MALICIOUS

Classifications: Spyware | Ransomware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe**
ID	#4194433
MD5	cf6ff9e0403b8d89e42ae54701026c1f
SHA1	a4f5cb11b9340f80a89022131fb525b888aa8bc6
SHA256	a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b
File Size	26.00 KB
Report Created	2022-04-26 02:15 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (15 rules, 33 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #2) svchost.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #2) svchost.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 258 files by appending the extension ".ampkcz".			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Internet Explorer / Edge, Total Commander, The Bat!.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
3/5	User Data Modification	Possibly drops ransom note files	1	Ransomware
	• (Process #2) svchost.exe possibly drops ransom note files (creates 42 instances of the file "readme.txt" in different locations).			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #2) svchost.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #2) svchost.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #2) svchost.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #1) a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe enables process privilege "SeDebugPrivilege". • (Process #2) svchost.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Enumerates running processes	2	-
	• (Process #1) a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe enumerates running processes. • (Process #2) svchost.exe enumerates running processes.			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #2) svchost.exe adds "c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\start menu\programs\startup\svchost.url" to Windows startup folder.			
1/5	Hide Tracks	Changes folder appearance	17	-

Score	Category	Operation	Count	Classification
		• (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\desktop". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\links". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\contacts". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\documents". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\downloads". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures\camera roll". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures\saved pictures". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\music". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\onedrive". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\saved games". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\favorites". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\favorites\links". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\searches". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\videos". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\internet explorer\quick launch". • (Process #2) svchost.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\internet explorer\quick launch\user pinned\taskbar".		
1/5	System Modification	Creates an unusually large number of files	1	-
		• (Process #2) svchost.exe creates an above average number of files.		
1/5	Execution	Executes itself	1	-
		• (Process #1) a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\Desktop\a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe.		

Mitre ATT&CK Matrix

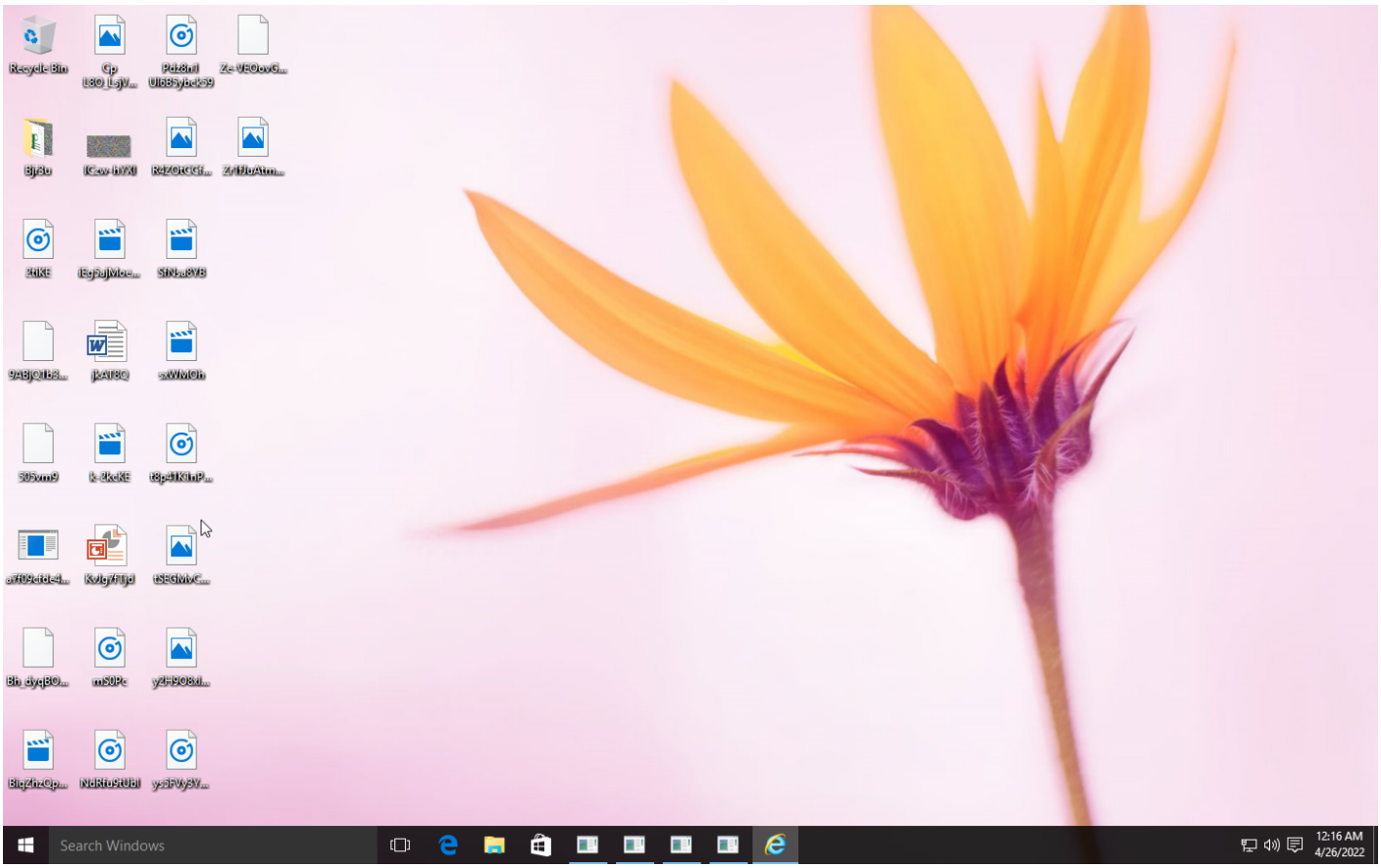
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1036 Masquerading	#T1081 Credentials in Files	#T1057 Process Discovery		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
						#T1083 File and Directory Discovery		#T1005 Data from Local System			

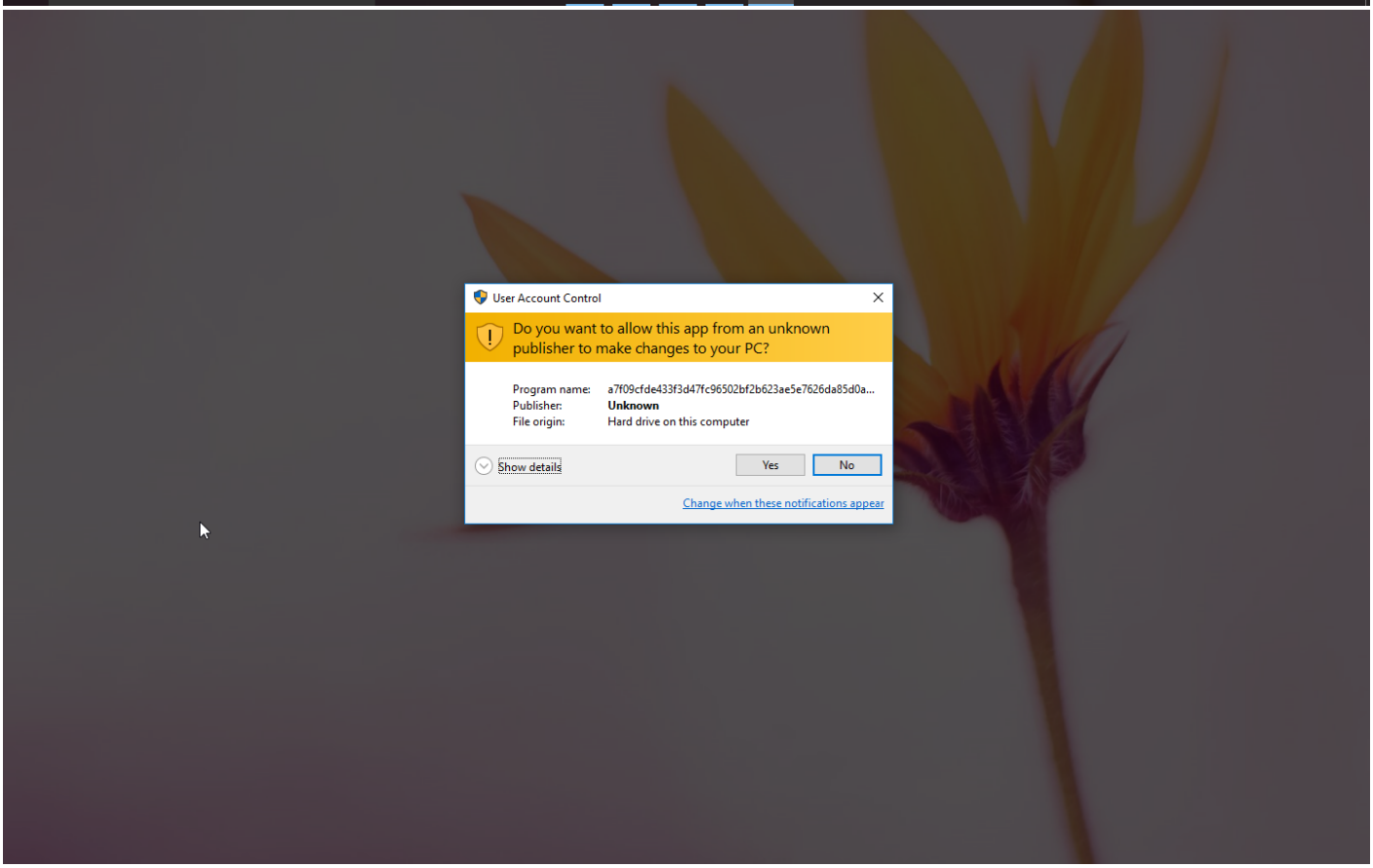
Sample Information

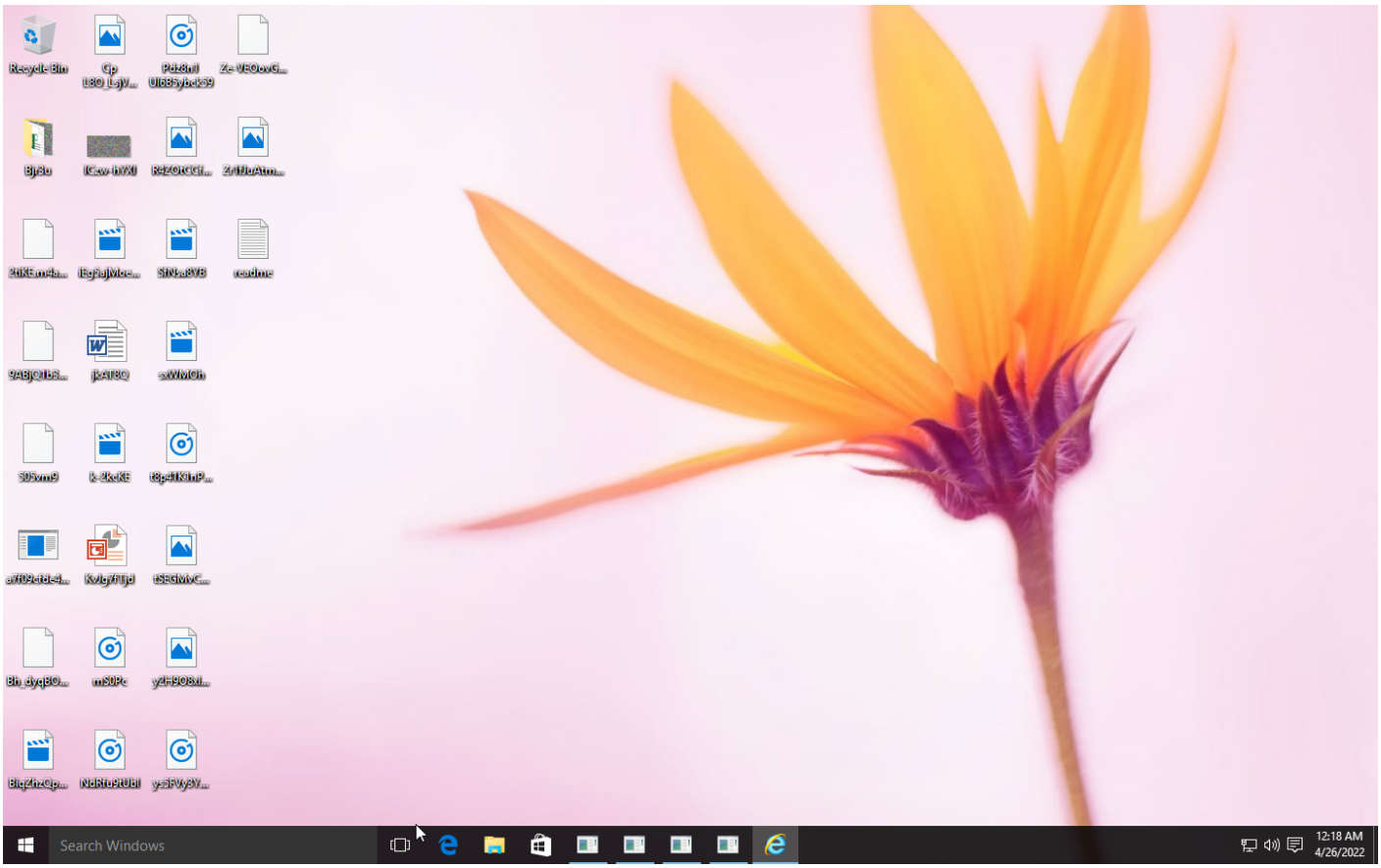
ID	#4194433
MD5	cf6ff9e0403b8d89e42ae54701026c1f
SHA1	a4f5cb11b9340f80a89022131fb525b888aa8bc6
SHA256	a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b
SSDeep	384:Uo3Mg/bqo25M0RHcY5pmyjuwzUHJhr91CHW8wNa9get:UWqo2Zn5pPjKphr9z8wNHet
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe
File Size	26.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-04-26 02:15 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	2
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Search Windows
12:16 AM
4/26/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
readme
Search Windows
12:18 AM
4/26/2022

