdfd5957ace971f2d8c98b4f0fee518	\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\-9rGFqsYF62c2hsP.mp3, \\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\-9rGFqsYF62c2hsP.mp3.06ak3t5y	Modified File	13.44 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
3888ede534a4ea8cde03157d5c11c19f866919207c3d794a4a0e566f95632298	\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\a48Mjh2iTKB2.mkv, \\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\a48Mjh2iTKB2.mkv.06ak3t5y	Modified File	16.51 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b4d4ff3c6e8c050afd1b5ad9c7b5dbe000d4f0cf718cac4933221ba9cb8c3081	\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\pdbwVn-Lz4hgbH1S6sRs.bmp, \\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\pdbwVn-Lz4hgbH1S6sRs.bmp.06ak3t5y	Modified File	65.56 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
0f30f75d5f648c70402d2232bf10b7b29d60ad03ab3fa518f8469f41528bbe83	\\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\WsOU.gif, \\?\C:\Users\kEecfMwgj\Desktop\aJV56WBKgKcY0uVz\Nmla9n22s\WsOU.gif.06ak3t5y	Modified File	56.01 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN
fb3e045ef6fea3562a87f41ae15231f8dab25e76115e1cf8893baa2ee9a2825f	\\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\alGqygXdyMjy5o\aZ3qnO44VBmYATaQO.m4a, \\?\C:\Users\kEecfMwgj\Music\EFD45sbjBLnjkaNBD8U_\alGqygXdyMjy5o\aZ3qnO44VBmYATaQO.m4a.06ak3t5y	Modified File	14.17 KB	application/octet-stream	Create, Delete, Read, Write, Access	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
\\?\C:\Users\kEecfMwgj\06ak3t5y-readme.txt	Dropped File	Create, Write, Access	SUSPICIOUS
C:\Users\kEecfMwgj\Desktop\sodinokibi.exe	Sample File	Access	CLEAN
C:\Windows\system32\win32kfull.sys	Accessed File	Access	CLEAN
C:\Windows\system32\win32k.sys	Accessed File	Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_hid-user.resources_31bf3856ad364e35_6.1.7600.16385_en-us_c19781a304e374a4.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_hid-user.resources_31bf3856ad364e35_6.1.7600.16385_en-us_c19781a304e374a4_hid.dll.mui_cccd5ae0	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_hid-user.resources_31bf3856ad364e35_6.1.7600.16385_en-us_c19781a304e374a4_hidserv.dll.mui_561adfc8	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..ce-router.resources_31bf3856ad364e35_6.1.7600.16385_en-us_243862f6e4997dad.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..ce-router.resources_31bf3856ad364e35_6.1.7600.16385_en-us_243862f6e4997dad_activeds.dll.mui_67414db4	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..core-base.resources_31bf3856ad364e35_6.1.7600.16385_en-us_c620663a0d83d04f.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..core-base.resources_31bf3856ad364e35_6.1.7600.16385_en-us_c620663a0d83d04f_winmm.dll.mui_224f6445	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..ence-infrastructure_31bf3856ad364e35_6.1.7601.17514_none_3337092d63596104.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..ence-infrastructure_31bf3856ad364e35_6.1.7601.17514_none_3337092d63596104_aelupsvc.dll_f420497b	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..ence-infrastructure_31bf3856ad364e35_6.1.7601.17514_none_3337092d63596104_apphelp.dll_7ce69c4a	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..ence-infrastructure_31bf3856ad364e35_6.1.7601.17514_none_3337092d63596104_sdbinst.exe_8725e339	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..ence-infrastructure_31bf3856ad364e35_6.1.7601.17514_none_3337092d63596104_shimeng.dll_2036b947	Accessed File	Delete, Access	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..es-interface-router_31bf3856ad364e35_6.1.7600.16385_none_b3eaf84f983a33ee.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..es-interface-router_31bf3856ad364e35_6.1.7600.16385_none_b3eaf84f983a33ee_activeds.dll_662643d7	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..es-interface-router_31bf3856ad364e35_6.1.7600.16385_none_b3eaf84f983a33ee_activeds.tlb_662648dd	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..llservice.resources_31bf3856ad364e35_6.1.7600.16385_en-us_b9c303c8bce24ecf.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..llservice.resources_31bf3856ad364e35_6.1.7600.16385_en-us_b9c303c8bce24ecf_axinstsv.dll.mui_be092a2d	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..llservice.resources_31bf3856ad364e35_6.1.7600.16385_en-us_b9c303c8bce24ecf_axinstui.exe.mui_aea34130	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..on-authui.resources_31bf3856ad364e35_6.1.7600.16385_en-us_e7718915b6ba8195.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..on-authui.resources_31bf3856ad364e35_6.1.7600.16385_en-us_e7718915b6ba8195_authui.dll.mui_19b92789	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..structure.resources_31bf3856ad364e35_6.1.7600.16385_en-us_541d3a4db051d913.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..structure.resources_31bf3856ad364e35_6.1.7600.16385_en-us_541d3a4db051d913_aelupsvc.dll.mui_5d6cb110	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..structure.resources_31bf3856ad364e35_6.1.7600.16385_en-us_541d3a4db051d913_apphelp.dll.mui_59096153	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-a..structure.resources_31bf3856ad364e35_6.1.7600.16385_en-us_541d3a4db051d913_sdbinst.exe.mui_258ad624	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-acledit.resources_31bf3856ad364e35_6.1.7600.16385_en-us_853b0789da5b1e2a.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-acledit.resources_31bf3856ad364e35_6.1.7600.16385_en-us_853b0789da5b1e2a_acledit.dll.mui_5f932ccb	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-acledit_31bf3856ad364e35_6.1.7600.16385_none_c3d671ef7642fced.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-acledit_31bf3856ad364e35_6.1.7600.16385_none_c3d671ef7642fced_acledit.dll_89da72d2	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-aclui.resources_31bf3856ad364e35_6.1.7600.16385_en-us_9dc6c5d5ca9cbc28.