MALICIOUS

Classifications: Ransomware

Threat Names: Trojan.Ransom.Agent.BX

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
Sample Name	**sosduf.exe**
ID	#486558
MD5	0ef0070dfc132fc368c950f0bef762a3
SHA1	572c864dfc9160e5aef2dcc9359bf909ca4ba1c5
SHA256	097d28021ffb26cb5b7d2d1377578cd6e2005549e44b5b2491fd310ecf50f7a8
File Size	2155.50 KB
Report Created	2021-05-11 07:42 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (7 rules, 7 matches)

Score	Category	Operation	Count	Classification
4/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) sosduf.exe modifies the content of multiple user files.			
4/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #1) sosduf.exe renames multiple user files.			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected the sample itself as "Trojan.Ransom.Agent.BX".			
4/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 209 files by appending the extension ".crypted".			
3/5	User Data Modification	Possibly drops ransom note files	1	Ransomware
	• (Process #1) sosduf.exe possibly drops ransom note files (creates 63 instances of the file "read_me_unlock.txt" in different locations).			
2/5	Anti Analysis	Tries to detect application sandbox	1	-
	• (Process #1) sosduf.exe tries to detect "wine" by calling GetProcAddress() on "wine_get_version".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) sosduf.exe resolves 38 API functions by name.			

Mitre ATT&CK Matrix

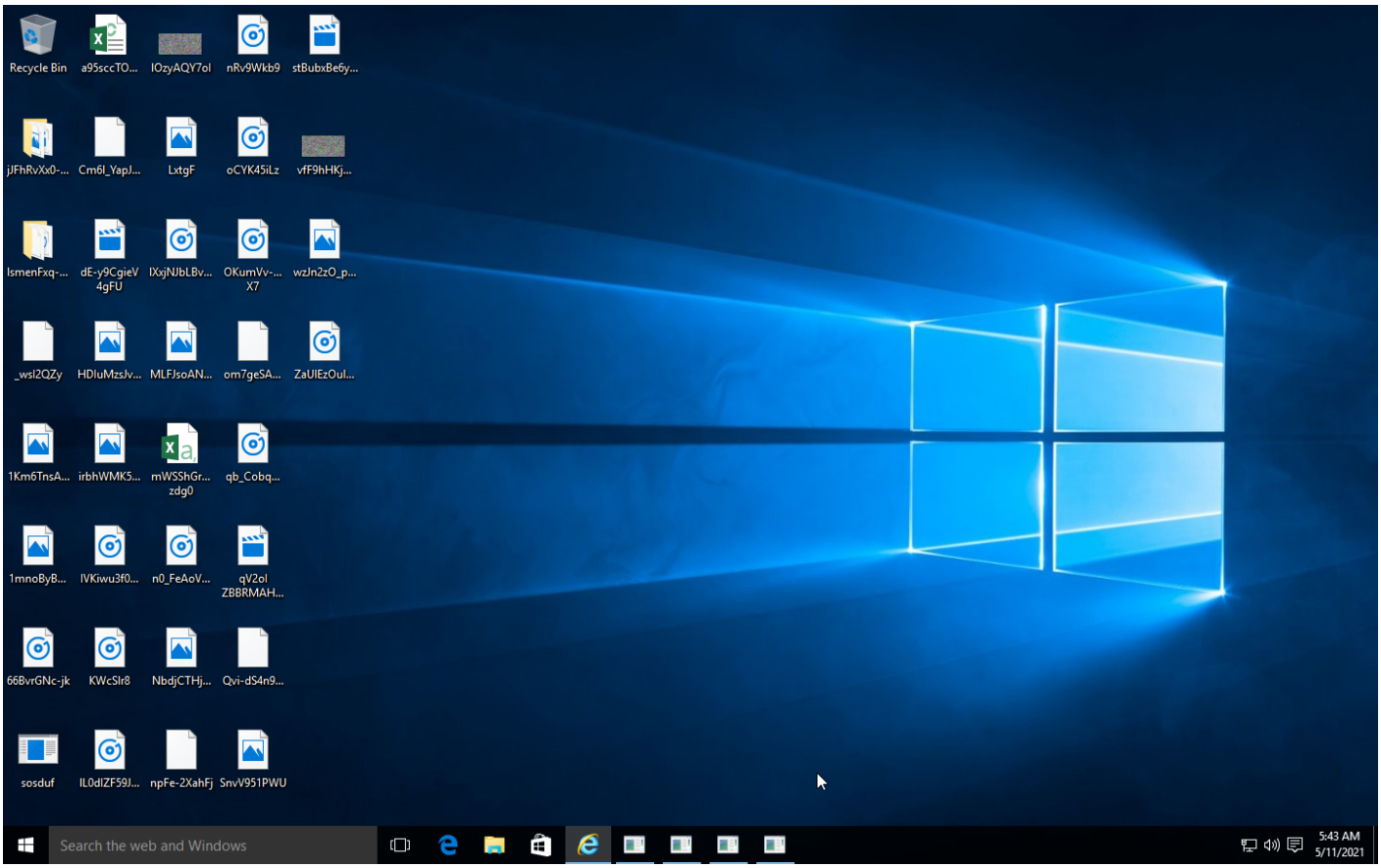
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
-	-	-	-	#T1497 Virtualization /Sandbox Evasion	-	#T1497 Virtualization /Sandbox Evasion	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	#T1486 Data Encrypted for Impact
-	-	-	-	#T1045 Software Packing	-	-	-	-	-	-	-

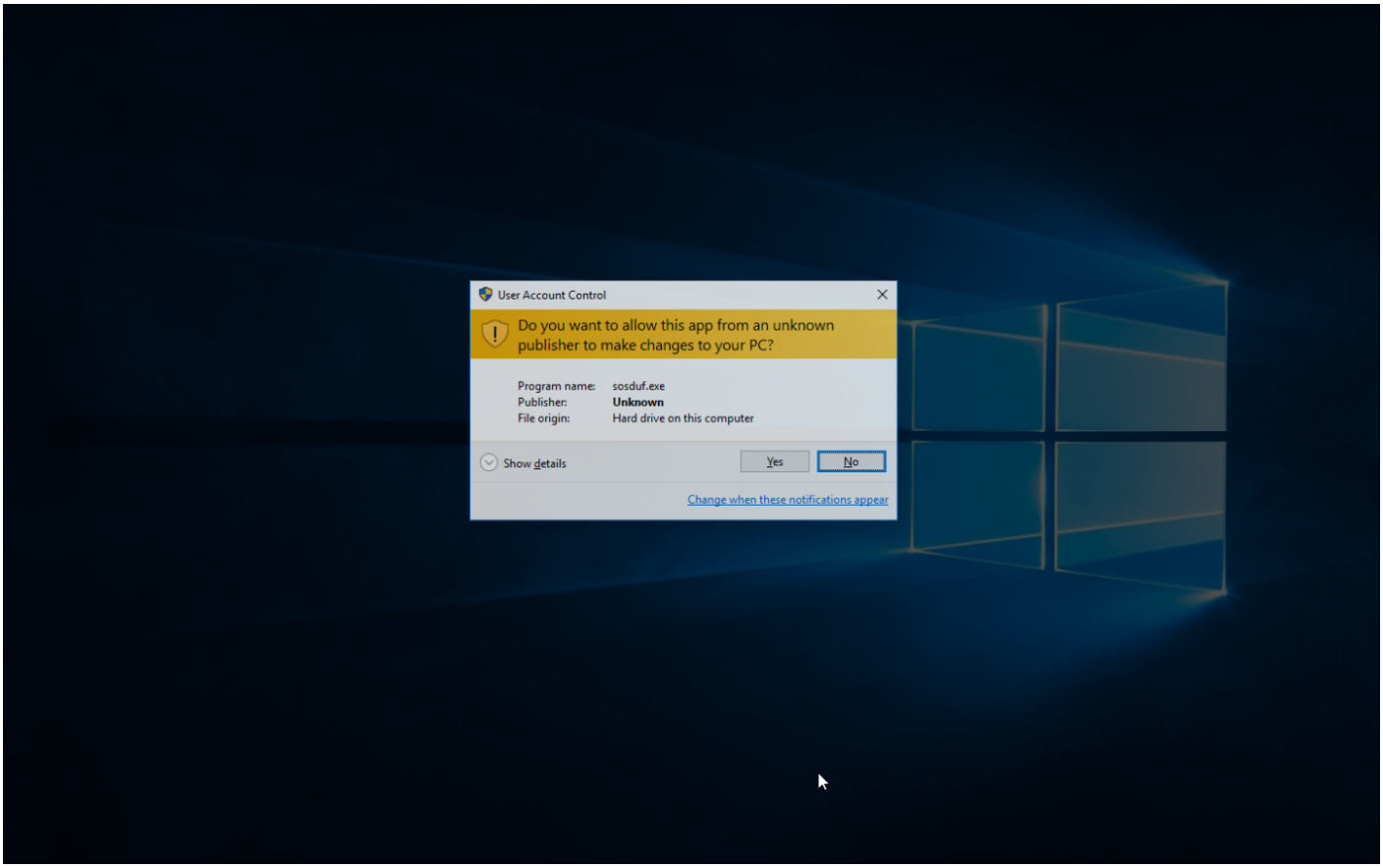
Sample Information

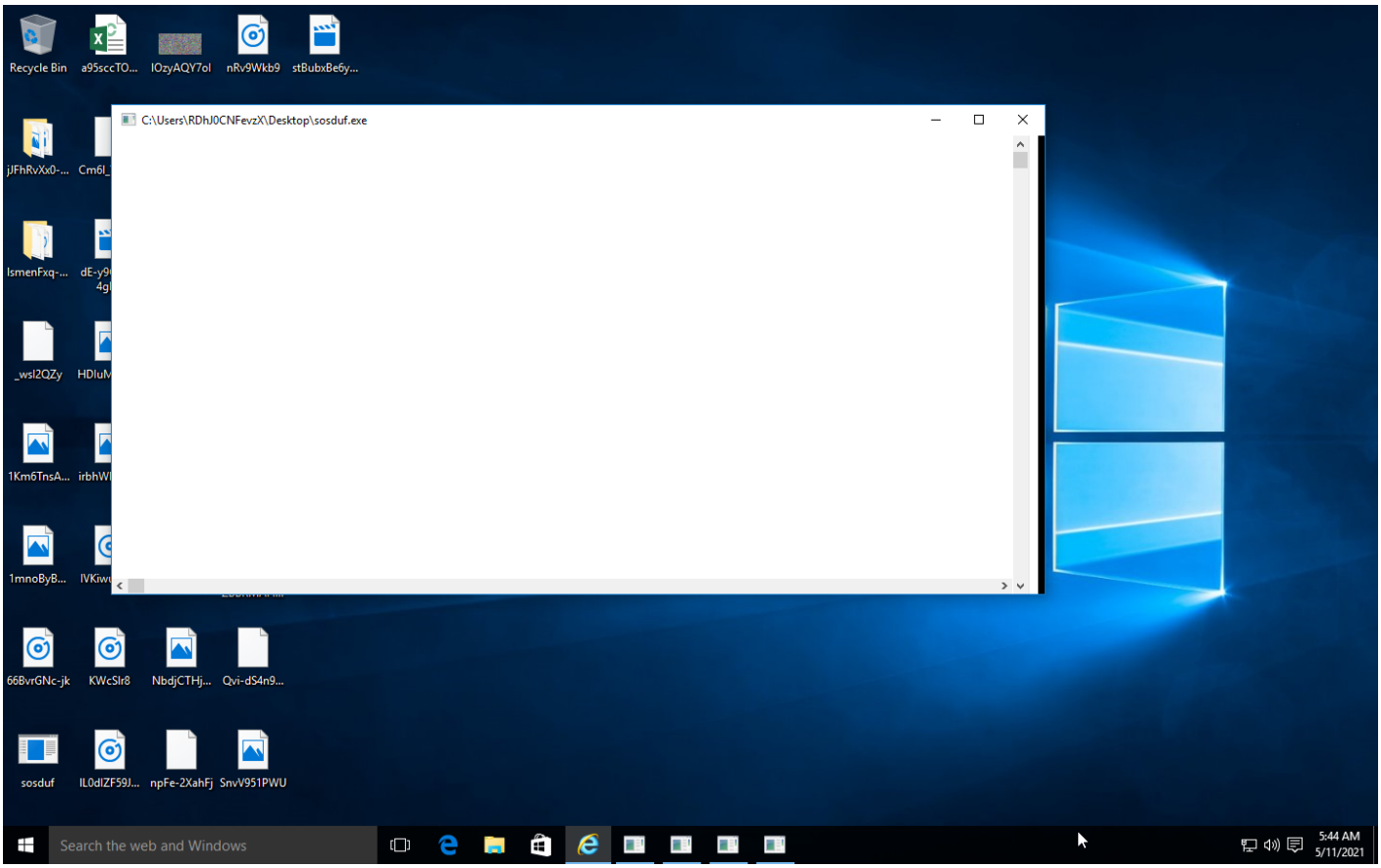
ID	1366756
MD5	0ef0070dfc132fc368c950f0bef762a3
SHA1	572c864dfc9160e5aef2dcc9359bf909ca4ba1c5
SHA256	097d28021ffb26cb5b7d2d1377578cd6e2005549e44b5b2491fd310ecf50f7a8
SSDeep	24576:O4tzlJ7As0QZi28TP4pK6uoLF/K8ctF5SA3dx2QiD3oLeus/hFeIqf0eaZgHwX+O:OIrfK8mF5ZNoXeXQXYpriCqg92+F1P
ImpHash	4035d2883e01d64f3e7a9dccb1d63af5
Filename	sosduf.exe
File Size	2155.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