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

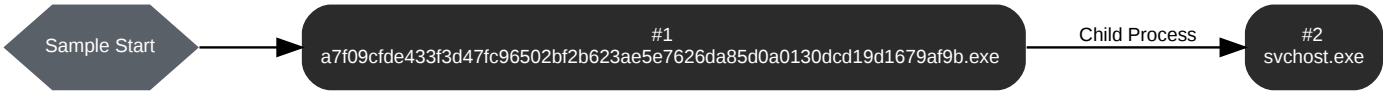
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 57091, Reason: Analysis Target
Unmonitor End Time	End Time: 142760, Reason: Terminated
Monitor duration	85.67s
Return Code	1
PID	2972
Parent PID	1184
Bitness	64 Bit

Dropped Files (13)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\svchost.exe	26.00 KB	a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b	✗
C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini	584 bytes	f7af421eec2af30d19ce4ed3a59073865a5574197b875bf96b8dc90bd8f9b7f6	✗
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini	756 bytes	6cbdb1532654851d5662dc4c398d41880f57a1a78b8f681bc52b8d2bcecf9ea4	✗
C:\Users\RDhJ0CNFevzX\Music\desktop.ini	884 bytes	6c0df953fc888b83950e0d5e033049905622b3878d1002c03ea9ee6cf6e38c52	✗
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini	884 bytes	4b8bb6c8f5e9abcbef09808f253b7620b77692ae4a8e7b2ed09b1641caa1403a	✗
C:\Users\RDhJ0CNFevzX\Videos\desktop.ini	884 bytes	a0ff65b781c28b6a0dab849a74aa3338f4fb3b9a41b5c43043e5316fd21a396b	✗
C:\Users\RDhJ0CNFevzX\Downloads\desktop.ini	584 bytes	017079a566e69bb5b37df87321d1fa95a7a300a4096a388f1cea9f235d59205e	✗
C:\Users\RDhJ0CNFevzX\OneDrive\desktop.ini	352 bytes	84f4227ffeaf1c4fe0523e7d609e58092177437564f0a5e47c77851d6b6c1222	✗
C:\Users\RDhJ0CNFevzX\Searches\desktop.ini	904 bytes	c8d8bd0cc71fba9732faa3ef80f43410b7a5618fc0afc992dcc867c81f2ca009	✗
C:\Users\RDhJ0CNFevzX\Contacts\desktop.ini	756 bytes	eb1e22c8ca8f9e75a4226da63a2baf9d0c39f2aa4c808bd651a25ad76282ff25	✗
C:\Users\RDhJ0CNFevzX\Favorites\desktop.ini	756 bytes	3a606a777f4c830a5e582c6dc83873bd84e271b4f0a06b40b5da60cda50dc71e	✗
C:\Users\RDhJ0CNFevzX\Links\desktop.ini	884 bytes	8d195d6cb0e0d4447034b742d38a6f32e265739619ccaca3242e7908167e005b	✗
C:\Users\RDhJ0CNFevzX\Saved Games\desktop.ini	584 bytes	f4de2c18c526d0e95dbc6535d934792ea663f68964bc26c3443fcc550f90c5a0	✗

Host Behavior

Type	Count
User	2
Process	126
System	2
Module	2583
File	2

Process #2: svchost.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\svchost.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\svchost.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Roaming\
Monitor Start Time	Start Time: 141706, Reason: Child Process
Unmonitor End Time	End Time: 297104, Reason: Terminated by Timeout
Monitor duration	155.40s
Return Code	Unknown
PID	1404
Parent PID	2972
Bitness	64 Bit

