MALICIOUS

Classifications: Ransomware

Threat Names: -

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe**
ID	#4191170
MD5	9fd056a806343253a57b3fb16260b16a
SHA1	6fe4d8992cd01266c26d28ef15fee7afa3ee0497
SHA256	baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299
File Size	230.50 KB
Report Created	2022-04-25 16:27 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (18 rules, 18 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #2) svhost.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #2) svhost.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 103 files by appending the extension ".coom".			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
3/5	Network Connection	All network connection attempts failed	1	-
	• Host "192.30.89.67" is unavailable.			
2/5	Hide Tracks	Deletes file after execution	1	-
	• (Process #1) baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe deletes executed executable "c:\users\rdhj0cnfevzx\appdata\local\temp\svhost.exe".			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #2) svhost.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe modifies memory of (process #2) svhost.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe alters context of (process #2) svhost.exe.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe starts (process #2) svhost.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe reads from (process #2) svhost.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #2) svhost.exe opens an outgoing TCP connection to host "192.30.89.67:11344".			

Score	Category	Operation	Count	Classification
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #2) svhost.exe tries to connect to TCP port 11344 at 192.30.89.67.			
1/5	Execution	Drops PE file	1	-
	• Drops file C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\svhost.exe.			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\svhost.exe".			
1/5	System Modification	Creates an unusually large number of files	1	-
	• (Process #2) svhost.exe creates an above average number of files.			
-	Trusted	Known clean file	1	-
	• File "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\svhost.exe" is a known clean file.			

Mitre ATT&CK Matrix

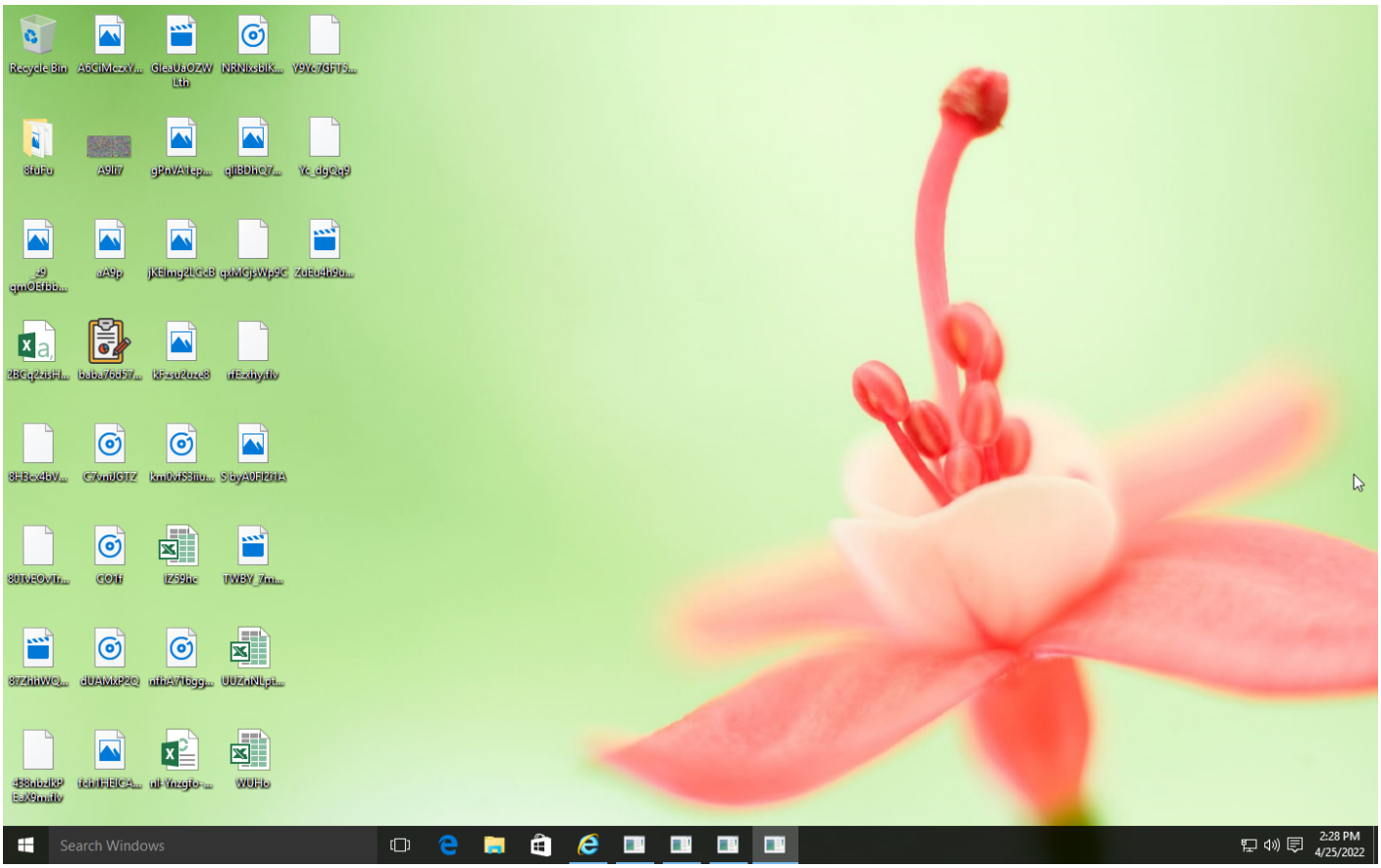
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection	#T1065 Uncommonly Used Port		#T1486 Data Encrypted for Impact
				#T1045 Software Packing				#T1005 Data from Local System			