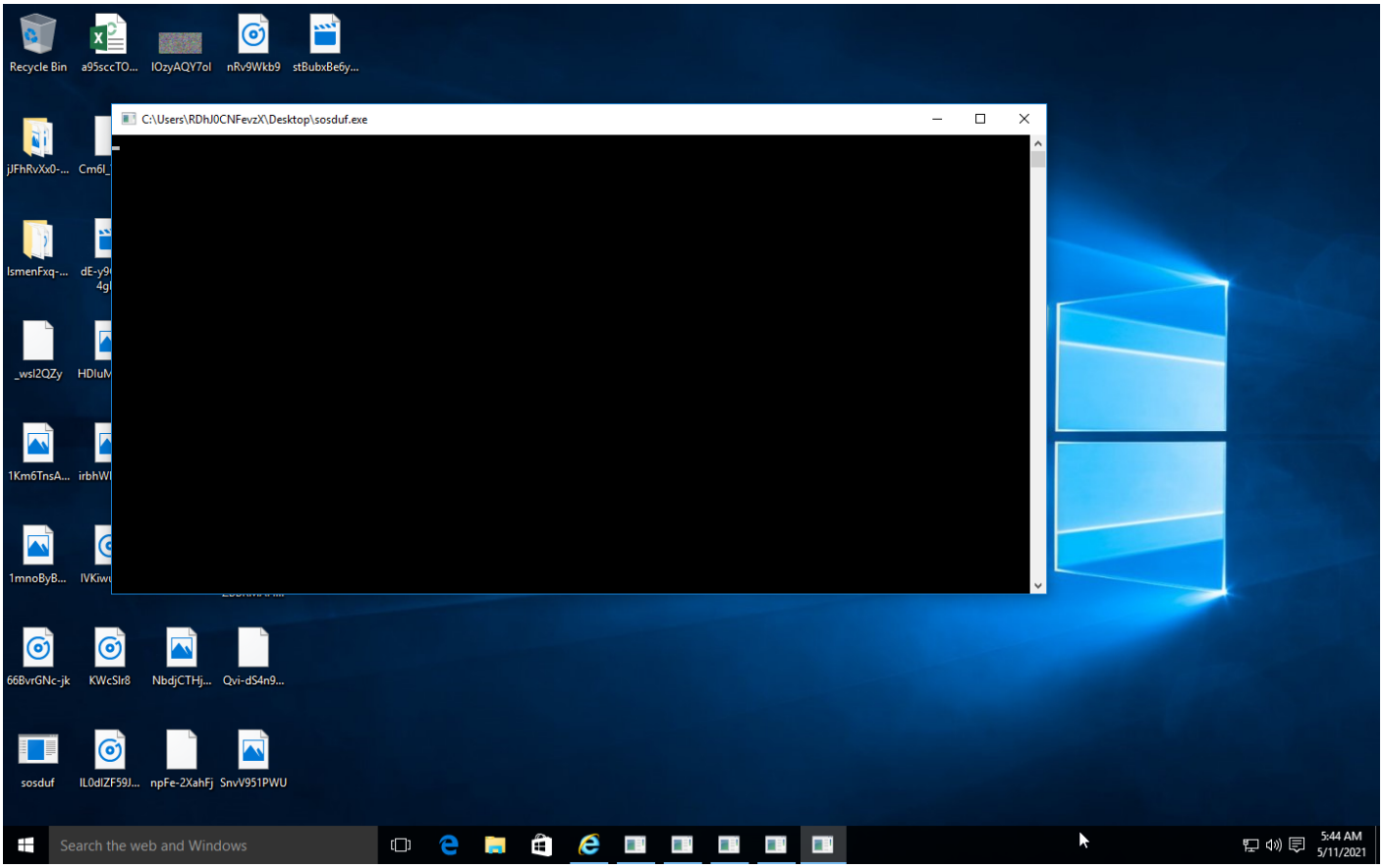
Analysis Information

Creation Time	2021-05-11 07:42 (UTC+2)
Analysis Duration	00:00:44
Termination Reason	All processes terminated
Number of Monitored Processes	1
Execution Successfull	False
Reputation Analysis 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	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
Search the web and Windows
5:43 AM
5/11/2021


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





Screenshots trunkated.

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 recivied

DNS Requests

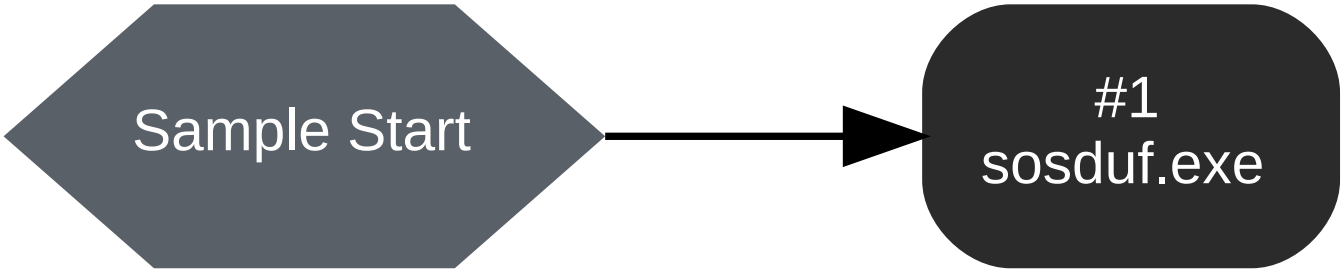
-

HTTP Requests

-

BEHAVIOR

Process Graph



Process #1: sosduf.exe

ID	1
Filename	c:\users\rdhj0cnfevzx\desktop\sosduf.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\sosduf.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 68202, Reason: Analysis Target
Unmonitor End Time	End Time: 102489, Reason: Terminated
Monitor Duration	34.29s
Return Code	0
PID	3012
Parent PID	2104
Bitness	32 Bit

Dropped Files (192)

Filename	File Size	SHA256	YARA Match
C:\vread_me_unlock.txt	696 bytes	dafc32c6ba65f27943b0e7e1c6f714a0c909904fb3156e7123f8a978f0948cd4	✕
C:\BOOTNXT	276 bytes	f03e0160cd46e409031bf4366a0a6b3279fad38972660ba07e2d552aef0d3eca	✕
C:\Users\Public\Libraries\RecordedTV.library-ms	1.24 KB	11b889b34580e81128cb625659cebfe2c52f944e9448c03b2ee36e139ab5a480	✕
C:\Users\RDhJ0CNFevzX\Desktop\1mnoByBkAMXa.png	3.49 KB	4f382abf44c7e6e14131c18b6930c12b9e2c91f2063bdefdbe19aec32d22a8f4	✕
C:\Users\RDhJ0CNFevzX\Desktop\66BvrGNc-jk.wav	86.28 KB	6583d2b11e52214880a379a77bad8de7fa0a5ebfaa5674af5a3d35d5c64becaf	✕
C:\Users\RDhJ0CNFevzX\Desktop\Cm6l_YapJvSAE.swf	61.66 KB	d6235aa8af9676f18293884ac0d517d1b78991b37b74defd9297395b36027ba7	✕
C:\Users\RDhJ0CNFevzX\Desktop\IVKiwu3f0ndhBaWgQn.m4a	6.05 KB	cad557b2cf91dc0d5ccfb974527e53302aabe08f080215fc7117bb7e9451e55a	✕
C:\Users\RDhJ0CNFevzX\Desktop\LxtgF.png	21.33 KB	2075f8d4db98fa81cd0b31a521dc8fdee0356bedb10c3eeefc330583eedf32f3	✕
C:\Users\RDhJ0CNFevzX\Desktop\NbdjCTHjUzBe.jpg	18.00 KB	4a7dab25f00d0da4ec0d1004267716f529c681cbeb8626a004227831d11bb18b	✕
C:\Users\RDhJ0CNFevzX\Desktop\OKumVv-WW9xG3 X7.wav	49.47 KB	607ccb07bb30c555b0a46fb1d5bc1e5f0ee1481f76a9e8f01a4a951e7222fc4c	✕
C:\Users\RDhJ0CNFevzX\Desktop\Qvi-dS4n9MsyIpDvRf.swf	20.18 KB	364f92b51442d0fc52376a60343f7e498b4b033338209d18d9651f38e43bfe95	✕
C:\Users\RDhJ0CNFevzX\Desktop\ZaUlEzOulRLVBjJU.m4a	22.31 KB	616c9a48339cd0548f3fc510bb81c61443ba001e48be71c2c365fd81bab9b387	✕
C:\Users\RDhJ0CNFevzX\Desktop_wsI2QZy.swf	73.28 KB	27fc7ef61b90f5ba1a60ee006af4c3aa156f322555581d956c4fb867c1780a98	✕
C:\Users\RDhJ0CNFevzX\Desktop\dE-y9CgieV 4gFU.mp4	30.63 KB	300c3bd75fbe915403953d6683ae02799ba801f9a43260fa97704c08c8f163c3	✕
C:\Users\RDhJ0CNFevzX\Desktop\irbhWMK5C3JR.bmp	18.87 KB	0125afe9aa5614999beec2bbe5ec2a72a035a5bc500b3deea108a6813f2a4fcc	✕
C:\Users\RDhJ0CNFevzX\Desktop\jFhRvXx0-HQg\AEQRz5sBzZhVu.bmp	32.96 KB	9041a983bfd70ff7e095a099b3a71ce2d113e31350f84fa20a306b72ab5a14c1	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\CVQ7.mp4	92.68 KB	cdb1dbfbc869c2267448e8f1290b4e25c75dd2bd74cdb0510bfae403a48c709a	✕
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\CtCB.avi	22.79 KB	665e6fd79ebe17961b2c44fbdf2451258794865951d2cfbcacaeb9ff67b6648a	✕
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\EmxH.ppt	49.04 KB	9fcc1af82e99c89a16f373d46da5c26f0604c209d433c19d0a1ec16848704336	✕
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\LYDVGBJ4IFd.png	28.80 KB	073265a5b37243adfb37c087359e29b3d7181027843c25ba2d04b8d17c21b952	✕
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\O7NH.jpg	22.54 KB	8dde11dcf6b714626675f8983e335fae77bde6e9cad8104ae19b2c8b79757afd	✕
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\Wl80P.png	44.34 KB	b3b71c4a5156ee136a1dc2fc7b6fd060d20af2b1d70ab92aedf7703ab3181c6b	✕
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\eRZYW5m\lLqBRPcatX7-wJ.mp3	90.49 KB	93dc8c8713406abec7daaa7b4b09524c593687c21ba1cf3cc54b624a1340ad1d	✕
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\eRZYW5m\p6jHL.avi	76.84 KB	0d920b2e0cc0a00fe819c26bb64e57300cd2dbdea433ed128f5948dc6ce2650f	✕
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\eRZYW5m\ySbQKDOOjrDH.m4a	28.92 KB	e63648fbbcdfa0b8a8a0d96fd4a509a265dbfedd4159f275a41dd949eb4fa7da	✕
C:\Users\RDhJ0CNFevzX\Desktop\lL0dIZF59JV6cM.wav	33.22 KB	42bc3d8c4ee24208edd3841f8a5d0469528effe0d8af1fcff7538d4c27bf6e6d	✕
C:\Users\RDhJ0CNFevzX\Desktop\lOzyAQY7oI.bmp	86.08 KB	56bf2147134e2a99e5c4e0cf03d1e68c236e1ed9344396e2fbaafd952c258ed4	✕
C:\Users\RDhJ0CNFevzX\Desktop\lsmenFxq-3ao\0dQqEwX7b_r-zpvAb.wav	80.97 KB	f7dd599deae3a3fcc0f4761b576bada215cd1bd36429a57527ab3d5c508d5485	✕
C:\Users\RDhJ0CNFevzX\Desktop\lsmenFxq-3ao\zQmIs_lj7.flv	14.30 KB	02343013cace7f41cf064a8f67030a21cd269fc04dbd4791e4b715a58b4cdc64	✕
C:\Users\RDhJ0CNFevzX\Desktop\qb_CobqM-NNuxFtHqK.mp3	39.99 KB	745b3caedfd761dda4dd669da326a9efb53558c1af5db85eb0f89c4453eb5150	✕
C:\Users\RDhJ0CNFevzX\Desktop\qV2oIZBBRMAHt8w.mkv	90.46 KB	a0a9ba6a5165cf1b15a0120e05b5f7d3c523bf85d06ed755827001572e22ba91	✕
C:\Users\RDhJ0CNFevzX\Desktop\vfF9hHKjAPNcKqxY4A.bmp	96.85 KB	646d2fda027c62de4c1812eabc626c1031c7fad0d2df23685f6d3444bcca050d	✕
C:\Users\RDhJ0CNFevzX\Desktop\stBubxBe6y6z4niQjh2c.avi	9.71 KB	becd8620bbb4904d232975870c5d970fc10d22c8e080544f890a280d1dcf211c	✕
C:\Users\RDhJ0CNFevzX\Documents\0kERH4Zo.rtf	97.41 KB	80e971041cbaacff6cf56314de6eef5fe0b1439f2a62cf8b4b839c57c82db168	✕
C:\Users\RDhJ0CNFevzX\Desktop\wzJn2zO_p-yHTkE3g4.gif	49.06 KB	c08effb4e819e0dc7e0b89b57bc37f3e0ebca209898c7e73433dc92150962b81	✕
C:\Users\RDhJ0CNFevzX\Documents\1fL3-I81Z4OYL.pptx	69.70 KB	374bb9037da1bc7cf61489e886913458c62189819bd862ef5b94a923803fb58e	✕
C:\Users\RDhJ0CNFevzX\Documents\4OoIYd_eSq8.pptx	8.46 KB	5f02735fc1340d37c68626a90f736ad58d360f2bef7a937915596ca5544723cf	✕
C:\Users\RDhJ0CNFevzX\Documents\4XkNQsq6XKr_P6HMwtn.doc	70.45 KB	422589100136a3118bee0deab644aa176f97aa90cb2ee0e5c1bebfb3a5bbb19e	✕
C:\Users\RDhJ0CNFevzX\Documents\6KaGGKzw-OwQUh4.docx	53.02 KB	99732b1c120076269b0490906bfc1f860ac989f136ccf71252c8b8cba7156528	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\90Gb-.docx	49.21 KB	205e931c7e02fcee15d150405d1bcbbc99e2b580a921e1126801baedd1f4ac4d	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\-JZ ca6GvEB8.xlsx	76.32 KB	230edc5ccad43dbb4fe1391a47b062b6716ca092b87560b3114a1deff3aa6cf4	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\-hL1jdjMmVRK1ZFL0_5B.docx	12.24 KB	aa5b08d9e9b6e27b3696d3a124b64b4e0f5485dd4c221ed2609ac264d65756f8	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\03GbZMlsTTv_yjD9Hjv.rtf	56.57 KB	6d7e8853eb42edc92ab2b469af3c5a99fec7e391b5f19a8f787b73f588623c36	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\CzW_XpqO6uC53L50.csv	16.96 KB	0fae70b22c155f85ffce6082e1624823d8e1fe441cc0a28e8fffeca7c6ec4e62	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\NJYrymxV9.xls	30.99 KB	5538ffdfc29eebd09f93d940f5e015bb1a2d6ac95c110a54e23be34281fd28f0	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\NvhgQY.xls	87.65 KB	127c2ef445381434aad4bcc3b9bce73e5d4b18b15475ae61530a469e8d0a6624	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\OsT7kWbXlqq8WJ.pps	6.02 KB	23a72b280643932080c87635466d3be91e73be6937c633d3d9c9e5af32bd912e	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\kHLccXDGcWmzYVg9CD\Ke4Xu6HrzU4nsA9.doc	97.10 KB	f317fa6efcefc31a43a672402d8a54caf75382402f571217dd55c6bf9c77e6a4	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\YYIkjg13SNtmwKdTH3.csv	43.05 KB	7426d7972f7ea9368cb1ec5b0a97bdc5eaa1a320d316d77d93d98e5ce95c797d	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\kHLccXDGcWmzYVg9CD\WmDqkoE85dUrhaVe.pps	30.22 KB	9db74e36096a1f21da8234952c0c17beb8af1f828ec345f0b085138c6e4f556f	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\kHLccXDGcWmzYVg9CD\aiei3.doc	36.16 KB	48a5a7ad2b5741e2807495e2a279f7334a907250b0a37372e59771672e9b910d	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\kHLccXDGcWmzYVg9CD\bNvBM12ZP88xhuWaAeV.docx	68.78 KB	0407e52a883a7053f4d24a3ebfb501cbd04db227c2f3f6cb66f669d10e3b3a0f	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\m9rQ-Zp.xls	58.05 KB	08efb434b71b963222a8c3c4b1471d7a3375d6ae7dec091309897763dbf9b802	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\zZgXN8tXya.docx	66.87 KB	1eb0042f129e006af39c4944cd4a9941fc34b63b4de6714fb12d4c3eaca6d45e	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\5m1S6Vhyy.xlsx	63.69 KB	4732a4c3b362d70298c24a6d3e46b86e5a09954066f2a7461e3192e9cc6ec75c	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\-3H43 g4.rtf	22.37 KB	0786e2a8d4542c7b37a5c6231be3f01a58e9738365a81fbcf1bf6d0ff903902a	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\0HS-m8AnET_.csv	45.72 KB	fb08576a9102125c0eea34d092b6011b247a0756b9c126be3959c81d1ab30cba	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\3evmoN uAcG8aZ.doc	36.86 KB	c3c5f84327644a9c9bc16c38fc27366c23760cdd8edbb589d4e5546e1830a3d4	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\CmqUn.odp	9.77 KB	38de5031590fd6df1211b50e9ca482f608974d54e80c652b2237618e5f4d8a9c	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\Kyrmv4S.odt	38.75 KB	2c00a21178be310f22b7097f741aa12a9bcb8fb99c74ce983f4e32edb70e9bff	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\aMrWoUh.pdf	25.36 KB	cc69138f99c10438820eb87fde5d54a223ab73e2fc7444bc5686d1ba3c48c647	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\keqkXJmj_XVc8NkMC.rtf	86.13 KB	84a90941f2fcd9edb319d336255084f6e150588bc9c1252c3d30ecc157b6dfe0	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\q8eTg6wNzG.odt	48.82 KB	935a8f29cb87afbf36bd665b2df089b634325555da0f7c7187437ca5751c38ff	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\ve5SvDA4.ods	87.54 KB	56c6895c645ebc93aba36b8cc3567717a905eb9e58b66052df22385322b07e8c	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\y8rkdvIeu_ne.odp	48.63 KB	d9c700170d31d0906ee103aa2bf784b6539e45bc8622369f3ec882b8153a4d6a	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\yrCi4R1znEIlicM.ods	80.46 KB	6e53d6f2c4674fcea668a11d9f793b595de1b401175cda6f80a5116cbc281512	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\C0S2WHYz.ppt	29.25 KB	94da9c6d70470f20da6418f857fe67a5296cb27e7cecd7f2017e53a926e3f83b	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\JnOi1dEaD9FVdj5H8I.docx	75.28 KB	6ef0b20ef2d828ca387b442dc4a948f9140f79aac250967824adab8c28790a01	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\kaeNBPAsAQQV.xlsx	67.43 KB	55c2eceef1ff3ffcbb67bc116ba1a16d3bdd2bcfde33defafff2c043ec807df4	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\sPOK hNDt-tgCki.rtf	39.68 KB	0c1671b07e7afc0a86b1275c9b322472b3f2b58595e668593a372fae7aa2f421	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\uluruq649yUtUP0eXHg7.pps	16.62 KB	a89b13182992a21b2335f0577ef47eb39c4099a4091611b060d4fe645c944981	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\byAxU_QdeSYuBunRt.csv	67.48 KB	d46cc31ecc4b408c854001b0ea27499974411d41ae3cabff3de0a35718a72a80	✕
C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\uk0z.xlsx	79.01 KB	eda9604414af5cce7685a1d6349d2d0b71b0c3200472ab412d48bd440633923f	✕
C:\Users\RDhJ0CNFevzX\Documents\H09VzhhJy701Zn.pptx	79.27 KB	761a3826a70842c97c1728bd4d1fa99ea4e919d1d3485b3912e9984da4abd280	✕