Dropped Files (237)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Templates\LiveContent\16\Managed\Document Themes\1033\TM03457444[[fn=Basis]].thmx.ampkcz	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini.ampkcz	584 bytes	f7af421eec2af30d19ce4ed3a59073865a5574197b875bf96b8dc90bd8f9b7f6	✗
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini.ampkcz	756 bytes	6cbdb1532654851d5662dc4c398d41880f57a1a78b8f681bc52b8d2bcecf9ea4	✗
C:\Users\RDhJ0CNFevzX\Music\desktop.ini.ampkcz	884 bytes	6c0df953fc888b83950e0d5e033049905622b3878d1002c03ea9ee6cf6e38c52	✗
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini.ampkcz	884 bytes	4b8bb6c8f5e9abcbef09808f253b7620b77692ae4a8e7b2ed09b1641caa1403a	✗
C:\Users\RDhJ0CNFevzX\Videos\desktop.ini.ampkcz	884 bytes	a0ff65b781c28b6a0dab849a74aa3338f4fb3b9a41b5c43043e5316fd21a396b	✗
C:\Users\RDhJ0CNFevzX\Downloads\desktop.ini.ampkcz	584 bytes	017079a566e69bb5b37df87321d1fa95a7a300a4096a388f1cea9f235d59205e	✗
C:\Users\RDhJ0CNFevzX\OneDrive\desktop.ini.ampkcz	352 bytes	84f4227ffeaf1c4fe0523e7d609e58092177437564f0a5e47c77851d6b6c1222	✗
C:\Users\RDhJ0CNFevzX\Searches\desktop.ini.ampkcz	904 bytes	c8d8bd0cc71fba9732faa3ef80f43410b7a5618fc0afc992dcc867c81f2ca009	✗
C:\Users\RDhJ0CNFevzX\Contacts\desktop.ini.ampkcz	756 bytes	eb1e22c8ca8f9e75a4226da63a2baf9d0c39f2aa4c808bd651a25ad76282ff25	✗
C:\Users\RDhJ0CNFevzX\Favorites\desktop.ini.ampkcz	756 bytes	3a606a777f4c830a5e582c6dc83873bd84e271b4f0a06b40b5da60cda50dc71e	✗
C:\Users\RDhJ0CNFevzX\Links\desktop.ini.ampkcz	884 bytes	8d195d6cb0e0d4447034b742d38a6f32e265739619ccaca3242e7908167e005b	✗
C:\Users\RDhJ0CNFevzX\Saved Games\desktop.ini.ampkcz	584 bytes	f4de2c18c526d0e95dbc6535d934792ea663f68964bc26c3443fcc550f90c5a0	✗
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\svchost.url	156 bytes	68c94fafad8b90d0ab84eebd082f90d15e94224b20ef18a767258439913318ac	✗
C:\Users\RDhJ0CNFevzX\Desktop\2tiKE.m4a	45.34 KB	661cb6050c8a3b102a157628ae64c8c20778923f8ccd4d71d39b92b5e404ed2c	✗
C:\Users\RDhJ0CNFevzX\Desktop\readme.txt	1.69 KB	82086da6a81e6606c29af9744461ccbdf6735cb1c3899383c83d07253426944f	✗
C:\Users\RDhJ0CNFevzX\Desktop\505vm9.swf	99.30 KB	c03879bd3bd08585432dd354eb94b463e94098ad50ed4b20f11f3b8c4357f598	✗
C:\Users\RDhJ0CNFevzX\Desktop\9ABjQ1b3wA2cIKcd.flv	124.13 KB	23ebc38c60fa5244a10f6ac7eaf289d0a9bec9091202390e1720cc0d5ccd6e3a	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\Bh_dyqBOzR8.swf	45.91 KB	c85dbbe2a39b2a51eb30beb8cc97348a1c0e7409df1f42ddd413bf569444bd96	✗
C:\Users\RDhJ0CNFevzX\Desktop\BiqZhzQpPpNFiiegsAS.mkv	34.01 KB	424f34e9f98781ea427679a4fc5b6c1c73548ef9c5ab9d790e4acc6833ec09d7	✗
C:\Users\RDhJ0CNFevzX\Desktop\Cp L8O_LsjVMCQa-Gl.gif	33.55 KB	b130258b2c6120ed13eda2b666eb61de5fc55a896f30c9fc9160ed299e4224d4	✗
C:\Users\RDhJ0CNFevzX\Desktop\lCzw-hYXl.bmp	125.30 KB	0fd44b5023c28b8af7003a7d0efd2f847b17f6b623c2b6a6681ab176a91a0b86	✗
C:\Users\RDhJ0CNFevzX\Desktop\iEg5ajMoeBZC.mp4	33.61 KB	dd93227ef6bb3ea8b1e1a998760c41d1b1d3f634b78aad466c2cbbf31327a704	✗
C:\Users\RDhJ0CNFevzX\Desktop\jkAT8Q.rtf	103.30 KB	c624dc44fc3dd28b2efbc4ca9872fc6d43b54373557203f379df2829cff9a456	✗
C:\Users\RDhJ0CNFevzX\Desktop\k-2kcKE.mkv	38.91 KB	fc1d968f8b7eb3c4e4f5383ebbf0ffb6d7d9826c8b362a656217e7be59107b6d	✗
C:\Users\RDhJ0CNFevzX\Desktop\KvJg7fTjd.ppt	119.66 KB	cf6c834adfc67033c09c2ae1df7dd7a1af4f809ffd9a3825bf02c03b5681cdff	✗
C:\Users\RDhJ0CNFevzX\Desktop\mS0Pc.m4a	119.76 KB	624d83ec7298a0a1a6737756732d8f9703693bdf0070525d4154ae3b16621ed7	✗
C:\Users\RDhJ0CNFevzX\Desktop\NdRfu9tUbl.wav	29.86 KB	12ac46bff6470b452efbfecb9462f7907665581c7cff1df4a9699f05f5ec3172	✗
C:\Users\RDhJ0CNFevzX\Desktop\Pdz8n1 UI6B5ybck59.mp3	86.01 KB	56304301be5a98a51fd97a5d4248d3a21c8c8ef749d845db13c7394ae778bf00	✗
C:\Users\RDhJ0CNFevzX\Desktop\R4ZOtCCfPyPi.png	75.68 KB	5a322652307a976814e0aa3f95a8b110dec90014ce1edb10340acfafcbe83b36	✗
C:\Users\RDhJ0CNFevzX\Desktop\SfNsa8YB.avi	106.61 KB	0eceb1421c44050fcf1b624b0146c391943dae9c6e7388c2cf2fa506eefccb17	✗
C:\Users\RDhJ0CNFevzX\Desktop\sxWMOh.mkv	36.95 KB	9f1c06a17224c9078ed033faaf9d5de69204fd2d17f7b7adddee100a4fb74eaf	✗
C:\Users\RDhJ0CNFevzX\Desktop\t8p41K1nPNZvX.m4a	33.66 KB	72357217b1e0c71a704afdce2f33c6540b32cecfebd115da8ac07865d179e2f9	✗
C:\Users\RDhJ0CNFevzX\Desktop\tSEGMvCPcMx.jpg	133.18 KB	d59da380eef6105df87a5a8ed2f28cc2772ee6bf712447d664a4a9f8271ac8bf	✗
C:\Users\RDhJ0CNFevzX\Desktop\y2H9O8xlmETgCAbycT.png	53.18 KB	80dff20331c1b2c2a8a1d1287eb2169933171c655e83e601596b1b8213d4c6c4	✗
C:\Users\RDhJ0CNFevzX\Desktop\ys5FVy3YwYbsg.m4a	115.86 KB	11f2e7aeb5619eebc6f4331e96d744d41e9b84dad28b2d5eff24b91df791a967	✗
C:\Users\RDhJ0CNFevzX\Desktop\Zr1fJuAtmLuvrKkw.gif	104.47 KB	e19a77d484aae043582db932f76ab330a33720964e689dceb414336af7390433	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\2HtL-q.csv	72.57 KB	1dc4d1b4f84bc9558fafe0f8c94da733903e841f874aa848bbe6a9bd055bdecb	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\7Bsy4NSMiVQmfv8k.m4a	52.41 KB	fa709d9f60e5e7cf3c16dc737af740ced3e869a9891224ca3abcbc7835f5302f	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\8LljmtPnMSEYSYG.csv	17.55 KB	58cbd82ca366a569a58d0154fc1882aa6d6956bb1d1f6a72bebba969581da2ee	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\8Vi4 VdapZ6YLX5Sp.flv	92.20 KB	4635a2b016bfa7a5bc15a444bea423954a8792d41ba8145370d1fd745d649d2f	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\BKUVLc.bmp	70.38 KB	d25c6b54a541c3e0710c98689f8071414c9515d200eb56292991fd1f2528a766	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\bz0WFA-cPHK_6RXp.m4a	87.38 KB	4aa9d3d6be9929d2d624a2ede42bf84e8bf43a3ec3f564ac4365ca40432097c3	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\ggv8WxB.gif	54.47 KB	cc748e70f0466a90791d387a628b364f3b948dbaf3ac8e652bfab27f051d1496	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\JHyJ2FcVg5iar.mp3	20.26 KB	aa1f95036688f12cefc6cdb2b853581a0aae54962a4eaf5eab4bc3c6849d22e2	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\mB4Ez1kKY5Cs.mp3	8.82 KB	f8a164e3494506bc339e900f637eaf84e6261b2250a81cec40cbc4c638e3e5e3	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\mFs5gB9Z3Uguw495HmEZ.jpg	28.57 KB	4dc1f6c913a2f07e3bebd0243d64bc1c146fa8cf105ec41e52b128b856200865	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\RPzmf9DjF1.pptx	99.91 KB	761f8472d4a5242384e357df4bf31b43056066063b235bae53e19e9c6561bd47	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\SjWyWkMIArJ.docx	64.49 KB	d20ca94441449a800b3635efcba51e30fd6efc8b93703a6f255bcc12c33725aa	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\VADyx2_L0xN.flv	104.09 KB	ae81e9dc1c0fedb91d16bad13b920c1fa04c0c048ac08d4e8ae0caadbd51c2ec	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\vXhGV8MRaVScOkV5f5.ods	130.34 KB	c8d379eedc4262209dec46fcbeeac89dbf35b3da66f40c52ebfb83bfe2b5f48e	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\WTyYMq00n.m4a	18.41 KB	0e49860c0c62c8e0d0578f7c65bc1fb9e4a5cb8c51c894ba394c31b1d9e46671	✗
C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\Y_Ku-Plvvx.png	2.28 KB	fdbc3968b1ff45b2e77394f1d7bfbe295d95c135a80151d6c8f229fb92e0e44b	✗
C:\Users\RDhJ0CNFevzX\Documents\8-58vgRqyz gS.pptx	82.47 KB	dee9357117bf3b93b3f1a47e9f0a6680a0523d00c03eb728a828b29c8f6ceb25	✗
C:\Users\RDhJ0CNFevzX\Documents\AEfN7e6MhjMF2F11JEs.xls	11.88 KB	42de96a80311b5611e4dc5f209a11c95d792f0eac61d0435f2ce201af5717d48	✗
C:\Users\RDhJ0CNFevzX\Documents\AJOZtXvu7QfT.odt	49.59 KB	c657a92c9d4001e439f3bee5e6a345c5d92220c1c2c3ea607f348c85272 71a81	✗
C:\Users\RDhJ0CNFevzX\Documents\BAJe.docx	81.11 KB	1d09c7420b537223c8ba6c1bc6b8ef183f3a348cd9732ff072f57964470ba820	✗
C:\Users\RDhJ0CNFevzX\Documents\EgNVA.pptx	18.01 KB	ccfa528394b2cb1da954b8369dbc38007277b2fe60249ec498520cc8231de369	✗
C:\Users\RDhJ0CNFevzX\Documents\foayjE.pptx	22.93 KB	6c080456c30c334bff543bfc7b062592a8daf2f1020c8c6b271c525be6470ab1	✗
C:\Users\RDhJ0CNFevzX\Documents\iOVreLoxPhj7stpatiPe.docx	53.38 KB	babca4a0b75187d59a92ad8de610cf7c101bd82248f2a22306e4c9f614701d89	✗
C:\Users\RDhJ0CNFevzX\Documents\Juhec_87-J -LcDPj7R.xlsx	103.51 KB	eef114d4d8374c4e11aed14e3e9a53dbb9c72720571cb76b81a53f32069d648d	✗
C:\Users\RDhJ0CNFevzX\Documents\LYfQAN97cU.doc	108.09 KB	420dd907d5bceca5e8228a3c1c78c6dceeedc19fb72e23c2e1bc3457038fd7cb	✗
C:\Users\RDhJ0CNFevzX\Documents\nh_ayDk4U dJuq.pptx	34.66 KB	d70beb8cc6d3fc73690659a30bfad4762859faa525425f4fa1ecc3cec6393353	✗
C:\Users\RDhJ0CNFevzX\Documents\NOUPcFxdi9.xlsx	120.53 KB	df04671d0ae9fcc93cd28d839a18cad265d5a0295469950666e5a190aae2fc11	✗
C:\Users\RDhJ0CNFevzX\Documents\NyHQqR6F02G_ox.pptx	81.91 KB	c9923d9e4be58436ac747994c54ac4f49843916ad119360290c12abcb08df169	✗
C:\Users\RDhJ0CNFevzX\Documents\qn--Dnwch0FHbbgzTTO.doc	108.22 KB	848975ebd101f2c6512c3f25bd125971aa390a93f3e4a48f0b9e554955b79723	✗
C:\Users\RDhJ0CNFevzX\Documents\reOIkC.xlsx	48.57 KB	aa0dfc5fd9c14fe931f14e5ca311ae413fb00df519c78fa5d82a055e3b7d8935	✗
C:\Users\RDhJ0CNFevzX\Documents\sBn Uk0ytdM055VR.doc	69.68 KB	201f8ad153ee9636579cc32490a72bdd719654c4dadcdc9e2179283408d41686	✗
C:\Users\RDhJ0CNFevzX\Documents\Sxq8yYPsbOADIX.xlsx	102.30 KB	265817724c55c272a9f2516703449d88a784fd50bf73d126653a75d88647da39	✗
C:\Users\RDhJ0CNFevzX\Documents\uDnFB3fA14uy4UENIcK.docx	126.55 KB	859a2ae9fcb99c2eec5d62ab7298253a7b4fd503af9875e4ef6e9f24fb35deec	✗
C:\Users\RDhJ0CNFevzX\Documents\vy87ulZFy.docx	110.84 KB	4f7bcc5b34ef798e941623c40aa381faa87b751f85b6ed263efc09a7a7429635	✗
C:\Users\RDhJ0CNFevzX\Documents\YdjNmFIdm.xlsx	50.43 KB	1bb9465174be973f26424f9c01f87e808bc8d372057113ba6148eedac1936a75	✗
C:\Users\RDhJ0CNFevzX\Documents\YyiJJhqdwi8qn.docx	88.32 KB	900b952abd5572a0fef4996d77b287633188d9966da0970eae8a48d64a893112	✗
C:\Users\RDhJ0CNFevzX\Documents\F_8pl8t\5EZ7tX.ods	106.55 KB	b73b6bd2e87d834e37a358bc346e074ab2cff549c775b6d0e80b35b51715f412	✗
C:\Users\RDhJ0CNFevzX\Documents\F_8pl8t\o0S4MtYXa7.odp	57.74 KB	5142fd16b5f469a953818d9faf56c9cb245e64a7c10b301d1e89dde720cf043a	✗
