MALICIOUS

Classifications: Ransomware, Wiper

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

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
Sample Name	**WindowsFormsApp1.exe**
ID	#361506
MD5	70117cfb0d652621da77c47c952fb81a
SHA1	3d841739fd18d02612851c10684631ddcdbc442c
SHA256	9e1609ab7f01b56a9476494d9b3bf5997380d466744b07ec5d9b20e416b10f08
File Size	1327.50 KB
Report Created	2021-04-10 02:39 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (7 rules, 11 matches)

Score	Category	Operation	Count	Classification
4/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) windowsformsapp1.exe modifies the content of multiple user files.			
4/5	User Data Modification	Deletes user files	1	Wiper
	• (Process #1) windowsformsapp1.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	1	-
	• Built-in AV detected the sample itself as "Gen:Heur.Ransom.REntS.Gen.1".			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• (Process #1) windowsformsapp1.exe is possibly trying to detect a VM via rdtsc.			
1/5	Hide Tracks	Changes folder appearance	5	-
	• (Process #1) windowsformsapp1.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\desktop". • (Process #1) windowsformsapp1.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures". • (Process #1) windowsformsapp1.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures\camera roll". • (Process #1) windowsformsapp1.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\pictures\saved pictures". • (Process #1) windowsformsapp1.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\documents".			
1/5	System Modification	Creates an unusually large number of files	1	-
	• (Process #1) windowsformsapp1.exe creates an above average number of files.			

Mitre ATT&CK Matrix

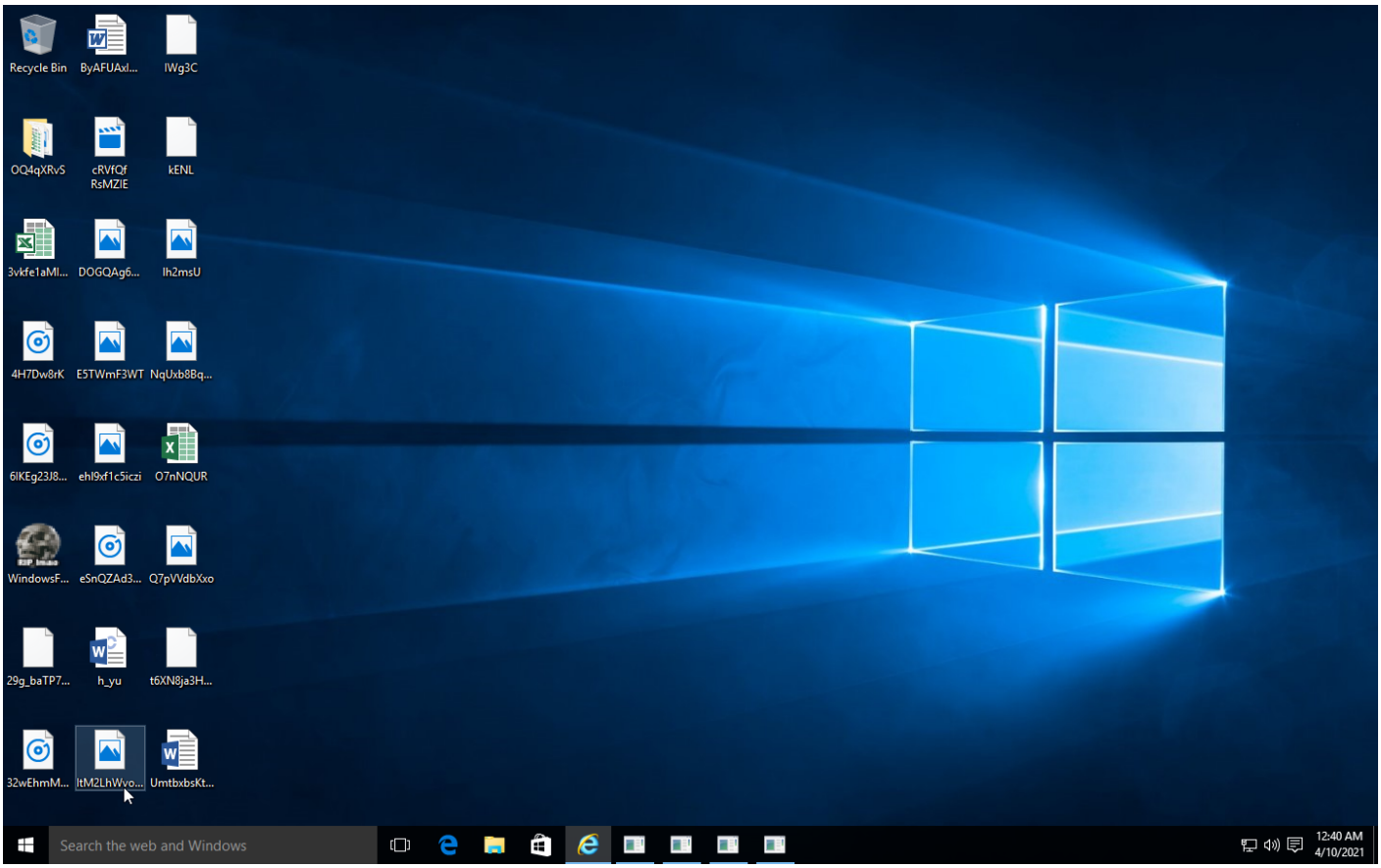
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
-	-	-	-	-	-	-	-	-	-	-	#T1486 Data Encrypted for Impact
-	-	-	-	-	-	-	-	-	-	-	#T1485 Data Destruction
-	-	-	-	#T1036 Masquerading	-	-	-	-	-	-	-
-	-	-	-	#T1497 Virtualization /Sandbox Evasion	-	#T1497 Virtualization /Sandbox Evasion	-	-	-	-	-
-	-	-	-	-	-	#T1124 System Time Discovery	-	-	-	-	-