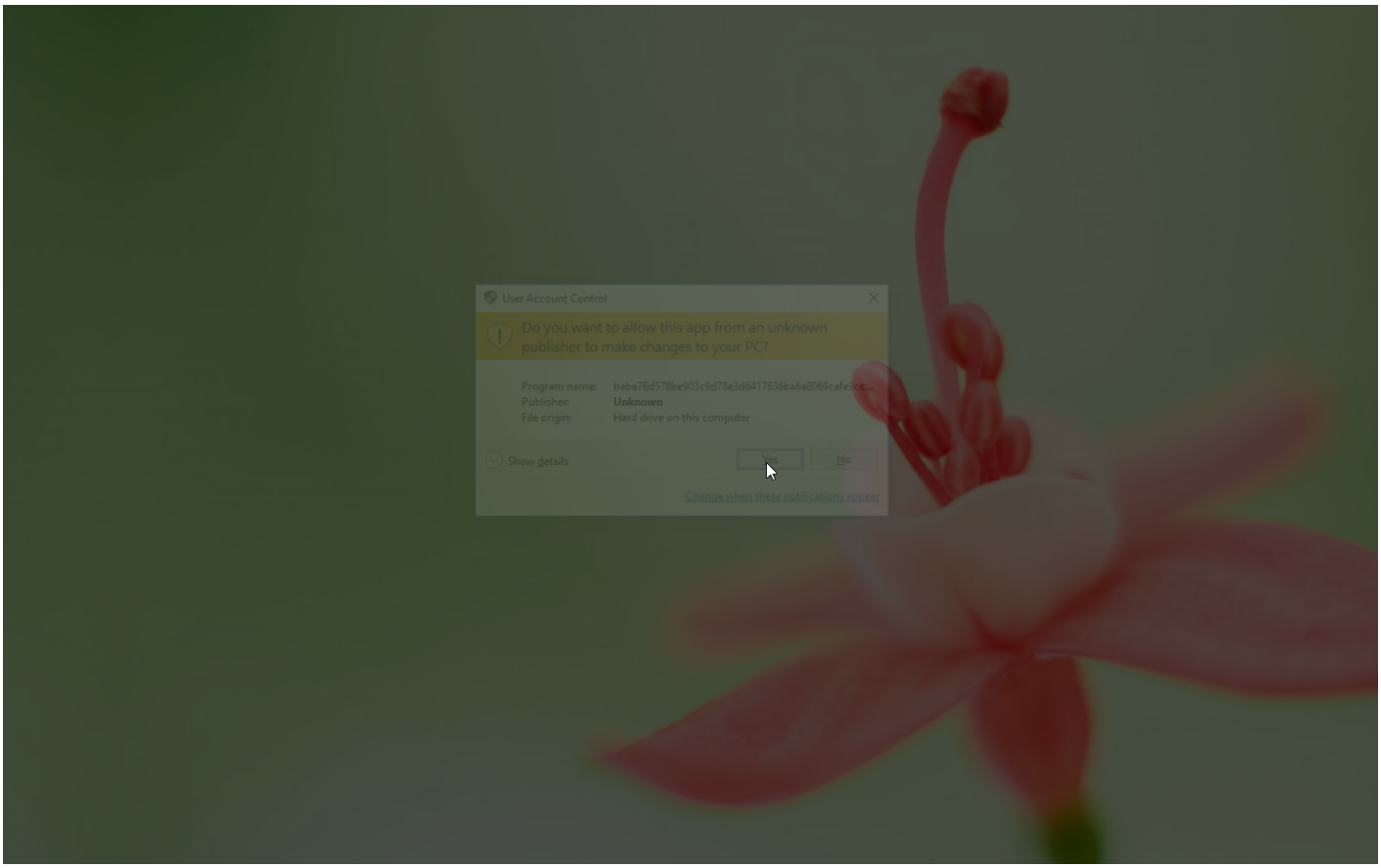
Sample Information

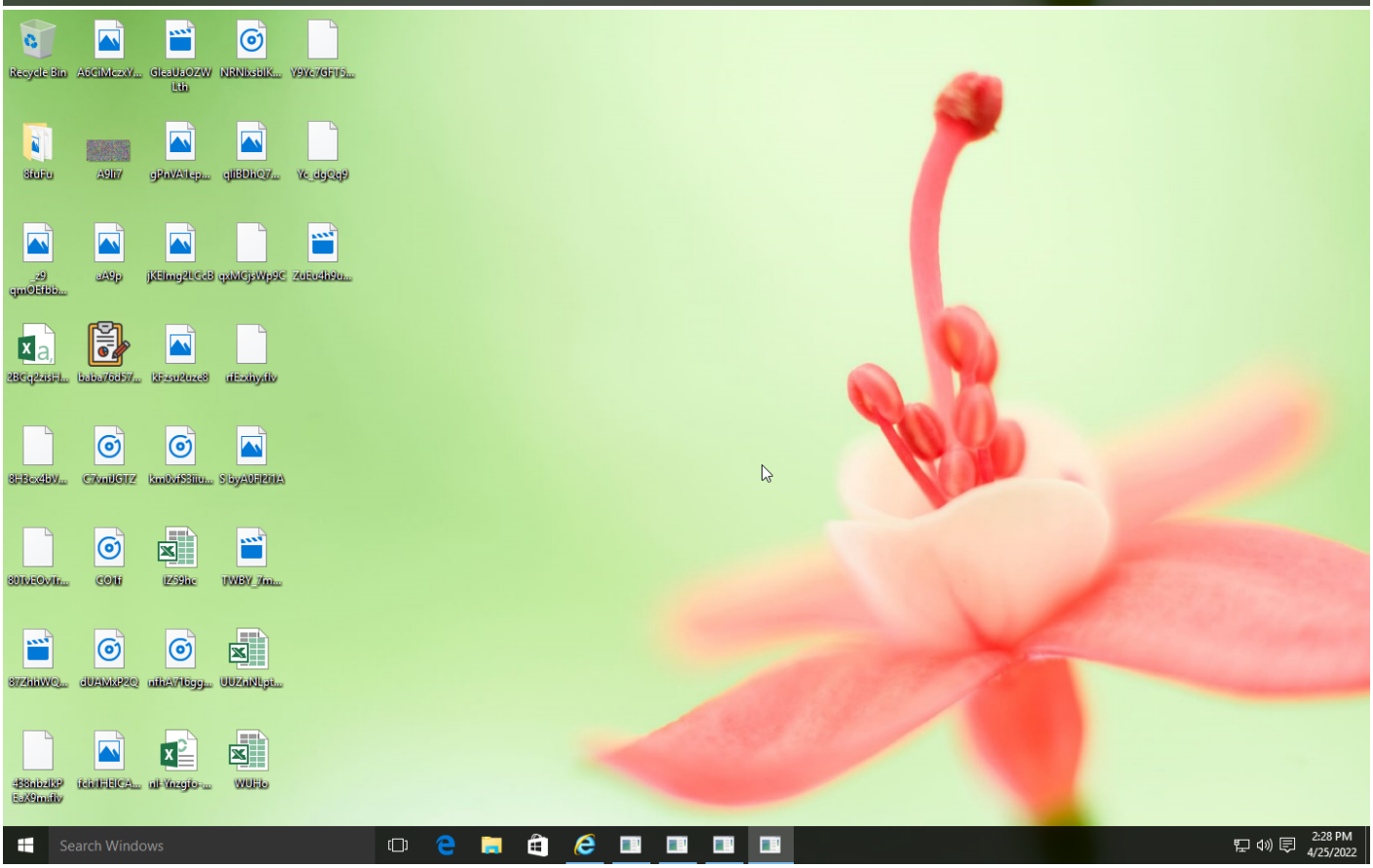
ID	#4191170
MD5	9fd056a806343253a57b3fb16260b16a
SHA1	6fe4d8992cd01266c26d28ef15fee7afa3ee0497
SHA256	baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299
SSDeep	3072:DUNBcGd4jXujV1lKEJWcYtRpOa0vfIBFYCZiEK0Pi+Gd2lxeF3l8h+SN+e0g:DGvd4C5nJWJRH0XIBFYchKwe
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe
File Size	230.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-04-25 16:27 (UTC+2)
Analysis Duration	00:03:58
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
2:28 PM
4/25/2022





Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

1 ports 11344

1 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

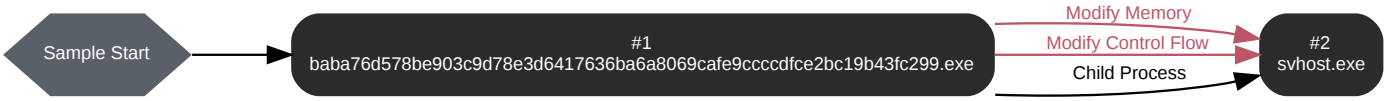
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 84108, Reason: Analysis Target
Unmonitor End Time	End Time: 147744, Reason: Terminated
Monitor duration	63.64s
Return Code	0
PID	1124
Parent PID	1184
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\svhost.exe	254.30 KB	2c75ad03937eee1046942d48b0fdc366e908dc00a5defc8f3b9513c7821a78b8	✖

Host Behavior

Type	Count
Environment	4
File	4
User	1
Process	1
System	1
Module	19
-	3
-	7

Process #2: svhost.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\svhost.exe
Command Line	"C:\Users\RDHJ0C~1\AppData\Local\Temp\svhost.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 129732, Reason: Child Process
Unmonitor End Time	End Time: 315710, Reason: Terminated by Timeout
Monitor duration	185.98s
Return Code	Unknown
PID	2092
Parent PID	1124
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe	0xc60	0x400000(4194304)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe	0xc60	0x402000(4202496)	0x1c000	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe	0xc60	0x41e000(4317184)	0x18e00	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe	0xc60	0x438000(4423680)	0x200	✓	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe	0xc60	0x35e008(3530760)	0x4	✓	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe	0xc60 / 0xbf8		-	✓	1

Dropped Files (103)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\2BCq2zisH1tDLrOOSW.csv	28.56 KB	e15fb0f7e86731ad15fef51cfa1fd65842b676e9a6789917e911b8d90d3fdc47	✗
C:\Users\RDhJ0CNFevzX\Desktop\438nbzIkP EaX9m.flv	8.27 KB	8b54f7f5ee40104ef09ce3111152092831a35967faed73bb8bc93fd0f08db427	✗
C:\Users\RDhJ0CNFevzX\Desktop\80TvEOvTr5nvyI.swf	5.66 KB	7126033375c6f2fed65e1eaebcd571086ab5cddf6f85890c78e90feb031abdd1	✗
C:\Users\RDhJ0CNFevzX\Desktop\8H3cx4bVP1NLZr8fhYb.swf	28.11 KB	54a4d5eeed216437f598832a3f91b3fda8edc6113b3e7d4aea7d5820b9f86eac	✗
C:\Users\RDhJ0CNFevzX\Desktop\A6CiMczxY2F3JXYRzK.png	45.27 KB	f75a3190f9a4d017be6a82d1934490e20374026278855b2cf54d77ef1253ea00	✗
C:\Users\RDhJ0CNFevzX\Desktop\A9li7.bmp	97.55 KB	cf51e630392a39e404a466508d4d0fb53151c141a280c6c12fc939820ba83b11	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\aA9p.png	57.72 KB	6a7d386832a959523d4db3ca7140e281972144f2cb924636165b3032325b0a13	✗
C:\Users\RDhJ0CNFevzX\Desktop\fch1HElCA7Cv3KXW.png	12.16 KB	ccc69f004e2c412ec9d7c8a4753f662c47704353c053b65daefe18986ad0db6e	✗
C:\Users\RDhJ0CNFevzX\Desktop\gPnVA1epmh.png	94.27 KB	141a2395f2d97c35f7da24d72188a2f8b285ac6f75bf852d497b19df01001d98	✗
C:\Users\RDhJ0CNFevzX\Desktop\jKElmg2LCcB.png	57.03 KB	e2c857d9a631269061ecee97493d6997a1e94be6e8d2e8dc959ca502036ad9ce	✗
C:\Users\RDhJ0CNFevzX\Desktop\kFzsu2uze8.jpg	30.11 KB	7ca8109ef7fcec60ac78181409bd553bc4f967ef6c82aee55909f2f673228e6d	✗
C:\Users\RDhJ0CNFevzX\Desktop\lZ59hc.xls	77.30 KB	b1c433ce6592762b0c75c3e3304e2e357432e01ae86fa8e2b5457e4bff9be071	✗
C:\Users\RDhJ0CNFevzX\Desktop\nl-Ynzgfo-bdwG.ods	31.83 KB	2a02a7515e97746c3fca5892147d9144c872a306d4cef86f1277cc754fcb375b	✗
C:\Users\RDhJ0CNFevzX\Desktop\qxMCjsWp9C.swf	74.19 KB	a3c9a54e2fdc598b80530c080cd4fe23794cc6e850c67142c427a42a70a881c2	✗
C:\Users\RDhJ0CNFevzX\Desktop\rfEzxhy.flv	76.03 KB	7005c7ea2d767b05d515cfca1eb41e4624adb6df0ff826a806004631f03ffbc6	✗
C:\Users\RDhJ0CNFevzX\Desktop\S byA0FI2i1A.jpg	96.86 KB	24ba5f74c775f01e224d56605fa4fecdcd6799f34436889feb685b35a678c57c	✗
C:\Users\RDhJ0CNFevzX\Desktop\UUZnNLpt1yyHK2REqD8.xls	36.98 KB	b2f13a5eaa83aaf2127b1c0e74af302f583bcc982201e46994fb76bb5774680d	✗
C:\Users\RDhJ0CNFevzX\Desktop\WUHo.xls	9.30 KB	77517b83d93f5c3e923557b37ae07a58186ba6bcb5ab7f14da4402aac5fbec24	✗
C:\Users\RDhJ0CNFevzX\Desktop\Y9Yc7GFT5o-.flv	16.22 KB	e87d2d8c53b39860bda28767890b9b5f7190e89279d88f574eda5ba46314ef26	✗
C:\Users\RDhJ0CNFevzX\Desktop\Yc_dgQq9.swf	41.48 KB	05ecf26c31753a8124731f855c7b61b1820da244b78f30349de684c858385297	✗
C:\Users\RDhJ0CNFevzX\Desktop_z9 qmOEfbbR2Ho.png	93.98 KB	e7e9de0f31308b1ae5a89c396e8bfea678fa758ef4f710809d01d011e011fadc	✗
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\0b2BYJ.bmp	6.11 KB	d396f448b8c5a4bde7f398025a89d7d7c6176efafe7c52e770b700e35b8c486e	✗
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\bCDo3xL3DQNnY-NDn8o.csv	40.14 KB	94dc130865f4a807a18e7fed19decf55ac523ba7e48b2568b1ffdd90006ede46	✗
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\BP7HIx-dC.docx	29.34 KB	928f7ac33846ee5cad9bc5981ac2c5b1b524e0293b14497adb18f475c16d67c6	✗
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\HTPNUNi5N0PRF7q49.flv	55.39 KB	d838b30140d23a9955d3cc05704a3a62a30b5953b5ccd9c67bbea9b06e3370ae	✗
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\IohkShS91M7hT3L\-iPNtWwPnLb_xVEK.xlsx	38.33 KB	c0d5f8efc0eb1526b5ffe4aac4cf508bf4f6dafd58e821ab1966e13396f7681a	✗
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\IohkShS91M7hT3L\a0LPQFabf2-tcp.flv	1.69 KB	9a72eaf70216310172229d9a4a6de5655cfab38f75733123702a5ea594a59253	✗
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\IohkShS91M7hT3L\T3Pjk61xtk9SizI9Gz7.jpg	61.70 KB	6e8e6a4c345693be9fa032d6672e244c45fdb22a05620bf166590d2698a6b446	✗
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\IohkShS91M7hT3L\Wy9hdiHoa5p6DL6.wav	8.86 KB	0f9336ae5205f674bbdbe21d17e74c20d3f1638da1493c306c2ecbac031233ff	✗
C:\Users\RDhJ0CNFevzX\Documents\0tvBM_QdD3TVO2ZA_6P.ods	46.30 KB	3642e7e80c63e9cc4e7cdfa3dbfe718c6e3dd1ab7c3c88c42d7812a3d1c7b0bc	✗
C:\Users\RDhJ0CNFevzX\Documents\1gCPCj5iJQW.csv	96.84 KB	d1cc01dab5902b4b311c2a26d708718ebf36ec007acb0b0197f7b1ddb90b8f15	✗
C:\Users\RDhJ0CNFevzX\Documents\1yj7pDeYv0wl_14KUOPt.rtf	65.09 KB	ccab5fd6bd99af7ae704a7fd1ab7e4a10b4df208b052cfb1098bd39190672a6e	✗
C:\Users\RDhJ0CNFevzX\Documents\22yziHM7PYbi2OW6R.pdf	1.25 KB	8cf72eafe875c25504c17282ba0a6488bb97b641f9fde335ec16da97f6d17e0a	✗
C:\Users\RDhJ0CNFevzX\Documents\2qxTT.pptx	52.78 KB	81288824f35bd9a255b3f81e535fe805e7bca849f77e3ad20b1e85038a4f3bdc	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\3wHRRIh-2tUJE8.doc	39.72 KB	ba7e01ab45743a2b707dc70d27f347592f99719671ba3146f9d4984335cbccd6	✗
C:\Users\RDhJ0CNFevzX\Documents\5BYO.pptx	93.28 KB	13f8413b5b86980bb7b484a129d6630d0d1cdc7c08ce8f1aa4be124a9f8b61f9	✗
C:\Users\RDhJ0CNFevzX\Documents\6_8C7Suq3sh2Zdvr.ppt	19.45 KB	d7870a8e98615a5ec087939e3303419288649dbeb321c651d5b3c94be2fc0e2e	✗
C:\Users\RDhJ0CNFevzX\Documents\7AVZTG3CoeJywumxSZt.docx	43.67 KB	588a6bc935767b601a8feeaa1056c4c3e69396a59dff8a4d8818664130774707	✗
C:\Users\RDhJ0CNFevzX\Documents\998Wb55hD8qLh4.xls	46.61 KB	0e4a63937a693364d2b94a820ac53154e6bb9859b590dcc82869aa292ad10731	✗
C:\Users\RDhJ0CNFevzX\Documents\A0KaGTxVHzRgI2NU.ods	95.28 KB	b80262022826f10485eae2972fd6da7eaf2e54b970e64413114770c26de4c3d4	✗
C:\Users\RDhJ0CNFevzX\Documents\Ai3doif_i6aorCOuoq.docx	47.47 KB	2db4e5a443be513dd5b87b33ef19689da21ab10a622e56d3595f09bc712d7f35	✗
C:\Users\RDhJ0CNFevzX\Documents\cJ6K_Ys9JTdNtND8.xlsx	94.20 KB	d4c3153a745d1c3ed12cd41bf54d87066a0072988ce0863e02a0ce987bc2c3af	✗
C:\Users\RDhJ0CNFevzX\Documents\DkBw3ckGM uF2SMdXz.pptx	86.55 KB	dbae078fc0401540047c3d29775b27221ab235ebd02cdd7f51e861561d9c4089	✗
C:\Users\RDhJ0CNFevzX\Documents\dXzsJ7_sQ.rtf	97.25 KB	a5c944814f0e67f8740d038ed5342e779aa1094d17f016fb6a7c0b529b085ad4	✗
C:\Users\RDhJ0CNFevzX\Documents\FgTsNOb7Ndvo.xlsx	14.67 KB	df2c68dcf656d6c85e953c3fa9343f0d636268d9899bf82ffad93c695fee4625	✗
C:\Users\RDhJ0CNFevzX\Documents\fiE7zb85t8B-.pptx	96.58 KB	f6110899c74114d91694f63cc328f5adddab464025b75e1babe5164fd109976e	✗
C:\Users\RDhJ0CNFevzX\Documents\FXtU7tJGkArCUt.pptx	83.55 KB	3d7e6d1c46b4d3afd2a73958727cdc24e51a14a406b1676584e71822a333069a	✗
C:\Users\RDhJ0CNFevzX\Documents\Gxt7.rtf	23.08 KB	fafd126a09f3b959bbd9271cde371dbe5dad48274fc99ba4c5457ae5ec62658a	✗
C:\Users\RDhJ0CNFevzX\Documents\h8t-RSY oy1WSABM.csv	81.06 KB	aa9bb541b5167d248f92afa776cbfae51ffc51885e34b684f02ccd675382e56f	✗
C:\Users\RDhJ0CNFevzX\Documents\hgaKU.odt	60.69 KB	01e42b8704ad13d654d0e63cbe98c23690335e523bf6cb68365798715c1d1243	✗
C:\Users\RDhJ0CNFevzX\Documents\iriH.docx	59.86 KB	e5e6d382d81d12b0cc319c67da575afd1ecaebefb72f2d3e91d6eef2c90f464b	✗
C:\Users\RDhJ0CNFevzX\Documents\iSv2CXAx0sO0nwq3.docx	17.33 KB	7c8505eaae344178b7ec11d47dddd0c50007b2dd0538e8d1c6fbad182f3f8162	✗
C:\Users\RDhJ0CNFevzX\Documents\LXAm.xlsx	31.59 KB	5047bdd2142c46029b0ae0c7f07556511947663c6830fdc2b0aa65830ae55886	✗
C:\Users\RDhJ0CNFevzX\Documents\LXf5O1UnE8gZ7VPN-X.docx	54.23 KB	f3a05676ee81b960d2a5c28cda2123bd769a33fff2debebd1593d259c4894206	✗
C:\Users\RDhJ0CNFevzX\Documents\Lxh6PbYU5lGk0.pptx	25.88 KB	3fa1b0f79cd5618a98f8f6baa7fb3d8b3a23de461ace5828945b8310d69b3080	✗
C:\Users\RDhJ0CNFevzX\Documents\lyrRYp D-2Z.docx	65.92 KB	c6eb0d31a5df935110e055a35a8a9f360f62e1c00f0f9ac0e3f7e06053e22047	✗
C:\Users\RDhJ0CNFevzX\Documents\MSNffSwckP FbcIEuI5.doc	78.94 KB	c4a934ff1b770b16fe08d02e4ba846b3aba1851bbd913383cf6ed8636976d303	✗
C:\Users\RDhJ0CNFevzX\Documents\n7hKHIqS.rtf	15.53 KB	0deb0b835f605497d7056411d0aa86b93889c0117b151a8f2b1d3f03ae3281e8	✗
C:\Users\RDhJ0CNFevzX\Documents\ocgatxC-6Ez0Hk_y.xls	62.09 KB	799b0cc81eecc8a9c5f5dfe82b567f522704aa6e1886425bc29b52a7f4871e45	✗
C:\Users\RDhJ0CNFevzX\Documents\owF5pa QZMhBD.rtf	40.98 KB	452e638f568640147aa3f7e716934ab850c909923580b5504652b90e99637181	✗
C:\Users\RDhJ0CNFevzX\Documents\p9uL--tRL_6UnNWprC.odt	18.34 KB	00bc795a0598d2558fef82f4c8bf08626d26a020b80a255ef1914dcd19700fd4	✗
C:\Users\RDhJ0CNFevzX\Documents\pSJLpn8DrUrz1-Xy6Fw_.pdf	72.83 KB	a9dc589b2d9436918db4b80f663436d430d35c76a30e794059744a14c3684696	✗
C:\Users\RDhJ0CNFevzX\Documents\q9j2C2vhqGqT8Y.xls	66.88 KB	44479e520698fbae9f8787827ec9223f4feb8ed2090cd825554780f294d908bd	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\Qi06Dg7iSL hMONv94Db.xlsx	4.36 KB	bbb3c72bbc35afe47310a1ec4c84ec4650a8e0091970e52e66cff80ebbb2ca8a	✗
C:\Users\RDhJ0CNFevzX\Documents\QqWlqDBqRFVAm vqX4DG.pdf	71.75 KB	46d3cd397a07a960a3f85cd98de6245531499564 47f918a821774b22cb7134f9	✗
C:\Users\RDhJ0CNFevzX\Documents\TDG1tR6SD8R 70ytf.docx	51.95 KB	b644719b90e1a75147b764ab49392848e3248f00509859a2b984c584b48b848a	✗
C:\Users\RDhJ0CNFevzX\Documents\uhTnuhWyZPoex.pdf	22.00 KB	9e021af9f7c465046fed09d5faffac30bcc95748c2bc229dadbb6b9cf394b4a8	✗
C:\Users\RDhJ0CNFevzX\Documents\ulwqDmYW8Ql.docx	23.08 KB	76c9d198b574b6bfbe59375208580173775d2a49164bbeaf8856261597df3213	✗
C:\Users\RDhJ0CNFevzX\Documents\vcYEH.doc	95.34 KB	7b3d99023fdcd45798c54846cb483255ef1a0c6460dbd49f02aba0ed63d8e94c	✗
C:\Users\RDhJ0CNFevzX\Documents\wlZTxESTUgU f3.xlsx	30.47 KB	76a798c096f4dd5c0d0f81d60cc49297e4ac4e475695b933205e1bbdaa4f4e0b	✗
C:\Users\RDhJ0CNFevzX\Documents\WU7S.xls	88.86 KB	9599ef6c49da900c87880afae7e547184bc0483d578556f6a5749022f3f0cb73	✗
C:\Users\RDhJ0CNFevzX\Documents\wVE9flHzacBjM.pptx	31.64 KB	6973f31a3a9f632fc64b682205f7eb1c4b1ea394350244cf91714f340edc062e	✗
C:\Users\RDhJ0CNFevzX\Documents\y8TckRi KxxqHv9oqq.xlsx	22.59 KB	88b3d08a86116029df3429832c56f7c55ffe4de9ca3cfc358105cc2bce584438	✗
C:\Users\RDhJ0CNFevzX\Documents\ZJRfdPfcL.xlsx	94.09 KB	120b89ad751288416e576464e44b00e7391370f8855d3ffaa69d84e833c56d71	✗
C:\Users\RDhJ0CNFevzX\Documents\ZWAFqo.pps	90.39 KB	6e6c7ce3bb40041384d5201759fd8ea6d5257e90eba49bd80dfb6aa21dd631ab	✗
C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst	265.02 KB	4921782a823a1c8b59c3e88e6ddf0dcf485b9d8455791b841d7ec70396a0e93d	✗
C:\Users\RDhJ0CNFevzX\Pictures\0AkGZ7RwHa9JQW9htg8.jpg	75.92 KB	6098f1882379befc16a857adbcad194e2309d01e39f122eb6f661b39b7e97bc0	✗
C:\Users\RDhJ0CNFevzX\Pictures\1XcD0L9HgO vAf jK.jpg	32.48 KB	85e35177e16678fb2d8d8826fc2c033618599d86bd17dfe100d1227cafada09d	✗
C:\Users\RDhJ0CNFevzX\Pictures\6HEzLSBE7gYZeO.jpg	91.19 KB	163959ad150074e6066f8005f4b646d206c37e94384ad668bf26537cf26b7ba7	✗
C:\Users\RDhJ0CNFevzX\Pictures\6xK8yFHYt9NwJGM.jpg	46.55 KB	bc8ef63fc11da90283dd5c7a29369af5f38dabd33dfe02fd2c7cee4b3b9038ff	✗
C:\Users\RDhJ0CNFevzX\Pictures\8YcKzqOL.png	49.84 KB	ff371df4d92526eca3ad94c02268b7466aa28944c4f06112f8e49de76cb585b0	✗
C:\Users\RDhJ0CNFevzX\Pictures\b4zTcHI.png	47.44 KB	17552553a6fd91c0c5bebdd56b4f99a922e2d111df62d3564a36bdf1076d50bf	✗
C:\Users\RDhJ0CNFevzX\Pictures\BreSk RqWy7z.png	40.33 KB	9527ff18363291373a64f960a37f1a60f5202cb34f8dd7a7a035097abf9236b9	✗
C:\Users\RDhJ0CNFevzX\Pictures\BRJpjfC.png	49.97 KB	0b7dbe17492a85ad9463ed7cc6327b2b3a9ba00001400aeccb1feca7e87d9e5a	✗
C:\Users\RDhJ0CNFevzX\Pictures\d-XNPCTgc1Q9.png	14.55 KB	1594bc7b3a00bc2804ca58e3b7ae0653f72f8ca544e993d489c1059c9359ee2c	✗
C:\Users\RDhJ0CNFevzX\Pictures\gSIkAFh.bmp	65.98 KB	9d3c40ad7f75a7aee9e4dde7f38387f6b8556352218a26d86b9530daa9395165	✗
C:\Users\RDhJ0CNFevzX\Pictures\gXgbf6roC6Lb.jpg	93.89 KB	a209ca4258228f71f239aeb2cbff8d25866ba9e70236e3b466929f3e1ec9939d	✗
C:\Users\RDhJ0CNFevzX\Pictures\hlxInIph.bmp	78.28 KB	94c3cc84678c7a24931034529b6c2d77681084646badfc4495880abd8eb6bf65	✗
C:\Users\RDhJ0CNFevzX\Pictures\l6Fm_t84SE.png	39.16 KB	9491751e6b317a6218862f84f38a1c259a9f9fe2c48bfbb82cbbdd71c91edf00	✗
C:\Users\RDhJ0CNFevzX\Pictures\ivsui27SVr1Y3.jpg	91.34 KB	0cb0a332b6c5f5b772cd881f39fdadf538bdb563fd50867f095b75197c729617	✗
C:\Users\RDhJ0CNFevzX\Pictures\lsOQhqoN27oebZQi8.jpg	76.56 KB	5dee207e5ac22a5d00606641617436b5c11790cc1150cbc0f89a5ef99b80591d	✗
C:\Users\RDhJ0CNFevzX\Pictures\mi45QG6WK.bmp	74.06 KB	096ab59452eac4b4c05ddc1c3d994f5e557197faf7eca9c3a2d150715bda61de	✗

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Pictures\mJaL9VXieT_.jpg	76.50 KB	95de58e9c9cf3e2948129024c97a42a7dbffa3658758470d1063a27f25d511f5	✗
C:\Users\RDhJ0CNFevzX\Pictures\NLit5D.bmp	50.14 KB	69d8817736c9079aafb8844adbe4248a6f0b004c667ec85a26dd37a66198e1d8	✗
C:\Users\RDhJ0CNFevzX\Pictures\prgQYDqfEtZPsUF.bmp	9.02 KB	e65495a8fa5200e17f57c0ee49e7652f7052f7955f28323021da106e2dce3a77	✗
C:\Users\RDhJ0CNFevzX\Pictures\srPT.bmp	26.41 KB	f0620d2fda5874bc322fd4e3f96a3a78cc6670fefbb4caf40c554a3be57d763f	✗
C:\Users\RDhJ0CNFevzX\Pictures\ssZyCkQ2_.png	27.69 KB	c828ec9c9c5e9b29edf8341dd372cd3d23cabb2c6b6b6bc6b5b6dd4222b0ad7a	✗
C:\Users\RDhJ0CNFevzX\Pictures\sy8Zc6o0W2Dpzb.jpg	16.19 KB	e754db4001aaa247897e0552d8a57875863a18a30ebb6366504321ee428c34d6	✗
C:\Users\RDhJ0CNFevzX\Pictures\thhlqm_vXfrhAkJgqh4.bmp	83.45 KB	decb37fceaed5e6063cbd3f253a95637bfef2f1042abf3b6cf03ba0de0dcc6b6	✗
C:\Users\RDhJ0CNFevzX\Pictures\Tq-YO c2w6Tz7VNGz.bmp	49.70 KB	a8acfbf2d1ad7622db131fd7c99e4ba042bcdd5d548b2c4d11fe977cd72108d8	✗
C:\Users\RDhJ0CNFevzX\Pictures\Vmb OG1vu5V_PXk.png	3.36 KB	9f872cdbc4f63626a89bc7e59a001dd43aaeb128b17ff68cafb75894750868fc	✗
C:\Users\RDhJ0CNFevzX\Pictures\ZfAtYXdgQ7TzJo4.bmp	10.19 KB	430552102a7da7e825641fad5a78f382f91b3fd0dfe02ded179fc7a4561775d3	✗
C:\Users\RDhJ0CNFevzX\Pictures_LbBOR Qp.bmp	27.08 KB	d851a3b59beffc3849d264752c5fa6d11a4ab3dcf0e6d61e81d7f0c24af15269	✗

Host Behavior

Type	Count
User	1
System	48
Module	63
Window	57
Registry	24
File	1389
-	10
Environment	4
Keyboard	25