C:\Users\RDhJ0CNFevzX\Documents\F_8pl8t\qQxnuP1.rtf	10.51 KB	0edf25825f5a0900c1d1f9583769986f87f7278e5f524009f513a87037b009a3	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\F_8pl8t\uvz3Z3AyRuC12.xlsx	49.16 KB	7d7bc09304bbbd4b5a0234815af74c76a7ae8b48d7fc3f4c9c1dda1bc0645ce1	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\-hnSJxj1Uj.xls	130.11 KB	7b8ef41751deee524aa34bfbacc776e0212953a5584504e6b2917d8e5d1beb04	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\0aqOojXPcy4.pptx	63.82 KB	13ebcfcf33d8b4372cf5c2dec5bd4442d672d2e47f409b5c1c0dd3df664c3b03	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\5JE02Kb.xls	53.93 KB	895ded3841774d208437c9d02fc21e723ef1e77f96fbd2bcb99b50eb326c8ad2	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\8G_KTv3fC9ZSX8qy.ods	52.47 KB	d68383ac76368d04e8b0889fb8e970f7a03ff76598ee2cf91cbbeca9e7f81b02	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\CFltAr.pdf	61.53 KB	de61fc75ab7b51fdee7c3e24ceb64566f5c5731d029a58220fe7c03a4183a1f7	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\dv1BjUamcjV9b3.ods	66.43 KB	910d7a2dc7cce6679d45f85bd08f42c19a9eec6eee6284080dbfa8c13f1f4de7	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\kDFn_YGXXw.xls	116.16 KB	ae99ca1dca84f38ed237c0eb72a813fa46a2f0d40cf6434fc09b7f05a874af28	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\pKWEXKp.pps	66.41 KB	07d800477d7e1b2757d9a4c615a97c9688209e7a8e19e279cb7e3a5c4edc1370	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\TyXrZ.docx	53.43 KB	4de4560180e5ae4cbacdb3a5c308cd70ff62f54093d2cb834ce4bae20c1b7629	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\D6AC.pptx	121.09 KB	43f4b4a554095cf21fc8907ed6a7b625533923fa29f3ca314ba5c970ac64640b	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\hV7Qa.ods	22.43 KB	24fb3ffc04b6e079aed1aaf272c0452026400fe4b9a7fdd5552a13e7b2396255	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\iANwPv2pHIptalL2csWw.xlsx	59.01 KB	8f549b4a2ce61b7e3138c5050ba09f8415c5b3f9ac12f10c7e03c75fdf91ba5c	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\bRsSZdBZoL qdvafNLF.pptx	8.28 KB	b97ff5521e842fcb86733c65089744b245e1c2404ac3ce47c070bf0c1e77dd39	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\FiPmvzuFqtW5HPbrQ_Z.pptx	71.16 KB	13b5013da36efcafec6c74d8e3e4a2dc4a5b87e8a94552c6342c2a79fbab30a2	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\G-GX1bLPx.docx	105.97 KB	83e55421362e288189a5ce6c24f1e2a3b98b22631b14dbe7d209c056929a9c95	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\NrPAwo00v KCQzI0375.xlsx	80.63 KB	42ab4a8a9e15486300616dd8161437d6dbccf859774ebd57bfb18609f62570e2	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\PI6cEP 9l.xls	94.53 KB	484dc562990aa99a4443f1f8a0ad88852ad07313a709d67715a20cf58a8e6ca6	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\T3aXJ7JnmiGblPU5.doc	7.61 KB	784cd3b795cd95b6869b979558821eadf39b9d133b90e39db7dc147eb439f911	✗
C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\Zxb9-KR.xlsx	47.05 KB	be8a9f7f945977c8fadfe61517cca4c6a50156f8a32f686b790634c38acd8dc3	✗
C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst	353.55 KB	22850ed64e134f7be68df8e98c69bb81a57a211cdb230ce10cc9ee18122eb65a	✗
C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\-K6OWWoFoPzYq-hdIX.pps	75.11 KB	7dfcad0c63c6211022a494e612ba474c62da0f6d2f6ddf63c2e5f0d6cdc2cee9	✗
C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\3m6lgzrLvSc6-KZCaxw7.rtf	60.22 KB	e8220e4b5ac83364554da56d2b99ce5704839847b7991f7d730d57f1f4f5fa93	✗
C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\5mb3rREI7ul1Pp.xls	114.72 KB	db253c43395290a997b9c6660605726c96f1c6eed24c54a1b88b9d5f6cd7bfeb	✗
C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\acXYO1yhB7sJfRK.doc	9.05 KB	8c99e27414c0e877097d89ef1e069755b33c34bee258c411b8240ed283412044	✗
C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\L4-0_ nb.pdf	59.76 KB	97a32cef66bb6d95dc96dd656797bb3ebb4e96a95e1f7038b9d9e75cf1807e19	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\tSQ.docx	48.91 KB	f9d387abf28b7330c44bc42a54bf875ff0cf410faef8259edf87499c9b3b8035	✗
C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\v3V2Y3Hpen0RMfAQo.odt	108.95 KB	7f9c728d4f0d79e5cb22a28859641d06c794f594c73b05525ec68e4fb4e7943c	✗
C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\YKV-eu9e6_WXh5sqju.pdf	33.82 KB	d35a4ddd161f511b20de5528faeedaf136a57354e4559ed0fa60bb7fa78e96ab	✗
C:\Users\RDhJ0CNFevzX\Pictures\AjN9y78hVh0UKrhnkL.jpg	118.97 KB	9e0416333fe0e883e3056eaa78a000b14bd0a6e3c9f0c618fd86c5e8d1cf8f86	✗
C:\Users\RDhJ0CNFevzX\Pictures\ejgt1B9nD_k9299.bmp	77.28 KB	1d9dee75789de609b87632d0b562c81c337ec7b2bdcbae647309fe5ce61b8295	✗
C:\Users\RDhJ0CNFevzX\Pictures\hVKydaZ1ZP.jpg	101.09 KB	d7eac1ca260d873434b3b7c928d100dd9e37927f153ddcb0f740a2d2010fb074	✗
C:\Users\RDhJ0CNFevzX\Pictures\JLVegM9vxb3bekfHf_.jpg	110.38 KB	9948f1d4ba23964fc662c32dd0269df0d0c4a473bf872fa75984a1445654d704	✗
C:\Users\RDhJ0CNFevzX\Pictures\k3 kfHWnlQpe4M9v.png	26.13 KB	679f364a17dbdf06c4ba09cafdc5559b763ee67f84e0374d8c33cec8a84a1117	✗
C:\Users\RDhJ0CNFevzX\Pictures\Ol3fbrHp3.png	35.05 KB	6e95f60c212a9b97f01b1e0728f1085d8d01dba5ec9038695567d85c302dde3a	✗
C:\Users\RDhJ0CNFevzX\Pictures\q2vCj7US.gif	79.09 KB	f0cf6c0626e045b6ff81042e5330b8ebbf6f600452c3c2d614343905e882698a	✗
C:\Users\RDhJ0CNFevzX\Pictures\UEaT.png	1.72 KB	0a3435c2fc86761a20d4eaaf627cd9e6ed979158f0f7aabbea61b005fb19270e	✗
C:\Users\RDhJ0CNFevzX\Pictures\yvmvXCdl-L2md.png	66.70 KB	2c66bbce148ef915a4e31aa847f09ff15012e8dfededcfbfeec2a9782f1cfb27	✗
C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\3avUxb1BL_1g12oSkH5.png	104.68 KB	72d12473cefc5bac3cd8a493c5e8b6b65543aee06ed718a513e15fb290934670	✗
C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\82EsZ7p-5diz.bmp	102.76 KB	be9a9f3bf42da831db4229207224106b0bcbc65276b5149371b9523d35fa2355	✗
C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\95XyOZRwahuGE.bmp	11.76 KB	e1cdfe2ebb0bdb6fa1fe8b8c4735795f6acb81dbd28a654b68a01bc3238a0284	✗
C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\pybRnums.gif	111.47 KB	5cbb34c01ca56902521ef22b5204c8567be02f4aec9e44232ec0a06ce6ff87ee	✗
C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\rC_A9e_Y_besF1X.gif	69.84 KB	73eb76c3870e4e4b6a351b664ddcba9de43b5161f8a6cc0a32a8a2c819d19f74	✗
C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\VxgH4lec2pnD.bmp	46.41 KB	15e6a7bc5ebecab8035754711fad7031db874d81408b4c4f9d0a2c4346819ef2	✗
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	456 bytes	c0be9aed4b7fec90a72ad32edd1454242bb5d17fc67be0200a7a1539bb189bcc	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\1vouFPcx5u2EPwdO.jpg	101.22 KB	19f081e541ace7a8d0dcad78d0003e7f67622e2ac8194bb7629cffd37d2327a6	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\E AOhji2.bmp	53.05 KB	441ed7ab44b48463780791355f4d31aa73738d916c92bf2d2e5f553250d961e5	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\fqUC.bmp	49.88 KB	7b84beae60fd2cf82746202469ba6af8b036e75046fea13b93dd0245c48f7868	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\kqG3aN.bmp	59.45 KB	48b9208854f869e876ed83eb6c2ff8a718a9986bf5dc213e76e3a643f546466d2	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\Q_Ekrnom6M-AaivdFcPZ.gif	14.55 KB	02b3ff6375d70168ec65439d0e1eb7f50b2e41a1faeda694e9d8c32281f310a5	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\U4hfL3Yd9m.bmp	101.43 KB	791878baedb4fa4618ab5261ced08b01efe24423228f84947a83e1dcb1bb7d89	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\ZlvJ2tjP.gif	81.28 KB	f23e422a2ce99fa6cfb61504cb5e708be006da46ccf5f19f7441903e13ebd652	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\Asuu1.gif	4.38 KB	66591ef7c80d0a6125b2a8ca833f56e590a11cab9d7ef01bb5e28e7c1aca7871	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\c5qjp_9.png	114.16 KB	77b88262b1de2127fb09ce3d273107262463b32ce15c15c70bfaf0268841cea9	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\i_HjOI0Pvfw-v.jpg	100.63 KB	b394d4405a627b58af408800d719a935c5a38ecb6f3c6b6e1b2bc272923bbef8	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\JGhfvZ7zWuY0.bmp	13.30 KB	f96fc06670a522fd0c9aa3399272492ddfd55ce7f1da7e902bab39f3db1ef653	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\NbFcv7r.png	129.53 KB	d1cb95dabf612cb0b32085e3e0b13335a9f8e8df2ecda1c6c0614fd526048537	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\PeNWmzhlJCX.gif	59.11 KB	952562d57f44afcd7b5bd2f5dd558b2e25ad4a850d25971acaed4829662 42e4f	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\sNU4ZxXwBcEpxou.gif	21.36 KB	9bda52b016e6ee2f173d5b3be7b5aa6ccffa2e911f9d779a51e0e68e3f0b0e03	✗
C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\yeL3pql1j.bmp	107.16 KB	91ff43ea499681825dbcc45840c64f7404d17fabe81bd2b0a875e259bb56425f	✗
C:\Users\RDhJ0CNFevzX\Pictures\LldMOQASD6\2Clz54JvlW_N1L.png	50.80 KB	90fff203ca59f46db51c1c2053f06039dbf33f51a72c38fae793b526a4100a22	✗
C:\Users\RDhJ0CNFevzX\Pictures\LldMOQASD6\VXDZKI.jpg	31.26 KB	9123a7e87c4af676d410b9878b06ae8c1a28101fc45ca6ebf7d07ba3964c018e	✗
C:\Users\RDhJ0CNFevzX\Pictures\LldMOQASD6\XlKnK1gfJe4zFhGoRY_F\AKzD1IY.png	53.57 KB	7ac5c05718c4bc2808705cfe600680efe2ab475237503a5c02b3e9ff499f2617	✗
C:\Users\RDhJ0CNFevzX\Pictures\LldMOQASD6\XlKnK1gfJe4zFhGoRY_F\QIc4be.bmp	8.49 KB	d40af9df95b3164c3d7432303d65dfb7a496b0a73a840c26fdaccb26ac91a2d0	✗
C:\Users\RDhJ0CNFevzX\Pictures\LldMOQASD6\XlKnK1gfJe4zFhGoRY_F\r5DQrDCs.gif	48.05 KB	de0e961fa4cb2d336ab24e823350850647ed710f3a81e0acc1f9818bdebcf084	✗
C:\Users\RDhJ0CNFevzX\Pictures\LldMOQASD6\XlKnK1gfJe4zFhGoRY_F\uOS_JODxfeSPDsu.png	50.24 KB	5f967c382afa37bce4dd2fd56fe9e2beb3da8f03a1537cedc28e9f198c882582	✗
C:\Users\RDhJ0CNFevzX\Pictures\LldMOQASD6\XlKnK1gfJe4zFhGoRY_F\uXWtciW8Mz.png	124.93 KB	e0ae14124ed672847b5c84c4e3db7365cc46a422727d90f514f4c6d47a234218	✗
C:\Users\RDhJ0CNFevzX\Pictures\LldMOQASD6\XlKnK1gfJe4zFhGoRY_F\xLsjiwCf3AooR.jpg	27.95 KB	de035d7f7f4409c463bd1895d2e932dd4c1d3486edf7af9532fa6192b33976fd	✗
C:\Users\RDhJ0CNFevzX\Pictures\LldMOQASD6\XlKnK1gfJe4zFhGoRY_F\YGxlk.png	131.93 KB	1c7aeda04d4808b67fdab0f7df33a00e2b897325c841c10eab5dbaab01cfcf10	✗
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini	456 bytes	23341d0da3cce4a29985128dec6b74cb1c5996a80528f9831f5a27e57c54d3bb	✗
C:\Users\RDhJ0CNFevzX\Music\Ec AoPKlkYeK4zcxY.m4a	62.24 KB	cbd02a7e1d70f870367dbc58c0522df548ef6a811a031c5660e2f37a55487f0d	✗
C:\Users\RDhJ0CNFevzX\Music\JWRhu6PW-N_JtHKHctzp.m4a	15.78 KB	6a16ed5b674c36f39ec95d0532efc05c0b06bbedbf9a5e831cba3f0de67a1083	✗
C:\Users\RDhJ0CNFevzX\Music\lnpwHWei4hMwarh_Gi.m4a	117.53 KB	b3c3c76ba64bb6035c555e687cc8c6b1a4df8cf9258ebed8a230bf1e769b0324	✗
C:\Users\RDhJ0CNFevzX\Music\aOr_0l-_\2tOwtNlJ rxX6vXCj.m4a	41.53 KB	4c3f7fbb4974db12994b0eb0cf972a021ecd03b0762a62a66d892ce9a0eb3ba8	✗