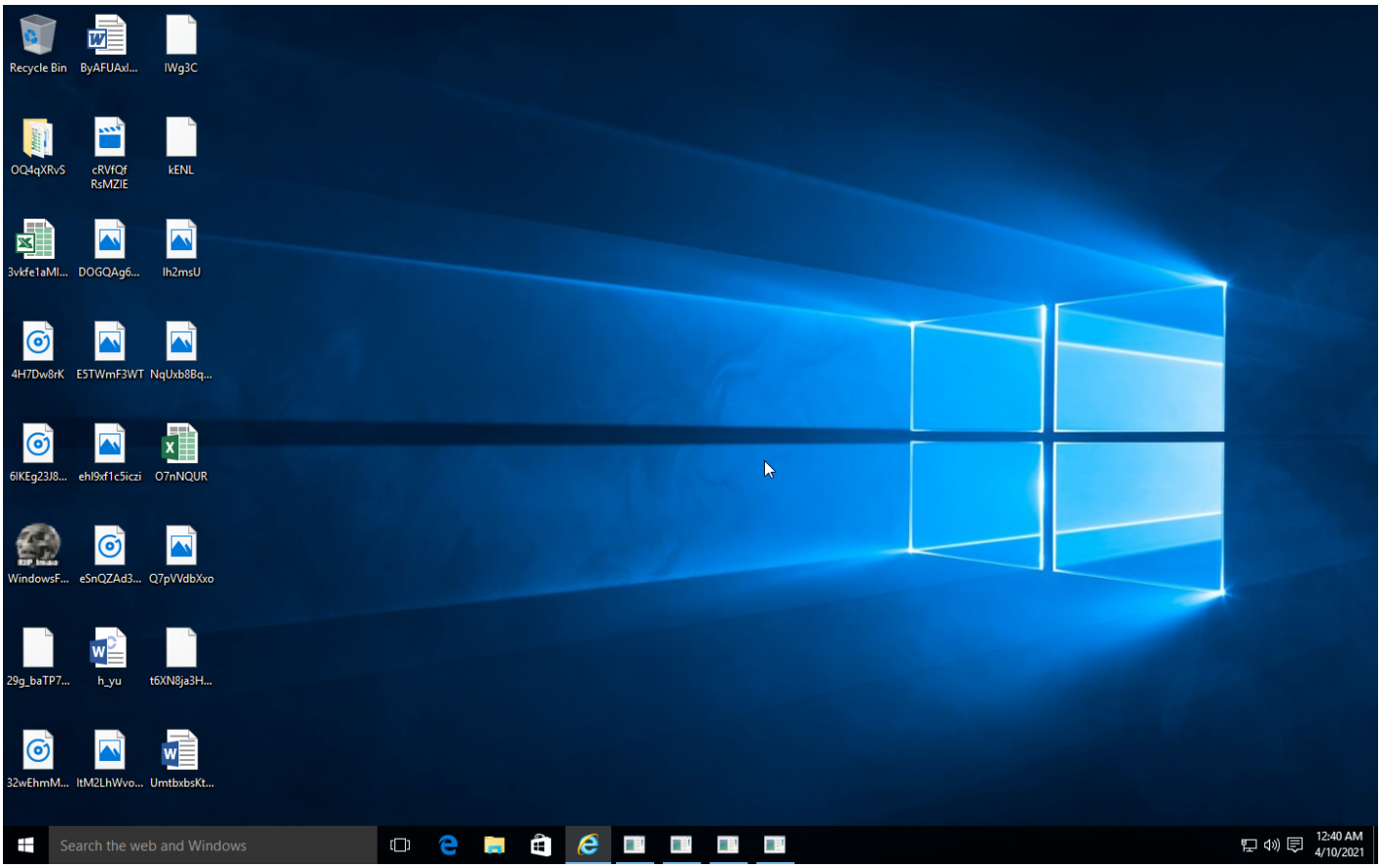
Sample Information

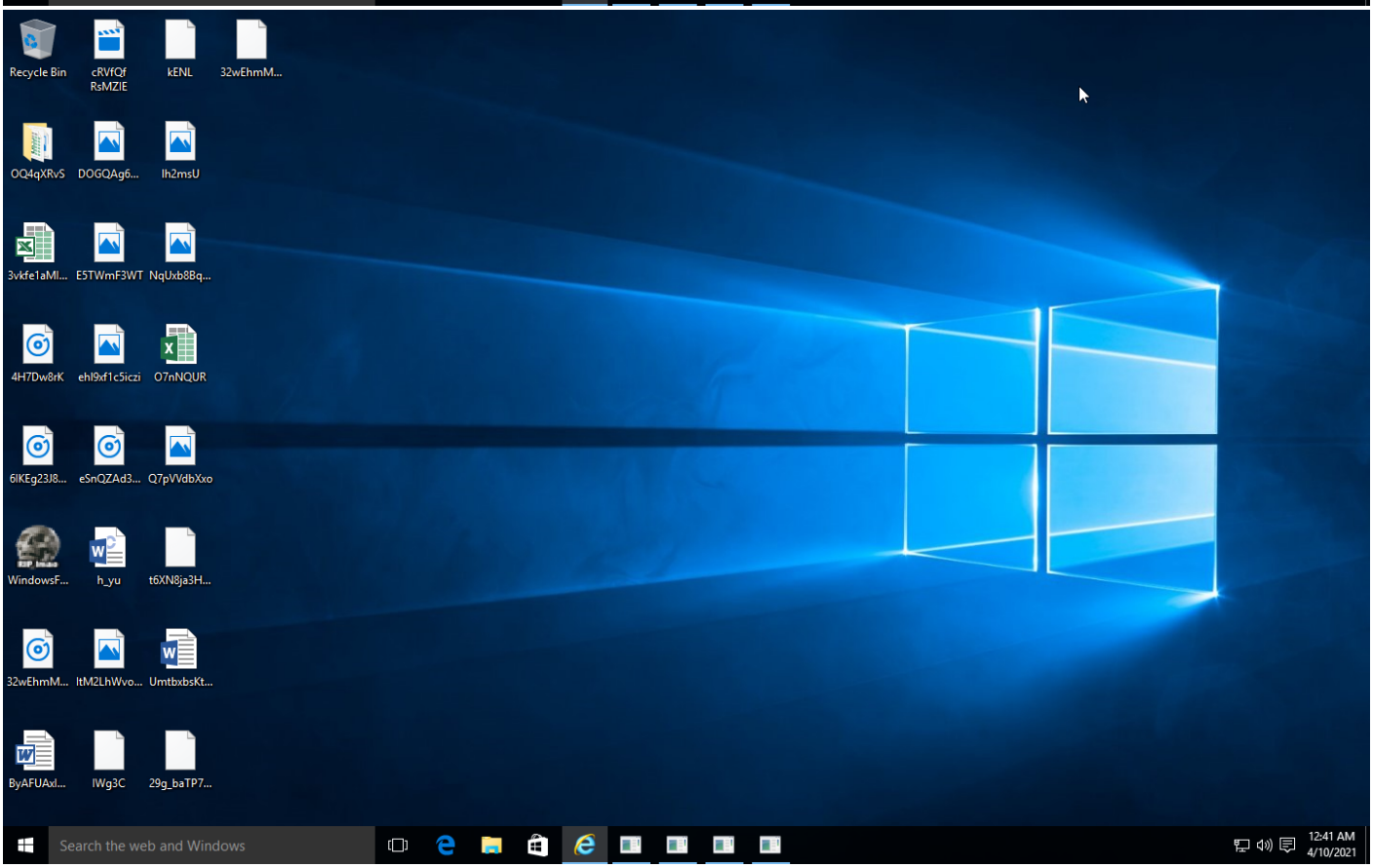
ID	1092345
MD5	70117cfb0d652621da77c47c952fb81a
SHA1	3d841739fd18d02612851c10684631ddcdbc442c
SHA256	9e1609ab7f01b56a9476494d9b3bf5997380d466744b07ec5d9b20e416b10f08
SSDeep	24576:nTSTiRsBE12BIVpT2QhYpAILUo/g9QZqpMC3QVbIoTdWR8SfEuGujqZF13z8H81:nT7RseZDT2tSbvQsIbe8YVjPH81
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
Filename	WindowsFormsApp1.exe
File Size	1327.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-04-10 02:39 (UTC+2)
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	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
ByAFUAxl...
IWg3C
OQ4qXRvS
cRVfQf RsMZIE
kENL
3vkfe1aMl...
DOGQAg6...
Ih2msU
4H7Dw8rK
E5TWmF3WT
NqUxb8Bq...
6IKEg23J8...
ehl9xf1c5iczi
O7nNQUR
WindowsF...
eSnQZAd3...
Q7pVVdbXxo
29g_baTP7...
h_yu
t6XN8ja3H...
32wEhmM...
ItM2LhWvo...
UmtbxbsKt...
Search the web and Windows
12:40 AM
4/10/2021





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

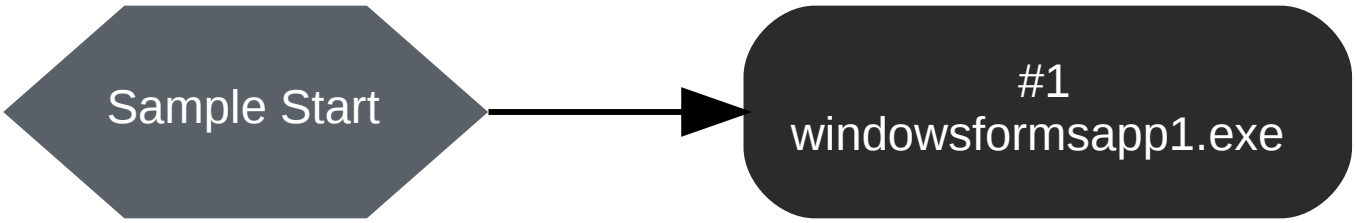
-

HTTP Requests

-

BEHAVIOR

Process Graph



Process #1: windowsformsapp1.exe

ID	1
Filename	c:\users\rdhj0cnfevzx\desktop\windowsformsapp1.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\WindowsFormsApp1.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 75694, Reason: Analysis Target
Unmonitor End Time	End Time: 316608, Reason: Terminated by Timeout
Monitor Duration	240.91s
Return Code	Unknown
PID	1748
Parent PID	2104
Bitness	32 Bit

Dropped Files (94)

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\29g_baTP7KEHQ7Ea.flv.crypted	73.38 KB	6c81af004df10dccd3458bc775ac173ab74c59c9afe79b77cb234f49e9c070f0	✕
C:\Users\RDhJ0CNFevzX\Desktop\32wEhmM49-3-4u.mp3.crypted	41.52 KB	062beb6621b73081aa90030e284959df3284836198f9a25c7cb4aa64de15c77b	✕
C:\Users\RDhJ0CNFevzX\Desktop\3vkfe1aMIgx2zhSpBLmx.xls.crypted	47.53 KB	352b4b9ed9a128d5c86cb80400074654e95eb9c9a6842bc3fc8a60d030cb0af1	✕
C:\Users\RDhJ0CNFevzX\Desktop\4H7Dw8rK.m4a.crypted	65.70 KB	4fd4ce5c07737def52551aca867aa0827fc80d9c84f8ca40a1d8487eaa6395e3	✕
C:\Users\RDhJ0CNFevzX\Desktop\6IKEg23J8Cgwjafy8.mp3.crypted	53.08 KB	df40c787eb4664a470c551d77d7263762d83ef34370ac25e1e8e84af57e69fe9	✕
C:\Users\RDhJ0CNFevzX\Desktop\ByAFUAxIt0mt9ks.rtf.crypted	3.41 KB	303b9e80ed8f64dc1eb335c704fce5bb081d5cf6d7437807a01d18fec933abe4	✕
C:\Users\RDhJ0CNFevzX\Desktop\cRVfQfRsMZIE.mkv.crypted	25.25 KB	dcddbeba7ece5ef7608dcc62afe5f950dbb1230f5e0aa14b28d729b56cb53512	✕
C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini.crypted	320 bytes	1ebe266012a5a8e78bc8f07ba026008c7f0140b9601465a2ca8e8693e530fb66	✕
C:\Users\RDhJ0CNFevzX\Desktop\DOGQAg6cAT1rQ.jpg.crypted	27.97 KB	6d75889b26b14216f093b6e1681b36769ab7eadf7e53512bc6fe9c290c2a7b80	✕
C:\Users\RDhJ0CNFevzX\Desktop\E5TWmF3WT.png.crypted	90.97 KB	f18ad99edfe11a49d7bd0e5b978f9ed38edd0b100fb865ba463ebb2e784e1853	✕
C:\Users\RDhJ0CNFevzX\Desktop\ehl9xf1c5icz i.gif.crypted	17.69 KB	b6aa438e9ad550693ecd344691c19f4ef181733f08e0cff809e38203085d9c9c	✕
C:\Users\RDhJ0CNFevzX\Desktop\eSnQZAd3O3h2-YvUE.wav.crypted	14.61 KB	d9a8f4df16989a2c909b9ed8a5499098fd3a307b2d36a12404400bf54c8d5039	✕
C:\Users\RDhJ0CNFevzX\Desktop\h_yu.odt.crypted	48.31 KB	7dee845c0e433ac85092b702b7bfa71d5ccb17c206efbe66c0ce0f75619c9807	✕
C:\Users\RDhJ0CNFevzX\Desktop\ItM2LhWvoIdX.gif.crypted	34.38 KB	2672272ca6d291617cd8fd0283738c80cdac8aa4fbaadefe0ff5630f7f5460cd	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\IWg3C.swf.crypted	24.50 KB	8459404b4ad6e652a9b5e3c8dc698d4398e91c13956529992148b59b16e5320a	✕
C:\Users\RDhJ0CNFevzX\Desktop\kENL.swf.crypted	86.47 KB	e57c9b839c0b2d5a82351d427b76366be14fb41461d6b7c5f3995fc76b8e2770	✕
C:\Users\RDhJ0CNFevzX\Desktop\lh2msU.png.crypted	94.48 KB	f9ccf4b038c1aef3444c489dc796b12a0dd738cba5d7be37f49a3186588d0514	✕
C:\Users\RDhJ0CNFevzX\Desktop\NqUxb8BqNUsRq.gif.crypted	54.88 KB	6721e26080d40fe32c7e31172e65401be84448f1f9af349c6517be6ee1735700	✕
C:\Users\RDhJ0CNFevzX\Desktop\O7nNQUR.xlsx.crypted	30.45 KB	5b3d957e8be507d362c05b1993f88e70c62cc4590bb4addf109eb2cd1845952e	✕
C:\Users\RDhJ0CNFevzX\Desktop\Q7pVVdbXxo.png.crypted	47.92 KB	7d719cfe063147260eca6d704360a9c9509205aa0e71aa861cddcf404c9a8ca0	✕
C:\Users\RDhJ0CNFevzX\Desktop\t6XN8ja3HMuFowM.flv.crypted	63.27 KB	d99f94c8ae2f3485ef19c2388c45dcc83d03b2d8c3dd46475822f0ebf7d4fdb2	✕
C:\Users\RDhJ0CNFevzX\Desktop\UmtbxbsKtyZHLBBT.docx.crypted	94.58 KB	3a5b1601c9d0cd66254b206eb7632a6ce6d2b8cb7065aacad99313c2c437e14a	✕
C:\Users\RDhJ0CNFevzX\Desktop\WindowsFormsApp1.exe.crypted	32 bytes	b37ab08dd7bb4c32f1f33ffa3579e4f83fa4e01f4131a9d7f8ec3fcde4ea8d9f	✕
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini.crypted	544 bytes	08f3c869c6006a4ecc1d6c0d2f6f0a980676237d007261f748b898403707fd05	✕
C:\Users\RDhJ0CNFevzX\Pictures\g9MMgrRsjdjl6y_K.bmp.crypted	6.50 KB	c8ce4d601ec0e99cb3a970e12135d886865a43df9c580de52fa1933f7c7d262b	✕
C:\Users\RDhJ0CNFevzX\Pictures\U212.bmp.crypted	56.17 KB	8c6c9cdd18d526df1e8fdd623baa5d482d5c0cddaa3cdadd660de5a110a9eaa0	✕
C:\Users\RDhJ0CNFevzX\Pictures\-JfZX1yolDrQOV0dKF\lla2.gif.crypted	13.12 KB	54cea2d9210e57973ccf1be0a9b962c2f2d5ae4243bdbb5604fab54503489f3d	✕
C:\Users\RDhJ0CNFevzX\Pictures\-VKddreP\CiQmPNkGQ5Aj.gif.crypted	79.62 KB	fd2710f81eef18bccbdd23f37116f559115da257403cba0edf0bea44a1d75772	✕
C:\Users\RDhJ0CNFevzX\Pictures\-VKddreP\EcWYWJ.bmp.crypted	86.11 KB	e7603b104a02e8669485618529098 07edddf659cf50ccb3ad42f55bfa56bf823	✕
C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S\EghA ewGW4m.png.crypted	25.89 KB	f9f4df118c1a3d5d08b019247930cb3f71530bed313fc1941dca4a348d4eddac	✕
C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S\hHEWCPQXSzJqw2.gif.crypted	93.31 KB	927b02b2d0bdbda71356d20f429b68ac601ffd9b27affb1da8ac0510a831d78c	✕
C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S\lBRcwvvbGmc7v.png.crypted	54.69 KB	80d826d52b847ec9b89f3e116fab5d4f9e90487204b45b2143c08990648ccb57	✕
C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S_iiP8T0MRXllm1tfjbq.jpg.crypted	20.06 KB	f856f827f5033231aeb79bd0615a5e855372ed8c09e5a9026281eeeb4b795de5	✕
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini.crypted	224 bytes	10f800e4eca6161c7e28c378652b7ccb1509d342e564d8c28579d43ed428669f	✕
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\0x80rwEK7GGdZi42.png.crypted	57.86 KB	d84b6ad3a6d4f6e9922912a447e167841c45e4249f2c7fe9ef1b40711a17e1b1	✕
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\FW6n2E74XencSxxVQ.gif.crypted	77.16 KB	c078c72f576101f0cf9d9f2eb49a0399a5a60c9dcfe22b5cfb89801846fe63f4	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\mwI3GQ.png.crypted	98.69 KB	068f4d0662f82f44409058f274ec765b1057943d7f0dc018b7df1c9acd6f397d	✕
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\CuISBRH73xpuIJ.gif.crypted	55.86 KB	b461bcc2185bf3f5cacb027ff6dfd4b3dc14c367411cf1dd62b1d7bf76373ba1	✕
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\qa qscB7dEB68md.jpg.crypted	26.83 KB	1229c79992c20f013e9bed579e8c4cfa4283bbe27abf42cfb65dd0f058f29e02	✕
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\qpgifz.png.crypted	45.70 KB	21e1470b1bfd2e3e3fb7d897533cf650c98c5a6de94f7631094d018b9165e379	✕
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\vjctOsc 9.png.crypted	21.58 KB	662635ea289d5b39c024e19d01a0592ef0af0b886fc396b41d1597a808d1d7bf	✕
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT_ZeJwDnDxE -.png.crypted	38.64 KB	7dffa18d28fea2c2931db3a70ad85e671206c8109850f843935a0ffa320e1aea	✕
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\LqJnDM9UiX9y__\QTFwbdIShFVlZcj.png.crypted	48.39 KB	ea129dfb35ce64121a2a073faf487ecff851c2a202d8627165f22eee0bdfb093	✕
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\e0M5eKRs.bmp.crypted	3.25 KB	7eba4f5dc8e476566e397db651ed096c2630cd169bd8b5b752ec008c8076fbb3	✕
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\px_OI5y_g2.png.crypted	68.81 KB	104d218fd7066f700ad7d026d3fa63e8db62f431168f89f4f9a7cf80d9444c20	✕
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\r4-BrEBkg1m4C8DiC.bmp.crypted	88.38 KB	b9fd03942b559b165b1eb850cdb627cbe77605f0e6191e1e7508f9a4d86f76c6	✕
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\2zACndvEh_8MXEx.jpg.crypted	90.98 KB	71d658cc92a4468e655ac5c8fd7813683a1d31116567178ba3a4787ce2cb8798	✕
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\3oj9wPcrY6MdQ7q3Fh.jpg.crypted	70.20 KB	9bf2ed32c7fea61dd92898864d04e0a5bed666d12ab40075c03eb74e84144d6f	✕
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\HWxI5_2sA0.png.crypted	56.09 KB	cae625143651de694951e33fbfaafc23ee89597e09e4a79cb419bc78e80c645e	✕
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\NJ5yLkiN9E2qioGH9nJs.bmp.crypted	63.56 KB	f47cd1ba9465225ab27ca5711716dda8f7ee3ca5ef3add2993fa26b7d985b918	✕
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\oA9pUEJthu- SjY71.gif.crypted	13.09 KB	53ea4de8bfebcfddf3a63b8c36f90e17ee5b691d51859ee0460b64d129edaa7d	✕
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini.crypted	224 bytes	421e9f5a7d81ab498ad67cb5b3af5b1883d8ace9fb968bd14cd8bef7d03ff9df	✕
C:\Users\RDhJ0CNFevzX\Documents\-dKCymjM6t.xls.crypted	50.73 KB	72446cc82f68113533ff6c962ccd98f1a4b013d96cae25eeffd7e2b98622366d	✕
C:\Users\RDhJ0CNFevzX\Documents\0i4blKWnXDBzRDzcOs.pps.crypted	75.47 KB	560c511c6656a4f1be1e96ea5e8098945a1c6b2dc3128ff9c56a1066ec821220	✕
C:\Users\RDhJ0CNFevzX\Documents\4AvDU315bNLSZ.docx.crypted	97.70 KB	e28d00c81bb240f7ad745ce4a22da085eac9e06fcc9eb0b8fee1e528a334acff	✕
C:\Users\RDhJ0CNFevzX\Documents\4oHiOkMBXj9.doc.crypted	7.41 KB	b4ea65425e5f5a707e99af4ffdb501efcfeb284933de4c47c71bf13280d05293	✕
C:\Users\RDhJ0CNFevzX\Documents\4txGY.xlsx.crypted	5.77 KB	83959da1aa0d5d8994b331c5eacbccb162b13e2cba0e64d8028b7fabc9a3c507	✕
C:\Users\RDhJ0CNFevzX\Documents\6hN4c63FU4H.odp.crypted	97.25 KB	0abb948741e4bd5ebe8cfbae781ef9379ba301cf53f1df5f0240a39654116fce	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\6u7pw7FlU48.pptx.crypted	62.41 KB	a4dffd2da4796660ac8c3ada915d317640b53daf17650b23522403282faf05d3	✕
C:\Users\RDhJ0CNFevzX\Documents\9owOKQ0XPX.docx.crypted	49.20 KB	396cab7c41247b381beb32ce228a5d0d07708fcdae38d040dcb3149cb203c1b7	✕
C:\Users\RDhJ0CNFevzX\Documents\9wXmWGHa4ITFRR.ppt.crypted	19.22 KB	eed3c15c30b05796ac2f99ded8f4ad1d115729b298cedc99f5fff054e5d5bf90	✕
C:\Users\RDhJ0CNFevzX\Documents\cfxIXSMlKxJA32om.pptx.crypted	99.61 KB	92bd64656220b76a336353d492896e002404edbb6b86bc0c19fb395d1b30394e	✕
C:\Users\RDhJ0CNFevzX\Documents\CTq2.pptx.crypted	84.59 KB	3f311566eaff3900d5815971c04f8c3537a27416d112cdb1137dbb6b94e0a86d	✕
C:\Users\RDhJ0CNFevzX\Documents\d9S_PU2YkSXvYiTdOmKi.pdf.crypted	93.30 KB	0276e229021a6c62640a21d4fef9a0201870036164b8927720f185dfcf857f31	✕
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini.crypted	448 bytes	3f01dd28ca5458aac2a8b58bbdc0ce9d7396ce84b0ac81fcc8f5d00170391cdb	✕
C:\Users\RDhJ0CNFevzX\Documents\dlKPNzm.xls.crypted	16.91 KB	09a07bc6afdbc66a7a2e16ddd60669e3aca2ddc49497d38abb80ba3ff2eccc01	✕
C:\Users\RDhJ0CNFevzX\Documents\e3rx.docx.crypted	94.47 KB	749bb11bc5253bba298477170cbd2221738645d18de6c3c239f90b3ea1c1f74f	✕
C:\Users\RDhJ0CNFevzX\Documents\elaXp_yU-M7.xls.crypted	92.20 KB	0868bdc07b310fa4398da07756779b9655c70efe3d298de96e09f6a775e19da5	✕
C:\Users\RDhJ0CNFevzX\Documents\F-mhE.xlsx.crypted	51.73 KB	7efd089958f1ef14370b36ac4a5061012b58773988bfbaeac0ff157277c0b8ac	✕
C:\Users\RDhJ0CNFevzX\Documents\FEBjEB3GAc8uG9QoiVe.docx.crypted	29.31 KB	deb8eb0e30f34065cc3f0a179fed84ec9d3b9c03f6a8d08cc60573ab21540099	✕
C:\Users\RDhJ0CNFevzX\Documents\fRqC9SKMJhEVA.xlsx.crypted	22.33 KB	55f9a72671c86717d3ff506050b046effe717961fa528376986cf347138996d2	✕
C:\Users\RDhJ0CNFevzX\Documents\gS1iFOFgOpmDYFaP2.csv.crypted	9.42 KB	f63abaca6314493f63d0433061cbc8465ce0484eb70a8cf04348b4476eea7f1b	✕
C:\Users\RDhJ0CNFevzX\Documents\Jyexb.pptx.crypted	49.44 KB	aab4a82a51f3c9bd536896ff9d285f4a2a524108fcc041ea8165529c86733875	✕
C:\Users\RDhJ0CNFevzX\Documents\mu_vUwdrfz9nK.pdf.crypted	85.61 KB	e5c044444048c7209c5d66001b6adb729c801a01b41f1dcb83f47fa1f159a8f2	✕
C:\Users\RDhJ0CNFevzX\Documents\nm8X6ZirdLU8kVJc.ots.crypted	35.25 KB	437314d453f679b8cb1df50cc42b9e89681dd5171405e071b96119ed06f622b5	✕
C:\Users\RDhJ0CNFevzX\Documents\RUjn1OdArdO.pptx.crypted	59.67 KB	7a10df1544c8f19992386fc9b36eca7aa50c5b30a99a8dd4db2ab81cfe2e4323	✕
C:\Users\RDhJ0CNFevzX\Documents\R_yNy4eoI-Ial9bDJahm.xlsx.crypted	24.45 KB	73b85484a691cc839f0438f49e38f8a71e9bdb00d9f490e6ed256fcdc4328878	✕
C:\Users\RDhJ0CNFevzX\Documents\sSCtLBz1rRC.docx.crypted	11.06 KB	8ca46be19556abbb9e0d295c057e76240906198bae4e4715a9bb4ad18d95ad9b	✕
C:\Users\RDhJ0CNFevzX\Documents\sS__yUDQ6eVd.xls.crypted	62.80 KB	dc191c3a785245d433c461bb79bbe5c7f201c56cf56a4b195d2c20fc839bae94	✕
C:\Users\RDhJ0CNFevzX\Documents\Tkfw1r1M5TW5.xlsx.crypted	91.86 KB	7d955dd41ea8c4e6ea75efc5ddefd348134d1a13cae1543b2da547ed04be6514	✕

Filename	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Documents\UWMAv1LvMInByi.odt.crypted	99.39 KB	6a5a3f6387d42fe44c77d03880fc8571c9c8fe8f63a509a25379cb6a1e1029ee	✕
C:\Users\RDhJ0CNFevzX\Documents\V4j6Gj72.doc.crypted	4.78 KB	c730e13edab05a43b2cfc855287f138ad9974974cacb837e046fc2df45d0d121	✕
C:\Users\RDhJ0CNFevzX\Documents\VVIj_dir5hfjCIYqyEk2.pps.crypted	17.95 KB	39c8b9a4c11285315d25ee519fb8be2f7e30450bbf02fb4f0ae180716fc425f1	✕
C:\Users\RDhJ0CNFevzX\Documents\zeGkvyC5a.pptx.crypted	6.31 KB	348f1b380f56247f6e5d64fb59a9b217517dfec00535253c010eafa4658e4ff9	✕
C:\Users\RDhJ0CNFevzX\Documents\zR8r9B.docx.crypted	28.75 KB	a5ad91cdee98b129e572494c00947c104913a234ea424bf4a0d84f96f44f7d34	✕
C:\Users\RDhJ0CNFevzX\Documents\ZZW2.pptx.crypted	57.39 KB	d5a7d64fdf078c40bd3e6679f952b02d52f069e1e1ff8bfdcefd3bceb85b23d0	✕
C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\15ihmDlL.ppt.crypted	84.58 KB	10e8f1b79780b3a6792de1e06409373de8b6bceabcba97813e32de7e3ab2664a	✕
C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\2d44 AU8ULin.ppt.crypted	30.23 KB	e3adda5e78ef8b8bb60b4bf3b53a6b1756e5614b1e6397bdcc0d7c8e1c58d691	✕
C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\7zlsQYuxwY.csv.crypted	77.33 KB	75bdf405c79ca919686efd96ffda1785b13e01e905d420ef04218d577c45a231	✕
C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\DXEc.docx.crypted	91.03 KB	b76e08e1cef8823e8d3eefc65c5208973145c22d20b5b77021f5421a9c192501	✕
C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\EkEyb-6ITf.pptx.crypted	82.06 KB	a89bb98bf9f604cd79bd35b37a727aba8cea7b877648096a72e65a2364cc66fd	✕
C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\ieNT9n_upIFSROR_S.ots.crypted	79.20 KB	71154f9be4a7eda1381016edff377b582917136ebfe65a8f56da63ee3e65e9be	✕
C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\jcvL 3fubnvUWf4cJt.xlsx.crypted	4.69 KB	422b27aa25ff8d0a480ae8825fcd23a632bc1e9a8374e0134e863819ee1f55c6	✕
C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\L PbXLT49O.pps.crypted	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✕

Host Behavior

Type	Count
Module	111
System	23
Window	89
Registry	3
File	1100

ARTIFACTS

File

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
9e1609ab7f01b56a9476494d9b3bf5997380d466744b07ec5d9b20e416b10f08	C:\Users\RDhJ0CNFevzX\Desktop\WindowsFormsApp1.exe	Sample File	1327.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
6c81af004df10dccd3458bc775ac173ab74c59c9afe79b77cb234f49e9c070f0	C:\Users\RDhJ0CNFevzX\Desktop\29g_baTP7KEHQ7Ea.flv.crypted	Dropped File	73.38 KB	application/octet-stream	Access, Write, Create	CLEAN
062beb6621b73081aa90030e284959df3284836198f9a25c7cb4aa64de15c77b	C:\Users\RDhJ0CNFevzX\Desktop\32wEhmM49-3-4u.mp3.crypted	Dropped File	41.52 KB	application/octet-stream	Access, Write, Create	CLEAN
352b4b9ed9a128d5c86cb80400074654e95eb9c9a6842bc3fc8a60d030cb0af1	C:\Users\RDhJ0CNFevzX\Desktop\3vkfe1aMIgx2zhSpBLmx.xls.crypted	Dropped File	47.53 KB	application/octet-stream	Access, Write, Create	CLEAN
4fd4ce5c07737def52551aca867aa0827fc80d9c84f8ca40a1d8487eaa6395e3	C:\Users\RDhJ0CNFevzX\Desktop\4H7Dw8rK.m4a.crypted	Dropped File	65.70 KB	application/octet-stream	Access, Write, Create	CLEAN
df40c787eb4664a470c551d77d7263762d83ef34370ac25e1e8e84af57e69fe9	C:\Users\RDhJ0CNFevzX\Desktop\6IKEg23J8Cgwjafy8.mp3.crypted	Dropped File	53.08 KB	application/octet-stream	Access, Write, Create	CLEAN
303b9e80ed8f64dc1eb335c704fce5bb081d5cf6d7437807a01d18fec933abe4	C:\Users\RDhJ0CNFevzX\Desktop\ByAFUAxIt0mt9ks.rtf.crypted	Dropped File	3.41 KB	application/octet-stream	Access, Write, Create	CLEAN
dcddbeba7ece5ef7608dcc62afe5f950dbb1230f5e0aa14b28d729b56cb53512	C:\Users\RDhJ0CNFevzX\Desktop\cRVfQfRsMZIE.mkv.crypted	Dropped File	25.25 KB	application/octet-stream	Access, Write, Create	CLEAN
1ebe266012a5a8e78bc8f07ba026008c7f0140b9601465a2ca8e8693e530fb66	C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini.crypted	Dropped File	320 bytes	application/octet-stream	Access, Write, Create	CLEAN
6d75889b26b14216f093b6e1681b36769ab7eadf7e53512bc6fe9c290c2a7b80	C:\Users\RDhJ0CNFevzX\Desktop\DOGQAg6cAT1rQ.jpg.crypted	Dropped File	27.97 KB	application/octet-stream	Access, Write, Create	CLEAN
f18ad99edfe11a49d7bd0e5b978f9ed38edd0b100fb865ba463ebb2e784e1853	C:\Users\RDhJ0CNFevzX\Desktop\E5TWmF3WT.png.crypted	Dropped File	90.97 KB	application/octet-stream	Access, Write, Create	CLEAN
b6aa438e9ad550693ecd344691c19f4ef181733f08e0cff809e38203085d9c9c	C:\Users\RDhJ0CNFevzX\Desktop\ehl9xf1c5iczi.gif.crypted	Dropped File	17.69 KB	application/octet-stream	Access, Write, Create	CLEAN
d9a8f4df16989a2c909b9ed8a5499098fd3a307b2d36a12404400bf54c8d5039	C:\Users\RDhJ0CNFevzX\Desktop\eSnQZAd3O3h2-YvUE.wav.crypted	Dropped File	14.61 KB	application/octet-stream	Access, Write, Create	CLEAN
7dee845c0e433ac85092b702b7bfa71d5ccb17c206efbe66c0ce0f75619c9807	C:\Users\RDhJ0CNFevzX\Desktop\h_yu.odt.crypted	Dropped File	48.31 KB	application/octet-stream	Access, Write, Create	CLEAN
2672272ca6d291617cd8fd0283738c80cdac8aa4fbaadefe0ff5630f7f5460cd	C:\Users\RDhJ0CNFevzX\Desktop\ItM2LhWvoIdX.gif.crypted	Dropped File	34.38 KB	application/octet-stream	Access, Write, Create	CLEAN
8459404b4ad6e652a9b5e3c8dc698d4398e91c13956529992148b59b16e5320a	C:\Users\RDhJ0CNFevzX\Desktop\IWg3C.swf.crypted	Dropped File	24.50 KB	application/octet-stream	Access, Write, Create	CLEAN
e57c9b839c0b2d5a82351d427b76366be14fb41461d6b7c5f3995fc76b8e2770	C:\Users\RDhJ0CNFevzX\Desktop\kENL.swf.crypted	Dropped File	86.47 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
f9ccf4b038c1aef3444c489dc796b12a0dd738cba5d7be37f49a3186588d0514	C:\Users\RDhJ0CNFevzX\Desktop\lh2msU.png.crypted	Dropped File	94.48 KB	application/octet-stream	Access, Write, Create	CLEAN
6721e26080d40fe32c7e31172e65401be84448f1f9af349c6517be6ee1735700	C:\Users\RDhJ0CNFevzX\Desktop\NqUxb8BqNUsRq.gif.crypted	Dropped File	54.88 KB	application/octet-stream	Access, Write, Create	CLEAN
5b3d957e8be507d362c05b1993f88e70c62cc4590bb4addf109eb2cd1845952e	C:\Users\RDhJ0CNFevzX\Desktop\O7nNQUR.xlsx.crypted	Dropped File	30.45 KB	application/octet-stream	Access, Write, Create	CLEAN
7d719cfe063147260eca6d704360a9c9509205aa0e71aa861cddcf404c9a8ca0	C:\Users\RDhJ0CNFevzX\Desktop\Q7pVVdbXxo.png.crypted	Dropped File	47.92 KB	application/octet-stream	Access, Write, Create	CLEAN
d99f94c8ae2f3485ef19c2388c45dcc83d03b2d8c3dd46475822f0ebf7d4fdb2	C:\Users\RDhJ0CNFevzX\Desktop\t6XN8ja3HMuFowM.flv.crypted	Dropped File	63.27 KB	application/octet-stream	Access, Write, Create	CLEAN
3a5b1601c9d0cd66254b206eb7632a6ce6d2b8cb7065aacad99313c2c437e14a	C:\Users\RDhJ0CNFevzX\Desktop\UmtbxbsKtyZHLBBT.docx.crypted	Dropped File	94.58 KB	application/octet-stream	Access, Write, Create	CLEAN
b37ab08dd7bb4c32f1f33ffa3579e4f83fa4e01f4131a9d7f8ec3fcde4ea8d9f	C:\Users\RDhJ0CNFevzX\Desktop\WindowsFormsApp1.exe.crypted	Dropped File	32 bytes	text/plain	Access, Write, Create	CLEAN
08f3c869c6006a4ecc1d6c0d2f6f0a980676237d007261f748b898403707fd05	C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini.crypted	Dropped File	544 bytes	application/octet-stream	Access, Write, Create	CLEAN
c8ce4d601ec0e99cb3a970e12135d886865a43df9c580de52fa1933f7c7d262b	C:\Users\RDhJ0CNFevzX\Pictures\g9MMgrRsjdjl6y_K.bmp.crypted	Dropped File	6.50 KB	application/octet-stream	Access, Write, Create	CLEAN
8c6c9cdd18d526df1e8fdd623baa5d482d5c0ddaa3cdadd660de5a110a9eaa0	C:\Users\RDhJ0CNFevzX\Pictures\U212.bmp.crypted	Dropped File	56.17 KB	application/octet-stream	Access, Write, Create	CLEAN
54cea2d9210e57973ccf1be0a9b962c2f2d5ae4243bdbb5604fab54503489f3d	C:\Users\RDhJ0CNFevzX\Pictures\-JfZX1yolDrQOV0dKF\lla2.gif.crypted	Dropped File	13.12 KB	application/octet-stream	Access, Write, Create	CLEAN
fd2710f81eef18bccbdd23f37116f559115da257403cba0edf0bea44a1d75772	C:\Users\RDhJ0CNFevzX\Pictures\-VKddreP\CiQmPNkGQ5Aj.gif.crypted	Dropped File	79.62 KB	application/octet-stream	Access, Write, Create	CLEAN
e7603b104a02e866948561852909807edddf659cf50ccb3ad42f55bfa56bf823	C:\Users\RDhJ0CNFevzX\Pictures\-VKddreP\EcWYWJ.bmp.crypted	Dropped File	86.11 KB	application/octet-stream	Access, Write, Create	CLEAN
f9f4df118c1a3d5d08b019247930cb3f71530bed313fc1941dca4a348d4eddac	C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S\EghAewGW4m.png.crypted	Dropped File	25.89 KB	application/octet-stream	Access, Write, Create	CLEAN
927b02b2d0bdbda71356d20f429b68ac601ffd9b27affb1da8ac0510a831d78c	C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S\hHEWCPQXSzJqw2.gif.crypted	Dropped File	93.31 KB	application/octet-stream	Access, Write, Create	CLEAN
80d826d52b847ec9b89f3e116fab5d4f9e90487204b45b2143c08990648ccb57	C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S\lBRcwvvbGmc7v.png.crypted	Dropped File	54.69 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
f856f827f5033231aeb79bd0615a5e855372ed8c09e5a9026281eeeb4b795de5	C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZvS_iiP8T0MRXllm1tfjbq.jpg.crypted	Dropped File	20.06 KB	application/octet-stream	Access, Write, Create	CLEAN
10f800e4eca6161c7e28c378652b7ccb1509d342e564d8c28579d43ed428669f	C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini.crypted	Dropped File	224 bytes	application/octet-stream	Access, Write, Create	CLEAN
d84b6ad3a6d4f6e9922912a447e167841c45e4249f2c7fe9ef1b40711a17e1b1	C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\0x80rwEK7GGdZi42.png.crypted	Dropped File	57.86 KB	application/octet-stream	Access, Write, Create	CLEAN
c078c72f576101f0cf9d9f2eb49a0399a5a60c9dcfe22b5cfb89801846fe63f4	C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\FW6n2E74XencSxxVQ.gif.crypted	Dropped File	77.16 KB	application/octet-stream	Access, Write, Create	CLEAN
068f4d0662f82f44409058f274ec765b1057943d7f0dc018b7df1c9acd6f397d	C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\mwI3GQ.png.crypted	Dropped File	98.69 KB	application/octet-stream	Access, Write, Create	CLEAN
b461bcc2185bf3f5cacb027ff6dfd4b3dc14c367411cf1dd62b1d7bf76373ba1	C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\CulSBRH73xpuIJ.gif.crypted	Dropped File	55.86 KB	application/octet-stream	Access, Write, Create	CLEAN
1229c79992c20f013e9bed579e8c4cfa4283bbe27abf42cfb65dd0f058f29e02	C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\qaqscB7dEB68md.jpg.crypted	Dropped File	26.83 KB	application/octet-stream	Access, Write, Create	CLEAN
21e1470b1bfd2e3e3fb7d897533cf650c98c5a6de94f7631094d018b9165e379	C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\qpgifz.png.crypted	Dropped File	45.70 KB	application/octet-stream	Access, Write, Create	CLEAN
662635ea289d5b39c024e19d01a0592ef0af0b886fc396b41d1597a808d1d7bf	C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\vjctOsc9.png.crypted	Dropped File	21.58 KB	application/octet-stream	Access, Write, Create	CLEAN
7dffa18d28fea2c2931db3a70ad85e671206c8109850f843935a0ffa320e1aea	C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT_ZeJwDnDxE-.png.crypted	Dropped File	38.64 KB	application/octet-stream	Access, Write, Create	CLEAN
ea129dfb35ce64121a2a073faf487ecff851c2a202d8627165f22eee0bdfb093	C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\LqJnDM9UiX9y__\QTFwbdIShFVlZcj.png.crypted	Dropped File	48.39 KB	application/octet-stream	Access, Write, Create	CLEAN
7eba4f5dc8e476566e397db651ed096c2630cd169bd8b5b752ec008c8076fbb3	C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\e0M5eKRs.bmp.crypted	Dropped File	3.25 KB	application/octet-stream	Access, Write, Create	CLEAN
104d218fd7066f700ad7d026d3fa63e8db62f431168f89f4f9a7cf80d9444c20	C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\px_OI5y_g2.png.crypted	Dropped File	68.81 KB	application/octet-stream	Access, Write, Create	CLEAN
b9fd03942b559b165b1eb850cdb627cbe77605f0e6191e1e7508f9a4d86f76c6	C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\r4-BrEBkg1m4C8DiC.bmp.crypted	Dropped File	88.38 KB	application/octet-stream	Access, Write, Create	CLEAN
71d658cc92a4468e655ac5c8fd7813683a1d31116567178ba3a4787ce2cb8798	C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\2zACndvEh_8MXEx.jpg.crypted	Dropped File	90.98 KB	application/octet-stream	Access, Write, Create	CLEAN
9bf2ed32c7fea61dd92898864d04e0a5bed666d12ab40075c03eb74e84144d6f	C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\3oj9wPcrY6MdQ7q3Fh.jpg.crypted	Dropped File	70.20 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
cae625143651de694951e33fbfaafc23ee89597e09e4a79cb419bc78e80c645e	C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\HWxI5_2sA0.png.crypted	Dropped File	56.09 KB	application/octet-stream	Access, Write, Create	CLEAN
f47cd1ba9465225ab27ca5711716dda8f7ee3ca5ef3add2993fa26b7d985b918	C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\NJ5yLkiN9E2qioGH9nJs.bmp.crypted	Dropped File	63.56 KB	application/octet-stream	Access, Write, Create	CLEAN
53ea4de8bfebcfddf3a63b8c36f90e17ee5b691d51859ee0460b64d129edaa7d	C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\oA9pUEJthu-SjY71.gif.crypted	Dropped File	13.09 KB	application/octet-stream	Access, Write, Create	CLEAN
421e9f5a7d81ab498ad67cb5b3af5b1883d8ace9fb968bd14cd8bef7d03ff9df	C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini.crypted	Dropped File	224 bytes	application/octet-stream	Access, Write, Create	CLEAN
72446cc82f68113533ff6c962ccd98f1a4b013d96cae25eeffd7e2b98622366d	C:\Users\RDhJ0CNFevzX\Documents\-dKCymjM6t.xls.crypted	Dropped File	50.73 KB	application/octet-stream	Access, Write, Create	CLEAN
560c511c6656a4f1be1e96ea5e8098945a1c6b2dc3128ff9c56a1066ec821220	C:\Users\RDhJ0CNFevzX\Documents\0i4blKWnXDBzRDzcOs.pps.crypted	Dropped File	75.47 KB	application/octet-stream	Access, Write, Create	CLEAN
e28d00c81bb240f7ad745ce4a22da085eac9e06fcc9eb0b8fee1e528a334acff	C:\Users\RDhJ0CNFevzX\Documents\4AvDU315bNLSZ.docx.crypted	Dropped File	97.70 KB	application/octet-stream	Access, Write, Create	CLEAN
b4ea65425e5f5a707e99af4ffdb501efcfeb284933de4c47c71bf13280d05293	C:\Users\RDhJ0CNFevzX\Documents\4oHiOkMBXj9.doc.crypted	Dropped File	7.41 KB	application/octet-stream	Access, Write, Create	CLEAN
83959da1aa0d5d8994b331c5eacbccb162b13e2cba0e64d8028b7fabc9a3c507	C:\Users\RDhJ0CNFevzX\Documents\4txGY.xlsx.crypted	Dropped File	5.77 KB	application/octet-stream	Access, Write, Create	CLEAN
0abb948741e4bd5ebe8cfbae781ef9379ba301cf53f1df5f0240a39654116fce	C:\Users\RDhJ0CNFevzX\Documents\6hN4c63FU4H.odp.crypted	Dropped File	97.25 KB	application/octet-stream	Access, Write, Create	CLEAN
a4dffd2da4796660ac8c3ada915d317640b53daf17650b23522403282faf05d3	C:\Users\RDhJ0CNFevzX\Documents\6u7pw7FlU48.pptx.crypted	Dropped File	62.41 KB	application/octet-stream	Access, Write, Create	CLEAN
396cab7c41247b381beb32ce228a5d0d07708fcdae38d040dcb3149cb203c1b7	C:\Users\RDhJ0CNFevzX\Documents\9owOKQ0XPX.docx.crypted	Dropped File	49.20 KB	application/octet-stream	Access, Write, Create	CLEAN
eed3c15c30b05796ac2f99ded8f4ad1d115729b298cedc99f5fff054e5d5bf90	C:\Users\RDhJ0CNFevzX\Documents\9wXmWGHa4ITFRR.ppt.crypted	Dropped File	19.22 KB	application/octet-stream	Access, Write, Create	CLEAN
92bd64656220b76a336353d492896e002404edbb6b86bc0c19fb395d1b30394e	C:\Users\RDhJ0CNFevzX\Documents\cfxIXSMlKxJA32om.pptx.crypted	Dropped File	99.61 KB	application/octet-stream	Access, Write, Create	CLEAN
3f311566eaff3900d5815971c04f8c3537a27416d112cdb1137dbb6b94e0a86d	C:\Users\RDhJ0CNFevzX\Documents\CTq2.pptx.crypted	Dropped File	84.59 KB	application/octet-stream	Access, Write, Create	CLEAN
0276e229021a6c62640a21d4fef9a0201870036164b8927720f185dfcf857f31	C:\Users\RDhJ0CNFevzX\Documents\d9S_PU2YkSXvYiTdOmKi.pdf.crypted	Dropped File	93.30 KB	application/octet-stream	Access, Write, Create	CLEAN
3f01dd28ca5458aac2a8b58bbdc0ce9d7396ce84b0ac81fcc8f5d00170391cdb	C:\Users\RDhJ0CNFevzX\Documents\desktop.ini.crypted	Dropped File	448 bytes	application/octet-stream	Access, Write, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
09a07bc6afdbc66a7a2e16ddd60669e3aca2ddc49497d38abb80ba3ff2eccc01	C:\Users\RDhJ0CNFevzX\Documents\dlKPNzm.xls.crypted	Dropped File	16.91 KB	application/octet-stream	Access, Write, Create	CLEAN
749bb11bc5253bba298477170cbd2221738645d18de6c3c239f90b3ea1c1f74f	C:\Users\RDhJ0CNFevzX\Documents\e3rx.docx.crypted	Dropped File	94.47 KB	application/octet-stream	Access, Write, Create	CLEAN
0868bdc07b310fa4398da07756779b9655c70efe3d298de96e09f6a775e19da5	C:\Users\RDhJ0CNFevzX\Documents\elaXp_yU-M7.xls.crypted	Dropped File	92.20 KB	application/octet-stream	Access, Write, Create	CLEAN
7efd089958f1ef14370b36ac4a5061012b58773988bfbaeac0ff157277c0b8ac	C:\Users\RDhJ0CNFevzX\Documents\F-mhE.xlsx.crypted	Dropped File	51.73 KB	application/octet-stream	Access, Write, Create	CLEAN
deb8eb0e30f34065cc3f0a179fed84ec9d3b9c03f6a8d08cc60573ab21540099	C:\Users\RDhJ0CNFevzX\Documents\FEBjEB3GAc8uG9QoiVe.docx.crypted	Dropped File	29.31 KB	application/octet-stream	Access, Write, Create	CLEAN
55f9a72671c86717d3ff506050b046effe717961fa528376986cf347138996d2	C:\Users\RDhJ0CNFevzX\Documents\fRqC9SKMJhEVA.xlsx.crypted	Dropped File	22.33 KB	application/octet-stream	Access, Write, Create	CLEAN
f63abaca6314493f63d0433061cbc8465ce0484eb70a8cf04348b4476eea7f1b	C:\Users\RDhJ0CNFevzX\Documents\gS1iFOFgOpmDYFaP2.csv.crypted	Dropped File	9.42 KB	application/octet-stream	Access, Write, Create	CLEAN
aab4a82a51f3c9bd536896ff9d285f4a2a524108fcc041ea8165529c86733875	C:\Users\RDhJ0CNFevzX\Documents\Jyexb.pptx.crypted	Dropped File	49.44 KB	application/octet-stream	Access, Write, Create	CLEAN
e5c044444048c7209c5d66001b6adb729c801a01b41f1dcb83f47fa1f159a8f2	C:\Users\RDhJ0CNFevzX\Documents\mu_vUwdrfz9nK.pdf.crypted	Dropped File	85.61 KB	application/octet-stream	Access, Write, Create	CLEAN
437314d453f679b8cb1df50cc42b9e89681dd5171405e071b96119ed06f622b5	C:\Users\RDhJ0CNFevzX\Documents\nm8X6ZirdLU8kVJc.ots.crypted	Dropped File	35.25 KB	application/octet-stream	Access, Write, Create	CLEAN
7a10df1544c8f19992386fc9b36eca7aa50c5b30a99a8dd4db2ab81cfe2e4323	C:\Users\RDhJ0CNFevzX\Documents\RUjn1OdArdO.pptx.crypted	Dropped File	59.67 KB	application/octet-stream	Access, Write, Create	CLEAN
73b85484a691cc839f0438f49e38f8a71e9bdb00d9f490e6ed256fcdc4328878	C:\Users\RDhJ0CNFevzX\Documents\R_yNy4eoI-Ial9bDJahm.xlsx.crypted	Dropped File	24.45 KB	application/octet-stream	Access, Write, Create	CLEAN
8ca46be19556abbb9e0d295c057e76240906198bae4e4715a9bb4ad18d95ad9b	C:\Users\RDhJ0CNFevzX\Documents\sSCtLBz1rRC.docx.crypted	Dropped File	11.06 KB	application/octet-stream	Access, Write, Create	CLEAN
dc191c3a785245d433c461bb79bbe5c7f201c56cf56a4b195d2c20fc839bae94	C:\Users\RDhJ0CNFevzX\Documents\sS__yUDQ6eVd.xls.crypted	Dropped File	62.80 KB	application/octet-stream	Access, Write, Create	CLEAN
7d955dd41ea8c4e6ea75efc5ddefd348134d1a13cae1543b2da547ed04be6514	C:\Users\RDhJ0CNFevzX\Documents\Tkfw1r1M5TW5.xlsx.crypted	Dropped File	91.86 KB	application/octet-stream	Access, Write, Create	CLEAN
6a5a3f6387d42fe44c77d03880fc8571c9c8fe8f63a509a25379cb6a1e1029ee	C:\Users\RDhJ0CNFevzX\Documents\UWMAv1LvMInByi.odt.crypted	Dropped File	99.39 KB	application/octet-stream	Access, Write, Create	CLEAN
c730e13edab05a43b2cfc855287f138ad9974974cacb837e046fc2df45d0d121	C:\Users\RDhJ0CNFevzX\Documents\V4j6Gj72.doc.crypted	Dropped File	4.78 KB	application/octet-stream	Access, Write, Create	CLEAN
39c8b9a4c11285315d25ee519fb8be2f7e30450bbf02fb4f0ae180716fc425f1	C:\Users\RDhJ0CNFevzX\Documents\VVIj_dir5hfjCIYqyEk2.pps.crypted	Dropped File	17.95 KB	application/octet-stream	Access, Write, Create	CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
348f1b380f56247f6e5d64fb59a9b217517dfec00535253c010eafa4658e4ff9	C:\Users\RDhJ0CNFevzX\Documents\zeGkvyC5a.pptx.crypted	Dropped File	6.31 KB	application/octet-stream	Access, Write, Create	CLEAN
a5ad91cdee98b129e572494c00947c104913a234ea424bf4a0d84f96f44f7d34	C:\Users\RDhJ0CNFevzX\Documents\zR8r9B.docx.crypted	Dropped File	28.75 KB	application/octet-stream	Access, Write, Create	CLEAN
d5a7d64fdf078c40bd3e6679f952b02d52f069e1e1ff8bfdcefd3bceb85b23d0	C:\Users\RDhJ0CNFevzX\Documents\ZZW2.pptx.crypted	Dropped File	57.39 KB	application/octet-stream	Access, Write, Create	CLEAN
10e8f1b79780b3a6792de1e06409373de8b6bceabcba97813e32de7e3ab2664a	C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\15ihmDlL.ppt.crypted	Dropped File	84.58 KB	application/octet-stream	Access, Write, Create	CLEAN
e3adda5e78ef8b8bb60b4bf3b53a6b1756e5614b1e6397bdcc0d7c8e1c58d691	C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\2d44AU8ULin.ppt.crypted	Dropped File	30.23 KB	application/octet-stream	Access, Write, Create	CLEAN
75bdf405c79ca919686efd96ffda1785b13e01e905d420ef04218d577c45a231	C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\7zlsQYuxwY.csv.crypted	Dropped File	77.33 KB	application/octet-stream	Access, Write, Create	CLEAN
b76e08e1cef8823e8d3efc65c5208973145c22d20b5b77021f5421a9c192501	C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\DXEc.docx.crypted	Dropped File	91.03 KB	application/octet-stream	Access, Write, Create	CLEAN
a89bb98bf9f604cd79bd35b37a727aba8cea7b877648096a72e65a2364cc66fd	C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\EkEyb-6ITf.pptx.crypted	Dropped File	82.06 KB	application/octet-stream	Access, Write, Create	CLEAN
71154f9be4a7eda1381016edff377b582917136ebfe65a8f56da63ee3e65e9be	C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\ieNT9n_upIFSROR_S.ots.crypted	Dropped File	79.20 KB	application/octet-stream	Access, Write, Create	CLEAN
422b27aa25ff8d0a480ae8825fcd23a632bc1e9a8374e0134e863819ee1f55c6	C:\Users\RDhJ0CNFevzX\Documents\IDhWz54EjpbS8oH\jcvL3fubnvUWf4cJt.xlsx.crypted	Dropped File	4.69 KB	application/octet-stream	Access, Write, Create	CLEAN

Filename

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\WindowsFormsApp1.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\29g_baTP7KEHQ7Ea.flv.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\29g_baTP7KEHQ7Ea.flv	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\32wEhmM49-3-4u.mp3.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\32wEhmM49-3-4u.mp3	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\3vkfe1aMIgx2zhSpBLmx.xls.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\3vkfe1aMIgx2zhSpBLmx.xls	Accessed File	Access, Read, Delete	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\4H7Dw8rK.m4a.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\4H7Dw8rK.m4a	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\6IKEg23J8Cgwjafy8.mp3.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\6IKEg23J8Cgwjafy8.mp3	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ByAFUAxIt0mt9ks.rtf.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ByAFUAxIt0mt9ks.rtf	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\cRVfQfRsMZIE.mkv.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\cRVfQfRsMZIE.mkv	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\DOGQAg6cAT1rQ.jpg.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\DOGQAg6cAT1rQ.jpg	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\E5TWmF3WT.png.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\E5TWmF3WT.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ehl9xf1c5iczi.gif.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ehl9xf1c5iczi.gif	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\eSnQZAd3O3h2-YvUE.wav.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\eSnQZAd3O3h2-YvUE.wav	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\h_yu.odt.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\h_yu.odt	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ItM2LhWvoIdX.gif.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\ItM2LhWvoIdX.gif	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\IWg3C.swf.crypted	Dropped File	Access, Write, Create	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\IWg3C.swf	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\kENL.swf.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\kENL.swf	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\lh2msU.png.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\lh2msU.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\NqUxb8BqNUsRq.gif.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\NqUxb8BqNUsRq.gif	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\O7nNQUR.xlsx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\O7nNQUR.xlsx	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Q7pVVdbXxo.png.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Q7pVVdbXxo.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\t6XN8ja3HMuFowM.flv.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\t6XN8ja3HMuFowM.flv	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\UmtbxbsKtyZHLBBT.docx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\UmtbxbsKtyZHLBBT.docx	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\WindowsFormsApp1.exe.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\WindowsFormsApp1.exe	Sample File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\desktop.ini	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\g9MMgrRsjdjl6y_K.bmp.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\g9MMgrRsjdjl6y_K.bmp	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\U212.bmp.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\U212.bmp	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\-JfZX1yolDrQOV0dKF\lla2.gif.crypted	Dropped File	Access, Write, Create	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\-JfZX1yolDrQOV0dKF\lla2.gif	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\-VKddreP\CiQmPNkGQ5Aj.gif.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\-VKddreP\CiQmPNkGQ5Aj.gif	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\-VKddreP\EcWYWJ.bmp.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\-VKddreP\EcWYWJ.bmp	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S\EghA ewGW4m.png.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S\EghA ewGW4m.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S\hHEWCPQXSzJqw2.gif.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S\hHEWCPQXSzJqw2.gif	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S\lBRcwvvbG mc7v.png.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S\lBRcwvvbG mc7v.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S_iiP8T0MRXllm1tfjbq.jpg.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\6oRmBG\uOigE gFQrZv S_iiP8T0MRXllm1tfjbq.jpg	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Camera Roll\desktop.ini	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\0x80rwEK7GGdZi42.png.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\0x80rwEK7GGdZi42.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\FW6n2E74XencSxxVQ.gif.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\FW6n2E74XencSxxVQ.gif	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\mwI3GQ.png.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\mwI3GQ.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\CulSBRH73xpuIJ.gif.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\CulSBRH73xpuIJ.gif	Accessed File	Access, Read, Delete	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\qa qscB7dEB68md.jpg.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\qa qscB7dEB68md.jpg	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\qpgifz.png.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\qpgifz.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\vjctOsc 9.png.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\vjctOsc 9.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT_ZeJwDnDxE -.png.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT_ZeJwDnDxE -.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\LqJnDM9UiX9y__\QTFwbdIShFVlZcj.png.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\ddsJ\WEJFbW0YT\LqJnDM9UiX9y__\QTFwbdIShFVlZcj.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\e0M5eKRs.bmp.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\e0M5eKRs.bmp	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\px_OI5y_g2.png.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\px_OI5y_g2.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\r4-BrEBkg1m4C8DiC.bmp.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\r4-BrEBkg1m4C8DiC.bmp	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\2zACndvEh_8MXEx.jpg.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\2zACndvEh_8MXEx.jpg	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\3oj9wPcrY6MdQ7q3Fh.jpg.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\3oj9wPcrY6MdQ7q3Fh.jpg	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\HWxI5_2sA0.png.crypted	Dropped File	Access, Write, Create	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\HWxI5_2sA0.png	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\NJ5yLkiN9E2qioGH9nJs.bmp.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\NJ5yLkiN9E2qioGH9nJs.bmp	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\oA9pUEJthu- SjY71.gif.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\m7eajC2\7f8H_D0pzn\oA9pUEJthu- SjY71.gif	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Pictures\Saved Pictures\desktop.ini	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\-dKCymjM6t.xls.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\-dKCymjM6t.xls	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\0i4blKWnXDBzRDzcOs.pps.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\0i4blKWnXDBzRDzcOs.pps	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\4AvDU315bNLSZ.docx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\4AvDU315bNLSZ.docx	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\4oHiOkMBXj9.doc.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\4oHiOkMBXj9.doc	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\4txGY.xlsx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\4txGY.xlsx	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\6hN4c63FU4H.odp.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\6hN4c63FU4H.odp	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\6u7pw7FlU48.pptx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\6u7pw7FlU48.pptx	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\9owOKQ0XPX.docx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\9owOKQ0XPX.docx	Accessed File	Access, Read, Delete	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\9wXmWGHa4ITFRR.ppt.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\9wXmWGHa4ITFRR.ppt	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\cfxIXSMlKxJA32om.pptx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\cfxIXSMlKxJA32om.pptx	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\CTq2.pptx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\CTq2.pptx	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\d9S_PU2YkSXvYiTdOmKi.pdf.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\d9S_PU2YkSXvYiTdOmKi.pdf	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\desktop.ini	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\dlKPNzm.xls.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\dlKPNzm.xls	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\e3rx.docx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\e3rx.docx	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\elaXp_yU-M7.xls.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\elaXp_yU-M7.xls	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\F-mhE.xlsx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\F-mhE.xlsx	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\FEBjEB3GAc8uG9QoiVe.docx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\FEBjEB3GAc8uG9QoiVe.docx	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\fRqC9SKMJhEVA.xlsx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\fRqC9SKMJhEVA.xlsx	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\gS1iFOFgOpmDYFaP2.csv.crypted	Dropped File	Access, Write, Create	CLEAN

Filename	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\gS1iFOFgOpmDYFaP2.csv	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Jyexb.pptx.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\Jyexb.pptx	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\mu_vUwdrfz9nK.pdf.crypted	Dropped File	Access, Write, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\mu_vUwdrfz9nK.pdf	Accessed File	Access, Read, Delete	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\nm8X6ZirdLU8kVJc.ots.crypted	Dropped File	Access, Write, Create	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	windowsformsapp1.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	windowsformsapp1.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	windowsformsapp1.exe	CLEAN

Process

Process Name	Commandline	Verdict
windowsformsapp1.exe	"C:\Users\RDhJ0CNFevzX\Desktop\WindowsFormsApp1.exe"	MALICIOUS

YARA / AV

Antivirus (1)

File Type	Threat Name	Filename	Verdict
SAMPLE	Gen:Heur.Ransom.REntS.Gen.1	C:\Users\RDhJ0CNFevzX\Desktop\WindowsFormsApp1.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	2021-04-09 20:24:46+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