Network Behavior

Type	Count
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299	C:\Users\RDhJ0CNFevzX\Desktop\baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe	Sample File	230.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
2c75ad03937eee1046942d48b0fdc366e908dc00a5defc8f3b9513c7821a78b8	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\svhost.exe, C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe	Dropped File	254.30 KB	application/vnd.microsoft.portable-executable	Create, Access, Write, Delete	SUSPICIOUS
e15fb0f7e86731ad15fef51cfa1fd65842b676e9a6789917e911b8d90d3fdc47	C:\Users\RDhJ0CNFevzX\Desktop\2BCq2zisH1tDLrOOSW.csv, C:\Users\RDhJ0CNFevzX\Desktop\2BCq2zisH1tDLrOOSW.csv.coom	Modified File	28.56 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
8b54f7f5ee40104ef09ce3111152092831a35967faed73bb8bc93fd0f08db427	C:\Users\RDhJ0CNFevzX\Desktop\438nbzIkP EaX9m.flv.coom, C:\Users\RDhJ0CNFevzX\Desktop\438nbzIkP EaX9m.flv	Modified File	8.27 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
7126033375c6f2fed65e1eaebcd571086ab5cddf6f85890c78e90feb031abdd1	C:\Users\RDhJ0CNFevzX\Desktop\80TvEOvTr5nvyI.swf, C:\Users\RDhJ0CNFevzX\Desktop\80TvEOvTr5nvyI.swf.coom	Modified File	5.66 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
54a4d5eeed216437f598832a3f91b3fda8edc6113b3e7d4aea7d5820b9f86eac	C:\Users\RDhJ0CNFevzX\Desktop\8H3cx4bVP1NLZr8fhYb.swf, C:\Users\RDhJ0CNFevzX\Desktop\8H3cx4bVP1NLZr8fhYb.swf.coom	Modified File	28.11 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
f75a3190f9a4d017be6a82d1934490e20374026278855b2cf54d77ef1253ea00	C:\Users\RDhJ0CNFevzX\Desktop\A6CiMczxY2F3JXYRzK.png, C:\Users\RDhJ0CNFevzX\Desktop\A6CiMczxY2F3JXYRzK.png.coom	Modified File	45.27 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
cf51e630392a39e404a466508d4d0fb53151c141a280c6c12fc939820ba83b11	C:\Users\RDhJ0CNFevzX\Desktop\A9li7.bmp.coom, C:\Users\RDhJ0CNFevzX\Desktop\A9li7.bmp	Modified File	97.55 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
6a7d386832a959523d4db3ca7140e281972144f2cb926466165b3032325b0a13	C:\Users\RDhJ0CNFevzX\Desktop\aA9p.png, C:\Users\RDhJ0CNFevzX\Desktop\aA9p.png.coom	Modified File	57.72 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
ccc69f004e2c412ec9d7c8a4753f662c47704353c053b65daefe18986ad0db6e	C:\Users\RDhJ0CNFevzX\Desktop\fch1HElCA7Cv3KXW.png.coom, C:\Users\RDhJ0CNFevzX\Desktop\fch1HElCA7Cv3KXW.png	Modified File	12.16 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
141a2395f2d97c35f7da24d72188a2f8b285ac6f75bf852d497b19df01001d98	C:\Users\RDhJ0CNFevzX\Desktop\gPnVA1epmh.png, C:\Users\RDhJ0CNFevzX\Desktop\gPnVA1epmh.png.coom	Modified File	94.27 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
e2c857d9a631269061ecee97493d6997a1e94be6e8d2e8dc959ca502036ad9ce	C:\Users\RDhJ0CNFevzX\Desktop\jKEImg2LCcB.png, C:\Users\RDhJ0CNFevzX\Desktop\jKEImg2LCcB.png.coom	Modified File	57.03 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
7ca8109ef7fcec60ac78181409bd553bc4f967ef6c82aee55909f2f673228e6d	C:\Users\RDhJ0CNFevzX\Desktop\kFzsu2uze8.jpg, C:\Users\RDhJ0CNFevzX\Desktop\kFzsu2uze8.jpg.coom	Modified File	30.11 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
b1c433ce6592762b0c75c3e3304e2e357432e01ae86fa8e2b5457e4bff9be071	C:\Users\RDhJ0CNFevzX\Desktop\lZ59hc.xls.coom, C:\Users\RDhJ0CNFevzX\Desktop\lZ59hc.xls	Modified File	77.30 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2a02a7515e97746c3fca5892147d9144c872a306d4cef86f1277cc754fcb375b	C:\Users\RDhJ0CNFevzX\Desktop\nl-Ynzgfo-bdwG.ods.coom, C:\Users\RDhJ0CNFevzX\Desktop\nl-Ynzgfo-bdwG.ods	Modified File	31.83 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
a3c9a54e2fdc598b80530c080cd4fe23794cc6e850c67142c427a42a70a881c2	C:\Users\RDhJ0CNFevzX\Desktop\qxMCjsWp9C.swf, C:\Users\RDhJ0CNFevzX\Desktop\qxMCjsWp9C.swf.coom	Modified File	74.19 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
7005c7ea2d767b05d515cfca1eb41e4624adb6df0ff826a806004631f03ffbc6	C:\Users\RDhJ0CNFevzX\Desktop\rfEzxhy.flv, C:\Users\RDhJ0CNFevzX\Desktop\rfEzxhy.flv.coom	Modified File	76.03 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
24ba5f74c775f01e224d56605fa4fecdcd6799f34436889feb685b35a678c57c	C:\Users\RDhJ0CNFevzX\Desktop\SbyA0FI2i1A.jpg.coom, C:\Users\RDhJ0CNFevzX\Desktop\SbyA0FI2i1A.jpg	Modified File	96.86 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
b2f13a5eaa83aaf2127b1c0e74af302f583bcc982201e46994fb76bb5774680d	C:\Users\RDhJ0CNFevzX\Desktop\UUZnNLpt1yyHK2REqD8.xls.coom, C:\Users\RDhJ0CNFevzX\Desktop\UUZnNLpt1yyHK2REqD8.xls	Modified File	36.98 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
77517b83d93f5c3e923557b37ae07a58186ba6bcb5ab7f14da4402aac5fbec24	C:\Users\RDhJ0CNFevzX\Desktop\WUHo.xls, C:\Users\RDhJ0CNFevzX\Desktop\WUHo.xls.coom	Modified File	9.30 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
e87d2d8c53b39860bda28767890b9b5f7190e89279d88f574eda5ba46314ef26	C:\Users\RDhJ0CNFevzX\Desktop\Y9Yc7GFT5o-.flv.coom, C:\Users\RDhJ0CNFevzX\Desktop\Y9Yc7GFT5o-.flv	Modified File	16.22 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
05ecf26c31753a8124731f855c7b61b1820da244b78f30349de684c858385297	C:\Users\RDhJ0CNFevzX\Desktop\Yc_dgQq9.swf, C:\Users\RDhJ0CNFevzX\Desktop\Yc_dgQq9.swf.coom	Modified File	41.48 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
e7e9de0f31308b1ae5a89c396e8bfea678fa758ef4f710809d01d011e011fadc	C:\Users\RDhJ0CNFevzX\Desktop_z9qmOEfbbR2Ho.png.coom, C:\Users\RDhJ0CNFevzX\Desktop_z9qmOEfbbR2Ho.png	Modified File	93.98 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d396f448b8c5a4bde7f398025a89d7d7c6176efafe7c52e770b700e35b8c486e	C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\0b2BYJ.bmp.coom, C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\0b2BYJ.bmp	Modified File	6.11 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
94dc130865f4a807a18e7fed19decf55ac523ba7e48b2568b1ffdd90006ede46	C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\bCDo3xL3DQNnY-NDn8o.csv.coom, C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\bCDo3xL3DQNnY-NDn8o.csv	Modified File	40.14 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
928f7ac33846ee5cad9bc5981ac2c5b1b524e0293b14497adb18f475c16d67c6	C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\BP7Hlx-dC.docx, C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\BP7Hlx-dC.docx.coom	Modified File	29.34 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d838b30140d23a9955d3cc05704a3a62a30b5953b5ccd9c67bbea9b06e3370ae	C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\HTPNUNi5N0PRF7q49.flv.coom, C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\HTPNUNi5N0PRF7q49.flv	Modified File	55.39 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
c0d5f8efc0eb1526b5ffe4aac4cf508bf4f6dafd58e821ab1966e13396f7681a	C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\-iPNtWwPnLb_xVEK.xlsx, C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\-iPNtWwPnLb_xVEK.xlsx.coom	Modified File	38.33 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9a72eaf70216310172229d9a4a6de5655cfab38f75733123702a5ea594a59253	C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\a0LPQFabf2-tcp.flv, C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\a0LPQFabf2-tcp.flv.coom	Modified File	1.69 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
6e8e6a4c345693be9fa032d6672e244c45fdb22a05620bf166590d2698a6b446	C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\T3Pjk61xtk9Sizl9Gz7.jpg.coom, C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\T3Pjk61xtk9Sizl9Gz7.jpg	Modified File	61.70 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
0f9336ae5205f674bbdbe21d17e74c20d3f1638da1493c306c2ecbac031233ff	C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\Wy9hdiHoa5p6DL6.wav.coom, C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\Wy9hdiHoa5p6DL6.wav	Modified File	8.86 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
3642e7e80c63e9cc4e7cdfa3dbfe718c6e3dd1ab7c3c88c42d7812a3d1c7b0bc	C:\Users\RDhJ0CNFevzX\Documents\0tvBM_QdD3TVO2ZA_6P.ods, C:\Users\RDhJ0CNFevzX\Documents\0tvBM_QdD3TVO2ZA_6P.ods.coom	Modified File	46.30 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d1cc01dab5902b4b311c2a26d708718ebf36ec007acb0b0197f7b1ddb90b8f15	C:\Users\RDhJ0CNFevzX\Documents\1gCPCj5iJQW.csv, C:\Users\RDhJ0CNFevzX\Documents\1gCPCj5iJQW.csv.coom	Modified File	96.84 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
ccab5fd6bd99af7ae704a7fd1ab7e4a10b4df208b052cfb1098bd39190672a6e	C:\Users\RDhJ0CNFevzX\Documents\1yj7pDeYv0wl_14KUOPt.rtf, C:\Users\RDhJ0CNFevzX\Documents\1yj7pDeYv0wl_14KUOPt.rtf.coom	Modified File	65.09 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
8cf72eafe875c25504c17282ba0a6488bb97b641f9fde335ec16da97f6d17e0a	C:\Users\RDhJ0CNFevzX\Documents\22yziHM7PYbi2OW6R.pdf, C:\Users\RDhJ0CNFevzX\Documents\22yziHM7PYbi2OW6R.pdf.coom	Modified File	1.25 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
81288824f35bd9a255b3f81e535fe805e7bca849f77e3ad20b1e85038a4f3bdc	C:\Users\RDhJ0CNFevzX\Documents\2qxTT.pptx.coom, C:\Users\RDhJ0CNFevzX\Documents\2qxTT.pptx	Modified File	52.78 KB	audio/mpeg	Access, Write, Create, Delete, Read	CLEAN
ba7e01ab45743a2b707dc70d27f347592f99719671ba3146f9d4984335cbccd6	C:\Users\RDhJ0CNFevzX\Documents\3wHRRIh-2tUJE8.doc, C:\Users\RDhJ0CNFevzX\Documents\3wHRRIh-2tUJE8.doc.coom	Modified File	39.72 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
13f8413b5b86980bb7b484a129d6630d0d1cdc7c08ce8f1aa4be124a9f8b61f9	C:\Users\RDhJ0CNFevzX\Documents\5BYO.pptx.coom, C:\Users\RDhJ0CNFevzX\Documents\5BYO.pptx	Modified File	93.28 KB	audio/mpeg	Access, Write, Create, Delete, Read	CLEAN
d7870a8e98615a5ec087939e33034192886 49dbeb321c651d5b3c94be2fc0e2e	C:\Users\RDhJ0CNFevzX\Documents\6_8C7Suq3sh2Zdvr.ppt, C:\Users\RDhJ0CNFevzX\Documents\6_8C7Suq3sh2Zdvr.ppt.coom	Modified File	19.45 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
588a6bc935767b601a8feeaa1056c4c3e69396a59dff8a4d8818664130774707	C:\Users\RDhJ0CNFevzX\Documents\7AVZTG3CoeJywumxSZt.docx, C:\Users\RDhJ0CNFevzX\Documents\7AVZTG3CoeJywumxSZt.docx.coom	Modified File	43.67 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
0e4a63937a693364d2b94a820ac53154e6bb9859b590dcc82869aa292ad10731	C:\Users\RDhJ0CNFevzX\Documents\998Wb55hD8qLh4.xls.coom, C:\Users\RDhJ0CNFevzX\Documents\998Wb55hD8qLh4.xls	Modified File	46.61 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
b80262022826f10485eae2972fd6da7eaf2e54b970e64413114770c26de4c3d4	C:\Users\RDhJ0CNFevzX\Documents\A0KaGTxVHzRgl2NU.ods.coom, C:\Users\RDhJ0CNFevzX\Documents\A0KaGTxVHzRgl2NU.ods	Modified File	95.28 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2db4e5a443be513dd5b87b33ef19689da21ab10a622e56d3595f09bc712d7f35	C:\Users\RDhJ0CNFevzX\Documents\Ai3doif_i6aorCOuoq.docx.coom, C:\Users\RDhJ0CNFevzX\Documents\Ai3doif_i6aorCOuoq.docx	Modified File	47.47 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d4c3153a745d1c3ed12cd41bf54d87066a0072988ce0863e02a0ce987bc2c3af	C:\Users\RDhJ0CNFevzX\Documents\cJ6K_Ys9JTdNtND8.xlsx, C:\Users\RDhJ0CNFevzX\Documents\cJ6K_Ys9JTdNtND8.xlsx.coom	Modified File	94.20 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
dbae078fc0401540047c3d29775b27221ab235ebd02cdd7f51e861561d9c4089	C:\Users\RDhJ0CNFevzX\Documents\DkBw3ckGM uF2SMdXz.pptx, C:\Users\RDhJ0CNFevzX\Documents\DkBw3ckGM uF2SMdXz.pptx.coom	Modified File	86.55 KB	audio/mpeg	Access, Write, Create, Delete, Read	CLEAN
a5c944814f0e67f8740d038ed5342e779aa1094d17f016fb6a7c0b529b085ad4	C:\Users\RDhJ0CNFevzX\Documents\dXzsJ7_sQ.rtf, C:\Users\RDhJ0CNFevzX\Documents\dXzsJ7_sQ.rtf.coom	Modified File	97.25 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
df2c68dcf656d6c85e953c3fa9343f0d636268d9899bf82ffad93c695fee4625	C:\Users\RDhJ0CNFevzX\Documents\FgTsNOb7Ndvo.xlsx, C:\Users\RDhJ0CNFevzX\Documents\FgTsNOb7Ndvo.xlsx.coom	Modified File	14.67 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
f6110899c74114d91694f63cc328f5adddab464025b75e1babe5164fd109976e	C:\Users\RDhJ0CNFevzX\Documents\fiE7zb85t8B-.pptx, C:\Users\RDhJ0CNFevzX\Documents\fiE7zb85t8B-.pptx.coom	Modified File	96.58 KB	audio/mpeg	Access, Write, Create, Delete, Read	CLEAN
3d7e6d1c46b4d3afd2a73958727cdc24e51a14a406b1676584e71822a333069a	C:\Users\RDhJ0CNFevzX\Documents\FXtU7tJGkArCUt.pptx, C:\Users\RDhJ0CNFevzX\Documents\FXtU7tJGkArCUt.pptx.coom	Modified File	83.55 KB	audio/mpeg	Access, Write, Create, Delete, Read	CLEAN
fafd126a09f3b959bbd9271cde371dbe5dad48274fc99ba4c5457ae5ec62658a	C:\Users\RDhJ0CNFevzX\Documents\Gxt7.rtf.coom, C:\Users\RDhJ0CNFevzX\Documents\Gxt7.rtf	Modified File	23.08 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
aa9bb541b5167d248f92afa776cbfae51ffc51885e34b684f02ccd675382e56f	C:\Users\RDhJ0CNFevzX\Documents\h8t-RSY oy1WSABM.csv, C:\Users\RDhJ0CNFevzX\Documents\h8t-RSY oy1WSABM.csv.coom	Modified File	81.06 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
01e42b8704ad13d654d0e63cbe98c23690335e523bf6cb68365798715c1d1243	C:\Users\RDhJ0CNFevzX\Documents\hgaKU.odt, C:\Users\RDhJ0CNFevzX\Documents\hgaKU.odt.coom	Modified File	60.69 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
e5e6d382d81d12b0cc319c67da575afd1ecaebefb72f2d3e91d6eef2c90f464b	C:\Users\RDhJ0CNFevzX\Documents\iriH.docx.coom, C:\Users\RDhJ0CNFevzX\Documents\iriH.docx	Modified File	59.86 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
7c8505eaae344178b7ec11d47dddd0c50007b2dd0538e8d1c6fbad182f3f8162	C:\Users\RDhJ0CNFevzX\Documents\iSv2CXAx0sO0nwq3.docx, C:\Users\RDhJ0CNFevzX\Documents\iSv2CXAx0sO0nwq3.docx.coom	Modified File	17.33 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
5047bdd2142c46029b0ae0c7f075566511947663c6830fdc2b0aa65830ae55886	C:\Users\RDhJ0CNFevzX\Documents\LXAm.xlsx.coom, C:\Users\RDhJ0CNFevzX\Documents\LXAm.xlsx	Modified File	31.59 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
f3a05676ee81b960d2a5c28cda2123bd769a33fff2debebd1593d259c4894206	C:\Users\RDhJ0CNFevzX\Documents\LXf5O1UnE8gZ7VPN-X.docx, C:\Users\RDhJ0CNFevzX\Documents\LXf5O1UnE8gZ7VPN-X.docx.coom	Modified File	54.23 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
3fa1b0f79cd5618a98f8f6baa7fb3d8b3a23de461ace5828945b8310d69b3080	C:\Users\RDhJ0CNFevzX\Documents\Lxh6PbYU5lGk0.pptx.coom, C:\Users\RDhJ0CNFevzX\Documents\Lxh6PbYU5lGk0.pptx	Modified File	25.88 KB	audio/mpeg	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c6eb0d31a5df935110e055a35a8a9f360f62e1c00f0f9ac0e3f7e06053e22047	C:\Users\RDhJ0CNFevzX\Documents\lyrRYp D-2Z.docx.coom, C:\Users\RDhJ0CNFevzX\Documents\lyrRYp D-2Z.docx	Modified File	65.92 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
c4a934ff1b770b16fe08d02e4ba846b3aba1851bbd913383cf6ed8636976d303	C:\Users\RDhJ0CNFevzX\Documents\MSNffSwckP FbcIEul5.doc, C:\Users\RDhJ0CNFevzX\Documents\MSNffSwckP FbcIEul5.doc.coom	Modified File	78.94 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
0deb0b835f605497d7056411d0aa86b93889c0117b151a8f2b1d3f03ae3281e8	C:\Users\RDhJ0CNFevzX\Documents\n7hKHIqS.rtf, C:\Users\RDhJ0CNFevzX\Documents\n7hKHIqS.rtf.coom	Modified File	15.53 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
799b0cc81eecc8a9c5f5dfe82b567f522704aa6e1886425bc29b52a7f4871e45	C:\Users\RDhJ0CNFevzX\Documents\ocgatxC-6Ez0Hk_y.xls, C:\Users\RDhJ0CNFevzX\Documents\ocgatxC-6Ez0Hk_y.xls.coom	Modified File	62.09 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
452e638f568640147aa3f7e716934ab850c909923580b5504652b90e99637181	C:\Users\RDhJ0CNFevzX\Documents\owF5pa QZMhBD.rtf.coom, C:\Users\RDhJ0CNFevzX\Documents\owF5pa QZMhBD.rtf	Modified File	40.98 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
00bc795a0598d2558fef82f4c8bf08626d26a020b80a255ef1914dcd19700fd4	C:\Users\RDhJ0CNFevzX\Documents\p9uL--tRL_6UnNWprC.odt, C:\Users\RDhJ0CNFevzX\Documents\p9uL--tRL_6UnNWprC.odt.coom	Modified File	18.34 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
a9dc589b2d9436918db4b80f663436d430d35c76a30e794059744a14c3684696	C:\Users\RDhJ0CNFevzX\Documents\pSJLpn8DrUrz1-Xy6Fw_.pdf.coom, C:\Users\RDhJ0CNFevzX\Documents\pSJLpn8DrUrz1-Xy6Fw_.pdf	Modified File	72.83 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
44479e520698fbae9f8787827ec9223f4feb8ed2090cd825554780f294d908bd	C:\Users\RDhJ0CNFevzX\Documents\q9j2C2vhqGqT8Y.xls.coom, C:\Users\RDhJ0CNFevzX\Documents\q9j2C2vhqGqT8Y.xls	Modified File	66.88 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
bbb3c72bbc35afe47310a1ec4c84ec4650a8e0091970e52e66cff80ebbb2ca8a	C:\Users\RDhJ0CNFevzX\Documents\Qi06Dg7iSL hMONv94Db.xlsx, C:\Users\RDhJ0CNFevzX\Documents\Qi06Dg7iSL hMONv94Db.xlsx.coom	Modified File	4.36 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
46d3cd397a07a960a3f85cd98de6245531499564 47f918a821774b22cb7134f9	C:\Users\RDhJ0CNFevzX\Documents\QqWlqDBqRFVAm vqX4DG.pdf.coom, C:\Users\RDhJ0CNFevzX\Documents\QqWlqDBqRFVAm vqX4DG.pdf	Modified File	71.75 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
b644719b90e1a75147b764ab49392848e3248f00509859a2b984c584b48b848a	C:\Users\RDhJ0CNFevzX\Documents\TDG1tR6SD8R 70ytf.docx.coom, C:\Users\RDhJ0CNFevzX\Documents\TDG1tR6SD8R 70ytf.docx	Modified File	51.95 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
9e021af9f7c465046fed09d5faffac30bcc95748c2bc229dadbb6b9cf394b4a8	C:\Users\RDhJ0CNFevzX\Documents\uhTnuhWyZPoex.pdf, C:\Users\RDhJ0CNFevzX\Documents\uhTnuhWyZPoex.pdf.coom	Modified File	22.00 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
76c9d198b574b6bfbe59375208580173775d2a49164bbeaf8856261597df3213	C:\Users\RDhJ0CNFevzX\Documents\ulwqDmYW8Ql.docx, C:\Users\RDhJ0CNFevzX\Documents\ulwqDmYW8Ql.docx.coom	Modified File	23.08 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
7b3d99023fdcd45798c54846cb483255ef1a0c6460dbd49f02aba0ed63d8e94c	C:\Users\RDhJ0CNFevzX\Documents\vcYEH.doc, C:\Users\RDhJ0CNFevzX\Documents\vcYEH.doc.coom	Modified File	95.34 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
76a798c096f4dd5c0d0f81d60cc49297e4ac4e475695b9333205e1bbdaa4f4e0b	C:\Users\RDhJ0CNFevzX\Documents\wIZTxESTUgU f3.xlsx.coom, C:\Users\RDhJ0CNFevzX\Documents\wIZTxESTUgU f3.xlsx	Modified File	30.47 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9599ef6c49da900c87880afae7e547184bc0483d578556f6a5749022f3f0cb73	C:\Users\RDhJ0CNFevzX\Documents\WU7S.xls.coom, C:\Users\RDhJ0CNFevzX\Documents\WU7S.xls	Modified File	88.86 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
6973f31a3a9f632fc64b682205f7eb1c4b1ea394350244cf91714f340edc062e	C:\Users\RDhJ0CNFevzX\Documents\wVE9flHzacBjM.pptx, C:\Users\RDhJ0CNFevzX\Documents\wVE9flHzacBjM.pptx.coom	Modified File	31.64 KB	audio/mpeg	Access, Write, Create, Delete, Read	CLEAN
88b3d08a86116029df3429832c56f7c55ffe4de9ca3cfc358105cc2bce584438	C:\Users\RDhJ0CNFevzX\Documents\y8TckRi KxxqHv9oqq.xlsx.coom, C:\Users\RDhJ0CNFevzX\Documents\y8TckRi KxxqHv9oqq.xlsx	Modified File	22.59 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
120b89ad751288416e576464e44b00e7391370f8855d3ffaa69d84e833c56d71	C:\Users\RDhJ0CNFevzX\Documents\ZJRfdPfcL.xlsx.coom, C:\Users\RDhJ0CNFevzX\Documents\ZJRfdPfcL.xlsx	Modified File	94.09 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
6e6c7ce3bb40041384d5201759fd8ea6d5257e90eba49bd80dfb6aa21dd631ab	C:\Users\RDhJ0CNFevzX\Documents\ZWAFqo.pps.coom, C:\Users\RDhJ0CNFevzX\Documents\ZWAFqo.pps	Modified File	90.39 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
4921782a823a1c8b59c3e88e6ddf0dcf485b9d8455791b841d7ec70396a0e93d	C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst.coom, C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst	Modified File	265.02 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
6098f1882379befc16a857adbcad194e2309d01e39f122eb6f661b39b7e97bc0	C:\Users\RDhJ0CNFevzX\Pictures\0AkGZ7RwHa9JQW9htg8.jpg, C:\Users\RDhJ0CNFevzX\Pictures\0AkGZ7RwHa9JQW9htg8.jpg.coom	Modified File	75.92 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
85e35177e16678fb2d8d8826fc2c033618599d86bd17dfe100d1227cafada09d	C:\Users\RDhJ0CNFevzX\Pictures\1XcD0L9HgO vAf jK.jpg, C:\Users\RDhJ0CNFevzX\Pictures\1XcD0L9HgO vAf jK.jpg.coom	Modified File	32.48 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
163959ad150074e6066f8005f4b646d206c37e94384ad668bf26537cf26b7ba7	C:\Users\RDhJ0CNFevzX\Pictures\6HEzLSBE7gYZeO.jpg, C:\Users\RDhJ0CNFevzX\Pictures\6HEzLSBE7gYZeO.jpg.coom	Modified File	91.19 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
bc8ef63fc11da90283dd5c7a29369af5f38dabd33dfe02fd2c7cee4b3b9038ff	C:\Users\RDhJ0CNFevzX\Pictures\6xK8yFHYt9NwJGM.jpg, C:\Users\RDhJ0CNFevzX\Pictures\6xK8yFHYt9NwJGM.jpg.coom	Modified File	46.55 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
ff371df4d92526eca3ad94c02268b7466aa28944c4f06112f8e49de76cb585b0	C:\Users\RDhJ0CNFevzX\Pictures\8YcKzqOL.png, C:\Users\RDhJ0CNFevzX\Pictures\8YcKzqOL.png.coom	Modified File	49.84 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
17552553a6fd91c0c5bebdd56b4f99a922e2d111df62d3564a36bdf1076d50bf	C:\Users\RDhJ0CNFevzX\Pictures\b4zTcHI.png, C:\Users\RDhJ0CNFevzX\Pictures\b4zTcHI.png.coom	Modified File	47.44 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
9527ff18363291373a64f960a37f1a60f5202cb34f8dd7a7a035097abf9236b9	C:\Users\RDhJ0CNFevzX\Pictures\BreSk RqWy7z.png, C:\Users\RDhJ0CNFevzX\Pictures\BreSk RqWy7z.png.coom	Modified File	40.33 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
0b7dbe17492a85ad9463ed7cc6327b2b3a9ba00001400aeccb1feca7e87d9e5a	C:\Users\RDhJ0CNFevzX\Pictures\BRJpjfC.png.coom, C:\Users\RDhJ0CNFevzX\Pictures\BRJpjfC.png	Modified File	49.97 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
1594bc7b3a00bc2804ca58e3b7ae0653f72f8ca544e993d489c1059c9359ee2c	C:\Users\RDhJ0CNFevzX\Pictures\d-XNPCTgc1Q9.png, C:\Users\RDhJ0CNFevzX\Pictures\d-XNPCTgc1Q9.png.coom	Modified File	14.55 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9d3c40ad7f75a7aee9e4dde7f38387f6b8556352218a26d86b9530daa9395165	C:\Users\RDhJ0CNFevzX\Pictures\gSlkAFh.bmp, C:\Users\RDhJ0CNFevzX\Pictures\gSlkAFh.bmp.coom	Modified File	65.98 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
a209ca4258228f71f239aeb2cbff8d25866ba9e70236e3b466929f3e1ec9939d	C:\Users\RDhJ0CNFevzX\Pictures\gXgbf6roC6Lb.jpg, C:\Users\RDhJ0CNFevzX\Pictures\gXgbf6roC6Lb.jpg.coom	Modified File	93.89 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
94c3cc84678c7a24931034529b6c2d77681084646badfc4495880abd8eb6bf65	C:\Users\RDhJ0CNFevzX\Pictures\hlxInlph.bmp, C:\Users\RDhJ0CNFevzX\Pictures\hlxInlph.bmp.coom	Modified File	78.28 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
9491751e6b317a6218862f84f38a1c259a9f9fe2c48bfbb82cbbdd71c91edf00	C:\Users\RDhJ0CNFevzX\Pictures\l6Fm_t84SE.png, C:\Users\RDhJ0CNFevzX\Pictures\l6Fm_t84SE.png.coom	Modified File	39.16 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
0cb0a332b6c5f5b772cd881f39fdadf538bdb563fd50867f095b75197c729617	C:\Users\RDhJ0CNFevzX\Pictures\ivsui27SVr1Y3.jpg.coom, C:\Users\RDhJ0CNFevzX\Pictures\ivsui27SVr1Y3.jpg	Modified File	91.34 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
5dee207e5ac22a5d00606641617436b5c11790cc1150cbc0f89a5ef99b80591d	C:\Users\RDhJ0CNFevzX\Pictures\lsOQhqoN27oebZQi8.jpg, C:\Users\RDhJ0CNFevzX\Pictures\lsOQhqoN27oebZQi8.jpg.coom	Modified File	76.56 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
096ab59452eac4b4c05ddc1c3d994f5e557197faf7eca9c3a2d150715bda61de	C:\Users\RDhJ0CNFevzX\Pictures\mi45QG6WK.bmp, C:\Users\RDhJ0CNFevzX\Pictures\mi45QG6WK.bmp.coom	Modified File	74.06 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
95de58e9c9cf3e2948129024c97a42a7dbffa3658758470d1063a27f25d511f5	C:\Users\RDhJ0CNFevzX\Pictures\mJaL9VXieT_.jpg.coom, C:\Users\RDhJ0CNFevzX\Pictures\mJaL9VXieT_.jpg	Modified File	76.50 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
69d8817736c9079aafb8844adbe4248a6f0b004c667ec85a26dd37a66198e1d8	C:\Users\RDhJ0CNFevzX\Pictures\NLit5D.bmp, C:\Users\RDhJ0CNFevzX\Pictures\NLit5D.bmp.coom	Modified File	50.14 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
e65495a8fa5200e17f57c0ee49e7652f7052f7955f28323021da106e2dce3a77	C:\Users\RDhJ0CNFevzX\Pictures\prgQYDqfEtZPsUF.bmp.coom, C:\Users\RDhJ0CNFevzX\Pictures\prgQYDqfEtZPsUF.bmp	Modified File	9.02 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
f0620d2fda5874bc322fd4e3f96a3a78cc6670fefbb4caf40c554a3be57d763f	C:\Users\RDhJ0CNFevzX\Pictures\srPT.bmp.coom, C:\Users\RDhJ0CNFevzX\Pictures\srPT.bmp	Modified File	26.41 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
c828ec9c9c5e9b29edf8341dd372cd3d23cabb2c6b6b6bc6b5b6dd4222b0ad7a	C:\Users\RDhJ0CNFevzX\Pictures\ssZyCkQ2_.png.coom, C:\Users\RDhJ0CNFevzX\Pictures\ssZyCkQ2_.png	Modified File	27.69 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
e754db4001aaa247897e0552d8a57875863a18a30ebb6366504321ee428c34d6	C:\Users\RDhJ0CNFevzX\Pictures\sy8Zc6o0W2Dpzb.jpg, C:\Users\RDhJ0CNFevzX\Pictures\sy8Zc6o0W2Dpzb.jpg.coom	Modified File	16.19 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
decb37fceaed5e6063cbd3f253a95637bfef2f1042abf3b6cf03ba0de0dcc6b6	C:\Users\RDhJ0CNFevzX\Pictures\thhlqm_vXfrhAkJgqh4.bmp.coom, C:\Users\RDhJ0CNFevzX\Pictures\thhlqm_vXfrhAkJgqh4.bmp	Modified File	83.45 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
a8acfbf2d1ad7622db131fd7c99e4ba042bcdd5d548b2c4d11fe977cd72108d8	C:\Users\RDhJ0CNFevzX\Pictures\Tq-YO c2w6Tz7VNGz.bmp.coom, C:\Users\RDhJ0CNFevzX\Pictures\Tq-YO c2w6Tz7VNGz.bmp	Modified File	49.70 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9f872cdbc4f63626a89bc7e59a001dd43aaeb128b17ff68cafb75894750868fc	C:\Users\RDhJ0CNFevzX\Pictures\VmbOG1vu5V_PXk.png, C:\Users\RDhJ0CNFevzX\Pictures\VmbOG1vu5V_PXk.png.coom	Modified File	3.36 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
430552102a7da7e825641fad5a78f382f91b3fd0dfe02ded179fc7a4561775d3	C:\Users\RDhJ0CNFevzX\Pictures\ZfAtYXdgQ7TzJo4.bmp, C:\Users\RDhJ0CNFevzX\Pictures\ZfAtYXdgQ7TzJo4.bmp.coom	Modified File	10.19 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
d851a3b59beffc3849d264752c5fa6d11a4ab3dcf0e6d61e81d7f0c24af15269	C:\Users\RDhJ0CNFevzX\Pictures_LbBOR Qp.bmp, C:\Users\RDhJ0CNFevzX\Pictures_LbBOR Qp.bmp.coom	Modified File	27.08 KB	application/octet-stream	Access, Write, Create, Delete, Read	CLEAN
b65a8f1dac0f41713ef3a4ab266b3c2eec7710713938fcd82ae1aa5c1c709098	-	Embedded File	14.00 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\FindMe	Accessed File	Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe.config	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\svhost.exe	Dropped File	Create, Access, Write, Delete	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe	Dropped File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\svhost.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\2BCq2zisH1tDLrOOSW.csv	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\2BCq2zisH1tDLrOOSW.csv.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\438nbzlkP EaX9m.flv	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\438nbzlkP EaX9m.flv.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\80TvEOvTr5nvyI.swf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\80TvEOvTr5nvyI.swf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8H3cx4bVP1NLZr8fhYb.swf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8H3cx4bVP1NLZr8fhYb.swf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\A6CiMczxY2F3JXYRzK.png	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\A6CiMczxY2F3JXYRzK.png.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\A9li7.bmp	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\A9li7.bmp.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\aA9p.png	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\aA9p.png.coom	Modified File	Access, Write, Create	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\fch1HElCA7Cv3KXW.png	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\fch1HElCA7Cv3KXW.png.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\gPnVA1epmh.png	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\gPnVA1epmh.png.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\jKElmg2LCcB.png	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\jKElmg2LCcB.png.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\kFzsu2uze8.jpg	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\kFzsu2uze8.jpg.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\lZ59hc.xls	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\lZ59hc.xls.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\nl-Ynzgfo-bdwG.ods	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\nl-Ynzgfo-bdwG.ods.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\qxMCjsWp9C.swf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\qxMCjsWp9C.swf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\rfEzxhy.flv	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\rfEzxhy.flv.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\S byA0FI2i1A.jpg	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\S byA0FI2i1A.jpg.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\UUZnNLpt1yyHK2REqD8.xls	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\UUZnNLpt1yyHK2REqD8.xls.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\WUHo.xls	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\WUHo.xls.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Y9Yc7GFT5o-.flv	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Y9Yc7GFT5o-.flv.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Yc_dgQq9.swf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Yc_dgQq9.swf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop_z9 qmOEfbbR2Ho.png	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop_z9 qmOEfbbR2Ho.png.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\0b2BYJ.bmp	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\0b2BYJ.bmp.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\bCDo3xL3DQNnY-NDn8o.csv	Modified File	Access, Write, Create, Delete, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\bCDo3xL3DQNnY-NDn8o.csv.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\BP7HIx-dC.docx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\BP7HIx-dC.docx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\HTPNUNi5N0PRF7q49.flv	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\HTPNUNi5N0PRF7q49.flv.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\-iPNtWwPnLb_xVEK.xlsx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\-iPNtWwPnLb_xVEK.xlsx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\a0LPQFabf2-tcp.flv	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\a0LPQFabf2-tcp.flv.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\T3Pjk61xtk9SizI9Gz7.jpg	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\T3Pjk61xtk9SizI9Gz7.jpg.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\Wy9hdiHoa5p6DL6.wav	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\8fuFu\lohkShS91M7hT3L\Wy9hdiHoa5p6DL6.wav.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\0tvBM_QdD3TVO2ZA_6P.ods	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\0tvBM_QdD3TVO2ZA_6P.ods.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\1gCPCj5iJQW.csv	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\1gCPCj5iJQW.csv.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\1yj7pDeYv0wl_14KUOPt.rtf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\1yj7pDeYv0wl_14KUOPt.rtf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\22yziHM7PYbi2OW6R.pdf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\22yziHM7PYbi2OW6R.pdf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\2qxTT.pptx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\2qxTT.pptx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\3wHRRIh-2tUJE8.doc	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\3wHRRIh-2tUJE8.doc.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\5BYO.pptx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\5BYO.pptx.coom	Modified File	Access, Write, Create	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\6_8C7Suq3sh2Zdvr.ppt	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\6_8C7Suq3sh2Zdvr.ppt.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\7AVZTG3CoeJywumxSZt.docx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\7AVZTG3CoeJywumxSZt.docx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\998Wb55hD8qLh4.xls	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\998Wb55hD8qLh4.xls.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\A0KaGTxVHzRgl2NU.ods	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\A0KaGTxVHzRgl2NU.ods.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Ai3doif_i6aorCOuoq.docx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Ai3doif_i6aorCOuoq.docx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\cJ6K_Ys9JTdNtND8.xlsx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\cJ6K_Ys9JTdNtND8.xlsx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\DkBw3ckGM uF2SMdXz.pptx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\DkBw3ckGM uF2SMdXz.pptx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\dXzsJ7_sQ.rtf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\dXzsJ7_sQ.rtf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\FgTsNOb7Ndvo.xlsx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\FgTsNOb7Ndvo.xlsx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\fiE7zb85t8B-.pptx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\fiE7zb85t8B-.pptx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\FXtU7tJGkArCUt.pptx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\FXtU7tJGkArCUt.pptx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Gxt7.rtf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Gxt7.rtf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\h8t-RSY oy1WSABM.csv	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\h8t-RSY oy1WSABM.csv.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\hgaKU.odt	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\hgaKU.odt.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\iriH.docx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\iriH.docx.coom	Modified File	Access, Write, Create	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\iSv2CXAx0sO0nwq3.docx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\iSv2CXAx0sO0nwq3.docx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\LXAm.xlsx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\LXAm.xlsx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\LXf5O1UnE8gZ7VPN-X.docx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\LXf5O1UnE8gZ7VPN-X.docx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Lxh6PbYU5lGk0.pptx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Lxh6PbYU5lGk0.pptx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\lyrRYp D-2Z.docx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\lyrRYp D-2Z.docx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\MSNffSwckP FbcIEuI5.doc	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\MSNffSwckP FbcIEuI5.doc.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\n7hKHIqS.rtf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\n7hKHIqS.rtf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\ocgatxC-6Ez0Hk_y.xls	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\ocgatxC-6Ez0Hk_y.xls.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\owF5pa QZMhBD.rtf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\owF5pa QZMhBD.rtf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\p9uL--tRL_6UnNWprC.odt	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\p9uL--tRL_6UnNWprC.odt.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\pSJLpn8DrUrz1-Xy6Fw_.pdf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\pSJLpn8DrUrz1-Xy6Fw_.pdf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\q9j2C2vhqGqT8Y.xls	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\q9j2C2vhqGqT8Y.xls.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Qi06Dg7iSL hMONv94Db.xlsx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Qi06Dg7iSL hMONv94Db.xlsx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\QqWlqDBqRFVAm vqX4DG.pdf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\QqWlqDBqRFVAm vqX4DG.pdf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\TDG1tR6SD8R 70ytf.docx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\TDG1tR6SD8R 70ytf.docx.coom	Modified File	Access, Write, Create	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\uhTnuhWyZPoex.pdf	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\uhTnuhWyZPoex.pdf.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\uIwqDmYW8QI.docx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\uIwqDmYW8QI.docx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vcYEH.doc	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\vcYEH.doc.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\wlZTxESTUgU f3.xlsx	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\wlZTxESTUgU f3.xlsx.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\WU7S.xls	Modified File	Access, Write, Create, Delete, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\WU7S.xls.coom	Modified File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\wVE9fIHzacBjM.pptx	Modified File	Access, Write, Create, Delete, Read	CLEAN

Reduced dataset

IP

IP Address	Domains	Country	Protocols	Verdict
192.30.89.67	-	Canada	TCP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	svhost.exe	CLEAN
HKEY_CURRENT_USER	access	svhost.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	svhost.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	svhost.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	svhost.exe	CLEAN

Process

Process Name	Commandline	Verdict
baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe	"C:\Users\RDhJ0CNFevzX\Desktop\baba76d578be903c9d78e3d6417636ba6a8069cafe9ccccdfce2bc19b43fc299.exe"	MALICIOUS
svhost.exe	"C:\Users\RDHJ0C~1\AppData\Local\Temp\svhost.exe"	SUSPICIOUS

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