Reduced dataset

Host Behavior

Type	Count
User	2
Process	111
System	2
Module	2438
File	9571

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b	C:\Users\RDhJ0CNFevzX\Desktop\a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\svchost.exe	Sample File	26.00 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	MALICIOUS
82086da6a81e6606c29af9744461ccbdf6735cb1c3899383c83d07253426944f	C:\Users\RDhJ0CNFevzX\Desktop\readme.txt, C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\readme.txt, C:\Users\RDhJ... ... 5zU4\readme.txt, C:\Users\RDhJ0CNFevzX\Music\l8lZVBLxnO5OrJ wF\readme.txt, C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\readme.txt	Dropped File	1.69 KB	text/plain	Access, Write, Create	SUSPICIOUS
f7af421eec2af30d19ce4ed3a59073865a5574197b875bf96b8dc90bd8f9b7f6	C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini, C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini.ampkcz	Modified File	584 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
6cbdb1532654851d5662dc4c398d41880f57a1a78b8f681bc52b8d2bcecf9ea4	C:\Users\RDhJ0CNFevzX\Documents\desktop.ini.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\desktop.ini	Modified File	756 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
6c0df953fc888b83950e0d5e033049905622b3878d1002c03ea9ee6cf6e38c52	C:\Users\RDhJ0CNFevzX\Music\desktop.ini, C:\Users\RDhJ0CNFevzX\Music\desktop.ini.ampkcz	Modified File	884 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
4b8bb6c8f5e9abcbef09808f253b7620b77692ae4a8e7b2ed09b1641caa1403a	C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini	Modified File	884 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
a0ff65b781c28b6a0dab849a74aa3338f4fb3b9a41b5c43043e5316fd21a396b	C:\Users\RDhJ0CNFevzX\Videos\desktop.ini, C:\Users\RDhJ0CNFevzX\Videos\desktop.ini.ampkcz	Modified File	884 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
017079a566e69bb5b37df87321d1fa95a7a300a4096a388f1cea9f235d59205e	C:\Users\RDhJ0CNFevzX\Downloads\desktop.ini.ampkcz, C:\Users\RDhJ0CNFevzX\Downloads\desktop.ini	Modified File	584 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
84f4227ffeaf1c4fe0523e7d609e58092177437564f0a5e47c77851d6b6c1222	C:\Users\RDhJ0CNFevzX\OneDrive\desktop.ini, C:\Users\RDhJ0CNFevzX\OneDrive\desktop.ini.ampkcz	Modified File	352 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
c8d8bd0cc71fba9732faa3ef80f43410b7a5618fc0afc992dcc867c81f2ca009	C:\Users\RDhJ0CNFevzX\Searches\desktop.ini, C:\Users\RDhJ0CNFevzX\Searches\desktop.ini.ampkcz	Modified File	904 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
eb1e22c8ca8f9e75a4226da63a2baf9d0c39f2aa4c808bd651a25ad76282ff25	C:\Users\RDhJ0CNFevzX\Contacts\desktop.ini.ampkcz, C:\Users\RDhJ0CNFevzX\Contacts\desktop.ini	Modified File	756 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
3a606a777f4c830a5e582c6dc83873bd84e271b4f0a06b40b5da60cda50dc71e	C:\Users\RDhJ0CNFevzX\Favorites\desktop.ini, C:\Users\RDhJ0CNFevzX\Favorites\desktop.ini.ampkcz	Modified File	756 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
8d195d6cb0e0d4447034b742d38a6f32e265739619ccaca3242e7908167e005b	C:\Users\RDhJ0CNFevzX\Links\desktop.ini.ampkcz, C:\Users\RDhJ0CNFevzX\Links\desktop.ini	Modified File	884 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f4de2c18c526d0e95dbc6535d934792ea663f68964bc26c3443fcc550f90c5a0	C:\Users\RDhJ0CNFevzX\Saved Games\desktop.ini.ampkcz, C:\Users\RDhJ0CNFevzX\Saved Games\desktop.ini	Modified File	584 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
661cb6050c8a3b102a157628ae64c8c20778923f8ccd4d71d39b92b5e404ed2c	C:\Users\RDhJ0CNFevzX\Desktop\2tiKE.m4a, C:\Users\RDhJ0CNFevzX\Desktop\2tiKE.m4a.ampkcz	Modified File	45.34 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
c03879bd3bd08585432dd354eb94b463e94098ad50ed4b20f11f3b8c4357f598	C:\Users\RDhJ0CNFevzX\Desktop\505vm9.swf.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\505vm9.swf	Modified File	99.30 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
23ebc38c60fa5244a10f6ac7eaf289d0a9bec9091202390e1720cc0d5ccd6e3a	C:\Users\RDhJ0CNFevzX\Desktop\9ABjQ1b3wA2cIKcd.flv.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\9ABjQ1b3wA2cIKcd.flv	Modified File	124.13 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
c85dbbe2a39b2a51eb30beb8cc97348a1c0e7409df1f42ddd413bf569444bd96	C:\Users\RDhJ0CNFevzX\Desktop\Bh_dyqBOzR8.swf.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\Bh_dyqBOzR8.swf	Modified File	45.91 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
424f34e9f98781ea427679a4fc5b6c1c73548ef9c5ab9d790e4acc6833ec09d7	C:\Users\RDhJ0CNFevzX\Desktop\BiqZhzQpPpNFiiegsAS.mkv.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\BiqZhzQpPpNFiiegsAS.mkv	Modified File	34.01 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
b130258b2c6120ed13eda2b666eb61de5fc55a896f30c9fc9160ed299e4224d4	C:\Users\RDhJ0CNFevzX\Desktop\CpL8O_LsjVMCQa-GI.gif, C:\Users\RDhJ0CNFevzX\Desktop\CpL8O_LsjVMCQa-GI.gif.ampkcz	Modified File	33.55 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
0fd44b5023c28b8af7003a7d0efd2f847b17f6b623c2b6a6681ab176a91a0b86	C:\Users\RDhJ0CNFevzX\Desktop\ICzw-hYXI.bmp, C:\Users\RDhJ0CNFevzX\Desktop\ICzw-hYXI.bmp.ampkcz	Modified File	125.30 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
dd93227ef6bb3ea8b1e1a998760c41d1b1d3f634b78aad466c2cbbf31327a704	C:\Users\RDhJ0CNFevzX\Desktop\iEg5ajMoeBZC.mp4.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\iEg5ajMoeBZC.mp4	Modified File	33.61 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
c624dc44fc3dd28b2efbc4ca9872fc6d43b54373557203f379df2829cff9a456	C:\Users\RDhJ0CNFevzX\Desktop\jkAT8Q.rtf.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\jkAT8Q.rtf	Modified File	103.30 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
fc1d968f8b7eb3c4e4f5383ebbf0ffb6d7d9826c8b362a656217e7be59107b6d	C:\Users\RDhJ0CNFevzX\Desktop\k-2kcKE.mkv, C:\Users\RDhJ0CNFevzX\Desktop\k-2kcKE.mkv.ampkcz	Modified File	38.91 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
cf6c834adfc67033c09c2ae1df7dd7a1af4f809ffd9a3825bf02c03b5681cdff	C:\Users\RDhJ0CNFevzX\Desktop\KvJg7fTjd.ppt.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\KvJg7fTjd.ppt	Modified File	119.66 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
624d83ec7298a0a1a6737756732d8f9703693bdf0070525d4154ae3b16621ed7	C:\Users\RDhJ0CNFevzX\Desktop\mS0Pc.m4a.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\mS0Pc.m4a	Modified File	119.76 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
12ac46bff6470b452efbfecb9462f7907665581c7cff1df4a9699f05f5ec3172	C:\Users\RDhJ0CNFevzX\Desktop\NdRfu9tUbl.wav.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\NdRfu9tUbl.wav	Modified File	29.86 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
56304301be5a98a51fd97a5d4248d3a21c8c8ef749d845db13c7394ae778bf00	C:\Users\RDhJ0CNFevzX\Desktop\Pdz8n1 UI6B5ybck59.mp3, C:\Users\RDhJ0CNFevzX\Desktop\Pdz8n1 UI6B5ybck59.mp3.ampkcz	Modified File	86.01 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5a322652307a976814e0aa3f95a8b110dec90014ce1edb10340acfafcbe83b36	C:\Users\RDhJ0CNFevzX\Desktop\R4ZOtCCfPyPi.png, C:\Users\RDhJ0CNFevzX\Desktop\R4ZOtCCfPyPi.png.ampkcz	Modified File	75.68 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
0eceb1421c44050fcf1b624b0146c391943dae9c6e7388c2cf2fa506eefccb17	C:\Users\RDhJ0CNFevzX\Desktop\SfNsa8YB.avi, C:\Users\RDhJ0CNFevzX\Desktop\SfNsa8YB.avi.ampkcz	Modified File	106.61 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
9f1c06a17224c9078ed033faaf9d5de69204fd2d17f7b7addee100a4fb74eaf	C:\Users\RDhJ0CNFevzX\Desktop\sxWMOh.mkv.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\sxWMOh.mkv	Modified File	36.95 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
72357217b1e0c71a704afdce2f33c6540b32cecfebd115da8ac07865d179e2f9	C:\Users\RDhJ0CNFevzX\Desktop\t8p41K1nPNZvX.m4a, C:\Users\RDhJ0CNFevzX\Desktop\t8p41K1nPNZvX.m4a.ampkcz	Modified File	33.66 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
d59da380eef6105df87a5a8ed2f28cc2772ee6bf712447d664a4a9f8271ac8bf	C:\Users\RDhJ0CNFevzX\Desktop\tSEGMvCPcMx.jpg, C:\Users\RDhJ0CNFevzX\Desktop\tSEGMvCPcMx.jpg.ampkcz	Modified File	133.18 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
80dff20331c1b2c2a8a1d1287eb2169933171c655e83e601596b1b8213d4c6c4	C:\Users\RDhJ0CNFevzX\Desktop\y2H9O8xlmETgCAbycT.png.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\y2H9O8xlmETgCAbycT.png	Modified File	53.18 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
11f2e7aeb5619eebc6f4331e96d744d41e9b84dad28b2d5eff24b91df791a967	C:\Users\RDhJ0CNFevzX\Desktop\ys5FVy3YwYbsg.m4a, C:\Users\RDhJ0CNFevzX\Desktop\ys5FVy3YwYbsg.m4a.ampkcz	Modified File	115.86 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
e19a77d484aae043582db932f76ab330a33720964e689dceb414336af7390433	C:\Users\RDhJ0CNFevzX\Desktop\Zr1fJuAtmLuvrKkw.gif, C:\Users\RDhJ0CNFevzX\Desktop\Zr1fJuAtmLuvrKkw.gif.ampkcz	Modified File	104.47 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
1dc4d1b4f84bc9558fafe0f8c94da733903e841f874aa848bbe6a9bd055bdecb	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\2HtL-q.csv.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\2HtL-q.csv	Modified File	72.57 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
fa709d9f60e5e7cf3c16dc737af740ced3e869a9891224ca3abcbc7835f5302f	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\7Bsy4NSMiVQmfv8k.m4a.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\7Bsy4NSMiVQmfv8k.m4a	Modified File	52.41 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
58cbd82ca366a569a58d0154fc1882aa6d6956bb1d1f6a72bebba969581da2ee	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\8LljmtPnMSEYSYG.csv, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\8LljmtPnMSEYSYG.csv.ampkcz	Modified File	17.55 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
4635a2b016bfa7a5bc15a444bea423954a8792d41ba8145370d1fd745d649d2f	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\8Vi4 VdapZ6YLX5Sp.flv.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\8Vi4 VdapZ6YLX5Sp.flv	Modified File	92.20 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
d25c6b54a541c3e0710c98689f8071414c9515d200eb56292991fd1f2528a766	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\BKUVLc.bmp.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\BKUVLc.bmp	Modified File	70.38 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
4aa9d3d6be9929d2d624a2ede42bf84e8bf43a3ec3f564ac4365ca40432097c3	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\bz0WFA-cPHK_6RXp.m4a.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\bz0WFA-cPHK_6RXp.m4a	Modified File	87.38 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
cc748e70f0466a90791d387a628b364f3b948dbaf3ac8e652bfab27f051d1496	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\ggv8WxB.gif, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\ggv8WxB.gif.ampkcz	Modified File	54.47 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
aa1f95036688f12cefc6cdb2b853581a0aae54962a4eaf5eab4bc3c6849d22e2	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\JHyJ2FcVg5iar.mp3, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\JHyJ2FcVg5iar.mp3.ampkcz	Modified File	20.26 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
f8a164e3494506bc339e900f637eaf84e6261b2250a81cec40cbc4c638e3e5e3	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\mB4Ez1kKY5Cs.mp3.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\mB4Ez1kKY5Cs.mp3	Modified File	8.82 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
4dc1f6c913a2f07e3bebd0243d64bc1c146fa8cf105ec41e52b128b856200865	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\mFs5gB9Z3Uguw495HmEZ.jpg.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\mFs5gB9Z3Uguw495HmEZ.jpg	Modified File	28.57 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
761f8472d4a5242384e357df4bf31b43056066063b235bae53e19e9c6561bd47	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\RPzmf9DjF1.pptx.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\RPzmf9DjF1.pptx	Modified File	99.91 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
d20ca94441449a800b3635efcba51e30fd6efc8b93703a6f255bcc12c33725aa	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\SjWyWkMIArJ.docx, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\SjWyWkMIArJ.docx.ampkcz	Modified File	64.49 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
ae81e9dc1c0fedb91d16bad13b920c1fa04c0c048ac08d4e8ae0caadbd51c2ec	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\VADyx2_L0xN.flv, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\VADyx2_L0xN.flv.ampkcz	Modified File	104.09 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
