MALICIOUS

Classifications: Wiper, Ransomware

Threat Names: Mal/Generic-S, Gen:Heur.Ransom.REntS.Gen.1, Gen:Heur.Ransom.RTH.1

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
Sample Name	**covid.exe**
ID	#303908
MD5	5313e9992ef078a5e58f9f416ce99645
SHA1	3efc88de42d37c02ee4f3ed4f78f7855d805869e
SHA256	372fa440571b4ab1db28d8736c9014e11d8e27277c094062f2c444b6b97e8182
File Size	16.00 KB
Report Created	2021-03-23 12:19 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (6 rules, 10 matches)

Score	Category	Operation	Count	Classification
4/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) covid.exe modifies the content of multiple user files.			
4/5	User Data Modification	Deletes user files	1	Wiper
	• (Process #1) covid.exe deletes multiple user files.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
4/5	Antivirus	Malicious content was detected by heuristic scan	2	-
	• Built-in AV detected the sample itself as "Gen:Heur.Ransom.REntS.Gen.1". • Built-in AV detected a memory dump of (process #1) covid.exe as "Gen:Heur.Ransom.RTH.1".			
1/5	Hide Tracks	Changes folder appearance	4	-
	• (Process #1) covid.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures". • (Process #1) covid.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures\camera roll". • (Process #1) covid.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures\saved pictures". • (Process #1) covid.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\documents".			
1/5	System Modification	Creates an unusually large number of files	1	-
	• (Process #1) covid.exe creates an above average number of files.			

Mitre ATT&CK Matrix

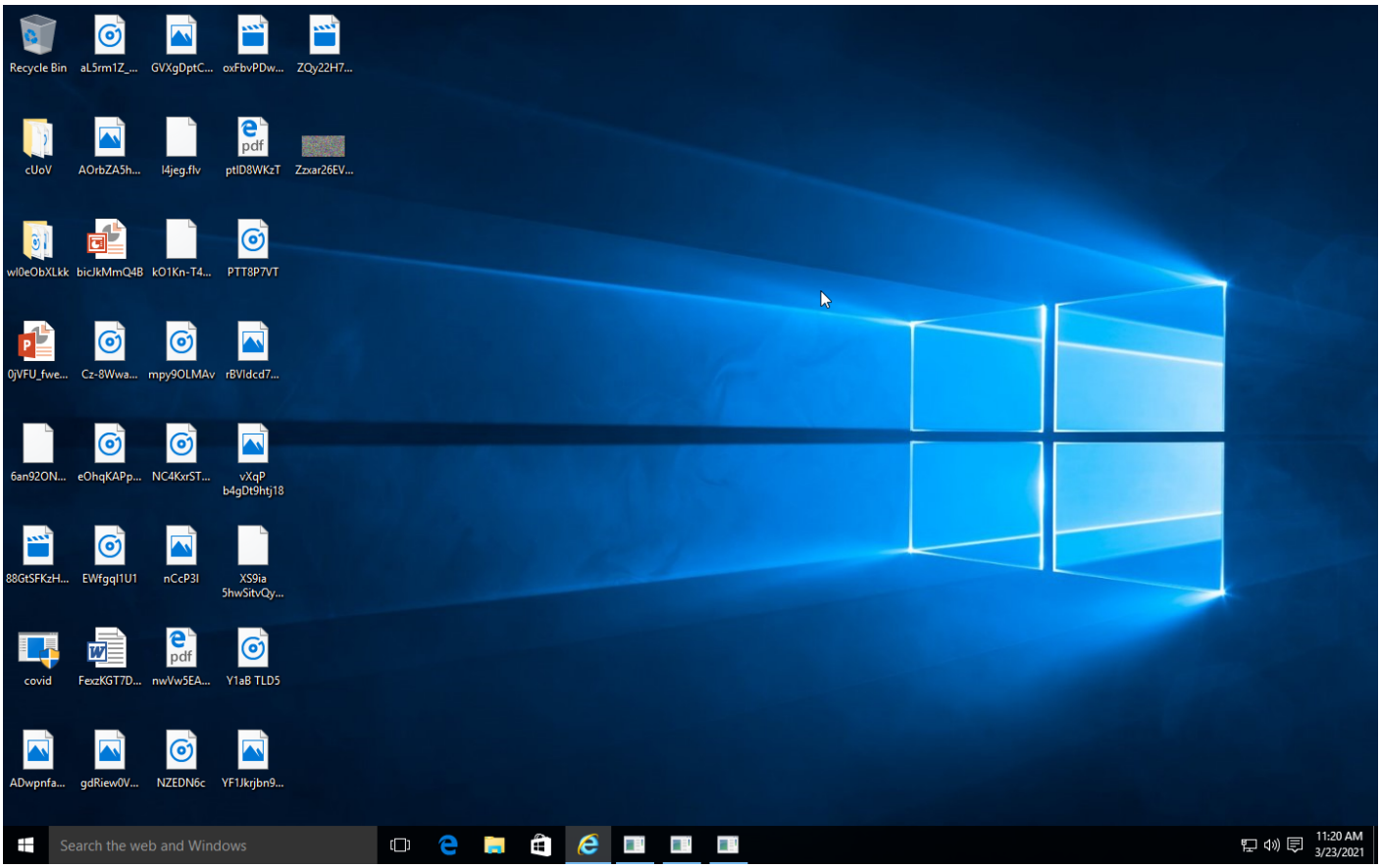
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
-	-	-	-	-	-	-	-	-	-	-	#T1486 Data Encrypted for Impact
-	-	-	-	-	-	-	-	-	-	-	#T1485 Data Destruction
-	-	-	-	#T1036 Masquerading	-	-	-	-	-	-	-