C:\Users\RDhJ0CNFevzX\Documents\HZH9ZrMuSr.pptx	55.52 KB	8fb4ae88e65fc73bc87c12a7c26971d3b20c0e14ad4e2339c6e5469101586067	✕
C:\Users\RDhJ0CNFevzX\Documents\I-BK4YVGg1b.rtf	12.24 KB	28d305fb8ade39739cc03321b9200520a32d89aa38c2bfdc52c137aa462fcca7	✕
C:\Users\RDhJ0CNFevzX\Documents\Lyucj2S2OOss7KdI.pptx	80.78 KB	c8291c809fbdf670309159a980f5e088ef92accda2d7960760269bbd4e682cc8	✕
C:\Users\RDhJ0CNFevzX\Documents\N11qWtgLG.docx	72.35 KB	c6fe364ba48b622975af956d273022a374ac7fcf5f6bf9a777ba58a984dccf52	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst	265.25 KB	7f804d0503ba4b24e5278d89e79a6161007f2167e6cd2efe183fe37a61fc0d62	✕
C:\Users\RDhJ0CNFevzX\Documents\VtkM6.xlsx	48.11 KB	d65f1e420c280b64aeed161dd1c7e600357f0d3b10761c1dab01f1954d8717c1	✕
C:\Users\RDhJ0CNFevzX\Documents\XnU2rHF.xlsx	30.79 KB	d07e6537a34cfe63be18e7bf95919931aa0afde234a3c28535c2d379a18e9891	✕
C:\Users\RDhJ0CNFevzX\Documents\iNydqE6ZqnU-cP.ppt	7.52 KB	2d6de8a82b2539f6363102ae37f50bd180d68e02388ba5c87e3578ca07a86d04	✕
C:\Users\RDhJ0CNFevzX\Documents\nlgyKb7bVH6VfuCYA.xlsx	25.79 KB	df038d57f9b6973c6dcf961962c32bfbf07691f6168c8921e1153004f46e3529	✕
C:\Users\RDhJ0CNFevzX\Documents\nzJDx.ods	83.99 KB	b0011a314a7e211f1eb01837fb4c003b5c3029fad9a21bbac973b7b4d9551d7c	✕
C:\Users\RDhJ0CNFevzX\Documents\qkKxpDXlhMxB7c.xlsx	80.27 KB	bb16314eb426a7679fa0071861869412b7d03f42b87417b1cedd16a1c75ec310	✕
C:\Users\RDhJ0CNFevzX\Documents\vTz7ukVPLfFQ.xlsx	29.87 KB	86226a708ef2fa92f240f619446c2393d3adcc1b7830ac639ced586f2a2401a1	✕
C:\Users\RDhJ0CNFevzX\Documents\vkTMaBRaJZ6X.docx	49.12 KB	63e53103722a8f5320672d726daf996a96e45c4b4754e59a20d6968ce4dc9fc9	✕
C:\Users\RDhJ0CNFevzX\Documents\wGU4.pps	12.74 KB	d611dc148233f741cb0f6c11049f1e7e872f8675586c60a0bb76173b7ab3c533	✕
C:\Users\RDhJ0CNFevzX\Documents\xP-_L.docx	67.95 KB	3da876deb6557ba24dc87d1acbd34567f374e7d6dabe77a4273fdf160ea9ea60	✕
C:\Users\RDhJ0CNFevzX\Favorites\Bing.url	468 bytes	28e82016f8697d22436fdc7dc861bf69a8bbf804eb43babf17db82ab0070c250	✕
C:\Users\RDhJ0CNFevzX\Links\Desktop.lnk	788 bytes	73a0cfe484b226b06ab91d93a8c3b2fc58eebd09cea1f43ddc87ee80ca40a0c4	✕
C:\Users\RDhJ0CNFevzX\Links\Downloads.lnk	1.21 KB	27ff7b70a5b2c1825f85d3950fb9f8b5812c93021031de92251c610553e1a068	✕
C:\Users\RDhJ0CNFevzX\Music\7VAU_SZVOE6QLBs72.mp3	90.70 KB	7a20d57ebd1bd2125bc7739bac61eb6b463a36d20ee3d89fd94ef4305ac097f7	✕
C:\Users\RDhJ0CNFevzX\Music\LYJqOLnG68IjaOKql90Y.mp3	58.49 KB	60cb4a4cf8939d95667c9943bad0bf553c5981d825b37670b13fb9fc89e02722	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\4Tbto3wSrq.wav	64.69 KB	c979526d9da3aa95fcfe5cfe157584b214842b6390df92385a50eeac199e9293	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\6LV1sbKK-D3XJvtWm.wav	87.98 KB	8f652d169c98e39df6b5480c385a05d4946219234545adfc3777a320ce493a35	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\3DHMCVhrKOMLCJNnzVMN.m4a	82.34 KB	4af20074fe0d622c946f08769323044d6065433276828c4679b1285a762e8b47	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\lwNwHTkANyQgUz1S.m4a	44.59 KB	eefab2c9436f46562c343d7d9b8edaf3575e36e2cab983f8c5a3b6901b58b671	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\PZ3cyOZFQ.wav	87.03 KB	c154518c0c7d5ba8a12a24467b388dfdeedd7ec5f83164b8411985106049891f	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\VEuQO6swH.mp3	69.79 KB	6f7b7426b0284b0a5e475183fc0c144a61f4d13e2934ff709506e77eb8f9ed67	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\dH60-76fNbZrdz2.m4a	78.31 KB	95f6832b9198f6bb8200a8290f343ea536b9cc6a9d3cbf77a3e5f7d01e6d8557	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\kZWl531.mp3	11.93 KB	7887def59ecb161a5d35e1ec34e00ca0a6a4825cf0dcf4f659bf2fda49950c6a	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\nIVzqLF49.wav	67.10 KB	b1f8d6476f168e1bc3847d3aaa821dde41f0ac15792fa46ef95063a0a999d59d	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\yCJwtHQtWZDZ3t2yyS\Xjg2XcAOL2hUX.mp3	34.46 KB	0f4cbf8b1aa85341e882db0fa0cfcac3098e46e325b86f415863855876acd337	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\yCJwtHQtWZDZ3t2yyS\lk6mWym4EJDZhiVbitZc.wav	76.18 KB	67b2c09c7c77ab908f39e8c1ef7f535b1932ed4aa0738c03a11273481d9d72fc	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\yCJwtHQtWZDZ3t2yyS\pG2YkrB6YC7l.wav	30.26 KB	be2c431d3043ff2e2f26cabb63c352a54cbfbc23f405b6deac20d07518e50393	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\yCJwtHQtWZDZ3t2yyS\sykSo4.wav	71.77 KB	b69d44ac487df8dbea2a348ecab38e240d160a1125cafc4c856ae21a9ac0f96e	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\mboAfofw_jCV.mp3	95.60 KB	de4747de37d34dfe15c9c84ff0d1ec251900d1f6fb84f0ef13d7eecaad5a5388	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\rFMIbNTh6SVXWCF.wav	68.59 KB	252c4e1a088d859a6f717787f23cf71f75c87805ff9da09d4098b6d57b38138c	✕
C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\uUrZ0.m4a	82.21 KB	afd5663d33165b3f5793a084dfd76f5fdce1a7ba21136f464f9273b9c310a4d0	✕
C:\Users\RDhJ0CNFevzX\Music\bUeCDFkN.wav	79.16 KB	47bbf1e04ab109ae87d819681784ec8f3544fdde9eb35f807666dca98e7def26	✕
C:\Users\RDhJ0CNFevzX\Music\hJz6V.mp3	67.86 KB	4d6cc384cbe32770043152535ff9acaca197dc9b622505c1e2af339d0a02fd8a	✕
C:\Users\RDhJ0CNFevzX\Music\jk6FfJO_dz.mp3	27.11 KB	05ade1ce13c516bd7657055576d600873c268e9d903bb4a054c7b414da5e7fad	✕
C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\-d7DGeGff4j3KRJnW.mp3	41.81 KB	f1e2090ff153f96c3debdd76879498789cc79e10f024ee526254ad1f723805db	✕
C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\A16LF.mp3	90.87 KB	0367daa7d369caca67782d4e025e6939d417e36079d715ce9bfe230998e101ef	✕
C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\ed92X-Z.mp3	87.88 KB	9203b1f0a23747d825dc8acfa49cefb936259bd9327a1276f760831dc6412009	✕
C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\kuL1W-h.wav	26.68 KB	9c39fc92f598b6895487ac098c80ff4adb57c55acfe5538598d5788784d58db7	✕
C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\nXPIvrum.wav	35.31 KB	d3f370e068426d527058a52bbcd247d2c5c5d2e5479e5811d97543378324b43b	✕
C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\tH2U4LxniYTrw.m4a	83.10 KB	5707aab131a415ca4dddc8d68878138eb1a13c15d890a86828604d8b8f43f9d5	✕
C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\MK7VWoo.mp3	57.41 KB	030cc3e5d9bfae47418a81cc0d1f3422fe6f11cd11189bba2e346be484083183	✕
C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\PGkxYB cz.mp3	60.27 KB	c84fbf38f33830ee692aa6629d386aafd3d01593d7eeaf4d1fa79f5efa654a57	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\Tj5pc8WH5_1HOaZF0.m4a	38.23 KB	227ab3169a97991485db06618d7e1142e24ca57ae0348bc83fe86602e0af22ad	✕
C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\nnjv0Ap0trl8.m4a	28.88 KB	0084c36539072b637b15c6b6fda2321988d7968983e36279c5197927e95004ae	✕
C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\ujenVfUz-oAJdo.m4a	73.23 KB	991395ba74866467601b85c5a5e629a5a36b8ad9d1e90533337f882ddcb77b90	✕
C:\Users\RDhJ0CNFevzX\Pictures\07tca.bmp	32.32 KB	4054d8c241c4f83cea49708c952c4a51e15812022faf2d00a7d792df89cd3168	✕
C:\Users\RDhJ0CNFevzX\Pictures\2V5CsG2h.jpg	86.43 KB	3555c28fda92bfff10c4c2170fe7dad223ff156ddf15d5dae39f8e1046409902	✕
C:\Users\RDhJ0CNFevzX\Pictures\2bKCQml.jpg	76.40 KB	69abc2ea1f38c02c8d79b0abdc451a32b6e41db5a7f19a2baaac38c60c7e23b7	✕
C:\Users\RDhJ0CNFevzX\Pictures\39ONyQqD1_0DcRWHisH.gif	93.72 KB	bca348c15ed38134678b18d549fe11996f918eb56594bfc7e57e801b99c10763	✕
C:\Users\RDhJ0CNFevzX\Pictures\8qMv.bmp	65.67 KB	b2c6db140b8bfb8857c929e0ba40ca6c12a1bdb03130af3d1e49d70da7169653	✕
C:\Users\RDhJ0CNFevzX\Pictures\955vc4ZtmelBq.jpg	43.02 KB	6e6b0615523101eeb300441d3a1fc9990c2582d497bd6b5a07cb782e6579a103	✕
C:\Users\RDhJ0CNFevzX\Pictures\Bg3SfdVdr.bmp	43.13 KB	d5c1149c3ba553fa7e8148f146c81e5bd307c68f38f34d803e9acb811d208a93	✕
C:\Users\RDhJ0CNFevzX\Pictures\HUFrMqUQLvETR0w0.png	90.27 KB	422bb0b31cfb8b015cb8c271d324d9c2c392a8f7db5a4b8ebe5cf6e139c937ef	✕
C:\Users\RDhJ0CNFevzX\Pictures\LL6gyxEm.png	16.45 KB	c076dd4462ce3308f529579addd770d6cfd1a67b4c9042f475aeca383d9b9b56	✕
C:\Users\RDhJ0CNFevzX\Pictures\NMFJzJl8.jpg	16.32 KB	5373dda45f6615cda77a344fc33f9d2c5cabf8e24bdb9c73fa2248eb9d69b7aa	✕
C:\Users\RDhJ0CNFevzX\Pictures\RnOyPWEf6b-wu.gif	84.45 KB	87c5501b4db59b676232a9e187edce93ac724609af8a2207cc925020b0b2d993	✕
C:\Users\RDhJ0CNFevzX\Pictures\VQj8UpePrP5Xy_.bmp	61.97 KB	7a25a1b7572e78f9a7298d68a2ae5786779560092b6a710624aeacfa100fe9d58	✕
C:\Users\RDhJ0CNFevzX\Pictures\WoPtTB-ZULyBg.gif	94.16 KB	f8ab43d3f0d6a803f3c136b22351609d4a26989c358245cbc80bff8bd4572a85	✕
C:\Users\RDhJ0CNFevzX\Pictures_DZRGDb6qOo Id v9KRz.jpg	14.52 KB	16a27235238255518c57a8a60659a9c1de82927701b6f3bbd1986b574f61a608	✕
C:\Users\RDhJ0CNFevzX\Pictures\cpuhbF55vB.gif	95.22 KB	4219ab582800450155115c8ee450246914d8c4caecfb4e187af9ab5141d69e9c	✕
C:\Users\RDhJ0CNFevzX\Pictures\gNpnccZzyR4yOQ7Kq4.bmp	43.25 KB	3f917da7cd2e02594559679c45ce75a8401e44be72d4ad15ba1de0be18ed40c5	✕
C:\Users\RDhJ0CNFevzX\Pictures\gg43vl1yr8pTZKBdPTM.jpg	10.04 KB	8c340c570cab9685d29f9afdde2c0772e2936e0d6b8e11ce9f541c3f0954687e	✕
C:\Users\RDhJ0CNFevzX\Pictures\jr8vAOj2RFtClQI1FqJs.png	24.48 KB	abd5971724529dcb307cbc0b9d6fc5506b2c35e7792fbf036a3463c7a121b3ff	✕
C:\Users\RDhJ0CNFevzX\Pictures\kZCD.jpg	70.86 KB	b1b30b2c27f56a98e99202478b08d575c4d3710c8dbb5cc5278c4b2672177bbd	✕
C:\Users\RDhJ0CNFevzX\Pictures\l8LiaunWih5ECuF.gif	34.45 KB	cc6a6b4bc58ae7ffd8a508afe4f0dfcf301bf039e2409eb2760729d94b15de8e	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Pictures\mh9xwYD.bmp	15.58 KB	ea83de99b04c2494fff7cad1f786ac067c02edb7c8b73fdffd14b766c0ec208c	✕
C:\Users\RDhJ0CNFevzX\Pictures\n5A2AmtZcP5kxq23 MP.jpg	29.88 KB	0e40d9d3e04c5772223d74ce66f7c125c4d64e6f8f2c490c51cc0a290f71d13d	✕
C:\Users\RDhJ0CNFevzX\Pictures\oEH_ZM5ZBY9lEd.jpg	11.25 KB	eadd77fd7aaf2cb3b0316f76e7b09159a4591b85bcd8e29264b5e01a977af98a	✕
C:\Users\RDhJ0CNFevzX\Pictures\qHoJ-z3pedpS.jpg	46.99 KB	64141dd6e7e5711186391caae144fc425a33f5b47b159262ea3f0fc96157566d	✕
C:\Users\RDhJ0CNFevzX\Pictures\vJ5FE.png	72.93 KB	55161240e6d79708031ad477fa232c312d973e8d5a27ff5e0baaa8467393a748	✕
C:\Users\RDhJ0CNFevzX\Pictures\wbH2qH6mqYuF9.png	71.55 KB	25d99d032307b53b16bb0a306f81bb700b2dec65b1beb56ed6fe25b56aadad50	✕

Reduced dataset

Host Behavior

Type	Count
Module	52
System	41
Environment	2
-	74
File	4937

ARTIFACTS

File

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
097d28021ffb26cb5b7d2d1377578cd6e2005549e44b5b2491fd310ecf50f7a8	C:\Users\RDhJ0CNFevzX\Desktop\sosduf.exe	Sample File	2155.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
dafc32c6ba65f27943b0e7e1c6f714a0c909904fb3156e7123f8a978f0948cd4	C:\Users\Default/read_me_unlock.txt, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG/read_me_unlock.txt, C:\Users\Pub...\...zX\Documents\Ea6EH7e6iYLk5qzARj9/read_me_unlock.txt, C:\Users\Public\Videos/read_me_unlock.txt, C:\Users\Public/read_me_unlock.txt	Dropped File	696 bytes	text/plain	Create, Write, Access	SUSPICIOUS
f03e0160cd46e409031bf4366a0a6b3279fad38972660ba07e2d552aef0d3eca	C:\BOOTNXT.crypted, C:\BOOTNXT	Modified File	276 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
11b889b34580e81128cb625659cebfe2c52f944e9448c03b2ee36e139ab5a480	C:\Users\Public\Libraries\RecordedTV.library-ms.crypted, C:\Users\Public\Libraries\RecordedTV.library-ms	Modified File	1.24 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
e729db9e9ee6d6f46d1d6f64fd70e652b435ebfc3621ea9cad0e55b482b51c55	C:\Users\RDhJ0CNFevzX\Desktop\1Km6TnsAdDf-JeC.jpg	Modified File	9.88 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
4f382abf44c7e6e14131c18b6930c12b9e2c91f2063bdefdbe19aec32d22a8f4	C:\Users\RDhJ0CNFevzX\Desktop\1mnoByBkAMXa.png.crypted, C:\Users\RDhJ0CNFevzX\Desktop\1mnoByBkAMXa.png	Modified File	3.49 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
6583d2b11e52214880a379a77bad8de7fa0a5ebfaa5674af5a3d35d5c64becaf	C:\Users\RDhJ0CNFevzX\Desktop\66BvrGNc-jk.wav, C:\Users\RDhJ0CNFevzX\Desktop\66BvrGNc-jk.wav.crypted	Modified File	86.28 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d6235aa8af9676f18293884ac0d517d1b78991b37b74defd9297395b36027ba7	C:\Users\RDhJ0CNFevzX\Desktop\Cm6l_YapJvSAE.swf, C:\Users\RDhJ0CNFevzX\Desktop\Cm6l_YapJvSAE.swf.crypted	Modified File	61.66 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
63044b99358d4f82c0ff67f666c026d44c8331172d52dfe9b35de44110b35ad0	C:\Users\RDhJ0CNFevzX\Desktop\HDIuMzsJvMzE8c5R.png	Modified File	9.18 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
cad557b2cf91dc0d5ccfb974527e53302aabe08f080215fc7117bb7e9451e55a	C:\Users\RDhJ0CNFevzX\Desktop\IVKiwu3f0ndhBaWgQn.m4a, C:\Users\RDhJ0CNFevzX\Desktop\IVKiwu3f0ndhBaWgQn.m4a.crypted	Modified File	6.05 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
abfc760d56025ca2f379d48a42d4a65ed018af1cde17967bb19de29d2cd4841e	C:\Users\RDhJ0CNFevzX\Desktop\KWcSlr8.m4a	Modified File	44.33 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
2075f8d4db98fa81cd0b31a521dc8fdee0356bedb10c3eeefc330583eedf32f3	C:\Users\RDhJ0CNFevzX\Desktop\LxtgF.png.crypted, C:\Users\RDhJ0CNFevzX\Desktop\LxtgF.png	Modified File	21.33 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
4a7dab25f00d0da4ec0d1004267716f529c681cbeb8626a004227831d11bb18b	C:\Users\RDhJ0CNFevzX\Desktop\NbdjCTHjUzBe.jpg, C:\Users\RDhJ0CNFevzX\Desktop\NbdjCTHjUzBe.jpg.crypted	Modified File	18.00 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
607ccb07bb30c555b0a46fb1d5bc1e5f0ee1481f76a9e8f01a4a951e7222fc4c	C:\Users\RDhJ0CNFevzX\Desktop\OKumVv-WW9xG3X7.wav.crypted, C:\Users\RDhJ0CNFevzX\Desktop\OKumVv-WW9xG3 X7.wav	Modified File	49.47 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
a771b610e469057e1d289884eacc1d84113e04596f47c6e33e765d6be35cbd8d	C:\Users\RDhJ0CNFevzX\Desktop\MLFJsoANMGkL6.png	Modified File	51.32 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
364f92b51442d0fc52376a60343f7e498b4b033338209d18d9651f38e43bfe95	C:\Users\RDhJ0CNFevzX\Desktop\Qvi-dS4n9MsyIpDvRf.swf, C:\Users\RDhJ0CNFevzX\Desktop\Qvi-dS4n9MsyIpDvRf.swf.crypted	Modified File	20.18 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0ab903ab0943ce3424409fac1c0cbca1cfb2e5421da888582f17572a5514f1cc	C:\Users\RDhJ0CNFevzX\Desktop\SnvV951PWU.png	Modified File	38.55 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
616c9a48339cd0548f3fc510bb81c61443ba001e48be71c2c365fd81bab9b387	C:\Users\RDhJ0CNFevzX\Desktop\ZaUlEzOulRLVBjJU.m4a, C:\Users\RDhJ0CNFevzX\Desktop\ZaUlEzOulRLVBjJU.m4a.crypted	Modified File	22.31 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
710c50f4f0980ae26271f70fc945d0ba1cc21f4947ec368725610e4155e71c25	C:\Users\RDhJ0CNFevzX\Desktop\a95sccTOOgBT.ods	Modified File	75.72 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
27fc7ef61b90f5ba1a60ee006af4c3aa156f322555581d956c4fb867c1780a98	C:\Users\RDhJ0CNFevzX\Desktop_wsI2QZy.swf.crypted, C:\Users\RDhJ0CNFevzX\Desktop_wsI2QZy.swf	Modified File	73.28 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
300c3bd75fbe9154039536683ae02799ba801f9a43260fa97704c08c8f163c3	C:\Users\RDhJ0CNFevzX\Desktop\dE-y9CgieV4gFU.mp4, C:\Users\RDhJ0CNFevzX\Desktop\dE-y9CgieV4gFU.mp4.crypted	Modified File	30.63 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0125afe9aa5614999beec2bbe5ec2a72a035a5bc500b3deea108a6813f2a4fcc	C:\Users\RDhJ0CNFevzX\Desktop\irbhWMK5C3JR.bmp.crypted, C:\Users\RDhJ0CNFevzX\Desktop\irbhWMK5C3JR.bmp	Modified File	18.87 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
9041a983bfd70ff7e095a099b3a71ce2d113e31350f84fa20a306b72ab5a14c1	C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\AEQRz5sBzZhVu.bmp, C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\AEQRz5sBzZhVu.bmp.crypted	Modified File	32.96 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
cdb1dbfbc869c2267448e8f1290b4e25c75dd2bd74cdb0510bfae403a48c709a	C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\CVQ7.mp4.crypted, C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\CVQ7.mp4	Modified File	92.68 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
665e6fd79ebe17961b2c44fbdf24512587948659 51d2cfbcacaeb9ff67b6648a	C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\CtCB.avi.crypted, C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\CtCB.avi	Modified File	22.79 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
9fcc1af82e99c89a16f373d46da5c26f0604c209d433c19d0a1ec16848704336	C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\EmxH.ppt, C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\EmxH.ppt.crypted	Modified File	49.04 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
073265a5b37243adfb37c087359e29b3d7181027843c25ba2d04b8d17c21b952	C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\LYDVGBJ4IFd.png, C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\LYDVGBJ4IFd.png.crypted	Modified File	28.80 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
8dde11dcf6b714626675f8983e335fae77bde6e9cad8104ae19b2c8b79757afd	C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\O7NH.jpg, C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\O7NH.jpg.crypted	Modified File	22.54 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b3b71c4a5156ee136a1dc2fc7b6fd060d20af2b1d70ab92aedf7703ab3181c6b	C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\Wl80P.png, C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\Wl80P.png.crypted	Modified File	44.34 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
57a1ddfc1ae0418e05d7f036e07a0cd87897b1bad2d66aac5a96ed3cb42cefa2	C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\eRZYW5m\DSGla4p6Xu.flv	Modified File	100.04 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
93dc8c8713406abec7daaa7b4b09524c593687c21ba1cf3cc54b624a1340ad1d	C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\eRZYW5m\ILqBRPcatX7-wJ.mp3.crypted, C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\eRZYW5m\ILqBRPcatX7-wJ.mp3	Modified File	90.49 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0d920b2e0cc0a00fe819c26bb64e57300cd2dbdea433ed128f5948dc6ce2650f	C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\eRZYW5m\p6jHL.avi, C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\eRZYW5m\p6jHL.avi.crypted	Modified File	76.84 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
e63648fbbcdfa0b8a8a0d96fd4a509a265dbfedd4159f275a41dd949eb4fa7da	C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\eRZYW5m\ySbQKDOOjrDH.m4a, C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\eRZYW5m\ySbQKDOOjrDH.m4a.crypted	Modified File	28.92 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
291011bfaa89f74852b5dd8de9160b427fa6822f39177bcab0d0bf391e506adb	C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\gSBPZvGU21Z-uNb.mkv	Modified File	68.75 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
42bc3d8c4ee24208edd3841f8a5d0469528effe0d8af1fcff7538d4c27bf6e6d	C:\Users\RDhJ0CNFevzX\Desktop\lL0dIZF59JV6cM.wav.crypted, C:\Users\RDhJ0CNFevzX\Desktop\lL0dIZF59JV6cM.wav	Modified File	33.22 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
593136f73a738466645caf0095d054538284495b8a3f8998b61efb1e1da50717	C:\Users\RDhJ0CNFevzX\Desktop\lXxjNJbLBvyc-mw.mp3	Modified File	36.75 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
56bf2147134e2a99e5c4e0cf03d1e68c236e1ed9344396e2fbaafd952c258ed4	C:\Users\RDhJ0CNFevzX\Desktop\lOzyAQY7ol.bmp, C:\Users\RDhJ0CNFevzX\Desktop\lOzyAQY7ol.bmp.crypted	Modified File	86.08 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
f7dd599deae3a3fcc0f4761b576bada215cd1bd36429a57527ab3d5c508d5485	C:\Users\RDhJ0CNFevzX\Desktop\lsmenFxq-3ao\0dQqEwX7b_r-zpvAb.wav, C:\Users\RDhJ0CNFevzX\Desktop\lsmenFxq-3ao\0dQqEwX7b_r-zpvAb.wav.crypted	Modified File	80.97 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
fec20a9db7ca6e53f96c5c610231f8cba6d0a565383c5b8472a11672e3aa00cf	C:\Users\RDhJ0CNFevzX\Desktop\lsmenFxq-3ao\3W3Heu.mkv	Modified File	34.29 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
6f0d82f5d8317f9b3574530a1725be731e4f429b62218d8e695d9ed5663144f2	C:\Users\RDhJ0CNFevzX\Desktop\lsmenFxq-3ao\AQIRwU.png	Modified File	19.01 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
6059d1a605ea899974b108cf01a45c917231ade0db4841b07f5857f5bf62cb36	C:\Users\RDhJ0CNFevzX\Desktop\lsmenFxq-3ao\EI7WNGL9jviw5Iu.pps	Modified File	6.13 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
02343013cace7f41cf064a8f67030a21cd269fc04dbd4791e4b715a58b4cdc64	C:\Users\RDhJ0CNFevzX\Desktop\lsmenFxq-3ao\zQmIs_lj7.flv, C:\Users\RDhJ0CNFevzX\Desktop\lsmenFxq-3ao\zQmIs_lj7.flv.crypted	Modified File	14.30 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
84dacb5df855fa89c0e42082ac1aad9a80e56d3c7726e276a94f0074a6667ce4	C:\Users\RDhJ0CNFevzX\Desktop\mWSShGr5fOizdg0.csv	Modified File	55.55 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
541d3012122445d63583025c1fd0333c00babb00711c01a4640b41d072f00f9a	C:\Users\RDhJ0CNFevzX\Desktop\n0_FeAoVLpX4idGJgs.wav	Modified File	77.89 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
5129c7ae217d57bbcfb4d54539be3c743d521bb47b3455c910823a32ef1170f4	C:\Users\RDhJ0CNFevzX\Desktop\nRv9Wkb9.mp3	Modified File	2.30 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
f93b2436781a2b741406db2cea2929faf0389c3444e27867a2f21ecbe6173fb0	C:\Users\RDhJ0CNFevzX\Desktop\npFe-2XahFj.swf	Modified File	60.34 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
b0a2160a2bc432ab998ac83981e59cbd0b53847d81920e77b4dbaa08a6b7293e	C:\Users\RDhJ0CNFevzX\Desktop\oCYK45iLz.m4a	Modified File	8.93 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
796a13033364f2b64348c447021b7393fbb0861ba62869c046a2d0b37ec5bd1b	C:\Users\RDhJ0CNFevzX\Desktop\om7geSAayM_.swf	Modified File	62.52 KB	application/octet-stream	Write, Delete, Access, Read	CLEAN
745b3caedfd761dda4dd669da326a9efb53558c1af5db85eb0f89c4453eb5150	C:\Users\RDhJ0CNFevzX\Desktop\qb_CobqM-NNuxFtHqK.mp3, C:\Users\RDhJ0CNFevzX\Desktop\qb_CobqM-NNuxFtHqK.mp3.crypted	Modified File	39.99 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
a0a9ba6a5165cf1b15a0120e05b5f7d3c523bf85d06ed755827001572e22ba91	C:\Users\RDhJ0CNFevzX\Desktop\qV2oIZBBRMAHt8w.mkv, C:\Users\RDhJ0CNFevzX\Desktop\qV2oIZBBRMAHt8w.mkv.crypted	Modified File	90.46 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
646d2fda027c62de4c1812eabc626c1031c7fad0d2df23685f6d3444bcca050d	C:\Users\RDhJ0CNFevzX\Desktop\vfF9hHKjAPNcKqxY4A.bmp.crypted, C:\Users\RDhJ0CNFevzX\Desktop\vfF9hHKjAPNcKqxY4A.bmp	Modified File	96.85 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
becd8620bbb4904d232975870c5d970fc10d22c8e080544f890a280d1dcf211c	C:\Users\RDhJ0CNFevzX\Desktop\stBubxBe6y6z4niQjh2c.avi.crypted, C:\Users\RDhJ0CNFevzX\Desktop\stBubxBe6y6z4niQjh2c.avi	Modified File	9.71 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
80e971041cbaacff6cf56314de6eef5fe0b1439f2a62cf8b4b839c57c82db168	C:\Users\RDhJ0CNFevzX\Documents\0kERH4Zo.rtf, C:\Users\RDhJ0CNFevzX\Documents\0kERH4Zo.rtf.crypted	Modified File	97.41 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
c08effb4e819e0dc7e0b89b57bc37f3e0ebca209898c7e73433dc92150962b81	C:\Users\RDhJ0CNFevzX\Desktop\wzJn2zO_p-yHTkE3g4.gif.crypted, C:\Users\RDhJ0CNFevzX\Desktop\wzJn2zO_p-yHTkE3g4.gif	Modified File	49.06 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
374bb9037da1bc7cf61489e886913458c62189819bd862ef5b94a923803fb58e	C:\Users\RDhJ0CNFevzX\Documents\1fL3-I81Z4OYL.pptx.crypted, C:\Users\RDhJ0CNFevzX\Documents\1fL3-I81Z4OYL.pptx	Modified File	69.70 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
5f02735fc1340d37c68626a90f736ad58d360f2bef7a937915596ca5544723cf	C:\Users\RDhJ0CNFevzX\Documents\4OolYd_eSq8.pptx, C:\Users\RDhJ0CNFevzX\Documents\4OolYd_eSq8.pptx.crypted	Modified File	8.46 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
422589100136a3118bee0deab644aa176f97aa90cb2ee0e5c1bebfb3a5bbb19e	C:\Users\RDhJ0CNFevzX\Documents\4XkNQsq6XKr_P6HMwtn.doc.crypted, C:\Users\RDhJ0CNFevzX\Documents\4XkNQsq6XKr_P6HMwtn.doc	Modified File	70.45 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
99732b1c120076269b0490906bfc1f860ac989f136ccf71252c8b8cba7156528	C:\Users\RDhJ0CNFevzX\Documents\6KaGGKzw-OwQUh4.docx, C:\Users\RDhJ0CNFevzX\Documents\6KaGGKzw-OwQUh4.docx.crypted	Modified File	53.02 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
205e931c7e02fcee15d150405d1bcbbc99e2b580a921e1126801baedd1f4ac4d	C:\Users\RDhJ0CNFevzX\Documents\90Gb-.docx.crypted, C:\Users\RDhJ0CNFevzX\Documents\90Gb-.docx	Modified File	49.21 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
230edc5ccad43dbb4fe1391a47b062b6716ca092b87560b3114a1deff3aa6cf4	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\-JZca6GvEB8.xlsx, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\-JZca6GvEB8.xlsx.crypted	Modified File	76.32 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
aa5b08d9e9b6e27b3696d3a124b64b4e0f5485dd4c221ed2609ac264d65756f8	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\-hL1jdjMmVRK1ZFL0_5B.docx.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\-hL1jdjMmVRK1ZFL0_5B.docx	Modified File	12.24 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
6d7e8853eb42edc92ab2b469af3c5a99fec7e391b5f19a8f787b73f588623c36	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\03GbZMlsTTv_yjD9Hjv.rtf.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\03GbZMlsTTv_yjD9Hjv.rtf	Modified File	56.57 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0fae70b22c155f85ffce6082e1624823d8e1fe441cc0a28e8fffeca7c6ec4e62	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\CzW_XpqO6uC53L50.csv, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\CzW_XpqO6uC53L50.csv.crypted	Modified File	16.96 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
5538ffdfc29eebd09f93d940f5e015bb1a2d6ac95c110a54e23be34281fd28f0	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\NJYrymxV9.xls, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\NJYrymxV9.xls.crypted	Modified File	30.99 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
127c2ef445381434aad4bcc3b9bce73e5d4b18b15475ae61530a469e8d0a6624	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\NvhgQY.xls, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\NvhgQY.xls.crypted	Modified File	87.65 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
23a72b280643932080c87635466d3be91e73be6937c633d3d9c9e5af32bd912e	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\OsT7kWbXlqq8WJ.pps.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\OsT7kWbXlqq8WJ.pps	Modified File	6.02 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
f317fa6efcefc31a43a672402d8a54caf75382402f571217dd55c6bf9c77e6a4	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\kHLccXDGcWmzYVg9CD\Ke4Xu6HrzU4nsA9.doc, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\kHLccXDGcWmzYVg9CD\Ke4Xu6HrzU4nsA9.doc.crypted	Modified File	97.10 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
7426d7972f7ea9368cb1ec5b0a97bdc5eaa1a320d316d77d93d98e5ce95c797d	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\YYIkjg13SNtmwKdTH3.csv, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\YYIkjg13SNtmwKdTH3.csv.crypted	Modified File	43.05 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
9db74e36096a1f21da8234952c0c17beb8af1f828ec345f0b085138c6e4f556f	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\kHLccXDGcWmzYVg9CD\WmDqkoE85dUrhaVe.pps, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\kHLccXDGcWmzYVg9CD\WmDqkoE85dUrhaVe.pps.crypted	Modified File	30.22 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
48a5a7ad2b5741e2807495e2a279f7334a907250b0a37372e59771672e9b910d	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\kHLccXDGcWmzYVg9CD\aiei3.doc.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\kHLccXDGcWmzYVg9CD\aiei3.doc	Modified File	36.16 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0407e52a883a7053f4d24a3ebfb501cbd04db227c2f3f6cb66f669d10e3b3a0f	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\kHLccXDGcWmzYVg9CD\bNvBM12ZP88xhuWaAeV.docx.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\kHLccXDGcWmzYVg9CD\bNvBM12ZP88xhuWaAeV.docx	Modified File	68.78 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
08efb434b71b963222a8c3c4b1471d7a3375d6ae7dec091309897763dbf9b802	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\m9rQ-Zp.xls, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\m9rQ-Zp.xls.crypted	Modified File	58.05 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
1eb0042f129e006af39c4944cd4a9941fc34b63b4de6714fb12d4c3eaca6d45e	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\zZgXN8tXya.docx.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\0T-Vkj2\zZgXN8tXya.docx	Modified File	66.87 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
4732a4c3b362d70298c24a6d3e46b86e5a09954066f2a7461e3192e9cc6ec75c	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\5m1S6Vhyy.xlsx, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\5m1S6Vhyy.xlsx.crypted	Modified File	63.69 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0786e2a8d4542c7b37a5c6231be3f01a58e9738365a81fbcf1bf6d0ff903902a	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\-3H43g4.rtf, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\-3H43g4.rtf.crypted	Modified File	22.37 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
fb08576a9102125c0eea34d092b6011b247a0756b9c126be3959c81d1ab30cba	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\0HS-m8AnET_.csv.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\0HS-m8AnET_.csv	Modified File	45.72 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
c3c5f84327644a9c9bc16c38fc27366c23760cdd8edbb589d4e5546e1830a3d4	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\3evmoNuAcG8aZ.doc.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\3evmoNuAcG8aZ.doc	Modified File	36.86 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
38de5031590fd6df1211b50e9ca482f608974d54e80c652b2237618e5f4d8a9c	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\CmqUn.odp.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\CmqUn.odp	Modified File	9.77 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
2c00a21178be310f22b7097f741aa12a9bcb8fb99c74ce983f4e32edb70e9bff	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\Kyrmv4S.odt.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\Kyrmv4S.odt	Modified File	38.75 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
cc69138f99c10438820eb87fde5d54a223ab73e2fc7444bc5686d1ba3c48c647	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\aMrWoUh.pdf, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\aMrWoUh.pdf.crypted	Modified File	25.36 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
84a90941f2fcd9edb319d336255084f6e150588bc9c1252c3d30ecc157b6dfe0	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\keqkXJmj_XVc8NkMC.rtf.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\keqkXJmj_XVc8NkMC.rtf	Modified File	86.13 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
935a8f29cb87afbf36bd665b2df089b634325555da0f7c7187437ca5751c38ff	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\q8eTg6wNzG.odt, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\q8eTg6wNzG.odt.crypted	Modified File	48.82 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
56c6895c645ebc93aba36b8cc3567717a905eb9e58b66052df22385322b07e8c	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\ve5SvDA4.ods.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\ve5SvDA4.ods	Modified File	87.54 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d9c700170d31d0906ee103aa2bf784b6539e45bc8622369f3ec882b8153a4d6a	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\y8rkdvIeu_ne.odp.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\y8rkdvIeu_ne.odp	Modified File	48.63 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
6e53d6f2c4674fcea668a11d9f793b595de1b401175cda6f80a5116cbc281512	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\yrCi4R1znEIlicM.ods, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\N4v2AJonjYIfePu-5ySR\yrCi4R1znEIlicM.ods.crypted	Modified File	80.46 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
94da9c6d70470f20da6418f857fe67a5296cb277ececd7f2017e53a926e3f83b	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\C0S2WHYz.ppt, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\C0S2WHYz.ppt.crypted	Modified File	29.25 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
6ef0b20ef2d828ca387b442dc4a948f9140f79aac250967824adab8c28790a01	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\JnOi1dEaD9FVdj5H8I.docx, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\JnOi1dEaD9FVdj5H8I.docx.crypted	Modified File	75.28 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
55c2eceef1ff3ffcbb67bc116ba1a16d3bdd2bcfde33defafff2c043ec807df4	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\kaeNBPAsAQQV.xlsx, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\kaeNBPAsAQQV.xlsx.crypted	Modified File	67.43 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0c1671b07e7afc0a86b1275c9b322472b3f2b58595e668593a372fae7aa2f421	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\sPOK hNDt-tgCki.rtf.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\sPOK hNDt-tgCki.rtf	Modified File	39.68 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
a89b13182992a21b2335f0577ef47eb39c4099a4091611b060d4fe645c944981	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\uIuruq649yUtUP0eXHg7.pps, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9_dteD\uIuruq649yUtUP0eXHg7.pps.crypted	Modified File	16.62 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
d46cc31ecc4b408c854001b0ea27499974411d41ae3cabff3de0a35718a72a80	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\byAxU_QdeSYuBunRt.csv, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\byAxU_QdeSYuBunRt.csv.crypted	Modified File	67.48 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
eda9604414af5cce7685a1d6349d2d0b71b0c3200472ab412d48bd440633923f	C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\uk0z.xlsx.crypted, C:\Users\RDhJ0CNFevzX\Documents\Ea6EH7e6iYLk5qzARj9\uk0z.xlsx	Modified File	79.01 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
761a3826a70842c97c1728bd4d1fa99ea4e919d1d3485b3912e9984da4abd280	C:\Users\RDhJ0CNFevzX\Documents\H09VzhhJy701Zn.pptx, C:\Users\RDhJ0CNFevzX\Documents\H09VzhhJy701Zn.pptx.crypted	Modified File	79.27 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
8fb4ae88e65fc73bc87c12a7c26971d3b20c0e14ad4e2339c6e5469101586067	C:\Users\RDhJ0CNFevzX\Documents\HZH9ZrMuSr.pptx, C:\Users\RDhJ0CNFevzX\Documents\HZH9ZrMuSr.pptx.crypted	Modified File	55.52 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
28d305fb8ade39739cc03321b9200520a32d89aa38c2bfdc52c137aa462fcca7	C:\Users\RDhJ0CNFevzX\Documents\I-BK4YVGg1b.rtf.crypted, C:\Users\RDhJ0CNFevzX\Documents\I-BK4YVGg1b.rtf	Modified File	12.24 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
c8291c809fbdf670309159a980f5e088ef92accda2d7960760269bbd4e682cc8	C:\Users\RDhJ0CNFevzX\Documents\Lyucj2S2OOss7KdI.pptx.crypted, C:\Users\RDhJ0CNFevzX\Documents\Lyucj2S2OOss7KdI.pptx	Modified File	80.78 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
c6fe364ba48b622975af956d273022a374ac7fcf5f6bf9a777ba58a984dccf52	C:\Users\RDhJ0CNFevzX\Documents\N11qWtgLG.docx, C:\Users\RDhJ0CNFevzX\Documents\N11qWtgLG.docx.crypted	Modified File	72.35 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
7f804d0503ba4b24e5278d89e79a6161007f2167e6cd2efe183fe37a61fc0d62	C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst.crypted, C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst	Modified File	265.25 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d65f1e420c280b64aeed161dd1c7e600357f0d3b10761c1dab01f1954d8717c1	C:\Users\RDhJ0CNFevzX\Documents\VtkM6.xlsx.crypted, C:\Users\RDhJ0CNFevzX\Documents\VtkM6.xlsx	Modified File	48.11 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d07e6537a34cfe63be18e7bf95919931aa0afde234a3c28535c2d379a18e9891	C:\Users\RDhJ0CNFevzX\Documents\XnU2rHF.xlsx.crypted, C:\Users\RDhJ0CNFevzX\Documents\XnU2rHF.xlsx	Modified File	30.79 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
2d6de8a82b2539f6363102ae37f50bd180d68e02388ba5c87e3578ca07a86d04	C:\Users\RDhJ0CNFevzX\Documents\iNydqE6ZqnU-cP.ppt, C:\Users\RDhJ0CNFevzX\Documents\iNydqE6ZqnU-cP.ppt.crypted	Modified File	7.52 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
df038d57f9b6973c6dcf961962c32bfbf07691f6168c8921e1153004f46e3529	C:\Users\RDhJ0CNFevzX\Documents\nlgyKb7bVH6VfuCYA.xlsx, C:\Users\RDhJ0CNFevzX\Documents\nlgyKb7bVH6VfuCYA.xlsx.crypted	Modified File	25.79 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b0011a314a7e211f1eb01837fb4c003b5c3029fad9a21bbac973b7b4d9551d7c	C:\Users\RDhJ0CNFevzX\Documents\nzJDx.ods, C:\Users\RDhJ0CNFevzX\Documents\nzJDx.ods.crypted	Modified File	83.99 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
bb16314eb426a7679fa0071861869412b7d03f42b87417b1cedd16a1c75ec310	C:\Users\RDhJ0CNFevzX\Documents\qkKxpDXlhMxB7c.xlsx, C:\Users\RDhJ0CNFevzX\Documents\qkKxpDXlhMxB7c.xlsx.crypted	Modified File	80.27 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
86226a708ef2fa92f240f619446c2393d3adcc1b7830ac639ced586f2a2401a1	C:\Users\RDhJ0CNFevzX\Documents\vTz7ukVPLfFQ.xlsx.crypted, C:\Users\RDhJ0CNFevzX\Documents\vTz7ukVPLfFQ.xlsx	Modified File	29.87 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
63e53103722a8f5320672d726daf996a96e45c4b4754e59a20d6968ce4dc9fc9	C:\Users\RDhJ0CNFevzX\Documents\vkTMaBRaJZ6X.docx, C:\Users\RDhJ0CNFevzX\Documents\vkTMaBRaJZ6X.docx.crypted	Modified File	49.12 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d611dc148233f741cb0f6c11049f1e7e872f8675586c60a0bb76173b7ab3c533	C:\Users\RDhJ0CNFevzX\Documents\wGU4.pps.crypted, C:\Users\RDhJ0CNFevzX\Documents\wGU4.pps	Modified File	12.74 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
3da876deb6557ba24dc87d1acbd34567f374e7d6dabe77a4273fdf160ea9ea60	C:\Users\RDhJ0CNFevzX\Documents\xP-_L.docx.crypted, C:\Users\RDhJ0CNFevzX\Documents\xP-_L.docx	Modified File	67.95 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
28e82016f8697d22436fdc7dc861bf69a8bbf804eb43babf17db82ab0070c250	C:\Users\RDhJ0CNFevzX\Favorites\Bing.url, C:\Users\RDhJ0CNFevzX\Favorites\Bing.url.crypted	Modified File	468 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
73a0cfe484b226b06ab91d93a8c3b2fc58eebd09cea1f43ddc87ee80ca40a0c4	C:\Users\RDhJ0CNFevzX\Links\Desktop.lnk.crypted, C:\Users\RDhJ0CNFevzX\Links\Desktop.lnk	Modified File	788 bytes	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
27ff7b70a5b2c1825f85d3950fb9f8b5812c93021031de92251c610553e1a068	C:\Users\RDhJ0CNFevzX\Links\Downloads.lnk, C:\Users\RDhJ0CNFevzX\Links\Downloads.lnk.crypted	Modified File	1.21 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
7a20d57ebd1bd2125bc7739bac61eb6b463a36d20ee3d89fd94ef4305ac097f7	C:\Users\RDhJ0CNFevzX\Music\7VAU_SZVOE6QLBs72.mp3, C:\Users\RDhJ0CNFevzX\Music\7VAU_SZVOE6QLBs72.mp3.crypted	Modified File	90.70 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
60cb4a4cf8939d95667c9943bad0bf553c5981d825b37670b13fb9fc89e02722	C:\Users\RDhJ0CNFevzX\Music\LYJqOLnG68IjaOKql90Y.mp3.crypted, C:\Users\RDhJ0CNFevzX\Music\LYJqOLnG68IjaOKql90Y.mp3	Modified File	58.49 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
c979526d9da3aa95fcfe5cfe157584b214842b6390df92385a50eeac199e9293	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\4Tbto3wSrq.wav, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\4Tbto3wSrq.wav.crypted	Modified File	64.69 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
8f652d169c98e39df6b5480c385a05d4946219234545adfc3777a320ce493a35	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\6LV1sbKK-D3XJvtWm.wav.crypted, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\6LV1sbKK-D3XJvtWm.wav	Modified File	87.98 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
4af20074fe0d622c946f08769323044d6065433276828c4679b1285a762e8b47	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\3DHMCVhrKOMLCJNnzVMN.m4a, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\3DHMCVhrKOMLCJNnzVMN.m4a.crypted	Modified File	82.34 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
eefab2c9436f46562c343d7d9b8edaf3575e36e2cab983f8c5a3b6901b58b671	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\IwNwHTkANyQgUz1S.m4a, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\IwNwHTkANyQgUz1S.m4a.crypted	Modified File	44.59 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
c154518c0c7d5ba8a12a24467b388dfdeedd7ec5f83164b84119851060491f	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\PZ3cyOZFQ.wav.crypted, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\PZ3cyOZFQ.wav	Modified File	87.03 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
6f7b7426b0284b0a5e475183fc0c144a61f4d13e2934ff709506e77eb8f9ed67	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\VEuQO6swH.mp3, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\VEuQO6swH.mp3.crypted	Modified File	69.79 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
95f6832b9198f6bb8200a8290f343ea536b9cc6a9d3cbf77a3e5f7d01e6d8557	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\dH60-76fNbZrdz2.m4a.crypted, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\dH60-76fNbZrdz2.m4a	Modified File	78.31 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
7887def59ecb161a5d35e1ec34e00ca0a6a4825cf0dcf4f659bf2fda49950c6a	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\kZWl531.mp3.crypted, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\LCvg4MHIIDFXE5UG\kZWl531.mp3	Modified File	11.93 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b1f8d6476f168e1bc3847d3aaa821dde41f0ac15792fa46ef95063a0a999d59d	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\nIVzqLF49.wav.crypted, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\nIVzqLF49.wav	Modified File	67.10 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0f4cbf8b1aa85341e882db0fa0cfcac3098e46e325b86f415863855876acd337	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\yCJwtHQtWZDZ3t2yyS\Xjg2XcAOL2hUX.mp3.crypted, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\yCJwtHQtWZDZ3t2yyS\Xjg2XcAOL2hUX.mp3	Modified File	34.46 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
67b2c09c7c77ab908f39e8c1ef7f535b1932ed4aa0738c03a11273481d9d72fc	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\yCJwtHQtWZDZ3t2yyS\lk6mWym4EJDZhiVbitZc.wav, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\yCJwtHQtWZDZ3t2yyS\lk6mWym4EJDZhiVbitZc.wav.crypted	Modified File	76.18 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
be2c431d3043ff2e2f26cabb63c352a54cbfbc23f405b6deac20d07518e50393	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\yCJwtHQtWZDZ3t2yyS\pG2YkrB6YC7l.wav.crypted, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\yCJwtHQtWZDZ3t2yyS\pG2YkrB6YC7l.wav	Modified File	30.26 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b69d44ac487df8dbea2a348ecab38e240d160a1125cafc4c856ae21a9ac0f96e	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\yCJwtHQtWZDZ3t2yyS\sykSo4.wav, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\7Wh9AxLTsfU1o4fqG\yCJwtHQtWZDZ3t2yyS\sykSo4.wav.crypted	Modified File	71.77 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
de4747de37d34dfe15c9c84ff0d1ec251900d1f6fb84f0ef13d7eecaad5a5388	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\mboAfofw_jCV.mp3.crypted, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\mboAfofw_jCV.mp3	Modified File	95.60 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
252c4e1a088d859a6f717787f23cf71f75c87805ff9da09d4098b6d57b38138c	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\rFMIbNTh6SVXWCF.wav, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\rFMIbNTh6SVXWCF.wav.crypted	Modified File	68.59 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
afd5663d33165b3f5793a084dfd76f5fdce1a7ba21136f464f9273b9c310a4d0	C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\uUrZ0.m4a.crypted, C:\Users\RDhJ0CNFevzX\Music\R2RbR0boE5Lx2X\uUrZ0.m4a	Modified File	82.21 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
47bbf1e04ab109ae87d819681784ec8f3544fdde9eb35f807666dca98e7def26	C:\Users\RDhJ0CNFevzX\Music\bUeCDFkN.wav.crypted, C:\Users\RDhJ0CNFevzX\Music\bUeCDFkN.wav	Modified File	79.16 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
4d6cc384cbe32770043152535ff9acaca197dc9b622505c1e2af339d0a02fd8a	C:\Users\RDhJ0CNFevzX\Music\hJz6V.mp3.crypted, C:\Users\RDhJ0CNFevzX\Music\hJz6V.mp3	Modified File	67.86 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
05ade1ce13c516bd7657055576d600873c268e9d903bb4a054c7b414da5e7fad	C:\Users\RDhJ0CNFevzX\Music\jk6FfJO_dz.mp3.crypted, C:\Users\RDhJ0CNFevzX\Music\jk6FfJO_dz.mp3	Modified File	27.11 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
f1e2090ff153f96c3debdd76879498789cc79e10f024ee526254ad1f723805db	C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\-d7DGeGff4j3KRJnW.mp3.crypted, C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\-d7DGeGff4j3KRJnW.mp3	Modified File	41.81 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0367daa7d369caca67782d4e025e6939d417e36079d715ce9bfe230998e101ef	C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\A16LF.mp3.crypted, C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\A16LF.mp3	Modified File	90.87 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
9203b1f0a23747d825dc8acfa49cefb936259bd9327a1276f760831dc6412009	C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\ed92X-Z.mp3, C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\ed92X-Z.mp3.crypted	Modified File	87.88 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
9c39fc92f598b6895487ac098c80ff4adb57c55acfe5538598d5788784d58db7	C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\kuL1W-h.wav, C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\kuL1W-h.wav.crypted	Modified File	26.68 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
d3f370e068426d527058a52bbcd247d2c5c5d2e5479e5811d97543378324b43b	C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\nXPIvrum.wav, C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\nXPIvrum.wav.crypted	Modified File	35.31 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
5707aab131a415ca4ddc8d68878138eb1a13c15d890a86828604d8b8f43f9d5	C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\tH2U4LxniYTrw.m4a.crypted, C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\DBjkoAN\tH2U4LxniYTrw.m4a	Modified File	83.10 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
030cc3e5d9bfae47418a81cc0d1f3422fe6f11cd11189bba2e346be484083183	C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\MK7VWoo.mp3, C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\MK7VWoo.mp3.crypted	Modified File	57.41 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
c84fbf38f33830ee692aa6629d386aafd3d01593d7eeaf4d1fa79f5efa654a57	C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\PGkxYB cz.mp3.crypted, C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\PGkxYB cz.mp3	Modified File	60.27 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
227ab3169a97991485db06618d7e1142e24ca57ae0348bc83fe86602e0af22ad	C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\Tj5pc8WH5_1HOaZF0.m4a, C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\Tj5pc8WH5_1HOaZF0.m4a.crypted	Modified File	38.23 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
0084c36539072b637b15c6b6fda2321988d7968983e36279c5197927e95004ae	C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\nnjv0Ap0trl8.m4a.crypted, C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\nnjv0Ap0trl8.m4a	Modified File	28.88 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
991395ba74866467601b85c5a5e629a5a36b8ad9d1e90533337f882ddcb77b90	C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\ujenVfUz-oAJdo.m4a, C:\Users\RDhJ0CNFevzX\Music\l3Ukg9xPqGI\ujenVfUz-oAJdo.m4a.crypted	Modified File	73.23 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
4054d8c241c4f83cea49708c952c4a51e15812022faf2d00a7d792df89cd3168	C:\Users\RDhJ0CNFevzX\Pictures\07tca.bmp.crypted, C:\Users\RDhJ0CNFevzX\Pictures\07tca.bmp	Modified File	32.32 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
3555c28fda92bfff10c4c2170fe7dad223ff156ddf15d5dae39f8e1046409902	C:\Users\RDhJ0CNFevzX\Pictures\2V5CsG2h.jpg, C:\Users\RDhJ0CNFevzX\Pictures\2V5CsG2h.jpg.crypted	Modified File	86.43 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
69abc2ea1f38c02c8d79b0abdc451a32b6e41db5a7f19a2baaac38c60c7e23b7	C:\Users\RDhJ0CNFevzX\Pictures\2bKCQml.jpg.crypted, C:\Users\RDhJ0CNFevzX\Pictures\2bKCQml.jpg	Modified File	76.40 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
bca348c15ed38134678b18d549fe11996f918eb56594bfc7e57e801b99c10763	C:\Users\RDhJ0CNFevzX\Pictures\39ONyQqD1_0DcRWHisH.gif.crypted, C:\Users\RDhJ0CNFevzX\Pictures\39ONyQqD1_0DcRWHisH.gif	Modified File	93.72 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
b2c6db140b8bfb8857c929e0ba40ca6c12a1bdb03130af3d1e49d70da7169653	C:\Users\RDhJ0CNFevzX\Pictures\8qMv.bmp, C:\Users\RDhJ0CNFevzX\Pictures\8qMv.bmp.crypted	Modified File	65.67 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN
6e6b0615523101eeb300441d3a1fc9990c2582d497bd6b5a07cb782e6579a103	C:\Users\RDhJ0CNFevzX\Pictures\955vc4ZtmelBq.jpg.crypted, C:\Users\RDhJ0CNFevzX\Pictures\955vc4ZtmelBq.jpg	Modified File	43.02 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
d5c1149c3ba553fa7e8148f146c81e5bd307c68f38f34d803e9acb811d208a93	C:\Users\RDhJ0CNFevzX\Pictures\Bg3SfdVdr.bmp.crypted, C:\Users\RDhJ0CNFevzX\Pictures\Bg3SfdVdr.bmp	Modified File	43.13 KB	application/octet-stream	Write, Access, Create, Read, Delete	CLEAN

Reduced dataset

Filename

Filename	Category	Operations	Verdict
C:\read_me_unlock.txt	Dropped File	Create, Write, Access	SUSPICIOUS
C:\	Accessed File	Access	CLEAN
C:\$Recycle.Bin	Accessed File	Access	CLEAN
C:\BOOTNXT	Modified File	Write, Delete, Access, Read	CLEAN
C:\BOOTSECT.BAK	Accessed File	Access	CLEAN
C:\Boot	Accessed File	Access	CLEAN
C:\BOOTNXT.crypted	Modified File	Create, Write, Access	CLEAN
C:\Documents and Settings	Accessed File	Access	CLEAN
C:\PerfLogs	Accessed File	Access	CLEAN
C:\PerfLogs/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Program Files	Accessed File	Access	CLEAN
C:\Program Files (x86)	Accessed File	Access	CLEAN
C:\ProgramData	Accessed File	Access	CLEAN
C:\Recovery	Accessed File	Access	CLEAN
C:\Recovery/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Recovery\WindowsRE	Accessed File	Access	CLEAN
C:\System Volume Information	Accessed File	Access	CLEAN
C:\Users	Accessed File	Access	CLEAN
C:\Users/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\All Users	Accessed File	Access	CLEAN
C:\Users\Default	Accessed File	Access	CLEAN
C:\Users\Default/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Default\AppData	Accessed File	Access	CLEAN
C:\Users\Default\Application Data	Accessed File	Access	CLEAN
C:\Users\Default\Cookies	Accessed File	Access	CLEAN
C:\Users\Default\Desktop	Accessed File	Access	CLEAN
C:\Users\Default\Desktop/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Default\Documents	Accessed File	Access	CLEAN
C:\Users\Default\Documents/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Default\Documents\My Music	Accessed File	Access	CLEAN

Filename	Category	Operations	Verdict
C:\Users\Default\Documents\My Pictures	Accessed File	Access	CLEAN
C:\Users\Default\Documents\My Videos	Accessed File	Access	CLEAN
C:\Users\Default\Downloads	Accessed File	Access	CLEAN
C:\Users\Default\Downloads/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Default\Favorites	Accessed File	Access	CLEAN
C:\Users\Default\Favorites/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Default\Links	Accessed File	Access	CLEAN
C:\Users\Default\Links/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Default\Local Settings	Accessed File	Access	CLEAN
C:\Users\Default\Music	Accessed File	Access	CLEAN
C:\Users\Default\Music/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Default\My Documents	Accessed File	Access	CLEAN
C:\Users\Default\NTUSER.DAT	Accessed File	Access	CLEAN
C:\Users\Default\NTUSER.DAT.LOG1	Accessed File	Access	CLEAN
C:\Users\Default\NTUSER.DAT.LOG2	Accessed File	Access	CLEAN
C:\Users\Default\NTUSER.DAT{62e13464-7ee5-11e5-80c4-a4badb40df56}.TM.blf	Accessed File	Access	CLEAN
C:\Users\Default\NTUSER.DAT{62e13464-7ee5-11e5-80c4-a4badb40df56}.TMContainer00000000000000000001.regtrans-ms	Accessed File	Access	CLEAN
C:\Users\Default\NTUSER.DAT{62e13464-7ee5-11e5-80c4-a4badb40df56}.TMContainer00000000000000000002.regtrans-ms	Accessed File	Access	CLEAN
C:\Users\Default\NetHood	Accessed File	Access	CLEAN
C:\Users\Default\Pictures	Accessed File	Access	CLEAN
C:\Users\Default\Pictures/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Default\PrintHood	Accessed File	Access	CLEAN
C:\Users\Default\Recent	Accessed File	Access	CLEAN
C:\Users\Default\Saved Games	Accessed File	Access	CLEAN
C:\Users\Default\Saved Games/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Default\SendTo	Accessed File	Access	CLEAN
C:\Users\Default\Start Menu	Accessed File	Access	CLEAN
C:\Users\Default\Templates	Accessed File	Access	CLEAN
C:\Users\Default\Videos	Accessed File	Access	CLEAN
C:\Users\Default\Videos/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Default User	Accessed File	Write, Access	CLEAN
C:\Users\Public	Accessed File	Access	CLEAN

Filename	Category	Operations	Verdict
C:\Users\Public/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Public\AccountPictures	Accessed File	Access	CLEAN
C:\Users\Public\AccountPictures/ read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Public\AccountPictures\desktop.ini	Accessed File	Access	CLEAN
C:\Users\Public\Desktop	Accessed File	Access	CLEAN
C:\Users\Public\Desktop/read_me_unlock.txt	Dropped File	Create, Access	CLEAN
C:\Users\Public\Desktop\desktop.ini	Accessed File	Access	CLEAN
C:\Users\Public\Documents	Accessed File	Access	CLEAN
C:\Users\Public\Documents/ read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Public\Documents\My Music	Accessed File	Access	CLEAN
C:\Users\Public\Documents\My Pictures	Accessed File	Access	CLEAN
C:\Users\Public\Documents\My Videos	Accessed File	Access	CLEAN
C:\Users\Public\Documents\desktop.ini	Accessed File	Access	CLEAN
C:\Users\Public\Downloads	Accessed File	Access	CLEAN
C:\Users\Public\Downloads/ read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Public\Downloads\desktop.ini	Accessed File	Access	CLEAN
C:\Users\Public\Libraries	Accessed File	Access	CLEAN
C:\Users\Public\Libraries/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Public\Libraries\RecordedTV.library-ms	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\Public\Libraries\desktop.ini	Accessed File	Access	CLEAN
C:\Users\Public\Music	Accessed File	Access	CLEAN
C:\Users\Public\Music/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Public\Music\desktop.ini	Accessed File	Access	CLEAN
C:\Users\Public\Pictures	Accessed File	Access	CLEAN
C:\Users\Public\Pictures/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Public\Pictures\desktop.ini	Accessed File	Access	CLEAN
C:\Users\Public\Videos	Accessed File	Access	CLEAN
C:\Users\Public\Videos/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\Public\Videos\desktop.ini	Accessed File	Access	CLEAN
C:\Users\Public\desktop.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX/ read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Application Data	Accessed File	Access	CLEAN

Filename	Category	Operations	Verdict
C:\Users\Public\Libraries\RecordedTV.library-ms.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Contacts	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Contacts/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Contacts\desktop.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Cookies	Accessed File	Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop/read_me_unlock.txt	Dropped File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\1Km6TnsAdDf-JeC.jpg	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\1mnoByBkAMXa.png	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\66BvrGNc-jk.wav	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\1Km6TnsAdDf-JeC.jpg.crypted	Accessed File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Cm6l_YapJvSAE.swf	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\1mnoByBkAMXa.png.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\HDIuMzsJvMzE8c5R.png	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\66BvrGNc-jk.wav.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\IVKiwu3f0ndhBaWgQn.m4a	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\KWcSlr8.m4a	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\LxtgF.png	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Cm6l_YapJvSAE.swf.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\MLFJsoANMGkL6.png	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\NbdjCTHjUzBe.jpg	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\OKumVv-WW9xG3 X7.wav	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\IVKiwu3f0ndhBaWgQn.m4a.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Qvi-dS4n9MsyIpDvRf.swf	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\SnvV951PWU.png	Modified File	Write, Delete, Access, Read	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\LxtgF.png.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\HDIuMzsJvMzE8c5R.png.crypted	Accessed File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\KWcSlr8.m4a.crypted	Accessed File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\NbdjCTHjUzBe.jpg.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ZaUlEzOulRLVBjJU.m4a	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop_wsI2QZy.swf	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\MLFJsoANMGkL6.png.crypted	Accessed File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Qvi-dS4n9MsyIpDvRf.swf.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\a95sccTOOgBT.ods	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\dE-y9CgieV 4gFU.mp4	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\OKumVv-WW9xG3 X7.wav.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\SnvV951PWU.png.crypted	Accessed File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ZaUlEzOulRLVBjJU.m4a.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\irbhWMK5C3JR.bmp	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg/read_me_unlock.txt	Dropped File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop_wsI2QZy.swf.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\a95sccTOOgBT.ods.crypted	Accessed File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\dE-y9CgieV 4gFU.mp4.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\irbhWMK5C3JR.bmp.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\AEQRz5sBzZhVu.bmp	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\jJFhRvXx0-HQg\CVQ7.mp4	Modified File	Write, Delete, Access, Read	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\jFhRvXx0-HQg\AEQRz5sBzZhVu.bmp.crypted	Modified File	Create, Write, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\jFhRvXx0-HQg\CtCB.avi	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\jFhRvXx0-HQg\EmxH.ppt	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\jFhRvXx0-HQg\LYDVGBJ4IFd.png	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\jFhRvXx0-HQg\O7NH.jpg	Modified File	Write, Delete, Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\jFhRvXx0-HQg\Wl80P.png	Modified File	Write, Delete, Access, Read	CLEAN

Reduced dataset

URL

-

Domain

-

IP

-

Email

-

Email Address

-

Mutex

-

Registry

-

Process

Process Name	Commandline	Verdict
sosduf.exe	"C:\Users\RDhJ0CNFevzX\Desktop\sosduf.exe"	MALICIOUS

YARA / AV

Antivirus (1)

File Type	Threat Name	Filename	Verdict
SAMPLE	Trojan.Ransom.Agent.BX	C:\Users\RDhJ0CNFevzX\Desktop\sosduf.exe	MALICIOUS

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

Analyzer Information

Analyzer Version	4.1.1
Dynamic Engine Version	4.1.1 / 02/08/2021 15:19
Static Engine Version	1.6.0
Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (November 12, 2020)
Built-in AV Database Update Release Date	2021-05-11 03:26:58+00:00
VTI Ruleset Version	3.8
YARA Built-in Ruleset Version	1.5
Analysis Report Layout Version	10

Software Information

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