c8d379eedc4262209dec46fcbeeac89dbf35b3da66f40c52ebfb83bfe2b5f48e	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\vXhGV8MRaVScOkV5f5.ods, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\vXhGV8MRaVScOkV5f5.ods.ampkcz	Modified File	130.34 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
0e49860c0c62c8e0d0578f7c65bc1fb9e4a5cb8c51c894ba394c31b1d9e46671	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\WTyYMq00n.m4a.ampkcz, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\WTyYMq00n.m4a	Modified File	18.41 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
fdbc3968b1ff45b2e77394f1d7bfbe295d95c135a80151d6c8f229fb92e0e44b	C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\Y_Ku-Plvvx.png, C:\Users\RDhJ0CNFevzX\Desktop\Bjr3u\Y_Ku-Plvvx.png.ampkcz	Modified File	2.28 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
dee9357117bf3b93b3f1a47e9f0a6680a0523d00c03eb728a828b29c8f6ceb25	C:\Users\RDhJ0CNFevzX\Documents\8-58vgRqyz gS.pptx.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\8-58vgRqyz gS.pptx	Modified File	82.47 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
42de96a80311b5611e4dc5f209a11c95d792f0eac61d0435f2ce201af5717d48	C:\Users\RDhJ0CNFevzX\Documents\AEfN7e6MhjMF2F11JEs.xls.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\AEfN7e6MhjMF2F11JEs.xls	Modified File	11.88 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
c657a92c9d4001e439f3bee5e6a345c5d92220c1c2c3ea607f348c8527271a81	C:\Users\RDhJ0CNFevzX\Documents\AJOZtXvu7QfT.odt.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\AJOZtXvu7QfT.odt	Modified File	49.59 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
1d09c7420b537223c8ba6c1bc6b8ef183f3a348cd9732ff072f57964470ba820	C:\Users\RDhJ0CNFevzX\Documents\BAJe.docx, C:\Users\RDhJ0CNFevzX\Documents\BAJe.docx.ampkcz	Modified File	81.11 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
ccfa528394b2cb1da954b8369dbc38007277b2fe60249ec498520cc8231de369	C:\Users\RDhJ0CNFevzX\Documents\EgNVA.pptx, C:\Users\RDhJ0CNFevzX\Documents\EgNVA.pptx.ampkcz	Modified File	18.01 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
6c080456c30c334bff543bfc7b062592a8daf2f1020c8c6b271c525be6470ab1	C:\Users\RDhJ0CNFevzX\Documents\foayjE.pptx, C:\Users\RDhJ0CNFevzX\Documents\foayjE.pptx.ampkcz	Modified File	22.93 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
babca4a0b75187d59a92ad8de610cf7c101bd82248f2a22306e4c9f614701d89	C:\Users\RDhJ0CNFevzX\Documents\iOVreLoxPhj7stpatiPe.docx, C:\Users\RDhJ0CNFevzX\Documents\iOVreLoxPhj7stpatiPe.docx.ampkcz	Modified File	53.38 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
eef114d4d8374c4e11aed14e3e9a53dbb9c72720571cb76b81a53f32069d648d	C:\Users\RDhJ0CNFevzX\Documents\Juhec_87-J -LcDPj7R.xlsx, C:\Users\RDhJ0CNFevzX\Documents\Juhec_87-J -LcDPj7R.xlsx.ampkcz	Modified File	103.51 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
420dd907d5bceca5e8228a3c1c78c6dceeedc19fb72e23c2e1bc3457038fd7cb	C:\Users\RDhJ0CNFevzX\Documents\LYfQAN97cU.doc.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\LYfQAN97cU.doc	Modified File	108.09 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
d70beb8cc6d3fc73690659a30bfad4762859faa525425f4fa1ecc3cec6393353	C:\Users\RDhJ0CNFevzX\Documents\nh_ayDk4U dJuq.pptx.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\nh_ayDk4U dJuq.pptx	Modified File	34.66 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
df04671d0ae9fcc93cd28d839a18cad265d5a0295469950666e5a190aae2fc11	C:\Users\RDhJ0CNFevzX\Documents\NOUPcFxdi9.xlsx.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\NOUPcFxdi9.xlsx	Modified File	120.53 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
c9923d9e4be58436ac747994c54ac4f49843916ad119360290c12abcb08df169	C:\Users\RDhJ0CNFevzX\Documents\NyHQqR6F02G_ox.pptx.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\NyHQqR6F02G_ox.pptx	Modified File	81.91 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
848975ebd101f2c6512c3f25bd125971aa390a93f3e4a48f0b9e554955b79723	C:\Users\RDhJ0CNFevzX\Documents\qn--Dnwch0FHbbgzTTO.doc, C:\Users\RDhJ0CNFevzX\Documents\qn--Dnwch0FHbbgzTTO.doc.ampkcz	Modified File	108.22 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
aa0dfc5fd9c14fe931f14e5ca311ae413fb00df519c78fa5d82a055e3b7d8935	C:\Users\RDhJ0CNFevzX\Documents\reOlkC.xlsx.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\reOlkC.xlsx	Modified File	48.57 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
201f8ad153ee9636579cc32490a72bdd719654c4dadcdc9e2179283408d41686	C:\Users\RDhJ0CNFevzX\Documents\sBn Uk0ytdM055VR.doc, C:\Users\RDhJ0CNFevzX\Documents\sBn Uk0ytdM055VR.doc.ampkcz	Modified File	69.68 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
265817724c55c272a9f2516703449d88a784fd50bf73d126653a75d88647da39	C:\Users\RDhJ0CNFevzX\Documents\Sxq8yYPsbOADIX.xlsx.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\Sxq8yYPsbOADIX.xlsx	Modified File	102.30 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
859a2ae9fcb99c2eec5d62ab7298253a7b4fd503af9875e4ef6e9f24fb35deec	C:\Users\RDhJ0CNFevzX\Documents\uDnFB3fA14uy4UENlcK.docx.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\uDnFB3fA14uy4UENlcK.docx	Modified File	126.55 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
4f7bcc5b34ef798e941623c40aa381faa87b751f85b6ed263efc09a7a7429635	C:\Users\RDhJ0CNFevzX\Documents\vy87ulZFy.docx, C:\Users\RDhJ0CNFevzX\Documents\vy87ulZFy.docx.ampkcz	Modified File	110.84 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
1bb9465174be973f26424f9c01f87e808bc8d372057113ba6148eedac1936a75	C:\Users\RDhJ0CNFevzX\Documents\YdjNmFIdm.xlsx, C:\Users\RDhJ0CNFevzX\Documents\YdjNmFIdm.xlsx.ampkcz	Modified File	50.43 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
900b952abd5572a0fef4996d77b2876331 88d9966da0970eae8a48d64a893112	C:\Users\RDhJ0CNFevzX\Documents\YyiJJhqdwi8qn.docx.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\YyiJJhqdwi8qn.docx	Modified File	88.32 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
b73b6bd2e87d834e37a358bc346e074ab2cff549c775b6d0e80b35b51715f412	C:\Users\RDhJ0CNFevzX\Documents\F_8pl8t\5EZ7tX.ods, C:\Users\RDhJ0CNFevzX\Documents\F_8pl8t\5EZ7tX.ods.ampkcz	Modified File	106.55 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5142fd16b5f469a953818d9fa f56c9cb245e64a7c10b301d1 e89dde720cf043a	C: \Users\RDhJ0CNFevzX\Documents\ F_8pl8t\o0S4MtYXa7.odp.ampkcz, C: \Users\RDhJ0CNFevzX\Documents\ F_8pl8t\o0S4MtYXa7.odp	Modified File	57.74 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
0edf25825f5a0900c1d1f9583 769986f87f7278e5f524009f5 13a87037b009a3	C: \Users\RDhJ0CNFevzX\Documents\ F_8pl8t\qQxnuP1.rtf.ampkcz, C: \Users\RDhJ0CNFevzX\Documents\ F_8pl8t\qQxnuP1.rtf	Modified File	10.51 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
7d7bc09304bbbd4b5a02348 15af74c76a7ae8b48d7fc3f4c 9c1dda1bc0645ce1	C: \Users\RDhJ0CNFevzX\Documents\ F_8pl8t\uvz3Z3AyRuC12.xlsx, C: \Users\RDhJ0CNFevzX\Documents\ F_8pl8t\uvz3Z3AyRuC12.xlsx.ampkcz	Modified File	49.16 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
7b8ef41751deee524aa34bfb acc776e0212953a5584504e 6b2917d8e5d1beb04	C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\-hnSJxj1Uj.xls.ampkcz, C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\-hnSJxj1Uj.xls	Modified File	130.11 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
13ebcfcf33d8b4372cf5c2dec 5bd4442d672d2e47f409b5c1 c0dd3df664c3b03	C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\0aqOojXPcy4.pptx, C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\0aqOojXPcy4.pptx.ampk cz	Modified File	63.82 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
895ded3841774d208437c9d 02fc21e723ef1e77f96fbd2bc b99b50eb326c8ad2	C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\5JE02Kb.xls.ampkcz, C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\5JE02Kb.xls	Modified File	53.93 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
d68383ac76368d04e8b0889f b8e970f7a03ff76598ee2cf91 cbbeca9e7f81b02	C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\8G_KTv3fC9ZSX8qy.ods .ampkcz, C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\8G_KTv3fC9ZSX8qy.ods	Modified File	52.47 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
de61fc75ab7b51fdee7c3e24 ceb64566f5c5731d029a5822 0fe7c03a4183a1f7	C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\CFltAr.pdf.ampkcz, C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\CFltAr.pdf	Modified File	61.53 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
910d7a2dc7cce6679d45f85b d08f42c19a9eec6eee628408 0dbfa8c13f1f4de7	C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\dv1BjUamcjV9b3.ods.a mpkcz, C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\dv1BjUamcjV9b3.ods	Modified File	66.43 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
ae99ca1dca84f38ed237c0eb 72a813fa46a2f0d40cf6434fc 09b7f05a874af28	C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\kDFn_YG XXw.xls.ampkcz, C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\kDFn_YG XXw.xls	Modified File	116.16 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
07d800477d7e1b2757d9a4c 615a97c9688209e7a8e19e2 79cb7e3a5c4edc1370	C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\pKWEXKp.pps, C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\pKWEXKp.pps.ampkcz	Modified File	66.41 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
4de4560180e5ae4cbacdb3a 5c308cd70ff62f54093d2cb83 4ce4bae20c1b7629	C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\TyXrZ.docx.ampkcz, C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\TyXrZ.docx	Modified File	53.43 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
43f4b4a554095cf21fc8907ed 6a7b625533923fa29f3ca314 ba5c970ac64640b	C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\xqlp\D6AC.pptx, C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\xqlp\D6AC.pptx.ampkcz	Modified File	121.09 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
24fb3ffc04b6e079aed1aaf27 2c0452026400fe4b9a7fdd55 52a13e7b2396255	C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\xqlp\hV7Qa.ods, C: \Users\RDhJ0CNFevzX\Documents\ JN3akvSGJi\xqlp\hV7Qa.ods.ampkcz	Modified File	22.43 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8f549b4a2ce61b7e3138c5050ba09f8415c5b3f9ac12f10c7e03c75fdf91ba5c	C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\iANwPv2pHlptaIL2csWw.xlsx, C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\iANwPv2pHlptaIL2csWw.xlsx.ampkcz	Modified File	59.01 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
b97ff5521e842fcb86733c65089744b245e1c2404ac3ce47c070bf0c1e77dd39	C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\bRsSZdBZoL qdvafNLF.pptx.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\bRsSZdBZoL qdvafNLF.pptx	Modified File	8.28 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
13b5013da36efcafec6c74d8e3e4a2dc4a5b87e8a94552c6342c2a79fbab30a2	C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\FiPmvzuFqtW5HPbrQ_Z.pptx.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\FiPmvzuFqtW5HPbrQ_Z.pptx	Modified File	71.16 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
83e55421362e288189a5ce6c24f1e2a3b98b22631b14dbe7d209c056929a9c95	C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\G-GX1bLPx.docx, C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\G-GX1bLPx.docx.ampkcz	Modified File	105.97 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
42ab4a8a9e15486300616dd8161437d6dbccf859774ebd57bfb18609f62570e2	C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\NrPAwo00v KCQzI0375.xlsx, C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\NrPAwo00v KCQzI0375.xlsx.ampkcz	Modified File	80.63 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
484dc562990aa99a4443f1f8a0ad88852ad07313a709d67715a20cf58a8e6ca6	C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\Pl6cEP9l.xls.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\Pl6cEP9l.xls	Modified File	94.53 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
784cd3b795cd95b6869b979558821eadf39b9d133b90e39db7dc147eb439f911	C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\T3aXJ7JnmiGblPU5.doc, C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\T3aXJ7JnmiGblPU5.doc.ampkcz	Modified File	7.61 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
be8a9f7f945977c8fadfe61517cca4c6a50156f8a32f686b790634c38acd8dc3	C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\Zxb9-KR.xlsx.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\JN3akvSGJi\xqlp\We3dETs\Zxb9-KR.xlsx	Modified File	47.05 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