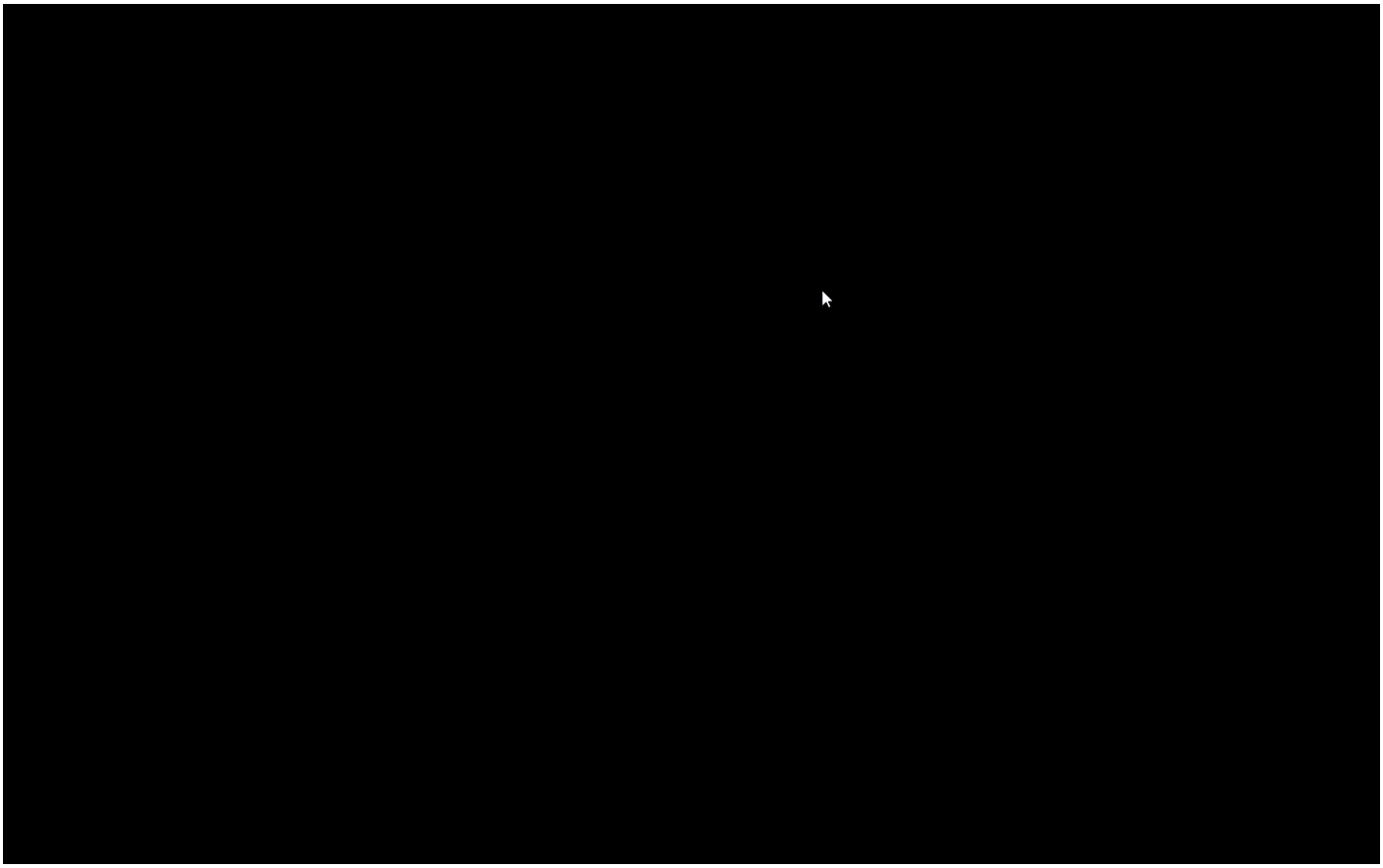
Sample Information

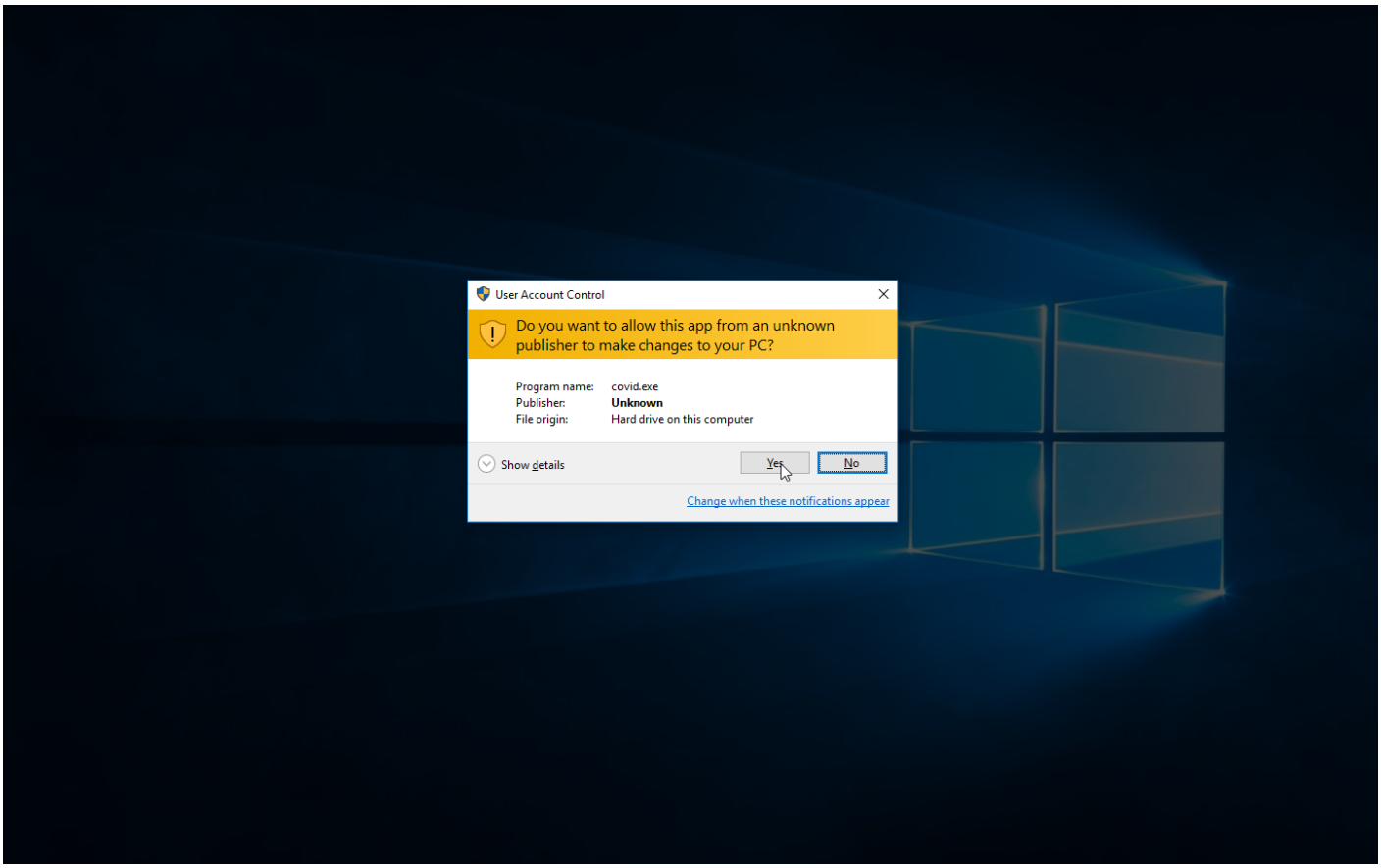
ID	927590
MD5	5313e9992ef078a5e58f9f416ce99645
SHA1	3efc88de42d37c02ee4f3ed4f78f7855d805869e
SHA256	372fa440571b4ab1db28d8736c9014e11d8e27277c094062f2c444b6b97e8182
SSDeep	384:BFOjDL3OyGtKgFKOwfyvHYYPNOcvifzrkYcKV1:BYjDL3wtKgFKKVkYYcKV1
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
Filename	covid.exe
File Size	16.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

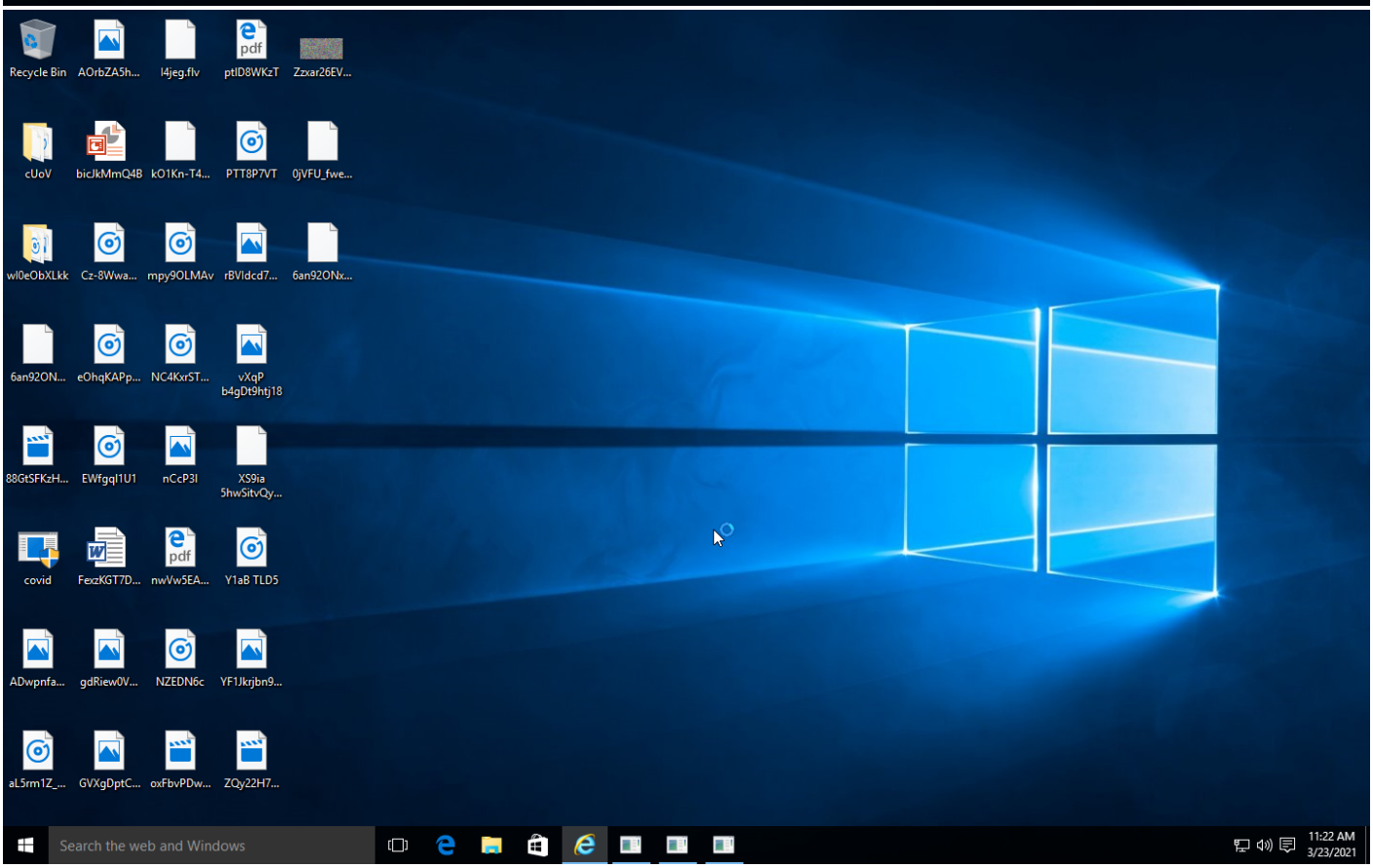
Analysis Information

Creation Time	2021-03-23 12:19 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
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	2
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
aL5rm1Z_...
GVXgDptC...
oxFbvPDw...
ZQy22H7...
cUoV
AOrbZA5h...
l4jeg.flv
ptID8WKzT
Zzxar26EV...
wl0eObXLkk
bicJkMmQ4B
kO1Kn-T4...
PTT8P7VT
0jVFU_fwe...
Cz-8Wwa...
mpy9OLMAv
rBVIdcd7...
6an92ON...
eOhqKAPp...
NC4KxrST...
vXqP b4gDt9htj18
88GtSFKzH...
EWfgql1U1
nCcP3I
XS9ia 5hwSitvQy...
covid
FexzKGT7D...
nwVw5EA...
Y1aB TLD5
ADwpnfa...
gdRiew0V...
NZEDN6c
YF1Jkrjbn9...
Search the web and Windows
11:20 AM
3/23/2021







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

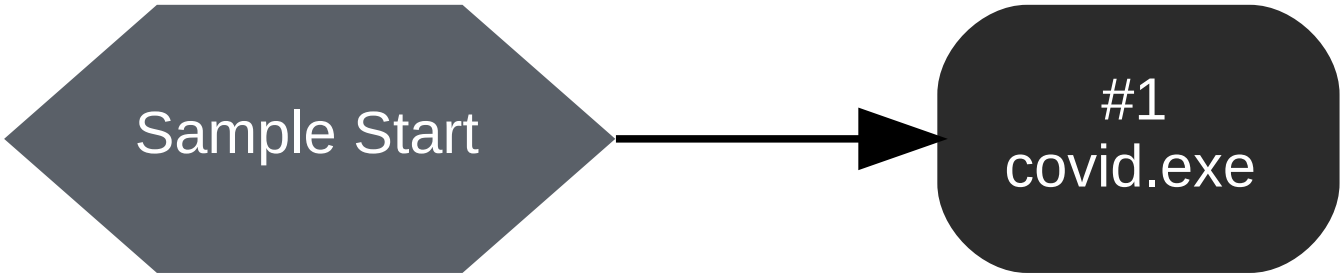
-

HTTP Requests

-

BEHAVIOR

Process Graph



Process #1: covid.exe

ID	1
Filename	c:\users\rdhj0cnfevzx\desktop\covid.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\covid.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 80513, Reason: Analysis Target
Unmonitor End Time	End Time: 325568, Reason: Terminated by Timeout
Monitor Duration	245.06s
Return Code	Unknown
PID	2724
Parent PID	2104
Bitness	64 Bit

Dropped Files (101)

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\0jVFU_fwepsE1hnB.pptx.ncovid	66.31 KB	1d5bc7c40a4f55a4d2422b2c3f211d5a056833f5beee26c7ee009baa1b18d3ae	✕
C:\Users\RDhJ0CNFevzX\Desktop\6an92ONxDM17h_.flv.ncovid	45.77 KB	ac7337c5719ecf76409a081df2ee419a45438c372c1492fbeaa198f4a8662922	✕
C:\Users\RDhJ0CNFevzX\Desktop\88GtSFKzH73_vJ.avi.ncovid	60.36 KB	6b2c48f43e178861dea71fb50c98721ef6bd7ef1317b7f98c4ed1963488899f7	✕
C:\Users\RDhJ0CNFevzX\Desktop\ADwpnfaKGM4F2saUkB.jpg.ncovid	31.69 KB	0e8aa69452a5d12d5e9b581714a69cb45524237613ff854fd577f23219140356	✕
C:\Users\RDhJ0CNFevzX\Desktop\aL5rm1Z_3UQgZuI.wav.ncovid	90.09 KB	89e2febc121bade7d5d7ce2d2b137ec7cb75bba7dfb4d13a5b2a37253c944bde	✕
C:\Users\RDhJ0CNFevzX\Desktop\AOrbZA5hkn0z42FZmF.jpg.ncovid	39.75 KB	4b6daa2028d3232e7a94f88f032cfc84e399c11f4e37653074aecb4332e0474e	✕
C:\Users\RDhJ0CNFevzX\Desktop\bicJkMmQ4B.ppt.ncovid	56.36 KB	7dc967042a448c5d49d303f1f337d2c6eec70f80a2dcf0b7bf423b6ab551ee45	✕
C:\Users\RDhJ0CNFevzX\Desktop\covid.exe.ncovid	32 bytes	67a68c737e382605c2ea4d9084b2ebb260b0727910eeaf02f0ed7be04b194a15	✕
C:\Users\RDhJ0CNFevzX\Pictures\-TZ5rzCIOrbdbR.png.ncovid	17.92 KB	05d73ecfcf6334fb43ab73d434997a0f93a4ad98e93ea02b18f24cdbde8b53db	✕
C:\Users\RDhJ0CNFevzX\Pictures\35-jfpA-mtUPvs5gV4mr.jpg.ncovid	11.45 KB	15a457e5b30c458e76cfda3fb9e8413b99e72f18a1d33168edb9d36bb1c63de1	✕
C:\Users\RDhJ0CNFevzX\Pictures\4qcvOht-riX9J3ZGd2AN.jpg.ncovid	32.77 KB	3d1e17c1417a718530a34c49e905a58667dd7961eb100dadc55a36719b36047e	✕
C:\Users\RDhJ0CNFevzX\Pictures\5eGY_O6oAQYCeYF.bmp.ncovid	89.95 KB	d81983f2a0575edf85f57b1eae2b66f1a6ea9b2425f7668cab600c037399e072	✕
C:\Users\RDhJ0CNFevzX\Pictures\7IGp2H4UWA.png.ncovid	14.06 KB	17c1e1732a9b92781f84ec156dbe7933e5eca21c80da2b5f2b0eb2922d9c4039	✕
C:\Users\RDhJ0CNFevzX\Pictures\8_L0.jpg.ncovid	24.48 KB	f8f79628d9036f44c6c5a684619141c0f682df4225e1351c2a9a6d6614e4c052	✕
C:\Users\RDhJ0CNFevzX\Pictures\aEzzAV.png.ncovid	53.11 KB	ee4c8f6d90d3ca99970a68c72404165bef6515125ab6922d2a3896375430ada1	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Pictures\CfMroH.bmp.ncovid	73.56 KB	7410d10d786a8f4e2ddeeebf0419478dbd0e55a21091c2bc4d069c5438fefeb9	✕
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini.ncovid	544 bytes	d3cfeaf9f792c911f029f7c01e70f4c44ec05e7744302e6de7a22b4299942b55	✕
C:\Users\RDhJ0CNFevzX\Pictures\l7J71mzGsYDYCBoUz.gif.ncovid	49.61 KB	45f0e201e68e686092e1dec756d37e8e636fd0c04652c08d8cfa0e314bc5f4cc	✕
C:\Users\RDhJ0CNFevzX\Pictures\leiqp5qQg.gif.ncovid	47.11 KB	a95c9cba41090b77c55ef5d905fc5d39222bf950f75820c45f17ebaa8d7df5e1	✕
C:\Users\RDhJ0CNFevzX\Pictures\iotg5jb-wcu3hO-.gif.ncovid	61.91 KB	b8258d075f777c98f4b4b6788e9756d051e871ad3dbdae6f917fafd15aad195b	✕
C:\Users\RDhJ0CNFevzX\Pictures\iTLuTdWLR4vAu.png.ncovid	21.56 KB	9326a4260ed7255af075448ca24f0a760aa33facc38dc25d76301df504999059	✕
C:\Users\RDhJ0CNFevzX\Pictures\lzk7bTMXw-1.png.ncovid	18.66 KB	5426a2d381f4924c8d4343318c353bced81825922b6ccd2285ec673695a1a8af	✕
C:\Users\RDhJ0CNFevzX\Pictures\ljeI.gif.ncovid	24.20 KB	e85a858af26948fafd5dc1713f572f53da86e3adca81f2e88abca2839acc906e	✕
C:\Users\RDhJ0CNFevzX\Pictures\ljhkhNwA93064H5W.gif.ncovid	56.92 KB	2e0ec880d35744db2068b98b623f6ec40092f5add6085a270e6c7e9aa05a55fa	✕
C:\Users\RDhJ0CNFevzX\Pictures\N0pnuWNn.jpg.ncovid	61.19 KB	7cd8a91ef7e57867d16dd8140ab152cc8133ecd997a9cde265dff4f06ecbc011	✕
C:\Users\RDhJ0CNFevzX\Pictures\Rne6z7RphV.jpg.ncovid	15.73 KB	830bd1388e6e173252fd1d3569ae6f3b247b2ea5f601a626829b82d6831843ac	✕
C:\Users\RDhJ0CNFevzX\Pictures\soB3UY84J.bmp.ncovid	88.33 KB	4881f0fae5599bd6406eb14694c97432316ec4fe0298f96b31adada67dc9a809	✕
C:\Users\RDhJ0CNFevzX\Pictures\V1CR3ZY6XRVc7QPNQ2G3.jpg.ncovid	73.73 KB	2b39d94cd5134e14a56930b1eb3275875cd4b158f54f4a9929d4a273ba6b287d	✕
C:\Users\RDhJ0CNFevzX\Pictures\WTv_2d9vuAAmrz9WS353.gif.ncovid	27.19 KB	1005f07d1366108966661ba00535de238ac04d0e1d34b147f9a0c00eefc46bef	✕
C:\Users\RDhJ0CNFevzX\Pictures\Y412g.jpg.ncovid	96.59 KB	044f5a00d7e78ae8b43442326f83c88e0ab58887a9d87f98009adc7f3721f2a1	✕
C:\Users\RDhJ0CNFevzX\Pictures\yQmXMOnbtf7h7HFf_BA.bmp.ncovid	55.73 KB	22a2e9a8a42a133d86b3c2e107b4ba1fd101d73cca3281c9eacd667af29227c3	✕
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini.ncovid	224 bytes	302604c29f40998b9323ef08bba76e9b3135d2c528e2cb2c0794a777ee9b2714	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\0zlvDRYF 8_DNOz.gif.ncovid	31.83 KB	bb576496f6f6aca18b008b22eb65fefa5fbfb3067e912e8fb75955183103269a	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\4Sf2rxZ-7lb.gif.ncovid	94.08 KB	6f5547f979b4e4b6135979fa5f782d7485eb3d83000a947db731684c9fcdf274	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\C_3uY_z.gif.ncovid	36.06 KB	a67fed3ec9c855edd65a211da47a53a3c68175ae098d6852d0c52eff644e00e8	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\dYaA_F5bFWX YC4AE.jpg.ncovid	100.02 KB	2b75ae53bf64ae96118e10ee85c58f86f2ead2cf34dab624cf63c5e3fe95628c	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\e8vhItq tNtLt5TtE.bmp.ncovid	69.34 KB	26127bcf1ec08286c768ddede79f9fdea9b2c60d60f4b886757c7e3b79c23c4d	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\ffD28EQZFv-o1x82.png.ncovid	78.73 KB	17795e9ba10b19441b9de656432eae8768e2311cbbdcd34c8348d9c4c17fef14	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\Fli1a9fCj4gSy.bmp.ncovid	31.78 KB	1afed97c9d9c8b4acbaa74faa875902ba753a96b2b1f1ac740778d1d97eef66e	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\fMtuTrlNKaoFFoK0.bmp.ncovid	82.42 KB	810b39dd346aeae75364771d86288446ab4c92703bd098cf1af7a59e39f850bf	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\lO0esS 0HHYKS.jpg.ncovid	59.70 KB	4b58ce5d1b33fac8f14740a572dc15bff87583bbe8603b42849613c9f352ff4e	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\OgmaIY.bmp.ncovid	83.59 KB	740d49ab4cd25ff7d1513ccd8109f5b29934da71834316455a69e97e1d7efe77	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\q2MHsGKaQ.png.ncovid	29.77 KB	6546184c1553936d7d8326a48ed7139bffc0be54cb58248df090e1a5c32dbeea	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\rJAWas8pDAbmp.png.ncovid	55.69 KB	901ba7a71351f1dba0152457b89bd6d7e12bf3ce1a22bb25cd86b18fec4bc2f1	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\Vnz6_hUjAg9jH3t30.bmp.ncovid	30.78 KB	42912d00ff85620d4425a52ffc24b5582861d1949d9c897bcb8a2ce3bacc2db2	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\vuyif.gif.ncovid	41.58 KB	25da1f81db0be5a35b6cfd3da56fc45aa8fcb7bd94d7fa3100d43d929e10381c	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\vwnzeoQ1jDssMQY.gif.ncovid	34.52 KB	65d2dbf2b3500557bbe51102ac59f484750f4aa7f20dfc7815c83d01848f69cc	✕
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\z-t5SKb go1vNMcR4.gif.ncovid	61.44 KB	840bb0b3173b34c170ec0f2521983e9bb1429eef322f925a8d39d737d274eead	✕
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini.ncovid	224 bytes	99bf178be4de39c567489e80b0d951f70f32131ab951049c078db1aae973d553	✕
C:\Users\RDhJ0CNFevzX\Documents\0Qov66TFlL71Vr.ods.ncovid	58.86 KB	a949ccba211a39c1279827b3221a6ed02b05df3b27307482c4eb2ab154eece14	✕
C:\Users\RDhJ0CNFevzX\Documents\568KyO2WPqAylkKb6J.xlsx.ncovid	92.12 KB	d061879db60d80e7643482b10edb6eab62df705c2f4c0154f9d91d410faa6145	✕
C:\Users\RDhJ0CNFevzX\Documents\70YjXp03lqF wav.docx.ncovid	38.28 KB	60be4eaa815bc4dc883004727b299bddab2dcf33ad23210866d43289262e2a72	✕
C:\Users\RDhJ0CNFevzX\Documents\76ll28SHkOO1S5RZA.pptx.ncovid	58.27 KB	8198eb6bd7d2ad1f01cf9535ab750886096667b2ab3084c98d34dc072a962c07	✕
C:\Users\RDhJ0CNFevzX\Documents\7p-yfll45o4qAG-.rtf.ncovid	79.11 KB	461f56ac9c7535d129c4ea29da01c2fb30a2a0eba5340c30b87c03debdc8e497	✕
C:\Users\RDhJ0CNFevzX\Documents\9duwNE_vpUogUDNE1V.xlsx.ncovid	55.47 KB	02ba0072fcd6d19a147b936d1d0e6fd372ad882114a685288c7c67c3d81bdac3	✕
C:\Users\RDhJ0CNFevzX\Documents\9Jh63.docx.ncovid	1.19 KB	8c48025169c65cff9664f4ca8bc2ed2799973741c473e22538682339352e9afd	✕
C:\Users\RDhJ0CNFevzX\Documents\9pqheIL3CaaI.docx.ncovid	65.47 KB	3808277cfd7502436b5889e5370b6626b7700604176134d2063b4561fdc252ed	✕
C:\Users\RDhJ0CNFevzX\Documents\axFXeggj.pdf.ncovid	30.61 KB	e896c78bfad108a092adf65a22d5e6b069868a9a39433fc490c3b5434db51126	✕
C:\Users\RDhJ0CNFevzX\Documents\bTgBDM_BLCIn 9g.pptx.ncovid	14.30 KB	72fa19436cdd456cdec119e4a2059bf6345cc8ee01a7abc61eba421881d604c1	✕
C:\Users\RDhJ0CNFevzX\Documents\c--oDETPCZEmFkX9R.docx.ncovid	46.73 KB	49e30f6dca8950b7c563df854b744c592ccb497212ac77e38b61a2b22f4071fb	✕
C:\Users\RDhJ0CNFevzX\Documents\c1uWbuECVbO7GtKW39T.pptx.ncovid	30.89 KB	966148b78ef9d84350fe597bd8df7475dcf3557d87a4d19822717ae20e376e8d	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\cDJMQ767y 9NDJF.csv.ncovid	27.02 KB	5ea0a0d182c7335b0d62341e818fd70b0044db11eaf9f93ae78d09e056869ae2	✕
C:\Users\RDhJ0CNFevzX\Documents\cWSN5bi9vhUj73qO.xlsx.ncovid	74.27 KB	553a8de0b5e0aa26c2405ecf3e33ab41ed46515dc5838a4a99cc40c36b6dcc1a	✕
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini.ncovid	448 bytes	557b8cf33837d5718aec9323d194b8fba8e6ab0eed9de900c2925db01224f522	✕
C:\Users\RDhJ0CNFevzX\Documents\ecwv2Je8.docx.ncovid	13.02 KB	3cbea3a0009af80a787513e3e095e6c2ee4c94a12fab0e78489411b5bbe53507	✕
C:\Users\RDhJ0CNFevzX\Documents\e3weHsPkukwCQ_rD1.pdf.ncovid	2.67 KB	1a44eb88ff99c7d57ccff784347eaf373971979e932d9ab75756a15348e3e4e4	✕
C:\Users\RDhJ0CNFevzX\Documents\EgsQo0UhXKVeTvl3SU4.xlsx.ncovid	40.53 KB	496dae4fa678dfc3a233821bfa31423e1cd8b5deb011a9b8cf08c9cb2a4ba5d9	✕
C:\Users\RDhJ0CNFevzX\Documents\Ez15cqKrqd8C42.xlsx.ncovid	46.41 KB	cd58f7cd7e4921b142b5851b1645f325202cf2b57d49148223703a15c5960c6b	✕
C:\Users\RDhJ0CNFevzX\Documents\flJgDYKYDnkfXH1E5C.csv.ncovid	37.67 KB	a272121b1e4b2cac90efa412bdbc1ab92efe904a2b7e97cbbc00bebbec1f2b58	✕
C:\Users\RDhJ0CNFevzX\Documents\FKV_Um7s1AtkG6SwRc.xlsx.ncovid	71.52 KB	ebb1af831f251ff0f17f4a7844c7b20b58176464f7ec581ecd971a803a3954e0	✕
C:\Users\RDhJ0CNFevzX\Documents\fvN5PmwQa.odt.ncovid	87.97 KB	f3fbba6c83c092a58269d97de235b0ca62895956c213638855aea17a149e9a1a	✕
C:\Users\RDhJ0CNFevzX\Documents\HjIAFUmQscCo 2L.ppt.ncovid	9.30 KB	263993ade5eb5cc3170a467517dcd2fd6c17d4369674b101a309ba1e128c1507	✕
C:\Users\RDhJ0CNFevzX\Documents\hJTYe7eOwos.pptx.ncovid	62.50 KB	4447619c565ca470aaa32688e9fec0107629313620e37db165a9063bb1569d72	✕
C:\Users\RDhJ0CNFevzX\Documents\JDRimLeWPyHLTdjUoJ.ppt.ncovid	35.69 KB	932e1f78ee2cf14af053f2c6a373fd03da290263bda84df4593169f03fd64ae1	✕
C:\Users\RDhJ0CNFevzX\Documents\Ji5Tbajt.xls.ncovid	39.23 KB	7cde66e43b64e4e261c56a1a2be735f7b345db3a17cda1f949be69e995b669d8	✕
C:\Users\RDhJ0CNFevzX\Documents\jXu_ngddt0WmrHz3gEIW.pptx.ncovid	33.30 KB	8bcce44c0c1a705c6c17ed05bc723d86bbdf9df3bb3b96c3b0fdf03e76ad7b30	✕
C:\Users\RDhJ0CNFevzX\Documents\KtLEO.rtf.ncovid	16.69 KB	4c55e313475a64256f0a379f757c8e9fadaf1c01210e2fd7c3a4c2861cfa1012	✕
C:\Users\RDhJ0CNFevzX\Documents\Lgwxj.doc.ncovid	15.44 KB	f5aacb8b81d42a2b70056fb13f778a88c4fcaa4a8cab9a2e2044a5bee11cac1c	✕
C:\Users\RDhJ0CNFevzX\Documents\Mho1kAIrYCh.docx.ncovid	39.72 KB	3aaa3fae7c16b234fa16f71a3e9f24eab8509fc9adfc66c4975a74aa6ff94f9e	✕
C:\Users\RDhJ0CNFevzX\Documents\n4XNFeLI8Mi4SE.docx.ncovid	16.44 KB	285d86b28a6c60b7bb140b03295ce43b932bff02df76d2f2fb51c64f27983ea3	✕
C:\Users\RDhJ0CNFevzX\Documents\nnMQFmGNl.xlsx.ncovid	10.50 KB	04c427a862db4a518d4e1e24e92c228e103f33ed128bb116d73ff9a5b2ad58cc	✕
C:\Users\RDhJ0CNFevzX\Documents\NOwnJ6AGI50mPI.pps.ncovid	72.70 KB	eeabd692efc5f057ccbbaa61bd69b407e9ffe1e43f615db5ad9865fb6a18a592	✕
C:\Users\RDhJ0CNFevzX\Documents\nzlHK8NwMZ86oh.docx.ncovid	21.34 KB	e0cad263db760301b1b0fcfd6c17373871a7c1a6767bfd11ec5eeb09eaf90fa2	✕
C:\Users\RDhJ0CNFevzX\Documents\OKqg.pptx.ncovid	91.91 KB	19c7d178e6accefb463e7811531515397326eeba4f7d0800c4be8f71aad60e33	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\pEpUMw_9Zcoad.csv.ncovid	93.80 KB	5c9e87822350ee7668b07b77068878bf9ea00e5cd999e0547381f755a3809b9a	✕
C:\Users\RDhJ0CNFevzX\Documents\Pxigi.rtf.ncovid	7.58 KB	8931315d733ce3e01eae64b3f08f6071d7acd406b114801dd6341a111f23e1a7	✕
C:\Users\RDhJ0CNFevzX\Documents\qes9g8fLDZ.odt.ncovid	71.44 KB	afb94795e9087f03355abe474e196e87d68f09ae08020625379b51e8f370a420	✕
C:\Users\RDhJ0CNFevzX\Documents\QOSULyfBxbm7V7 _F.odt.ncovid	10.47 KB	8527b3a49a1b370625cdea1e6008041df947532ff305e899f2aaca87d25f16bd	✕
C:\Users\RDhJ0CNFevzX\Documents\rHZ_lf-3p.docx.ncovid	17.12 KB	c94179853675aa5bbb5b1695f55bfb723ee7d2e08ef967eb7871c0c10f24abcd	✕
C:\Users\RDhJ0CNFevzX\Documents\sD-nmkQy yW.docx.ncovid	19.20 KB	d23cb59e165bb7b637b27d512cb54b9d088a6568dca0f812c68f7f24c3ca853e	✕
C:\Users\RDhJ0CNFevzX\Documents\UjcF5Fxqgs2AfHh9_uwc.doc.ncovid	95.94 KB	518ffd407eb71ce684185b54ee08de1a8f2e3d09717bc0704ed093e86d390f1a	✕
C:\Users\RDhJ0CNFevzX\Documents\uK_cajxxD7q1FH6.docx.ncovid	42.17 KB	209512b336bd4b134c871cf842b31681ef57cf5120e0c92653a1f214d3fc84fa	✕
C:\Users\RDhJ0CNFevzX\Documents\VgCrC4n9vd-j-Mu8i.pptx.ncovid	39.77 KB	3bf52c67cf7611c93c123d4dacc2b4f9f2e3aded8d1e20f3d6f4940751447ce4	✕
C:\Users\RDhJ0CNFevzX\Documents\VkzL2G-1q5yzVgCvx.docx.ncovid	48.16 KB	6fa1c3278e90dd796913ce4e60ecca74ae0bc32405762d70c561d0de48bdc0f7	✕
C:\Users\RDhJ0CNFevzX\Documents\XGb73bZ.odt.ncovid	59.45 KB	3dc94702d1c6f5c1243be645f28a644ccba0110187eda683503b32c9ce9e1fcb	✕
C:\Users\RDhJ0CNFevzX\Documents\XuhXtcsvkk4kAz8BQGV3.docx.ncovid	97.67 KB	45cdcd82029e2c147ed71ee1e5b05e0ec44b70126d7780f4d8cb78c6911af587	✕
C:\Users\RDhJ0CNFevzX\Documents\XzpwLTxYTuIlcq9.xlsx.ncovid	83.22 KB	574e6e6ebc4b01adb80db04239c1fce35571a07ff5bccb27d04bb792c0805ad2	✕
C:\Users\RDhJ0CNFevzX\Documents\yGgVErNaD-GX.odp.ncovid	83.23 KB	9a81b0ec017e93caf160d08e15741525f16b2196c505ecff9f3d9fe5238cfed7	✕
C:\Users\RDhJ0CNFevzX\Documents\Yngu.csv.ncovid	10.03 KB	812c0cdeaa37add1e85a1ba79f3cd75a7530f59c6df8e6ef8afdb51976f28f1e	✕
C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst.ncovid	265.05 KB	22988ff09d3c0f368d306d693e911eb157a250703af90c61299f0d8365b88535	✕
C:\Users\RDhJ0CNFevzX\Desktop___RECOVER__FILES__.ncovid.txt	5.37 KB	b8eb775c60d63d3e22dcdfd455a7d1d3531c1530978a15c7e05e3df946db030d	✕

Host Behavior

Type	Count
Module	81
System	57
Window	14
Registry	3
Keyboard	28
File	1191

ARTIFACTS

File

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
372fa440571b4ab1db28d8736c9014e11d8e27277c094062f2c444b6b97e8182	C:\Users\RDhJ0CNFevzX\Desktop\covid.exe	Sample File	16.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
1d5bc7c40a4f55a4d2422b2c3f211d5a056833f5beee26c7ee009baa1b18d3ae	C:\Users\RDhJ0CNFevzX\Desktop\0jVFU_fwepsE1hnB.pptx.ncovid	Dropped File	66.31 KB	application/octet-stream	Access, Write, Create	CLEAN
ac7337c5719ecf76409a081df2ee419a45438c372c1492fbeaa198f4a8662922	C:\Users\RDhJ0CNFevzX\Desktop\6an92ONxDM17h_.flv.ncovid	Dropped File	45.77 KB	application/octet-stream	Access, Write, Create	CLEAN
6b2c48f43e178861dea71fb50c98721ef6bd7ef1317b7f98c4ed1963488899f7	C:\Users\RDhJ0CNFevzX\Desktop\88GtSFKzH73_vJ.avi.ncovid	Dropped File	60.36 KB	application/octet-stream	Access, Write, Create	CLEAN
0e8aa69452a5d12d5e9b581714a69cb45524237613ff854fd577f23219140356	C:\Users\RDhJ0CNFevzX\Desktop\ADwpnfaKGM4F2saUkB.jpg.ncovid	Dropped File	31.69 KB	application/octet-stream	Access, Write, Create	CLEAN
89e2febc121bade7d5d7ce2d2b137ec7cb75bba7dfb4d13a5b2a37253c944bde	C:\Users\RDhJ0CNFevzX\Desktop\aL5rm1Z_3UQgZuI.wav.ncovid	Dropped File	90.09 KB	application/octet-stream	Access, Write, Create	CLEAN
4b6daa2028d3232e7a94f88f032cfc84e399c11f4e37653074aecb4332e0474e	C:\Users\RDhJ0CNFevzX\Desktop\AOrbZA5hkn0z42FZmF.jpg.ncovid	Dropped File	39.75 KB	application/octet-stream	Access, Write, Create	CLEAN
7dc967042a448c5d49d303f1f337d2c6eec70f80a2dcf0b7bf423b6ab551ee45	C:\Users\RDhJ0CNFevzX\Desktop\bicJkMmQ4B.ppt.ncovid	Dropped File	56.36 KB	application/octet-stream	Access, Write, Create	CLEAN
67a68c737e382605c2ea4d9084b2ebb260b0727910eeaf02f0ed7be04b194a15	C:\Users\RDhJ0CNFevzX\Desktop\covid.exe.ncovid	Dropped File	32 bytes	application/octet-stream	Access, Write, Create	CLEAN
05d73ecfcf6334fb43ab73d434997a0f93a4ad98e93ea02b18f24cdbde8b53db	C:\Users\RDhJ0CNFevzX\Pictures\-TZ5rzCIOrbdbR.png.ncovid	Dropped File	17.92 KB	application/octet-stream	Access, Write, Create	CLEAN
15a457e5b30c458e76cfda3fb9e8413b99e72f18a1d33168edb9d36bb1c63de1	C:\Users\RDhJ0CNFevzX\Pictures\35-jfpA-mtUPvs5gV4mr.jpg.ncovid	Dropped File	11.45 KB	application/octet-stream	Access, Write, Create	CLEAN
3d1e17c1417a718530a34c49e905a58667dd7961eb100dadc55a36719b36047e	C:\Users\RDhJ0CNFevzX\Pictures\4qcvOht-riX9J3ZGd2AN.jpg.ncovid	Dropped File	32.77 KB	application/octet-stream	Access, Write, Create	CLEAN
d81983f2a0575edf85f57b1eae2b66f1a6ea9b2425f7668cab600c037399e072	C:\Users\RDhJ0CNFevzX\Pictures\5eGY_O6oAQYCeYF.bmp.ncovid	Dropped File	89.95 KB	application/octet-stream	Access, Write, Create	CLEAN
17c1e1732a9b92781f84ec156dbe7933e5eca21c80da2b5f2b0eb2922d9c4039	C:\Users\RDhJ0CNFevzX\Pictures\7IGp2H4UWA.png.ncovid	Dropped File	14.06 KB	application/octet-stream	Access, Write, Create	CLEAN
f8f79628d9036f44c6c5a684619141c0f682df4225e1351c2a9a6d6614e4c052	C:\Users\RDhJ0CNFevzX\Pictures\8_L0.jpg.ncovid	Dropped File	24.48 KB	application/octet-stream	Access, Write, Create	CLEAN
ee4c8f6d90d3ca99970a68c72404165bef6515125ab6922d2a3896375430ada1	C:\Users\RDhJ0CNFevzX\Pictures\aEzzAV.png.ncovid	Dropped File	53.11 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
7410d10d786a8f4e2ddeebf0419478dbd0e55a21091c2bc4d069c5438fefeb9	C:\Users\RDhJ0CNFevzX\Pictures\CfMroH.bmp.ncovid	Dropped File	73.56 KB	application/octet-stream	Access, Write, Create	CLEAN
d3cfeaf9f792c911f029f7c01e70f4c44ec05e7744302e6de7a22b4299942b55	C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini.ncovid	Dropped File	544 bytes	application/octet-stream	Access, Write, Create	CLEAN
45f0e201e68e686092e1dec756d37e8e636fd0c04652c08d8cfa0e314bc5f4cc	C:\Users\RDhJ0CNFevzX\Pictures\l7J71mzGsYDYCBoUz.gif.ncovid	Dropped File	49.61 KB	application/octet-stream	Access, Write, Create	CLEAN
a95c9cba41090b77c55ef5d905fc5d39222bf950f75820c45f17ebaa8d7df5e1	C:\Users\RDhJ0CNFevzX\Pictures\leiqp5qQg.gif.ncovid	Dropped File	47.11 KB	application/octet-stream	Access, Write, Create	CLEAN
b8258d075f777c98f4b4b6788e9756d051e871ad3dbdae6f917fafd15aad195b	C:\Users\RDhJ0CNFevzX\Pictures\iotg5jb-wcu3hO-.gif.ncovid	Dropped File	61.91 KB	application/octet-stream	Access, Write, Create	CLEAN
9326a4260ed7255af075448ca24f0a760aa33facc38dc25d76301df5049990 59	C:\Users\RDhJ0CNFevzX\Pictures\iTLuTdWLR4vAu.png.ncovid	Dropped File	21.56 KB	application/octet-stream	Access, Write, Create	CLEAN
5426a2d381f4924c8d4343318c353bced81825922b6ccd2285ec673695a1a8af	C:\Users\RDhJ0CNFevzX\Pictures\lzk7bTMXw-1.png.ncovid	Dropped File	18.66 KB	application/x-dosexec	Access, Write, Create	CLEAN
e85a858af26948fafd5dc1713f572f53da86e3adca81f2e88abca2839acc906e	C:\Users\RDhJ0CNFevzX\Pictures\ljeI.gif.ncovid	Dropped File	24.20 KB	application/octet-stream	Access, Write, Create	CLEAN
2e0ec880d35744db2068b98b623f6ec40092f5add6085a270e6c7e9aa05a55fa	C:\Users\RDhJ0CNFevzX\Pictures\ljhkhNwA93064H5W.gif.ncovid	Dropped File	56.92 KB	application/octet-stream	Access, Write, Create	CLEAN
7cd8a91ef7e57867d16dd8140ab152cc8133ecd997a9cde265dff4f06ecbc011	C:\Users\RDhJ0CNFevzX\Pictures\N0pnuWNn.jpg.ncovid	Dropped File	61.19 KB	application/octet-stream	Access, Write, Create	CLEAN
830bd1388e6e173252fd1d3569ae6f3b247b2ea5f601a626829b82d6831843ac	C:\Users\RDhJ0CNFevzX\Pictures\Rne6z7RphV.jpg.ncovid	Dropped File	15.73 KB	application/octet-stream	Access, Write, Create	CLEAN
4881f0fae5599bd6406eb14694c97432316ec4fe0298f96b31adada67dc9a809	C:\Users\RDhJ0CNFevzX\Pictures\soB3UY84J.bmp.ncovid	Dropped File	88.33 KB	application/octet-stream	Access, Write, Create	CLEAN
2b39d94cd5134e14a56930b1eb3275875cd4b158f54f4a9929d4a273ba6b287d	C:\Users\RDhJ0CNFevzX\Pictures\V1CR3ZY6XRVc7QPNQ2G3.jpg.ncovid	Dropped File	73.73 KB	application/octet-stream	Access, Write, Create	CLEAN
1005f07d1366108966661ba00535de238ac04d0e1d34b147f9a0c00eefc46bef	C:\Users\RDhJ0CNFevzX\Pictures\WTv_2d9vuAAmrz9WS353.gif.ncovid	Dropped File	27.19 KB	application/octet-stream	Access, Write, Create	CLEAN
044f5a00d7e78ae8b43442326f83c88e0ab58887a9d87f98009adc7f3721f2a1	C:\Users\RDhJ0CNFevzX\Pictures\Y412g.jpg.ncovid	Dropped File	96.59 KB	application/octet-stream	Access, Write, Create	CLEAN
22a2e9a8a42a133d86b3c2e107b4ba1fd101d73cca3281c9eacd667af29227c3	C:\Users\RDhJ0CNFevzX\Pictures\yQmXMOnbtf7h7HFf_BA.bmp.ncovid	Dropped File	55.73 KB	application/octet-stream	Access, Write, Create	CLEAN
302604c29f40998b9323ef08bba76e9b3135d2c528e2cb2c0794a777ee9b2714	C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini.ncovid	Dropped File	224 bytes	application/octet-stream	Access, Write, Create	CLEAN
bb576496f6f6aca18b008b22eb65fefa5fbfb3067e912e8fb75955183103269a	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\0zlvDRYF8_DNOz.gif.ncovid	Dropped File	31.83 KB	application/x-dosexec	Access, Write, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
6f5547f979b4e4b6135979fa5f782d7485eb3d83000a947db731684c9fcdf274	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\4Sf2rxZ-7lb.gif.ncovid	Dropped File	94.08 KB	application/octet-stream	Access, Write, Create	CLEAN
a67fed3ec9c855edd65a211da47a53a3c68175ae098d6852d0c52eff644e00e8	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\C_3uY_z.gif.ncovid	Dropped File	36.06 KB	application/octet-stream	Access, Write, Create	CLEAN
2b75ae53bf64ae96118e10ee85c58f86f2ead2cf34dab624cf63c5e3fe95628c	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\dYaA_F5bFWXYC4AE.jpg.ncovid	Dropped File	100.02 KB	application/octet-stream	Access, Write, Create	CLEAN
26127bcf1ec08286c768ddede79f9fdea9b2c60d60f4b886757c7e3b79c23c4d	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\e8vhItqtNtLt5TtE.bmp.ncovid	Dropped File	69.34 KB	application/octet-stream	Access, Write, Create	CLEAN
17795e9ba10b19441b9de656432eae8768e2311cbbdcd34c8348d9c4c17fef14	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\ffD28EQZFv-o1x82.png.ncovid	Dropped File	78.73 KB	application/octet-stream	Access, Write, Create	CLEAN
1afed97c9d9c8b4acbaa74faa875902ba753a96b2b1f1ac740778d1d97eef66e	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\Fli1a9fCj4gSy.bmp.ncovid	Dropped File	31.78 KB	application/octet-stream	Access, Write, Create	CLEAN
810b39dd346aeae75364771d86288446ab4c92703bd098cf1af7a59e39f850bf	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\fMtuTrlNKaoFFoK0.bmp.ncovid	Dropped File	82.42 KB	application/octet-stream	Access, Write, Create	CLEAN
4b58ce5d1b33fac8f14740a572dc15bff87583bbe8603b42849613c9f352ff4e	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\lO0esS0HHYKS.jpg.ncovid	Dropped File	59.70 KB	application/octet-stream	Access, Write, Create	CLEAN
740d49ab4cd25ff7d1513ccd8109f5b29934da71834316455a69e97e1d7efe77	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\OgmalY.bmp.ncovid	Dropped File	83.59 KB	application/octet-stream	Access, Write, Create	CLEAN
6546184c1553936d7d8326a48ed7139bffc0be54cb58248df090e1a5c32dbeea	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\q2MHsGKaQ.png.ncovid	Dropped File	29.77 KB	application/octet-stream	Access, Write, Create	CLEAN
901ba7a71351f1dba0152457b89bd6d7e12bf3ce1a22bb25cd86b18fec4bc2f1	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\rJAWas8pDAbmp.png.ncovid	Dropped File	55.69 KB	application/octet-stream	Access, Write, Create	CLEAN
42912d00ff85620d4425a52ffc24b5582861d1949d9c897bcb8a2ce3bacc2db2	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\Vnz6_hUjAg9jH3t30.bmp.ncovid	Dropped File	30.78 KB	application/octet-stream	Access, Write, Create	CLEAN
25da1f81db0be5a35b6cfd3da56fc45aa8fcb7bd94d7fa3100d43d929e10381c	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\vuyif.gif.ncovid	Dropped File	41.58 KB	application/octet-stream	Access, Write, Create	CLEAN
65d2dbf2b3500557bbe51102ac59f484750f4aa7f20dfc7815c83d01848f69cc	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\vwnzeoQ1jDssMQY.gif.ncovid	Dropped File	34.52 KB	application/octet-stream	Access, Write, Create	CLEAN
840bb0b3173b34c170ec0f2521983e9bb1429eef322f925a8d39d737d274eead	C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\z-t5SKbgo1vNMcR4.gif.ncovid	Dropped File	61.44 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
99bf178be4de39c567489e80b0d951f70f32131ab951049c078db1aae973d553	C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini.ncovid	Dropped File	224 bytes	application/octet-stream	Access, Write, Create	CLEAN
a949ccba211a39c1279827b3221a6ed02b05df3b27307482c4eb2ab154eece14	C:\Users\RDhJ0CNFevzX\Documents\0Qov66TFlL71Vr.ods.ncovid	Dropped File	58.86 KB	application/octet-stream	Access, Write, Create	CLEAN
d061879db60d80e7643482b10edb6eab62df705c2f4c0154f9d91d410faa6145	C:\Users\RDhJ0CNFevzX\Documents\568KyO2WPqAyIkKb6J.xlsx.ncovid	Dropped File	92.12 KB	application/octet-stream	Access, Write, Create	CLEAN
60be4eaa815bc4dc883004727b299bddab2dcf33ad23210866d43289262e2a72	C:\Users\RDhJ0CNFevzX\Documents\70YjXp03IqF wav.docx.ncovid	Dropped File	38.28 KB	application/octet-stream	Access, Write, Create	CLEAN
8198eb6bd7d2ad1f01cf9535ab750886096667b2ab3084c98d34dc072a962c07	C:\Users\RDhJ0CNFevzX\Documents\76Il28SHkOO1S5RZA.pptx.ncovid	Dropped File	58.27 KB	application/octet-stream	Access, Write, Create	CLEAN
461f56ac9c7535d129c4ea29da01c2fb30a2a0eba5340c30b87c03debdc8e497	C:\Users\RDhJ0CNFevzX\Documents\7p-yfll45o4qAG-.rtf.ncovid	Dropped File	79.11 KB	application/octet-stream	Access, Write, Create	CLEAN
02ba0072fcd6d19a147b936d1d0e6fd372ad882114a685288c7c67c3d81bdac3	C:\Users\RDhJ0CNFevzX\Documents\9duwNE_vpUogUDNE1V.xlsx.ncovid	Dropped File	55.47 KB	application/octet-stream	Access, Write, Create	CLEAN
8c48025169c65cff9664f4ca8bc2ed2799973741c473e22538682339352e9afd	C:\Users\RDhJ0CNFevzX\Documents\9Jh63.docx.ncovid	Dropped File	1.19 KB	application/octet-stream	Access, Write, Create	CLEAN
3808277cfd7502436b5889e5370b6626b7700604176134d2063b4561fdc252ed	C:\Users\RDhJ0CNFevzX\Documents\9pqheIL3CaaI.docx.ncovid	Dropped File	65.47 KB	application/octet-stream	Access, Write, Create	CLEAN
e896c78bfad108a092adf65a22d5e6b069868a9a39433fc490c3b5434db51126	C:\Users\RDhJ0CNFevzX\Documents\axFXeggj.pdf.ncovid	Dropped File	30.61 KB	application/octet-stream	Access, Write, Create	CLEAN
72fa19436cdd456cdec119e4a2059bf6345cc8ee01a7abc61eba421881d604c1	C:\Users\RDhJ0CNFevzX\Documents\bTgBDM_BLCIn 9g.pptx.ncovid	Dropped File	14.30 KB	application/octet-stream	Access, Write, Create	CLEAN
49e30f6dca8950b7c563df854b744c592ccb497212ac77e38b61a2b22f4071fb	C:\Users\RDhJ0CNFevzX\Documents\c--oDETPCZEmFkX9R.docx.ncovid	Dropped File	46.73 KB	application/octet-stream	Access, Write, Create	CLEAN
966148b78ef9d84350fe597bd8df7475dcf3557d87a4d19822717ae20e376e8d	C:\Users\RDhJ0CNFevzX\Documents\c1uWbuECVbO7GtKW39T.pptx.ncovid	Dropped File	30.89 KB	application/octet-stream	Access, Write, Create	CLEAN
5ea0a0d182c7335b0d62341e818fd70b0044db11eaf9f93ae78d09e056869ae2	C:\Users\RDhJ0CNFevzX\Documents\cDJMQ767y9NDJF.csv.ncovid	Dropped File	27.02 KB	application/octet-stream	Access, Write, Create	CLEAN
553a8de0b5e0aa26c2405ecf3e33ab41ed46515dc5838a4a99cc40c36b6dcc1a	C:\Users\RDhJ0CNFevzX\Documents\cWSN5bi9vhUj73qO.xlsx.ncovid	Dropped File	74.27 KB	application/octet-stream	Access, Write, Create	CLEAN
557b8cf33837d5718aec9323d194b8fba8e6ab0eed9de900c2925db01224f522	C:\Users\RDhJ0CNFevzX\Documents\desktop.ini.ncovid	Dropped File	448 bytes	application/octet-stream	Access, Write, Create	CLEAN
3cbea3a0009af80a787513e3e095e6c2ee4c94a12fab0e78489411b5bbe53507	C:\Users\RDhJ0CNFevzX\Documents\ecwv2Je8.docx.ncovid	Dropped File	13.02 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
1a44eb88ff99c7d57ccff784347eaf373971979e932d9ab75756a15348e3e4e4	C:\Users\RDhJ0CNFevzX\Documents\e3weHsPkukwCQ_rD1.pdf.ncovid	Dropped File	2.67 KB	application/octet-stream	Access, Write, Create	CLEAN
496dae4fa678dfc3a233821bfa31423e1cd8b5deb011a9b8cf08c9cb2a4ba5d9	C:\Users\RDhJ0CNFevzX\Documents\EgsQo0UhXKVeTvl3SU4.xlsx.ncovid	Dropped File	40.53 KB	application/octet-stream	Access, Write, Create	CLEAN
cd58f7cd7e4921b142b5851b1645f325202cf2b57d49148223703a15c5960c6b	C:\Users\RDhJ0CNFevzX\Documents\Ez15cqKrqd8C42.xlsx.ncovid	Dropped File	46.41 KB	application/octet-stream	Access, Write, Create	CLEAN
a272121b1e4b2cac90efa412bdbc1ab92efe904a2b7e97cbbc00bebbec1f2b58	C:\Users\RDhJ0CNFevzX\Documents\flJgDYKYDnkfXH1E5C.csv.ncovid	Dropped File	37.67 KB	application/octet-stream	Access, Write, Create	CLEAN
ebb1af831f251ff0f17f4a7844c7b20b58176464f7ec581ecd971a803a3954e0	C:\Users\RDhJ0CNFevzX\Documents\FKV_Um7s1AtkG6SwRc.xlsx.ncovid	Dropped File	71.52 KB	application/octet-stream	Access, Write, Create	CLEAN
f3fbba6c83c092a582699d97de235b0ca62895956c213638855aea17a149e9a1a	C:\Users\RDhJ0CNFevzX\Documents\fvN5PmwQa.odt.ncovid	Dropped File	87.97 KB	application/octet-stream	Access, Write, Create	CLEAN
263993ade5eb5cc3170a467517dcd2fd6c17d4369674b101a309ba1e128c1507	C:\Users\RDhJ0CNFevzX\Documents\HjIAFUmQscCo 2L.ppt.ncovid	Dropped File	9.30 KB	application/octet-stream	Access, Write, Create	CLEAN
4447619c565ca470aaa32688e9fec0107629313620e37db165a9063bb1569d72	C:\Users\RDhJ0CNFevzX\Documents\hJTYe7eOwos.pptx.ncovid	Dropped File	62.50 KB	application/octet-stream	Access, Write, Create	CLEAN
932e1f78ee2cf14af053f2c6a373fd03da290263bda84df4593169f03fd64ae1	C:\Users\RDhJ0CNFevzX\Documents\JDRimLeWPyHLTdjUoJ.ppt.ncovid	Dropped File	35.69 KB	application/octet-stream	Access, Write, Create	CLEAN
7cde66e43b64e4e261c56a1a2be735f7b345db3a17cda1f949be69e995b669d8	C:\Users\RDhJ0CNFevzX\Documents\Ji5Tbajt.xls.ncovid	Dropped File	39.23 KB	application/octet-stream	Access, Write, Create	CLEAN
8bcce44c0c1a705c6c17ed05bc723d86bbdf9df3bb3b96c3b0fdf03e76ad7b30	C:\Users\RDhJ0CNFevzX\Documents\jXu_ngddt0WmrHz3gElW.pptx.ncovid	Dropped File	33.30 KB	application/octet-stream	Access, Write, Create	CLEAN
4c55e313475a64256f0a379f757c8e9fadaf1c01210e2fd7c3a4c2861cfa1012	C:\Users\RDhJ0CNFevzX\Documents\KtLEO.rtf.ncovid	Dropped File	16.69 KB	application/octet-stream	Access, Write, Create	CLEAN
f5aacb8b81d42a2b70056fb13f778a88c4fcaa4a8cab9a2e2044a5bee11cac1c	C:\Users\RDhJ0CNFevzX\Documents\Lgwxj.doc.ncovid	Dropped File	15.44 KB	application/octet-stream	Access, Write, Create	CLEAN
3aaa3fae7c16b234fa16f71a3e9f24eab8509fc9adfc66c4975a74aa6ff94f9e	C:\Users\RDhJ0CNFevzX\Documents\Mho1kAlrYCh.docx.ncovid	Dropped File	39.72 KB	application/octet-stream	Access, Write, Create	CLEAN
285d86b28a6c60b7bb140b03295ce43b932bff02df76d2f2fb51c64f27983ea3	C:\Users\RDhJ0CNFevzX\Documents\n4XNFeLI8Mi4SE.docx.ncovid	Dropped File	16.44 KB	application/octet-stream	Access, Write, Create	CLEAN
04c427a862db4a518d4e1e24e92c228e103f33ed128bb116d73ff9a5b2ad58cc	C:\Users\RDhJ0CNFevzX\Documents\nnMQFmGNl.xlsx.ncovid	Dropped File	10.50 KB	application/octet-stream	Access, Write, Create	CLEAN
eeabd692efc5f057ccbbaa61bd69b407e9ffe1e43f615db5ad9865fb6a18a592	C:\Users\RDhJ0CNFevzX\Documents\NOwnJ6AGI50mPI.pps.ncovid	Dropped File	72.70 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
e0cad263db760301b1b0fcfd6c17373871a7c1a6767bfd11ec5eeb09eaf90fa2	C:\Users\RDhJ0CNFevzX\Documents\nzlHK8NwMZ86oh.docx.ncovid	Dropped File	21.34 KB	application/octet-stream	Access, Write, Create	CLEAN
19c7d178e6accefb463e7811531515397326eeba4f7d0800c4be8f71aad60e33	C:\Users\RDhJ0CNFevzX\Documents\OKqg.pptx.ncovid	Dropped File	91.91 KB	application/octet-stream	Access, Write, Create	CLEAN
5c9e87822350ee7668b07b77068878bf9ea00e5cd999e0547381f755a3809b9a	C:\Users\RDhJ0CNFevzX\Documents\pEpUMw_9Zcoad.csv.ncovid	Dropped File	93.80 KB	application/octet-stream	Access, Write, Create	CLEAN
8931315d733ce3e01eae64b3f08f6071d7acd406b114801dd6341a111f23e1a7	C:\Users\RDhJ0CNFevzX\Documents\Pxigi.rtf.ncovid	Dropped File	7.58 KB	application/octet-stream	Access, Write, Create	CLEAN
afb94795e9087f03355abe474e196e87d68f09ae08020625379b51e8f370a420	C:\Users\RDhJ0CNFevzX\Documents\qes9g8fLDZ.odt.ncovid	Dropped File	71.44 KB	application/octet-stream	Access, Write, Create	CLEAN
8527b3a49a1b370625cdea1e6008041df947532ff305e899f2aaca87d25f16bd	C:\Users\RDhJ0CNFevzX\Documents\QOSULyfBxbm7V7 _F.odt.ncovid	Dropped File	10.47 KB	application/octet-stream	Access, Write, Create	CLEAN
c94179853675aa5bbb5b1695f55bfb723ee7d2e08ef967eb7871c0c10f24abcd	C:\Users\RDhJ0CNFevzX\Documents\rHZ_lf-3p.docx.ncovid	Dropped File	17.12 KB	application/octet-stream	Access, Write, Create	CLEAN
d23cb59e165bb7b637b27d512cb54b9d088a6568dca0f812c68f7f24c3ca853e	C:\Users\RDhJ0CNFevzX\Documents\sD-nmkQyyW.docx.ncovid	Dropped File	19.20 KB	application/octet-stream	Access, Write, Create	CLEAN
518ffd407eb71ce684185b54ee08de1a8f2e3d09717bc0704ed093e86d390f1a	C:\Users\RDhJ0CNFevzX\Documents\UjcF5Fxqgs2AfHh9_uwc.doc.ncovid	Dropped File	95.94 KB	application/octet-stream	Access, Write, Create	CLEAN
209512b336bd4b134c871cf842b31681ef57cf5120e0c92653a1f214d3fc84fa	C:\Users\RDhJ0CNFevzX\Documents\uK_cajxxD7q1FH6.docx.ncovid	Dropped File	42.17 KB	application/octet-stream	Access, Write, Create	CLEAN
3bf52c67cf7611c93c123d4dacc2b4f9f2e3aded8d1e20f3d6f4940751447ce4	C:\Users\RDhJ0CNFevzX\Documents\VgCrC4n9vd-j-Mu8i.pptx.ncovid	Dropped File	39.77 KB	application/octet-stream	Access, Write, Create	CLEAN
6fa1c3278e90dd796913ce4e60ecca74ae0bc32405762d70c561d0de48bdc0f7	C:\Users\RDhJ0CNFevzX\Documents\VkzL2G-1q5yzVgCvx.docx.ncovid	Dropped File	48.16 KB	application/octet-stream	Access, Write, Create	CLEAN
3dc94702d1c6f5c1243be645f28a644ccba0110187eda683503b32c9ce9e1fcb	C:\Users\RDhJ0CNFevzX\Documents\XGb73bZ.odt.ncovid	Dropped File	59.45 KB	application/octet-stream	Access, Write, Create	CLEAN
45cdcd82029e2c147ed71ee1e5b05e0ec44b70126d7780f4d8cb78c6911af587	C:\Users\RDhJ0CNFevzX\Documents\XuhXtcsvkk4kAz8BQGV3.docx.ncovid	Dropped File	97.67 KB	application/octet-stream	Access, Write, Create	CLEAN
574e6e6ebc4b01adb80db04239c1fce35571a07ff5bccb27d04bb792c0805ad2	C:\Users\RDhJ0CNFevzX\Documents\XzpwLTxYTuIIcq9.xlsx.ncovid	Dropped File	83.22 KB	application/octet-stream	Access, Write, Create	CLEAN
9a81b0ec017e93caf160d08e15741525f16b2196c505ecff9f3d9fe5238cfed7	C:\Users\RDhJ0CNFevzX\Documents\yGgVErNaD-GX.odp.ncovid	Dropped File	83.23 KB	application/octet-stream	Access, Write, Create	CLEAN
812c0cdeaa37add1e85a1ba79f3cd75a7530f59c6df8e6ef8afdb51976f28f1e	C:\Users\RDhJ0CNFevzX\Documents\Yngu.csv.ncovid	Dropped File	10.03 KB	application/octet-stream	Access, Write, Create	CLEAN
22988ff09d3c0f368d306d693e911eb157a250703af90c61299f0d8365b88535	C:\Users\RDhJ0CNFevzX\Documents\Outlook Files\achoo@gdllo.de.pst.ncovid	Dropped File	265.05 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
b8eb775c60d63d3e22dcdfd455a7d1d3531c1530978a15c7e05e3df946db030d	C:\Users\RDhJ0CNFevzX\Desktop___RECOVER__FILES__.ncovid.txt	Dropped File	5.37 KB	text/plain	Access, Write, Create	CLEAN

Filename

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\0jVFU_fwepsE1hnB.pptx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\0jVFU_fwepsE1hnB.pptx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\6an92ONxDM17h_.flv.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\6an92ONxDM17h_.flv	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\88GtSFKzH73_vJ.avi.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\88GtSFKzH73_vJ.avi	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ADwpnfaKGM4F2saUkB.jpg.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ADwpnfaKGM4F2saUkB.jpg	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\aL5rm1Z_3UQgZuI.wav.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\aL5rm1Z_3UQgZuI.wav	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\AOrbZA5hkn0z42FZmF.jpg.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\AOrbZA5hkn0z42FZmF.jpg	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\bicJkMmQ4B.ppt.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\bicJkMmQ4B.ppt	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\covid.exe.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\covid.exe	Sample File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\-TZ5rzCIOrbdbR.png.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\-TZ5rzCIOrbdbR.png	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\35-jfpA-mtUPvs5gV4mr.jpg.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\35-jfpA-mtUPvs5gV4mr.jpg	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\4qcvOht-riX9J3ZGd2AN.jpg.ncovid	Dropped File	Access, Write, Create	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\4qcvOht-riX9J3ZGd2AN.jpg	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\5eGY_O6oAQYCeYF.bmp.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\5eGY_O6oAQYCeYF.bmp	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\7IGp2H4UWA.png.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\7IGp2H4UWA.png	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\8_L0.jpg.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\8_L0.jpg	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\aEzzAV.png.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\aEzzAV.png	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\CfMroH.bmp.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\CfMroH.bmp	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\I7J71mzGsYDYCBoUz.gif.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\I7J71mzGsYDYCBoUz.gif	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\leiqp5qQg.gif.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\leiqp5qQg.gif	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\iotg5jb-wcu3hO-.gif.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\iotg5jb-wcu3hO-.gif	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\iTLuTdWLR4vAu.png.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\iTLuTdWLR4vAu.png	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\lzk7bTMXw-1.png.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\lzk7bTMXw-1.png	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ljeI.gif.ncovid	Dropped File	Access, Write, Create	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\ljeI.gif	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ljhkhNwA93064H5W.gif.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ljhkhNwA93064H5W.gif	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\N0pnuWNn.jpg.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\N0pnuWNn.jpg	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Rne6z7RphV.jpg.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Rne6z7RphV.jpg	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\soB3UY84J.bmp.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\soB3UY84J.bmp	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\V1CR3ZY6XRVc7QPNQ2G3.jpg.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\V1CR3ZY6XRVc7QPNQ2G3.jpg	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\WTv_2d9vuAAmrz9WS353.gif.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\WTv_2d9vuAAmrz9WS353.gif	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Y412g.jpg.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Y412g.jpg	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\yQmXMOnbtf7h7HFf_BA.bmp.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\yQmXMOnbtf7h7HFf_BA.bmp	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\0zlvDRYF 8_DNOz.gif.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\0zlvDRYF 8_DNOz.gif	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\4Sf2rxZ-7lb.gif.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\4Sf2rxZ-7lb.gif	Accessed File	Read, Access, Delete	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\C_3uY_z.gif.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\C_3uY_z.gif	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\dYaA_F5bFWX YC4AE.jpg.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\dYaA_F5bFWX YC4AE.jpg	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\e8vhItq tNtLt5TtE.bmp.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\e8vhItq tNtLt5TtE.bmp	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\ffD28EQZFv-o1x82.png.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\ffD28EQZFv-o1x82.png	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\Fli1a9fCj4gSy.bmp.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\Fli1a9fCj4gSy.bmp	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\fMtuTrlNKaoFFoK0.bmp.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\fMtuTrlNKaoFFoK0.bmp	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\lO0esS 0HHYKS.jpg.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\lO0esS 0HHYKS.jpg	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\OgmalY.bmp.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\OgmalY.bmp	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\q2MHsGKaQ.png.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\q2MHsGKaQ.png	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\rJAWas8pDAbmp.png.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\rJAWas8pDAbmp.png	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\Vnz6_hUjAg9jH3t30.bmp.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\Vnz6_hUjAg9jH3t30.bmp	Accessed File	Read, Access, Delete	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\vuyif.gif.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\vuyif.gif	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\vwnzeoQ1jDssMQY.gif.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\vwnzeoQ1jDssMQY.gif	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\z-t5SKb go1vNMcR4.gif.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\gQVD1CNgqQdWgWk\z-t5SKb go1vNMcR4.gif	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\0Qov66TFlL71Vr.ods.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\0Qov66TFlL71Vr.ods	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\568KyO2WPqAylkKb6J.xlsx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\568KyO2WPqAylkKb6J.xlsx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\70YjXp03IqF wav.docx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\70YjXp03IqF wav.docx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\76lI28SHkOO1S5RZA.pptx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\76lI28SHkOO1S5RZA.pptx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\7p-yfll45o4qAG-.rtf.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\7p-yfll45o4qAG-.rtf	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\9duwNE_vpUogUDNE1V.xlsx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\9duwNE_vpUogUDNE1V.xlsx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\9Jh63.docx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\9Jh63.docx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\9pqheIL3Caal.docx.ncovid	Dropped File	Access, Write, Create	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\9pqheIL3CaaI.docx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\axFXeggj.pdf.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\axFXeggj.pdf	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\bTgBDM_BLCIn 9g.pptx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\bTgBDM_BLCIn 9g.pptx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\c--oDETPCZEmFkX9R.docx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\c--oDETPCZEmFkX9R.docx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\c1uWbuECVbO7GtKW39T.pptx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\c1uWbuECVbO7GtKW39T.pptx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\cDJMQ767y 9NDJF.csv.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\cDJMQ767y 9NDJF.csv	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\cWSN5bi9vhUj73qO.xlsx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\cWSN5bi9vhUj73qO.xlsx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\ecwv2Je8.docx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\ecwv2Je8.docx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\e3weHsPkukwCQ_rD1.pdf.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\e3weHsPkukwCQ_rD1.pdf	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\EgsQo0UhXKVeTvl3SU4.xlsx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\EgsQo0UhXKVeTvl3SU4.xlsx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Ez15cqKrqd8C42.xlsx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Ez15cqKrqd8C42.xlsx	Accessed File	Read, Access, Delete	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\flJgDYKYDnkfXH1E5C.csv.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\flJgDYKYDnkfXH1E5C.csv	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\FKV_Um7s1AtkG6SwRc.xlsx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\FKV_Um7s1AtkG6SwRc.xlsx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\fvN5PmwQa.odt.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\fvN5PmwQa.odt	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\HjIAFUmQscCo 2L.ppt.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\HjIAFUmQscCo 2L.ppt	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\hJTYe7eOwos.pptx.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\hJTYe7eOwos.pptx	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\JDRimLeWPyHLTdjUoJ.ppt.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\JDRimLeWPyHLTdjUoJ.ppt	Accessed File	Read, Access, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Ji5Tbajt.xls.ncovid	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Ji5Tbajt.xls	Accessed File	Read, Access, Delete	CLEAN

Reduced dataset

URL

-

Domain

-

IP

-

Email

-

Email Address

-

Mutex

-

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	covid.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	covid.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	covid.exe	CLEAN

Process

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

YARA / AV

Antivirus (2)

File Type	Threat Name	Filename	Verdict
SAMPLE	Gen:Heur.Ransom.REntS.Gen.1	C:\Users\RDhJ0CNFevzX\Desktop\covid.exe	MALICIOUS
MEMORY_DUMP	Gen:Heur.Ransom.RTH.1	-	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	2021-03-23 09:59:16+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