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-aclui.resources_31bf3856ad364e35_6.1.7600.16385_en-us_9dc6c5d5ca9cbc28_aclui.dll.mui_adadbfb7	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-aclui_31bf3856ad364e35_6.1.7600.16385_none_b0ff4fc4cd57c163.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-aclui_31bf3856ad364e35_6.1.7600.16385_none_b0ff4fc4cd57c163_aclui.dll_ebee9df6	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-acproxy_31bf3856ad364e35_6.1.7600.16385_none_520444733f7b8add.manifest	Accessed File	Delete, Access	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-acproxy_31bf3856ad364e35_6.1.7600.16385_none_520444733f7b8add_acproxy.dll_5d65b262	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-activexcompat_31bf3856ad364e35_8.0.7601.17514_none_6f29eb5391300db2.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-activexproxy_31bf3856ad364e35_6.1.7601.17514_none_703438df00e9e0d7.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-activexproxy_31bf3856ad364e35_6.1.7601.17514_none_703438df00e9e0d7_actxprxy.dll_82133921	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-advapi32.resources_31bf3856ad364e35_6.1.7600.16385_en-us_747e69daca85f63e.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-advapi32.resources_31bf3856ad364e35_6.1.7600.16385_en-us_747e69daca85f63e_advapi32.dll.mui_28c7718f	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-advapi32_31bf3856ad364e35_6.1.7600.16385_none_3f3d4351a032bf57.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-advapi32_31bf3856ad364e35_6.1.7600.16385_none_3f3d4351a032bf57_advapi32.dll_9512793c	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-agpsettings_31bf3856ad364e35_6.1.7600.16385_none_cb02d84df678436e.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-appid.resources_31bf3856ad364e35_6.1.7600.16385_en-us_921f7aaac68bcb70.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-appid.resources_31bf3856ad364e35_6.1.7600.16385_en-us_921f7aaac68bcb70_appidapi.dll.mui_b6af37bb	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-appid.resources_31bf3856ad364e35_6.1.7600.16385_en-us_921f7aaac68bcb70_appidsvc.dll.mui_6717e231	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-appid_31bf3856ad364e35_6.1.7601.18741_none_b54e921cc8e1f204.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-appid_31bf3856ad364e35_6.1.7601.18741_none_b54e921cc8e1f204_appid-ppdlic.xrm-ms_67ebc09b	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-appid_31bf3856ad364e35_6.1.7601.18741_none_b54e921cc8e1f204_appid.sys_fe1d01e3	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-appid_31bf3856ad364e35_6.1.7601.18741_none_b54e921cc8e1f204_appidapi.dll_affa6810	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-appid_31bf3856ad364e35_6.1.7601.18741_none_b54e921cc8e1f204_appidcertstorecheck.exe_03352f5f	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-appid_31bf3856ad364e35_6.1.7601.18741_none_b54e921cc8e1f204_appidpolicyconverter.exe_83972af0	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-appid_31bf3856ad364e35_6.1.7601.18741_none_b54e921cc8e1f204_appidsvc.dll_b571c01a	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-atl_31bf3856ad364e35_6.1.7600.16385_none_0715316d7363738e.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-atl_31bf3856ad364e35_6.1.7600.16385_none_0715316d7363738e_atl.dll_0c7220db	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-audio-mmecore-base_31bf3856ad364e35_6.1.7600.16385_none_11d4ade16b61222e.manifest	Accessed File	Delete, Access	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-audio-mmecore-base_31bf3856ad364e35_6.1.7600.16385_none_11d4ade16b61222e_winmm.dll_08d4f5e8	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-authentication-authui_31bf3856ad364e35_6.1.7601.17514_none_6a1982860c076c38.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-authentication-authui_31bf3856ad364e35_6.1.7601.17514_none_6a1982860c076c38_authui.dll_05ff9fd2	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-authentication-authui_31bf3856ad364e35_6.1.7601.17514_none_6a1982860c076c38_authui.ptxml_399d39fd	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-axinstallservice_31bf3856ad364e35_6.1.7601.17514_none_352b5454878cd498.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-axinstallservice_31bf3856ad364e35_6.1.7601.17514_none_352b5454878cd498_axinstsv.dll_ebc2b91e	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-axinstallservice_31bf3856ad364e35_6.1.7601.17514_none_352b5454878cd498_axinstui.exe_eba3b15b	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..endencies.resources_31bf3856ad364e35_6.1.7600.16385_en-us_06b4240709238ea6.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..environment-windows_31bf3856ad364e35_6.1.7601.18741_none_c73b18fba3854417.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..environment-windows_31bf3856ad364e35_6.1.7601.18741_none_c73b18fba3854417_setbcdlocale.dll_77bec53b	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..environment-windows_31bf3856ad364e35_6.1.7601.18741_none_c73b18fba3854417_winload.efi_75834aa0	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..environment-windows_31bf3856ad364e35_6.1.7601.18741_none_c73b18fba3854417_winload.exe_75835076	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..environment-windows_31bf3856ad364e35_6.1.7601.18741_none_c73b18fba3854417_winresume.efi_85cd069f	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..environment-windows_31bf3856ad364e35_6.1.7601.18741_none_c73b18fba3854417_winresume.exe_85cd1215	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..gertransport-serial_31bf3856ad364e35_6.1.7600.16385_none_6daa7ec5c65bf5bc.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..gertransport-serial_31bf3856ad364e35_6.1.7600.16385_none_6daa7ec5c65bf5bc_kdcom.dll_db5e7744	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..iagnostic.resources_31bf3856ad364e35_6.1.7600.16385_en-us_12de4907a4bd1cfc.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..iagnostic.resources_31bf3856ad364e35_6.1.7600.16385_en-us_12de4907a4bd1cfc_memtest.efi.mui_71e15c22	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..ironment-dvd-efisys_31bf3856ad364e35_6.1.7601.17514_none_c0c6eceaf97c4827.manifest	Accessed File	Delete, Access	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..ironment-dvd-efisys_31bf3856ad364e35_6.1.7601.17514_none_c0c6eceaf97c4827_efisys.bin_0bfd8f26	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..isc-tools.resources_31bf3856ad364e35_6.1.7600.16385_en-us_3f3bc9163ae8cff9.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..isc-tools.resources_31bf3856ad364e35_6.1.7600.16385_en-us_3f3bc9163ae8cff9_expand.exe.mui_3f54e013	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..isc-tools.resources_31bf3856ad364e35_6.1.7600.16385_en-us_3f3bc9163ae8cff9_netmsg.dll.mui_ab0f7c73	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_cs-cz_97769b281ba398b8.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_cs-cz_97769b281ba398b8_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_cs-cz_97769b281ba398b8_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_da-dk_34b07b4f11e994b7.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_da-dk_34b07b4f11e994b7_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_da-dk_34b07b4f11e994b7_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_de-de_31dc108b13bfe951.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_de-de_31dc108b13bfe951_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_de-de_31dc108b13bfe951_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_el-gr_da723e1e02d551df.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_el-gr_da723e1e02d551df_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_el-gr_da723e1e02d551df_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_en-us_dacce684029df516.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_en-us_dacce684029df516_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_en-us_dacce684029df516_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_es-es_da98436802c4e6bb.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_es-es_da98436802c4e6bb_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_es-es_da98436802c4e6bb_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_fi-fi_79b34814f7ded8e5.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_fi-fi_79b34814f7ded8e5_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_fi-fi_79b34814f7ded8e5_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_fr-fr_7d4fb966f596fd1d.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_fr-fr_7d4fb966f596fd1d_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_fr-fr_7d4fb966f596fd1d_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_hu-hu_c4c039aed9f6cc39.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_hu-hu_c4c039aed9f6cc39_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_hu-hu_c4c039aed9f6cc39_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_it-it_6777afadccc8e29b.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_it-it_6777afadccc8e29b_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_it-it_6777afadccc8e29b_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_ja-jp_099d2ebabfe3f476.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_ja-jp_099d2ebabfe3f476_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_ja-jp_099d2ebabfe3f476_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_ko-kr_ad070b6fb254bb8c.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_ko-kr_ad070b6fb254bb8c_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_ko-kr_ad070b6fb254bb8c_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_nb-no_95998ca48a79e748.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_nb-no_95998ca48a79e748_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_nb-no_95998ca48a79e748_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_nl-nl_93d8d7e28ba5f11d.manifest	Accessed File	Delete, Access	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_nl-nl_93d8d7e28ba5f11d_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_nl-nl_93d8d7e28ba5f11d_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_pl-pl_da15326470c85ed1.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_pl-pl_da15326470c85ed1_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_pl-pl_da15326470c85ed1_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_pt-br_dc691d086f51f2b5.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_pt-br_dc691d086f51f2b5_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_pt-br_dc691d086f51f2b5_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_pt-pt_dd4aec746ec16291.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_pt-pt_dd4aec746ec16291_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_pt-pt_dd4aec746ec16291_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_ru-ru_23edfe3853a2f0bd.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_ru-ru_23edfe3853a2f0bd_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_ru-ru_23edfe3853a2f0bd_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_sv-se_bfe8e8ad4acbfb18.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_sv-se_bfe8e8ad4acbfb18_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_sv-se_bfe8e8ad4acbfb18_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_tr-tr_68f632f43987fd09.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_tr-tr_68f632f43987fd09_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_tr-tr_68f632f43987fd09_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_zh-cn_3a5350f1e9bfcf28.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_zh-cn_3a5350f1e9bfcf28_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_zh-cn_3a5350f1e9bfcf28_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_zh-hk_38fe497fea9b41b8.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_zh-hk_38fe497fea9b41b8_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_zh-hk_38fe497fea9b41b8_bootmgr.efi.mui_be5d0075	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_zh-tw_3e4f8e47e730ab98.manifest	Accessed File	Delete, Access	CLEAN
\\?\C:\Windows\winsxs\Backup\amd64_microsoft-windows-b..nager-efi.resources_31bf3856ad364e35_6.1.7600.16385_zh-tw_3e4f8e47e730ab98_bootmgfw.efi.mui_a6e78cfa	Accessed File	Delete, Access	CLEAN

Reduced dataset

Mutex

Name	Operations	Parent Process Name	Verdict
Global\DAE678E1-967E-6A19-D564-F7FCA6E7AEBC	access	sodinokibi.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\recfg	create, access	sodinokibi.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\recfg	create, access	sodinokibi.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\recfg\pk_key	write, access	sodinokibi.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\recfg\sk_key	write, access	sodinokibi.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\recfg\0_key	write, access	sodinokibi.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\recfg\rnd_ext	read, write, access	sodinokibi.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters	access	sodinokibi.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Domain	read, access	sodinokibi.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\International	access	sodinokibi.exe	CLEAN
HKEY_CURRENT_USER\Control Panel\International\LocaleName	read, access	sodinokibi.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	sodinokibi.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\productName	read, access	sodinokibi.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\recfg\stat	read, write, access	sodinokibi.exe	CLEAN

Process

Process Name	Commandline	Verdict
sodinokibi.exe	"C:\Users\kEecfMwgj\Desktop\sodinokibi.exe"	MALICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures	SUSPICIOUS
vssadmin.exe	vssadmin.exe Delete Shadows /All /Quiet	CLEAN
vssvc.exe	C:\Windows\system32\vssvc.exe	CLEAN

YARA / AV

YARA (17)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5
Ransomware	Sodinokibi_CVE_2018_8453	Sodinokibi Ransomware using CVE-2018-8453	Memory Dump	-	-	5/5

Antivirus (15)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.Brsecmon.1	C:\Users\kEecfMwgj\Desktop\sodinokibi.exe	MALICIOUS
Memory Dump	Trojan.Brsecmon.1	-	MALICIOUS
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS

File Type	Threat Name	File Name	Verdict
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS
Memory Dump	Generic.Ransom.Sodinokibi.F8A01CC1	-	MALICIOUS

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

Analyzer Information

Analyzer Version	4.2.2
Dynamic Engine Version	4.2.2 / 06/07/2021 03:43
Static Engine Version	4.2.2.0
Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-07-03 15:03:48+00:00
AV Exceptions Version	4.2.2.13 / 2021-06-02 18:07:39
VTI Ruleset Version	4.2.2.27 / 2021-06-28 06:25:30
YARA Built-in Ruleset Version	4.2.2.18
Link Detonation Heuristics Version	-
Signature Trust Store Version	4.2.2.13 / 2021-06-02 18:07:39
Analysis Report Layout Version	10

Software Information

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