22850ed64e134f7be68df8e98c69bb81a57a211cdb230ce10cc9ee18122eb65a	C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst	Modified File	353.55 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
7dfcad0c63c6211022a494e612ba474c62da0f6d2f6ddf63c2e5f0d6cdc2cee9	C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\-K6OWWoFoPzYq-hdlX.pps.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\-K6OWWoFoPzYq-hdlX.pps	Modified File	75.11 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
e8220e4b5ac83364554da56d2b99ce5704839847b7991f7d730d57f1f4f5fa93	C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\3m6lgzrLvSc6-KZCaxw7.rtf.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\3m6lgzrLvSc6-KZCaxw7.rtf	Modified File	60.22 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
db253c43395290a997b9c6660605726c96f1c6eed24c54a1b88b9d5f6cd7bfeb	C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\5mb3rREI7ul1Pp.xls, C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\5mb3rREI7ul1Pp.xls.ampkcz	Modified File	114.72 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8c99e27414c0e877097d89ef1e069755b33c34bee258c411b8240ed283412044	C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\acXYO1yhB7sJfRK.doc, C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\acXYO1yhB7sJfRK.doc.ampkcz	Modified File	9.05 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
97a32cef66bb6d95dc96dd656797bb3ebb4e96a95e1f7038b9d9e75cf1807e19	C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\L4-0_ nb.pdf.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\L4-0_ nb.pdf	Modified File	59.76 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
f9d387abf28b7330c44bc42a54bf875ff0cf410faef8259edf87499c9b3b8035	C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\tSQ.docx.ampkcz, C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\tSQ.docx	Modified File	48.91 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
7f9c728d4f0d79e5cb22a28859641d06c794f594c73b05525ec68e4fb4e7943c	C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\v3V2Y3Hpen0RMfAQo.odt, C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\v3V2Y3Hpen0RMfAQo.odt.ampkcz	Modified File	108.95 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
d35a4ddd161f511b20de5528faeedaf136a57354e4559ed0fa60bb7fa78e96ab	C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\YKV-eu9e6_WXh5sqju.pdf, C:\Users\RDhJ0CNFevzX\Documents\Yvp 2zOqN8\YKV-eu9e6_WXh5sqju.pdf.ampkcz	Modified File	33.82 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
9e0416333fe0e883e3056eaa78a000b14bd0a6e3c9f0c618fd86c5e8d1cf8f86	C:\Users\RDhJ0CNFevzX\Pictures\AjN9y78hVh0UKrhnkL.jpg, C:\Users\RDhJ0CNFevzX\Pictures\AjN9y78hVh0UKrhnkL.jpg.ampkcz	Modified File	118.97 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
1d9dee75789de609b87632d0b562c81c337ec7b2bdcbae647309fe5ce61b8295	C:\Users\RDhJ0CNFevzX\Pictures\ejgt1B9nD_k9299.bmp, C:\Users\RDhJ0CNFevzX\Pictures\ejgt1B9nD_k9299.bmp.ampkcz	Modified File	77.28 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
d7eac1ca260d873434b3b7c928d100dd9e37927f153ddcb0f740a2d2010fb074	C:\Users\RDhJ0CNFevzX\Pictures\hVKydaZ1ZP.jpg, C:\Users\RDhJ0CNFevzX\Pictures\hVKydaZ1ZP.jpg.ampkcz	Modified File	101.09 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
9948f1d4ba23964fc662c32dd0269df0d0c4a473bf872fa75984a1445654d704	C:\Users\RDhJ0CNFevzX\Pictures\JLVegM9vxb3bekfHf_.jpg, C:\Users\RDhJ0CNFevzX\Pictures\JLVegM9vxb3bekfHf_.jpg.ampkcz	Modified File	110.38 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
679f364a17dbdf06c4ba09cafdc5559b763ee67f84e0374d8c33cec8a84a1117	C:\Users\RDhJ0CNFevzX\Pictures\k3kfHWnlQpe4M9v.png, C:\Users\RDhJ0CNFevzX\Pictures\k3kfHWnlQpe4M9v.png.ampkcz	Modified File	26.13 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
6e95f60c212a9b97f01b1e0728f1085d8d01dba5ec9038695567d85c302dde3a	C:\Users\RDhJ0CNFevzX\Pictures\OI3fbrHp3.png.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\OI3fbrHp3.png	Modified File	35.05 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
f0cf6c0626e045b6ff81042e5330b8ebbf6f600452c3c2d614343905e882698a	C:\Users\RDhJ0CNFevzX\Pictures\q2vCj7US.gif.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\q2vCj7US.gif	Modified File	79.09 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
0a3435c2fc86761a20d4eaaf627cd9e6ed979158f0f7aabbea61b005fb19270e	C:\Users\RDhJ0CNFevzX\Pictures\UEaT.png, C:\Users\RDhJ0CNFevzX\Pictures\UEaT.png.ampkcz	Modified File	1.72 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
2c66bbce148ef915a4e31aa847f09ff15012e8dfededcfbfeec2a9782f1cfb27	C:\Users\RDhJ0CNFevzX\Pictures\yvmvXCdl-L2md.png.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\yvmvXCdl-L2md.png	Modified File	66.70 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
72d12473cefc5bac3cd8a493c5e8b6b65543aee06ed718a513e15fb290934670	C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\3avUxb1BL_1g12oSkH5.png, C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\3avUxb1BL_1g12oSkH5.png.ampkcz	Modified File	104.68 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
be9a9f3bf42da831db4229207224106b0bcbc65276b5149371b9523d35fa2355	C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\82EsZ7p-5diz.bmp.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\82EsZ7p-5diz.bmp	Modified File	102.76 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
e1cdfe2ebb0bdb6fa1fe8b8c4735795f6acb81dbd28a654b68a01bc3238a0284	C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\95XyOZRwahuGE.bmp, C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\95XyOZRwahuGE.bmp.ampkcz	Modified File	11.76 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
5cbb34c01ca56902521ef22b5204c8567be02f4aec9e44232ec0a06ce6ff87ee	C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\pybRnums.gif.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\pybRnums.gif	Modified File	111.47 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
73eb76c3870e4e4b6a351b664ddcba9de43b5161f8a6cc0a32a8a2c819d19f74	C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\rC_A9e_Y_besF1X.gif, C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\rC_A9e_Y_besF1X.gif.ampkcz	Modified File	69.84 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
15e6a7bc5ebecab8035754711fad7031db874d81408b4c4f9d0a2c4346819ef2	C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\VxgH4lec2pnD.bmp, C:\Users\RDhJ0CNFevzX\Pictures\2y3wsQSAY8Vuz\VxgH4lec2pnD.bmp.ampkcz	Modified File	46.41 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
c0be9aed4b7fec90a72ad32edd1454242bb5d17fc67be0200a7a1539bb189bcc	C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	Modified File	456 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
19f081e541ace7a8d0dcad78d0003e7f67622e2ac8194bb7629cffd37d2327a6	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\1vouFPcx5u2EPwdO.jpg, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\1vouFPcx5u2EPwdO.jpg.ampkcz	Modified File	101.22 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
441ed7ab44b48463780791355f4d31aa73738d916c92bf2d2e5f553250d961e5	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\E AOhji2.bmp, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\E AOhji2.bmp.ampkcz	Modified File	53.05 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
7b84beae60fd2cf82746202469ba6af8b036e75046fea13b93dd0245c48f7868	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\fqUC.bmp, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\fqUC.bmp.ampkcz	Modified File	49.88 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
48b9208854f869e876ed83eb6c2ff8a718a9986bf5dc213e76e3a643f54646d2	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\kqG3aN.bmp, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\kqG3aN.bmp.ampkcz	Modified File	59.45 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
02b3ff6375d70168ec65439d0e1eb7f50b2e41a1faeda694e9d8c32281f310a5	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\Q_Ekrnom6M-AaivdFcPZ.gif, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\Q_Ekrnom6M-AaivdFcPZ.gif.ampkcz	Modified File	14.55 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
791878baedb4fa4618ab5261ced08b01efe24423228f84947a83e1dcb1bb7d89	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\U4hfL3Yd9m.bmp, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\U4hfL3Yd9m.bmp.ampkcz	Modified File	101.43 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f23e422a2ce99fa6cfb61504cb5e708be006da46ccf5f19f7441903e13ebd652	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\ZIvJ2tjP.gif.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\ZIvJ2tjP.gif	Modified File	81.28 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
66591ef7c80d0a6125b2a8ca833f56e590a11cab9d7ef01bb5e28e7c1aca7871	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\Asuu1.gif, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\Asuu1.gif.ampkcz	Modified File	4.38 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
77b88262b1de2127fb09ce3d273107262463b32ce15c15c70bfaf0268841cea9	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\c5qjp_9.png.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\c5qjp_9.png	Modified File	114.16 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
b394d4405a627b58af408800d719a935c5a38ecb6f3c6b6e1b2bc272923bbef8	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\i_HjOI0Pvfw-v.jpg, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\i_HjOI0Pvfw-v.jpg.ampkcz	Modified File	100.63 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
f96fc06670a522fd0c9aa3399272492ddfd55ce7f1da7e902bab39f3db1ef653	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\JGhfvZ7zWuY0.bmp.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\JGhfvZ7zWuY0.bmp	Modified File	13.30 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
d1cb95dabf612cb0b32085e3e0b13335a9f8e8df2ecda1c6c0614fd526048537	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\NbFcv7r.png.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\NbFcv7r.png	Modified File	129.53 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
952562d57f44afcd7b5bd2f5dd558b2e25ad4a850d25971acaed482966242e4f	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\PeNWmzhlJCX.gif.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\PeNWmzhlJCX.gif	Modified File	59.11 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
9bda52b016e6ee2f173d5b3be7b5aa6ccffa2e911f9d779a51e0e68e3f0b0e03	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\sNU4ZxXwBcEpxou.gif.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\sNU4ZxXwBcEpxou.gif	Modified File	21.36 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
91ff43ea499681825dbcc45840c64f7404d17fabe81bd2b0a875e259bb56425f	C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\yeL3pqI1j.bmp, C:\Users\RDhJ0CNFevzX\Pictures\iLPJWM2Zw-c\slPu\yeL3pqI1j.bmp.ampkcz	Modified File	107.16 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
90fff203ca59f46db51c1c2053f06039dbf33f51a72c38fae793b526a4100a22	C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\2Clz54JvlW _N1L.png, C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\2Clz54JvlW _N1L.png.ampkcz	Modified File	50.80 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
9123a7e87c4af676d410b9878b06ae8c1a28101fc45ca6ebf7d07ba3964c018e	C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\VXDZKI.jpg, C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\VXDZKI.jpg.ampkcz	Modified File	31.26 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
7ac5c05718c4bc2808705cfe600680efe2ab475237503a5c02b3e9ff499f2617	C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\AKzD1lY.png, C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\AKzD1lY.png.ampkcz	Modified File	53.57 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
d40af9df95b3164c3d7432303d65dfb7a496b0a73a840c26fdaccb26ac91a2d0	C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\Qlc4be.bmp.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\Qlc4be.bmp	Modified File	8.49 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
de0e961fa4cb2d336ab24e823350850647ed710f3a81e0acc1f9818bdebcf084	C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\r5DQrDCs.gif, C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\r5DQrDCs.gif.ampkcz	Modified File	48.05 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
5f967c382afa37bce4dd2fd56fe9e2beb3da8f03a1537cedc28e9f198c882582	C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\uOS_JODxfeSPDsu.png.ampkcz, C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\uOS_JODxfeSPDsu.png	Modified File	50.24 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
e0ae14124ed672847b5c84c4e3db7365cc46a422727d90f514f4c6d47a234218	C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\uXWtciW8Mz.png, C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\uXWtciW8Mz.png.ampkcz	Modified File	124.93 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
de035d7f7f4409c463bd1895d2e932dd4c1d3486edf7af9532fa6192b33976fd	C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\xLsjiwCf3AooR.jpg, C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\xLsjiwCf3AooR.jpg.ampkcz	Modified File	27.95 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
1c7aeda04d4808b67fdab0f7df33a00e2b897325c841c10eab5dbaab01cfcf10	C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\YGxlk.png, C:\Users\RDhJ0CNFevzX\Pictures\LIdMOQASD6\XlKnK1gfJe4zFhGoRY_F\YGxlk.png.ampkcz	Modified File	131.93 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
23341d0da3cce4a29985128dec6b74cb1c5996a80528f9831f5a27e57c54d3bb	C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini, C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini.ampkcz	Modified File	456 bytes	text/plain	Access, Write, Create, Delete, Read	CLEAN
cbd02a7e1d70f870367dbc58c0522df548ef6a811a031c5660e2f37a55487f0d	C:\Users\RDhJ0CNFevzX\Music\EcAoPKlkYeK4zcxY.m4a, C:\Users\RDhJ0CNFevzX\Music\EcAoPKlkYeK4zcxY.m4a.ampkcz	Modified File	62.24 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
6a16ed5b674c36f39ec95d0532efc05c0b06bbedbf9a5e831cba3f0de67a1083	C:\Users\RDhJ0CNFevzX\Music\JWRhu6PW-N_JtHKHctzp.m4a, C:\Users\RDhJ0CNFevzX\Music\JWRhu6PW-N_JtHKHctzp.m4a.ampkcz	Modified File	15.78 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
b3c3c76ba64bb6035c555e687cc8c6b1a4df8cf9258ebed8a230bf1e769b0324	C:\Users\RDhJ0CNFevzX\Music\InpwHWei4hMwarh_Gi.m4a, C:\Users\RDhJ0CNFevzX\Music\InpwHWei4hMwarh_Gi.m4a.ampkcz	Modified File	117.53 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
4c3f7fbb4974db12994b0eb0cf972a021ecd03b0762a626d892ce9a0eb3ba8	C:\Users\RDhJ0CNFevzX\Music\aOr_0l-_\2tOwtNlJ rxX6vXCj.m4a, C:\Users\RDhJ0CNFevzX\Music\aOr_0l-_\2tOwtNlJ rxX6vXCj.m4a.ampkcz	Modified File	41.53 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN
8acb130d588bee42a83223e4831cead03c3ffe49d62cfe50f5e36995c7dc0a83	C:\Users\RDhJ0CNFevzX\Music\aOr_0l-_\3lo_eiMEsy9m.m4a, C:\Users\RDhJ0CNFevzX\Music\aOr_0l-_\3lo_eiMEsy9m.m4a.ampkcz	Modified File	49.11 KB	text/plain	Access, Write, Create, Delete, Read	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\readme.txt	Dropped File	Access, Write, Create	SUSPICIOUS
C:\Program Files\Windows NT\winscp.exe	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wow64.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\wow64win.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wow64cpu.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows NT\those.exe	Accessed File	Access	CLEAN
C:\Windows\system32\dwm.exe	Accessed File	Access	CLEAN
C:\Windows\system32\KERNEL32.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\KERNELBASE.dll	Accessed File	Access	CLEAN
C:\Windows\system32\apphelp.dll	Accessed File	Access	CLEAN
C:\Windows\system32\msvcrt.dll	Accessed File	Access	CLEAN
C:\Windows\system32\advapi32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\sechost.dll	Accessed File	Access	CLEAN
C:\Windows\system32\RPCRT4.dll	Accessed File	Access	CLEAN
C:\Windows\system32\gdi32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\USER32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\dwmredir.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\udwm.dll	Accessed File	Access	CLEAN
C:\Windows\system32\dwmcore.dll	Accessed File	Access	CLEAN
C:\Windows\system32\OLEAUT32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\combase.dll	Accessed File	Access	CLEAN
C:\Windows\system32\bcryptPrimitives.dll	Accessed File	Access	CLEAN
C:\Windows\system32\dcomp.dll	Accessed File	Access	CLEAN
C:\Windows\system32\CoreMessaging.dll	Accessed File	Access	CLEAN
C:\Windows\system32\IMM32.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\uxtheme.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\dwmghost.dll	Accessed File	Access	CLEAN
C:\Windows\system32\dwmapi.dll	Accessed File	Access	CLEAN
C:\Windows\system32\d3d11.dll	Accessed File	Access	CLEAN
C:\Windows\system32\dxgi.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsCodecs.dll	Accessed File	Access	CLEAN
C:\Windows\system32\kernel.appcore.dll	Accessed File	Access	CLEAN
C:\Windows\system32\clbcatq.dll	Accessed File	Access	CLEAN
C:\Windows\System32\UIAnimation.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ism32k.dll	Accessed File	Access	CLEAN
C:\Windows\system32\avrt.dll	Accessed File	Access	CLEAN
C:\Windows\System32\Windows.Gaming.Input.dll	Accessed File	Access	CLEAN
C:\Windows\system32\CFGMGR32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\shcore.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\d3d10warp.dll	Accessed File	Access	CLEAN
C:\Windows\system32\d2d1.dll	Accessed File	Access	CLEAN
C:\Windows\system32\XmlLite.dll	Accessed File	Access	CLEAN
C:\Windows\system32\Cabinet.dll	Accessed File	Access	CLEAN
C:\Program Files\Windows Media Player\boy.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Sidebar\isspos.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\foxmailincmail.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Reference Assemblies\bitkinex.exe	Accessed File	Access	CLEAN
C:\Windows\system32\svchost.exe	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ucrtbase.dll	Accessed File	Access	CLEAN
C:\Windows\system32\user32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\GDI32.dll	Accessed File	Access	CLEAN
C:\Windows\System32\Geolocation.dll	Accessed File	Access	CLEAN
C:\Windows\System32\msvcp110_win.dll	Accessed File	Access	CLEAN
C:\Windows\System32\BiWinrt.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\twinapi.appcore.dll	Accessed File	Access	CLEAN
C:\Windows\System32\USERENV.dll	Accessed File	Access	CLEAN
C:\Windows\system32\profapi.dll	Accessed File	Access	CLEAN
C:\Windows\System32\bcrypt.dll	Accessed File	Access	CLEAN
C:\Windows\System32\deviceaccess.dll	Accessed File	Access	CLEAN
C:\Windows\System32\LocationFrameworkPS.dll	Accessed File	Access	CLEAN
c:\windows\system32\es.dll	Accessed File	Access	CLEAN
c:\windows\system32\fntcache.dll	Accessed File	Access	CLEAN
c:\windows\system32\FontProvider.dll	Accessed File	Access	CLEAN
c:\windows\system32\nsisvc.dll	Accessed File	Access	CLEAN
C:\Windows\system32\NSI.dll	Accessed File	Access	CLEAN
c:\windows\system32\netprofmsvc.dll	Accessed File	Access	CLEAN
c:\windows\system32\nlaapi.dll	Accessed File	Access	CLEAN
C:\Windows\System32\npmproxy.dll	Accessed File	Access	CLEAN
C:\Windows\system32\ole32.dll	Accessed File	Access	CLEAN
c:\windows\system32\winhttp.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WS2_32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\mswsock.dll	Accessed File	Access	CLEAN
c:\windows\system32\IPHLPAPI.DLL	Accessed File	Access	CLEAN
c:\windows\system32\WINNSI.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\powrprof.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
c:\windows\system32\dhcpcsvc6.DLL	Accessed File	Access	CLEAN
c:\windows\system32\dhcpcsvc.DLL	Accessed File	Access	CLEAN
C:\Windows\system32\DNSAPI.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WlanRadioManager.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wlanapi.dll	Accessed File	Access	CLEAN
C:\Windows\system32\BthRadioMedia.dll	Accessed File	Access	CLEAN
C:\Windows\system32\cfgmgr32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\DEVOBJ.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\bluetoothapis.dll	Accessed File	Access	CLEAN
C:\Windows\System32\rasadhlp.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\gpapi.dll	Accessed File	Access	CLEAN
c:\windows\system32\licensemanagersvc.dll	Accessed File	Access	CLEAN
c:\windows\system32\LicenseManager.dll	Accessed File	Access	CLEAN
c:\windows\system32\CLIPC.dll	Accessed File	Access	CLEAN
C:\Windows\System32\Windows.StateRepository.dll	Accessed File	Access	CLEAN
C:\Windows\System32\StateRepository.Core.dll	Accessed File	Access	CLEAN
c:\windows\system32\CRYPTSP.dll	Accessed File	Access	CLEAN
C:\Windows\system32\rsaenh.dll	Accessed File	Access	CLEAN
C:\Windows\system32\CRYPTBASE.dll	Accessed File	Access	CLEAN
C:\Windows\System32\Windows.Security.Authentication.OnlineId.dll	Accessed File	Access	CLEAN
C:\Windows\System32\wuapi.dll	Accessed File	Access	CLEAN
C:\Windows\system32\CRYPT32.dll	Accessed File	Access	CLEAN
C:\Windows\system32\MSASN1.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WINTRUST.dll	Accessed File	Access	CLEAN
C:\Windows\System32\UpdatePolicy.dll	Accessed File	Access	CLEAN
C:\Windows\System32\wups.dll	Accessed File	Access	CLEAN
c:\windows\system32\wdi.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\sxs.dll	Accessed File	Access	CLEAN
C:\Windows\system32\perftrack.dll	Accessed File	Access	CLEAN
C:\Windows\System32\WinTypes.dll	Accessed File	Access	CLEAN
C:\Windows\System32\msxml6.dll	Accessed File	Access	CLEAN
C:\Windows\System32\Windows.Web.dll	Accessed File	Access	CLEAN
C:\Windows\System32\iertutil.dll	Accessed File	Access	CLEAN
C:\Windows\system32\windows.storage.dll	Accessed File	Access	CLEAN
C:\Windows\system32\shlwapi.dll	Accessed File	Access	CLEAN
C:\Windows\system32\DPAPI.DLL	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\System32\ActXPrxy.dll	Accessed File	Access	CLEAN
C:\Windows\System32\Windows.Security.Authentication.Web.Core.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\msauserext.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\AuthBroker.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\wkscli.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\netutils.dll	Accessed File	Access	CLEAN
C:\Windows\System32\BitsProxy.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\wmiprvse.exe	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\FastProx.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\NCObjAPI.DLL	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\wbemcomn.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\bcrypt.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\wbemprox.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\wbemsvc.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\wmiutils.dll	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\wmiprov.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\ntmarta.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\WMICLNT.dll	Accessed File	Access	CLEAN
C:\Windows\System32\wbem\WmiPerfClass.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\pdh.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\wevtapi.dll	Accessed File	Access	CLEAN
c:\windows\system32\windows.staterepository.dll	Accessed File	Access	CLEAN
c:\windows\system32\StateRepository.Core.dll	Accessed File	Access	CLEAN
c:\windows\system32\tileobjserver.dll	Accessed File	Access	CLEAN
c:\windows\system32\msvcp110_win.dll	Accessed File	Access	CLEAN
c:\windows\system32\ESENT.dll	Accessed File	Access	CLEAN
c:\windows\system32\urlmon.dll	Accessed File	Access	CLEAN
c:\windows\system32\iertutil.dll	Accessed File	Access	CLEAN
C:\Windows\System32\CRYPTSP.dll	Accessed File	Access	CLEAN
C:\Windows\system32\bcrypt.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\wtsapi32.dll	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\WINSTA.dll	Accessed File	Access	CLEAN
C:\Windows\system32\USERENV.dll	Accessed File	Access	CLEAN
C:\Windows\system32\SspiCli.dll	Accessed File	Access	CLEAN
C:\Program Files\Windows Multimedia Platform\fling.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft.NET\whatsapp.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files (x86)\Windows Media Player\spgagentservice.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Portable Devices\centralcreditcard.exe	Accessed File	Access	CLEAN

Reduced dataset

Process

Process Name	Commandline	Verdict
a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe	"C:\Users\RDhJ0CNFevzX\Desktop\a7f09cfde433f3d47fc96502bf2b623ae5e7626da85d0a0130dcd19d1679af9b.exe"	MALICIOUS
svchost.exe	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\svchost.exe"	MALICIOUS

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

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

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows