MALICIOUS

Classifications: Ransomware

Threat Names: -

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe**
ID	#5460025
MD5	65e18bae9b8c42b63bf3b969d3cdb6ca
SHA1	de1e804c81536890bccc963920095ade140b5173
SHA256	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955
File Size	14.97 KB
Report Created	2022-09-21 09:24 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (9 rules, 13 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) 66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #1) 66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 120 files by appending the extension ".paradox".			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
3/5	Network Connection	Connects to a CMS hoster	1	-
	• (Process #1) 66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe connects to a hosted Wordpress site at https://media.threatpost.com/wp-content/uploads/sites/103/2020/01/03130357/ransomware.jpeg.			
2/5	System Modification	Changes the desktop wallpaper	1	-
	• (Process #1) 66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe sets the desktop wallpaper to the file "C:\RDhJ0CNFevzX\wallpaper.jpg".			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) 66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe enables process privilege "SeDebugPrivilege".			
1/5	Network Connection	Performs DNS request	3	-
	• (Process #1) 66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe resolves host name "en3ez7v505kx8.x.pipedream.net" to IP "-". • (Process #1) 66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe resolves host name "www.google.com" to IP "216.58.212.164". • (Process #1) 66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe resolves host name "media.threatpost.com" to IP "13.226.153.98".			
1/5	Network Connection	Connects to remote host	3	-
	• (Process #1) 66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe opens an outgoing TCP connection to host "13.226.153.98:443". • (Process #1) 66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe opens an outgoing TCP connection to host "216.58.212.164:443". • (Process #1) 66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe opens an outgoing TCP connection to host "3.228.107.54:443".			
-	Trusted	File has embedded known clean URL	1	-
	• Extracted URL "https://translate.google.de/?hl=de&tab=wT" is a known clean URL.			

Mitre ATT&CK Matrix

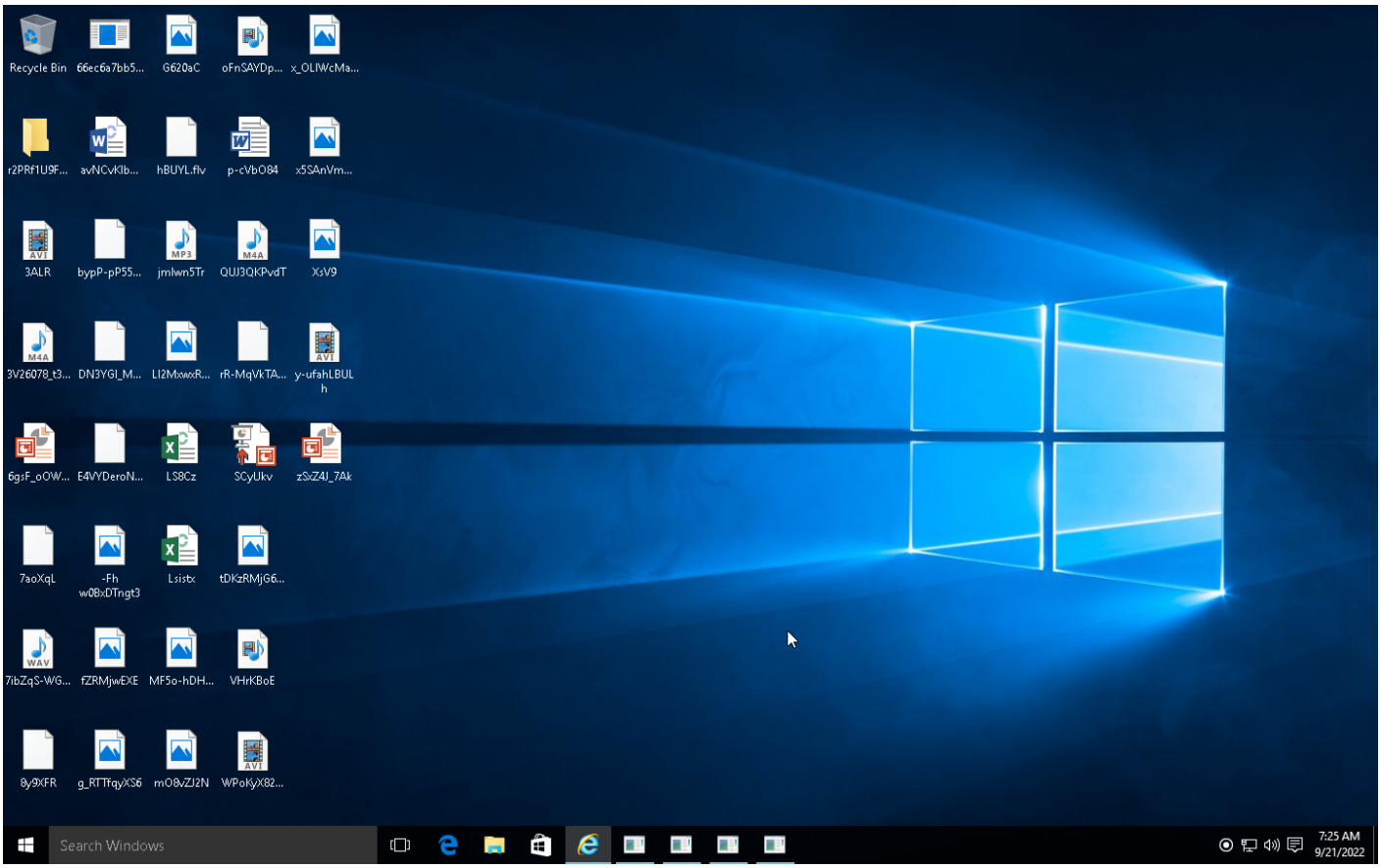
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
											#T1491 Defacement
											#T1486 Data Encrypted for Impact

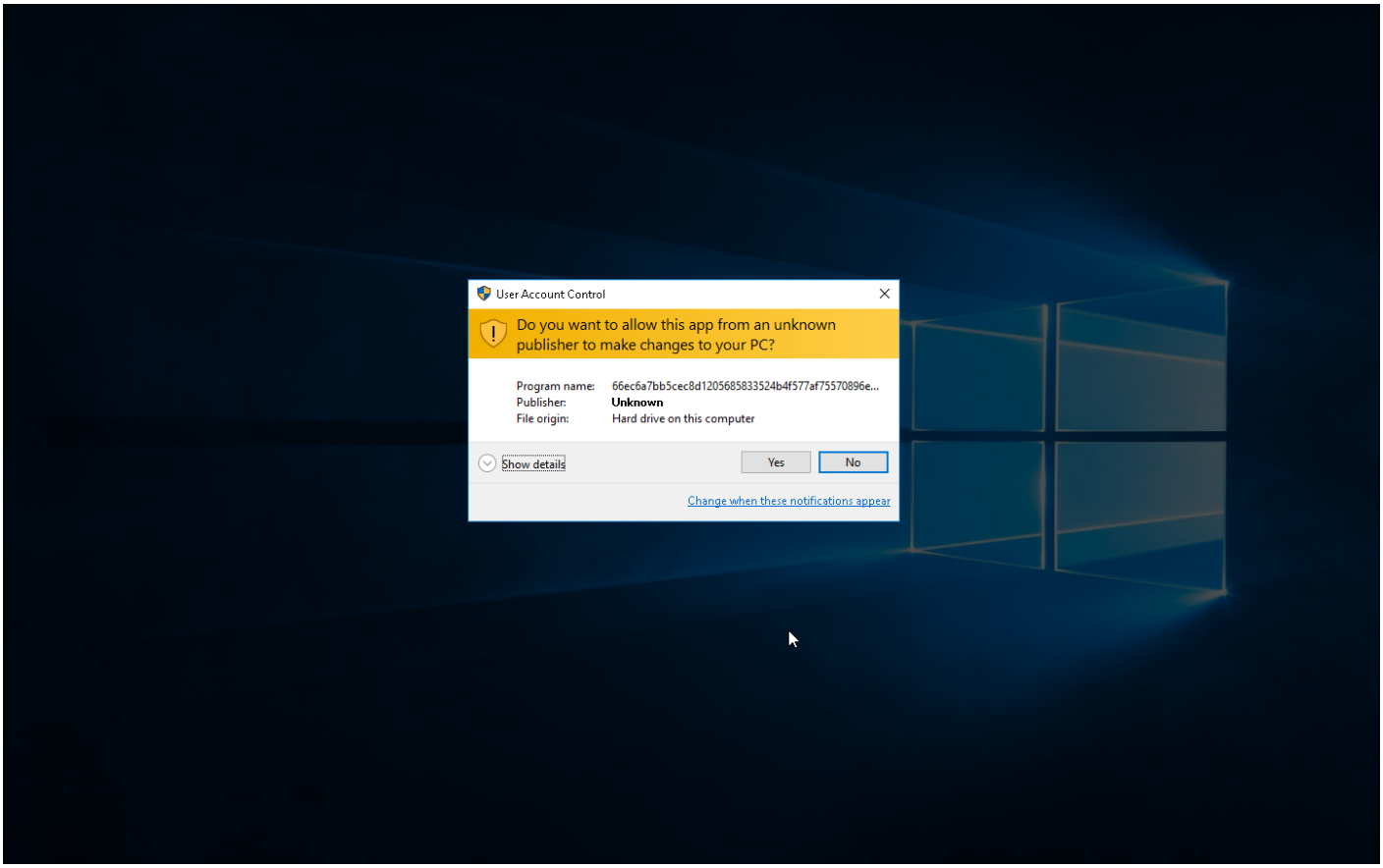
Sample Information

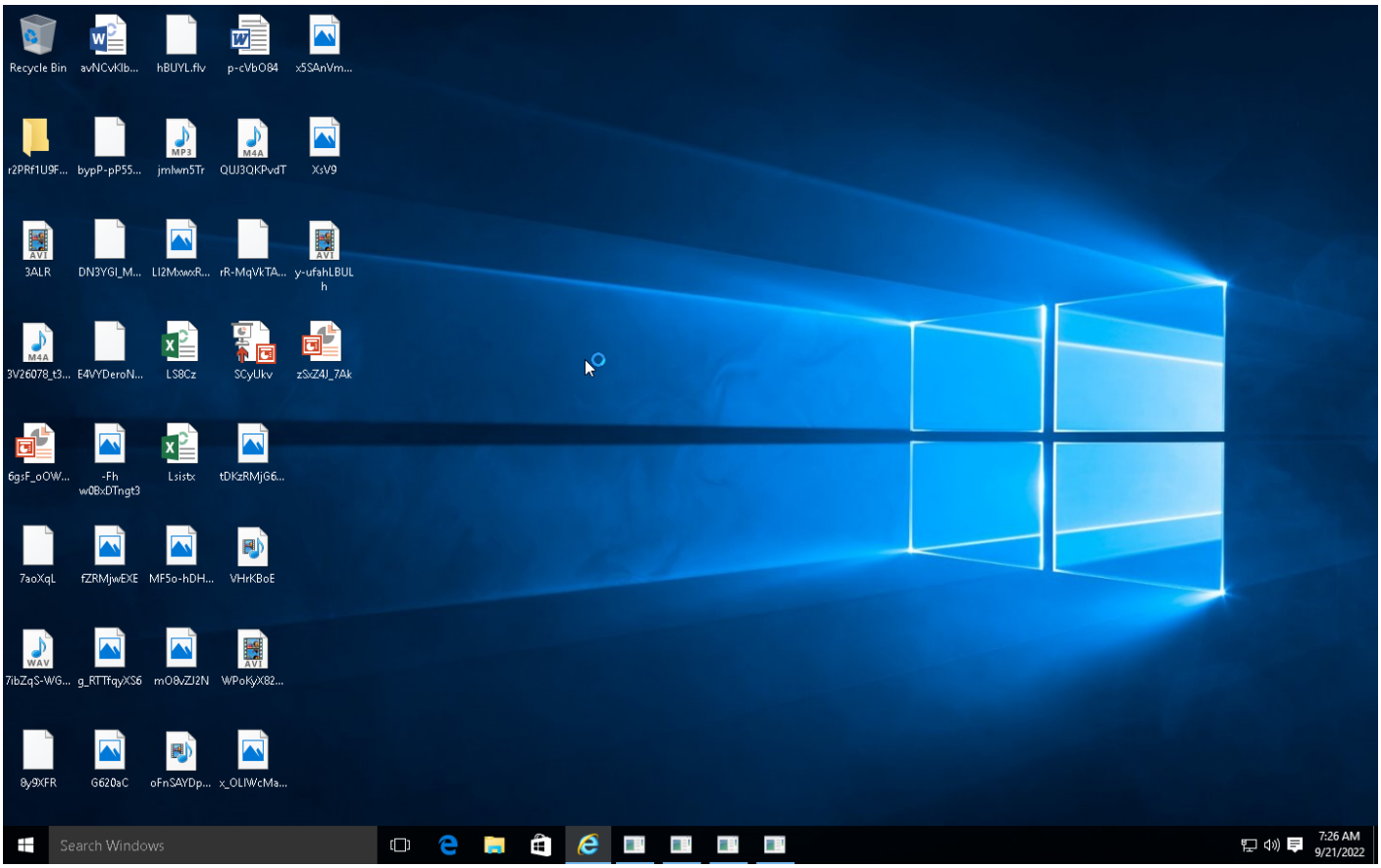
ID	#5460025
MD5	65e18bae9b8c42b63bf3b969d3cdb6ca
SHA1	de1e804c81536890bccc963920095ade140b5173
SHA256	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955
SSDeep	192:VwmJXzXNuc0T+IKdOdabU2iB8CXg6Sm/hlVN4nLnC/31im5ccz5a86IoIfVp1Us:Km5+bU276HzV2nLKlXBEltfV4s
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe
File Size	14.97 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

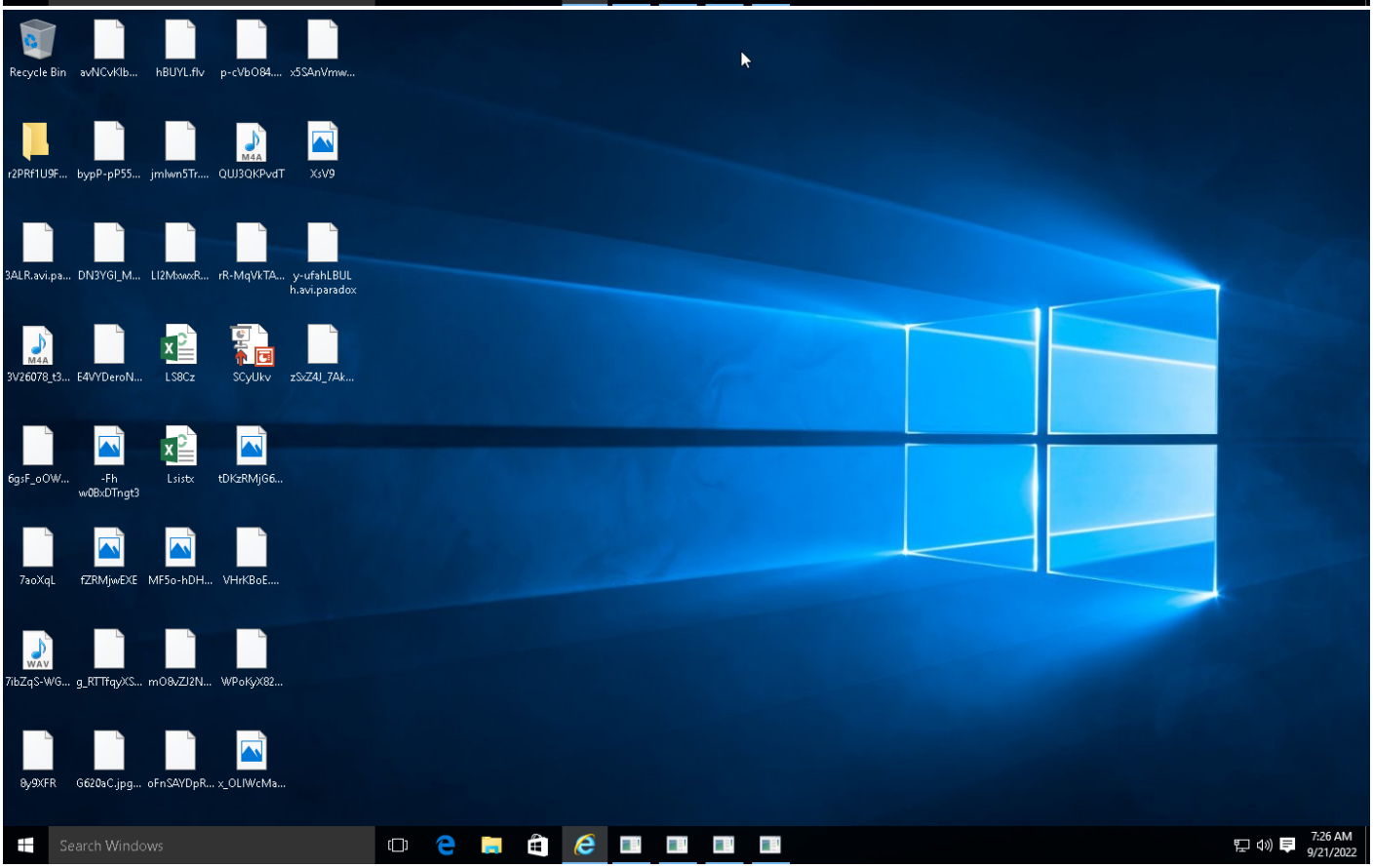
Analysis Information

Creation Time	2022-09-21 09:24 (UTC+2)
Analysis Duration	00:01:26
Termination Reason	All processes terminated
Number of Monitored Processes	1
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
66ec6a7bb5...
G620aC
oFnSAYDp...
x_OLIWcMa...
r2PRf1U9F...
avNCvKlb...
hBUYL.flv
p-cVbO84
x5SAnVm...
3ALR
bypP-pP55...
jmlwn5Tr
QUJ3QKPvdT
XsV9
3V26078_t3...
DN3YGI_M...
LI2MxwxR...
rR-MqVkTA...
y-ufahLBULh
6gsF_oOW...
E4VYDeroN...
LS8Cz
SCyUkv
zSvZ4J_7Ak
7aoXqL
-Fhw0BxDTngt3
Lsistx
tDKzRMjG6...
7ibZqS-WG...
fZRMjwEXE
MF5o-hDH...
VHrKBoE
8y9XFR
g_RTTfqyXS6
mO8vZJ2N
WPoKyX82...
Search Windows
7:25 AM
9/21/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 66ec6a7bb5cec8d1205685833524b4f577af75570896e...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

5.40 KB total sent

348.49 KB total received

3 ports 53, 443, 445

4 contacted IP addresses

28 URLs extracted

2 files downloaded

0 malicious hosts detected

DNS

3 DNS requests for 3 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 2 servers

3 sessions, 4.35 KB sent, 342.16 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://video.google.de/?hl=de&tab=wv	-	-		0 bytes	NA
GET	http://www.google.de/history/optout?hl=de	-	-		0 bytes	NA
GET	http://www.google.de/preferences?hl=de	-	-		0 bytes	NA
GET	https://maps.google.de/maps?hl=de&tab=wl	-	-		0 bytes	NA
GET	https://photos.google.com/?tab=wq&pageId=none	-	-		0 bytes	NA
GET	https://apis.google.com	-	-		0 bytes	NA
GET	https://drive.google.com/?tab=wo	-	-		0 bytes	NA
GET	https://mail.google.com/mail/?tab=wm	-	-		0 bytes	NA
GET	https://accounts.google.com/ServiceLogin?hl=de&passive=true&continue=https://www.google.com/&ec=GAZAAQ	-	-		0 bytes	NA
GET	https://lh3.googleusercontent.com/ogw/default-user=s24	-	-		0 bytes	NA
GET	https://lh3.googleusercontent.com/ogw/default-user=s96	-	-		0 bytes	NA
GET	https://www.blogger.com/?tab=wj	-	-		0 bytes	NA
GET	https://calendar.google.com/calendar?tab=wc	-	-		0 bytes	NA
GET	https://play.google.com/?hl=de&tab=w8	-	-		0 bytes	NA
GET	https://news.google.com/?tab=wn	-	-		0 bytes	NA
GET	https://docs.google.com/document/?usp=docs_alc	-	-		0 bytes	NA
GET	https://www.youtube.com/?tab=w1	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://www.google.com/finance?tab=we	-	-		0 bytes	NA
GET	https://www.google.com/setprefdomain?prefdom=DE&prev=https://www.google.de/&sig=K_ZHphx3Bg0wcMwtFW0rN51J6FWWc%3D	-	-		0 bytes	NA
GET	https://blog.google/intl/de-de/produkte/suchen-entdecken/kraftstoffsparende-routen-google-maps/	-	-		0 bytes	NA
GET	https://books.google.de/?hl=de&tab=wp	-	-		0 bytes	NA
GET	https://translate.google.de/?hl=de&tab=wT	-	-		0 bytes	NA
GET	https://www.google.de/intl/de/about/products?tab=wh	-	-		0 bytes	NA
GET	https://www.google.de/imghp?hl=de&tab=wi	-	-		0 bytes	NA
GET	https://www.google.de/shopping?hl=de&source=og&tab=wf	-	-		0 bytes	NA
GET	https://www.google.de/webhp?tab=ww	-	-		0 bytes	NA
GET	https://www.gstatic.com	-	-		0 bytes	NA
GET	https://www.google.com	-	-		0 bytes	NA
GET	https://media.threatpost.com/wp-content/uploads/sites/103/2020/01/03130357/ransomware.jpeg	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	en3ez7v505kx8.x.pipedream.net	NO_ERROR			NA
A	www.google.com	NO_ERROR	216.58.212.164		NA
A	media.threatpost.com, d2x8sklh0hjsql.cloudfront.net	NO_ERROR	13.226.153.98, 13.226.153.2, 13.226.153.79, 13.226.153.42	d2x8sklh0hjsql.cloudfront.net	NA

BEHAVIOR

Process Graph

Process #1: 66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 70676, Reason: Analysis Target
Unmonitor End Time	End Time: 147526, Reason: Terminated
Monitor duration	76.85s
Return Code	0
PID	5000
Parent PID	1648
Bitness	32 Bit

Dropped Files (123)

File Name	File Size	SHA256	YARA Match
C:\RDhJ0CNFevzX\wallpaper.jpg	270.87 KB	5a0f1bee7543cc12a19a01b79774ea07f1b5499823e6ccbc69f13109811f6b6b	✖
C:\Users\RDhJ0CNFevzX\Documents\BS18p.pptx.paradox	11.28 KB	9c85f1aea919253002c46a273591f78a8a96c9d14accb77d5afb0e430040c26c	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\afV1uedQpAS.jpg.paradox	8.33 KB	459d2439ff70d66ed0a193272d20a2663735d12462ed83e678f1b5dfce8c7092	✖
c:\users\rdhj0cnfevzx\desktop\6gsf_oowdub.ppt.paradox	72.47 KB	2fd288b109d353fcb7a533e0a5f31da232a35d48eda39df0482021dc020ca046	✖
c:\users\rdhj0cnfevzx\videos\bjumhphwyeayyo.mp4.paradox	15.67 KB	57ae662cbcf60a1d5e3bfd82a42ce12e30520edd18e72a1325d88d22322d5f76	✖
C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\zJcxa5nxH\NB7uoxXXE8jGPi9mjkAl\X-s1lcrQ8YRADHirKDU.mp3.paradox	59.56 KB	7d9bdc88f0e46dfcd1f8807812af009d2e4bc279e42145c657323edbbeb742a2	✖
C:\Users\RDhJ0CNFevzX\Videos\-cAxiI.mp4.paradox	85.98 KB	59488544f7c7073fa11c4a83953916430f13895280c90dec9365eeff17161401	✖
c:\users\rdhj0cnfevzx\documents\a8etnoann.pptx.paradox	58.12 KB	dc257e671d93f00267a8b1207e6d30cedfb7ca33de2df5d0f585273ea02d1d2e	✖
C:\Users\RDhJ0CNFevzX\Documents\bxkuQ7Rq0NwFlu_.xlsx.paradox	63.20 KB	659f2a05ba6841e28dd5a0810a0ab6a300bef5ff51ddb224327345e69dc1aaf2	✖
c:\users\rdhj0cnfevzx\desktop\wpokyx82om8q4ed.avi.paradox	13.72 KB	38416e4893e516c719afb26abfd25e3c7d8189ea6a5c2b6c97efbc9fb3bc5f9d	✖
C:\Users\RDhJ0CNFevzX\Documents\mQx7YPEejtyQadEX8L.docx.paradox	23.95 KB	f5415b69e38be94519ef0a39284799e6120aa154b21f5c9660703f449555d29b	✖
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\QHmblmZbOvDP\mSyv2w.xls.paradox	3.66 KB	e031084b05c7d01d6907ba39c4404d8b1bbc19d8d6a3f1e4ee15c3bcec8b6d34	✖
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\MjBQf.csv.paradox	63.66 KB	fdd7b577b14e9ccd7b32ea9673217c34e2270c22a7bb8fd802a815662bfc654a	✖
C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\zJcxa5nxH\KbKeXzFPaOL6PVtTCqk\GlHGlizt9V.mp3.paradox	6.50 KB	c6ce2208505f65aacb34ec3bd6c87467fb32e61bfa7109caab60fc7a02f65ba1	✖
C:\Users\RDhJ0CNFevzX\Music\LOcciO2KhP5kfwX2op\Vxx1vR6KrqxFVGqkI.mp3.paradox	8.53 KB	cd5218ff43ed2fe83aaf014982be2eb67a8023e761ac281fd7c62fdcc1d27eb1	✖
C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\dXYm4e1-8H.jpg.paradox	55.12 KB	9c9d6f0e9a82cccaffc4f90a0c27c135cfab6b765fa104544b12d549206c3eae	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\Tq-PzJp1KCl6Fslt9az.jpg.paradox	68.33 KB	89f1cc2e3e0871de6661f823bcf41d936e70c9e4cf59d9f19c1d25f2cdfb478c	✖

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Videos\DJ9dTzhHBcmwI.mp4.paradox	17.16 KB	0248f8454f75ce6eda9c656a5fc4acb2a4db0f91197d4257481a7c7d302e175f	✖
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\WrmtmocH.rtf.paradox	20.95 KB	bfc7390af294816a888a741b3a9b1b9c24a4362f8d7b0fa591f2db9b3a889225	✖
C:\Users\RDhJ0CNFevzX\Videos\BoiFgH0vw1T6k.mp4.paradox	45.64 KB	b14e8d51807a961b080eb56c7e0651493b6677e20e9aa48ec2a89ed5938a3953	✖
c:\users\rdhj0cnfevzx\videos\2ivawd92lo3sa8a.avi.paradox	69.69 KB	c196b6fb25bbed289eb7d693ff6413795bae3a03132fd1c49769347b6438f7aa	✖
C:\Users\RDhJ0CNFevzX\Documents\iBJ0lud-.docx.paradox	38.47 KB	d2b05b1efa862f92953a0b7b96ea15adb07e7eb995c292dbf9b139dbcff138c4	✖
C:\Users\RDhJ0CNFevzX\Videos\51mUVK4.mkv.paradox	57.55 KB	c13c59feb5f2fb5124024e8fdec69e85f700bc46ec5eab3ca80ab0ed91043aa7	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\8MdVti1_bQ.bmp.paradox	31.31 KB	989b284a46c460ff82bed14ac1eb79a2f576846e238f204ade451311a6b8e736	✖
C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\lnmC0XMyDQ9.jpg.paradox	84.53 KB	dbc134414b67216a9781a276074dbda3f2ebd881cf9acb3eb2e531c94e83844b	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\5EFkJZZxsJD.bmp.paradox	53.03 KB	5e4f381c7a048033641251154bf9a1cd438855be66c1749a7e9f932410bdc7dd	✖
c:\users\rdhj0cnfevzx\desktop\g620ac.jpg.paradox	72.97 KB	d14ad5d2d1e9e8f758aa59cea6257bb3852ab8b0437ca517fd736631ab655896	✖
c:\users\rdhj0cnfevzx\pictures\grg40lzkz\gj7zisxgu3qt22qtqmq3.bmp.paradox	67.44 KB	5a65c16a50cc5beddeb97b2a8a64f4422d6c3f96801cbc284ad72cc6dd0b09c8	✖
C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\XGbXp3C5lHRkkh6wQq.png.paradox	15.38 KB	181118868111c3b2d5c0abac1fe0d0cbe5cfe2f27ad22edfca84c15c541d09f0	✖
C:\Users\RDhJ0CNFevzX\Documents\VGfbvj_4ydSGlCX-gZ2F.doc.paradox	43.28 KB	e8a677cf242e2e3012623c302edbec74c4e678645f0524a1bc09e6fccde18220	✖
c:\users\rdhj0cnfevzx\music\7kmdfrdw\zjcxa5nxh\34k8hu-8.mp3.paradox	83.27 KB	cf934a1a28bd8cba651fb7227357f5f3ea8fee990748630703f62de713631afa	✖
c:\users\rdhj0cnfevzx\documents\bmrg6ivdxlyg.docx.paradox	64.73 KB	efea52137a720b79b3de8238729bb9e5983e1ec18858d773f26ade265807984c	✖
C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\qmD8S.jpg.paradox	7.05 KB	ec0adb4cc6de1cfab0790b86fe2b19252c96b85cbfd1fbbff554ba07c5b9fb3d	✖
C:\Users\RDhJ0CNFevzX\Desktop\mO8vZJ2N.png.paradox	30.52 KB	2dca734c8344212468dc0e709573e30cf1c794ce62883aa092875551df224a8d	✖
c:\users\rdhj0cnfevzx\documents\rbybf.xlsx.paradox	14.59 KB	2945576e77b9b61fe170f40eccec4a629ae0d6159dbd3af624cea4c57151f730	✖
C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\w2yJe78igCw.bmp.paradox	79.64 KB	d2bbad53393bda1703c8e9d4a8254cbb13b5acdcfceedd374ddfb15aa3bde59e	✖
c:\users\rdhj0cnfevzx\documents\iho0bqr\yiwvx.xls.paradox	77.80 KB	f0d818c2ae2c349084a923bdcda1bdc0445fa7b82ad274dc3fb6ed99fba8fd82	✖
c:\users\rdhj0cnfevzx\pictures\grg40lzkz\ooloeayy74zgh4\1q19rg6lpi7qsur.jpg.paradox	74.00 KB	58f7526198b64699cf80985a3797e9f8da776707985c69a903dc3bc095e5b1c9	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\OoloEAyY74Zgh4\0gPNtabbl3ZU6Tj.png.paradox	68.98 KB	019d87b7a4799be5f343b1a45f4a8a46e20c4dae7a1812868933cdd27b72d822	✖
C:\Users\RDhJ0CNFevzX\Videos\B7N7KqDrR.mkv.paradox	70.52 KB	c8631d245702cc73be9f22153af690b2b8fc534ef1f9d8939791109fc58d7701	✖
c:\users\rdhj0cnfevzx\documents\jvyz5g.pptx.paradox	79.44 KB	e2271c3ef87548f28b9e4802351d9239ddd17b6ad1480af0a95607b99439453c	✖
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\gXAZTSzU cdzSa7dD9\nYbgdcIRhW1rqJ.xls.paradox	62.09 KB	f97c1a06dc1a2d83db3c5e90a11d0e9ad6a8f0abcc6f1a0d01a0ceb2f7a4004a	✖
c:\users\rdhj0cnfevzx\documents\lqrcfpqe87lzqn.ppt.paradox	74.22 KB	4a2574153b24e0ec2b3df2396e03fd4fdea2c27cba5fc74a5ebe3b4b4197e157	✖

File Name	File Size	SHA256	YARA Match
c:\users\rdhj0cnfevzx\pictures\grg40lzkz\d6g892w9ejaoqh6ubp3.bmp.paradox	21.09 KB	eeeae6f8d62b264810db18bf26b1fe24b964bc570e9fad7d8c2e329ecdbee3db	✖
C:\Users\RDhJ0CNFevzX\Videos\CPp1byDqsSfWme.mp4.paradox	15.09 KB	d4e1561c69568c7689338105e7a64bb56ce07e5c91b692914641908b698efad6	✖
c:\users\rdhj0cnfevzx\pictures\cdvsbna\uim5.png.paradox	48.95 KB	1115f963b40d41453dbd9354d58c885d0b55dd4b72b034395f9117cb3b19b57e	✖
C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\CdIpDdd5KAfj8fH3OK3.xls.paradox	88.89 KB	080a18878545119f0939531b7724333fd0b43ff942b33f029c986810142b5bdc	✖
c:\users\rdhj0cnfevzx\documents\lfdjxcuknymx.ppt.paradox	83.58 KB	1aa9f475db6eeec39387c8eef6a2a6e0cf7bde1df16f7d4bc6fd9544f9606130	✖
c:\users\rdhj0cnfevzx\documents\iho0bqr\zl803n95eqjd1.doc.paradox	98.61 KB	636f7c42011053f3de50e8ab6643563787ab05ca6c441114ce3bcde8702c4f42	✖
C:\Users\RDhJ0CNFevzX\Desktop\READ_ME.txt	138 bytes	d9fa129ac7725d6d37f985054cc7434c48188726baa05d71141006afd1c9e60c	✖
C:\Users\RDhJ0CNFevzX\Videos\85VAmns.avi.paradox	51.67 KB	4ee1cbfb959d99bbd6e1acec88c5b50db8807f90f34af5642ed3ed66c681f51f	✖
C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\sipKm5LRXD_iepz2cq.jpg.paradox	87.58 KB	18b7238c671e6addce46ccc30435beaddc4490bfb171e51af00c0245f15ac67c	✖
c:\users\rdhj0cnfevzx\videos\a7_2itm9fk.mkv.paradox	21.73 KB	7d8dfb762ec845cf0b61d90788e1ab1cfee1f720b7ab51569a094fce707e7c43	✖
c:\users\rdhj0cnfevzx\documents\equm7or1t3w19x6ke.docx.paradox	76.38 KB	3f6c5aea0ee89e7633cc9669b4d3de76892858dc202366d71b432c69185ca211	✖
c:\users\rdhj0cnfevzx\documents\c9b91yr5nnhgvskp8es.pptx.paradox	16.47 KB	c286f898c2b7a6c04f33cd2da207f1e61d830cd404fea4d6611ee1d6f534705b	✖
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\bV9qL.docx.paradox	66.38 KB	23140e720e5c2e69e50fdd9b242a30612b88ff7b0d876721cca103a9460ae4b6	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\uG 0XjLM.jpg.paradox	88.77 KB	ea7bac26ace714529e19210bac6aed42e4682a6e7af488d13b49ec945366cdb7	✖
C:\Users\RDhJ0CNFevzX\Videos\kJaRIROETbuz_IQQ.mkv.paradox	49.38 KB	8e767b2ab7ce8b1cc26238d9fb21e6cb4a5a0cab0b59665b52551929f9a9ed6c	✖
c:\users\rdhj0cnfevzx\desktop\g_rttfqyxs6.jpg.paradox	95.73 KB	bc5e2372af59ee6d8deb21745a2172d61811027e7453cef1d80ec67634a58153	✖
C:\Users\RDhJ0CNFevzX\Videos\KbDpI-xXRv_7VEG.mkv.paradox	67.92 KB	c04f2793884a523392493ca987384af5571f214cd7b6cbd48455e5cc299935cb	✖
C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\lu7q0VmcZ_G6Dq.bmp.paradox	57.45 KB	31fc65f844bb0d088825149c4e9695af0e4233b74c527cf6818135971604a8af	✖
C:\Users\RDhJ0CNFevzX\Videos\zGMZOxL0WD.avi.paradox	61.11 KB	73cba56ce996b4c11c51d5ae848d38cf671a6cbd8f07050e82e26d7e5578eacc	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\OoloEAyY 74Zgh4\On_Q970XJbNE6EtRfPN.bmp.paradox	78.47 KB	3d580b9e4c277091029dfb523570a2d47f1094a2b2162b9a3183caa2bcabb881	✖
C:\Users\RDhJ0CNFevzX\Videos\23WDO ZYI.avi.paradox	60.38 KB	b8327e9e9c6c65653d1a2e4f551b8034fe35e0a4fd66d1e87424ecfcb3f1dd09	✖
C:\Users\RDhJ0CNFevzX\Music\LOcciO2KhP5kfwX2op\bhpdCMF2_qxg\YUU6tBaYq0t.mp3.paradox	21.36 KB	cfdb1fb10910b521b5630e4e47be1e1f32226bf7e6cbc95052a2c4faa5422999	✖
C:\Users\RDhJ0CNFevzX\Documents\Axeso-6WCbUVjz.xlsx.paradox	95.50 KB	6cd8ac5f4f81619146ace8ba383b589afbdc224d76682a355969d2d48b1fd400	✖
C:\Users\RDhJ0CNFevzX\Documents\Udu1XE4Hd0I8gwhDhX2.odt.paradox	87.09 KB	2f9e7761b0790d938073bfb0ea9d4a8e9b3b18a9f8d63e67a6b1bd7ba379c592	✖
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\NxW3d3OjYtrQDUX.pptx.paradox	57.09 KB	725245244785de23c24b49d981b4fdeb6c806baca19354e24442a4c095de1e7a	✖
c:\users\rdhj0cnfevzx\music\loccio2khp5kfwx2op\chzujdwb.mp3.paradox	89.77 KB	4d6c326972292276a4c727706a4d59aea1929a66f108412301925baa10b0c77a	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\hD6 t-A2anl.jpg.paradox	27.39 KB	35686fdba7b521571ce0a5b39af7d3186efb74b22c220f16ce9a2fee85f8a55b	✖

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\OoloEAyY74Zgh4\WQWnpehTBFCALVb.bmp.paradox	14.80 KB	20cf6677a4a830a294fc9ff17b651db656149cc9d5a2b9132133e2122c84616f	✖
c:\users\rdhj0cnfevzx\desktop\r2prf1u9fnysjo7qvmv\ihb.mkv.paradox	50.00 KB	168462ab9f6fadabda24cbb734766ee67d510c4f3c0160a8f4632e48851ede52	✖
C:\Users\RDhJ0CNFevzX\Desktop\avNCvKlbZERjJ6.odt.paradox	56.75 KB	f049ef2889f4cc58d2f5d771e87c920322bdef7a6ee767631f75a169142db908	✖
C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\0ltsVjI3Z5uTF3b.mp3.paradox	68.02 KB	e871433d224d3a181fca60351a69fded476b14c1b5500f744386b9b393e562d5	✖
C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\zJcxa5nxH\xow2-jtbjjD9\uFm6gFL_KjdhgP.mp3.paradox	68.20 KB	94904df68c428f0a47ccf12ded46a05e1694c41d4b3adb4244e5feab897422fd	✖
C:\Users\RDhJ0CNFevzX\Desktop\zSxZ4J_7Ak.ppt.paradox	66.83 KB	4bf36c17e3e47cfb6b9eb27a644ed456f44b75a96a29e78bc78c56974e391c17	✖
c:\users\rdhj0cnfevzx\videos\vlzh24-yjiutkgunnug.avi.paradox	47.62 KB	8b24a1cea75cb4e7d6621f7516eaf46aae46198b064c1826cdeaf174ee6c2611	✖
c:\users\rdhj0cnfevzx\music\7kmdfrdw\zjcxa5nxh\nb7uoxxxe8jgpi9mjkal\buigcjetpjo.mp3.paradox	87.88 KB	1346f74c749874146f1f4a0fbe4d4a8989e3f2f893f9cf76d9a50dad5f6f3b4d	✖
c:\users\rdhj0cnfevzx\pictures\ssva9xc4 h39.jpg.paradox	56.75 KB	6da8d5fc30c85ef923295ba5b855ad20c525b1e87e9db7e53bde6592c43a6eaa	✖
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\gXAZTSzU cdzSa7dD9\hAG8_BLENEWKevuN.pptx.paradox	79.66 KB	f8aa5e8d924bf5670dee190a44cc6bb6c22d401c08aee5983b5678f0134f8df4	✖
C:\Users\RDhJ0CNFevzX\Desktop\VHrKBoE.mkv.paradox	90.83 KB	e3f6fded6759b5a1caf0231977527b94173aec748a3ecee7d4d984d2a4852e92	✖
c:\users\rdhj0cnfevzx\pictures\grg40lzkz\3 pbelo2sufc.png.paradox	58.14 KB	d59f99aee8c962f618b0bafdd07b27263cb4dd282a09634c359649c01a019610	✖
c:\users\rdhj0cnfevzx\documents_p4fctiw.xlsx.paradox	36.20 KB	6a8b51605f148496b0db99f48cb3daf3a8c6e2819c06617432be01650e2ded37	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\MEHNk_Kk\XzYboTZ.png.paradox	78.05 KB	4432ac296f6497b31731a795a9327f8fb4b121a3fa30ae73578efef044bdc0d1	✖
C:\Users\RDhJ0CNFevzX\Links\Downloads.lnk.paradox	992 bytes	c81700334d04995faa698d5954baf31769e4a3712c1a403ae1339e3e1e86bbff	✖
c:\users\rdhj0cnfevzx\pictures\cdvsbna\ysw39t6l-twgke-iut8k.jpg.paradox	27.05 KB	70fc788511e8ee723b6f23406a2432c2af402c591ba6583cf82f918c0675c026	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\xbnzj.bmp.paradox	79.19 KB	7e27ba0d572b29543e7cc8f83154adef5ffcada5b291a4548fb52754ffa13fe8	✖
c:\users\rdhj0cnfevzx\desktop\ll2mxwxrhwpc2d.jpg.paradox	97.44 KB	d8945e92a1d6731d7bec984291db328f7dcb6855b2605a6497304c22c6f691bb	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\MEHNk_Kk\otYR0bcDOHhVdwK.jpg.paradox	70.80 KB	50af6fe9f65721c166385fcb3ee48d34643a67ab68c7b5be272cf207940af16c	✖
c:\users\rdhj0cnfevzx\documents\iho0bqr\uzvi-cud-zha-\gxaztszucdzsa7dd9\mousogoar.odt.paradox	80.09 KB	d071867ccbf81309b79138af6fc9a7cc98f736c50513ad6fbee40962019a06bf	✖
c:\users\rdhj0cnfevzx\pictures\qwlzs.bmp.paradox	22.83 KB	0ff7bbdd5cb87c1314e3efda75ebf9ea55eee1a67c20f7da3964df097c286de1	✖
C:\Users\RDhJ0CNFevzX\Videos\4DG-or0-b.avi.paradox	44.78 KB	e729ddc5de1c41f3fc0201a279c3ca19acad69370b944a4656769826091e2b1d	✖
C:\Users\RDhJ0CNFevzX\Videos\c_1zZ88519M.mkv.paradox	13.83 KB	c8cedc88faebb214cc419584c834cd351481d50bebc1ffe4a7cbe527598ad075	✖
c:\users\rdhj0cnfevzx\videos\jtmnbzore3sk2mh.mp4.paradox	51.09 KB	335a457d58599725bbfd21437fe23e7dee7626bedad25d5175169229f151711b	✖
C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\8uC8KGTO2.mp3.paradox	23.47 KB	4c88a1be124469b26fbb8b1a40a63401cdbdf880beba32d5614fad8b5ee0f9e4	✖
C:\Users\RDhJ0CNFevzX\Desktop\x5SAnVmwCY.bmp.paradox	57.55 KB	b3c9b0b35b02dcef8693dea8c3136e61a8502896013332496 3e2f39df22db600	✖
c:\users\rdhj0cnfevzx\documents\iho0bqr\d4afyfsf.pdf.paradox	75.48 KB	e7e0d744af3a0f3ce71a55b5449ae19fd865ec1bde4606326bee2669ec1c23cc	✖

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\p-cVbO84.doc.paradox	25.86 KB	450d7651105ded3a58622c19964515c92f98ffb84a1346e428bb3cc9b1645a52	✖
C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\LykQr.jpg.paradox	62.94 KB	082d4dbc6951f8fb9b84e019657f59d8e73da61b3171eeae441b5580b5c43831	✖
C:\Users\RDhJ0CNFevzX\Documents\dAFINowb06QqRO4uOt.docx.paradox	1.80 KB	120db168df996c228b8b57c2c20dff3d84aa9064db72c6123ede86324f677489	✖
c:\users\rdhj0cnfevzx\documents\xib 5.pptx.paradox	24.27 KB	ec7b9f4e7d9a0daf2988728998065fdaf5383ca9de781b3266d0b05d0d531c52	✖
c:\users\rdhj0cnfevzx\desktop\jmlwn5tr.mp3.paradox	34.91 KB	9c5146eff3d2cfeb01456845afce842dc6c364c64a59ac0aed1ee1c7c7c3d6df	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\xS_92T-iMJ.bmp.paradox	9.16 KB	698b380664ab3f33b5d614b9a05c392801baa2020ee2238eff77e3d153888313	✖
c:\users\rdhj0cnfevzx\pictures\grg40lzkz\mehnk_kk\g-jrstvi0xfw.bmp.paradox	93.56 KB	30852a59b57014c2dc471d79776e3456e1d41522029986f5e6f1d4b50791c208	✖
C:\Users\RDhJ0CNFevzX\Videos\Ue6Gzt3lTeB7E.mp4.paradox	13.78 KB	a0f93220e43c84e7e51f121830e0d2eab14094a2bd533e8ca1b42aa4d035af5a	✖
c:\users\rdhj0cnfevzx\documents\iho0bqr\pm-yxcrz5dlv.csv.paradox	77.95 KB	2c94e644813ee226baf70cd5d6a18184201ba1fd79b41545d2e706b62a22784e	✖
C:\Users\RDhJ0CNFevzX\Videos\voHnl GNKaLfJq0z.mkv.paradox	74.05 KB	5fbde2e4c61b652ff203d938fb15c8758bbe4c6334566dcc35cf8f4e3e30a9f8	✖
c:\users\rdhj0cnfevzx\links\desktop.lnk.paradox	528 bytes	de007681989f36f81abe8a692dc0ac9eb7e7b42097dfabe4e4430017161006a3	✖
C:\Users\RDhJ0CNFevzX\Desktop\3ALR.avi.paradox	97.91 KB	fa935a077b87c97d5c3c779208f40ad3d16fd934e7c4d6e2a2edcd88586d1bbc	✖
C:\Users\RDhJ0CNFevzX\Videos\W1H9qw8y.mkv.paradox	35.08 KB	4895e9ba2ded9ee433eb76154f92a2b2dca80c348f27eedbf6600718d60a0079	✖
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\8 N3.docx.paradox	24.36 KB	f7bd6db8df52ba1a2cfdcc6dbd6fbd0b7fbbdc360abe3d4c3f8b2931bcae23be	✖
c:\users\rdhj0cnfevzx\desktop\ofnsaydprzb46.mkv.paradox	68.45 KB	859ec1c090b214c8eb6740a7efe4370da0c61b0407e57328f22537b4068b3002	✖
c:\users\rdhj0cnfevzx\desktop\r2prf1u9fnysjo7qvmv\moljpyipfv.jpg.paradox	61.59 KB	65dbb09bd7c4e6880c080e75c83e144835f697f9321db82968f3493ea06435f7	✖
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\93rPWrjGSl.jpg.paradox	81.42 KB	0626213b982abfdf90dc619ae1442fbf8c6629a4cfbfb856bd62c1be873871a4	✖
c:\users\rdhj0cnfevzx\documents\ixibdt gx.docx.paradox	38.33 KB	cb2ac6a1af9a572046d49e653e85196b43f19c8b690979fdcee45ea45c33aaf5	✖
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\gXAZTSzU cdzSa7dD9\Fd2XhevfRzd.odt.paradox	15.38 KB	b9109acade865bfeebc18315eaf188a3a911908124ad17f42bf6043ee2f2bb4a	✖
C:\Users\RDhJ0CNFevzX\Documents\DoE cR5.xlsx.paradox	39.67 KB	7cf8c2e6df2d2169dfe13c2bc56f0d3c34bbbbf8a720730055df8eef40595e44	✖
C:\Users\RDhJ0CNFevzX\Desktop\y-ufahLBUL h.avi.paradox	48.92 KB	86067e67b91c39503d370788eff82898b34a1465fbb2262313d3f398278cad0f	✖
c:\users\rdhj0cnfevzx\documents\pzrq3ttlp58bkco.docx.paradox	39.11 KB	e5703d02884387de0a0381167499beb8781ecacd938ea8659f907683d3192497	✖
C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\LbG_zixT9ffs2A.bmp.paradox	78.45 KB	db3d36c5a38ca189f8db2a287639bcdfa8d59270eff49387f24675b37ff37db7	✖
C:\Users\RDhJ0CNFevzX\Videos\A-MC1ceN9T2G9.mkv.paradox	60.56 KB	7424e1e089532598d76d0a75b90293e75ef7663863452a52352187e12195510c	✖
c:\users\rdhj0cnfevzx\music\loccio2khp5kfwx 2op\rez9jflaxipy.mp3.paradox	58.91 KB	2c17502ed3a6775b717898c681e20f152bbd3e668f282cfda8dee954aab21dbc	✖
C:\RDhJ0CNFevzX\Rand123\local.exe	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Registry	35
User	2
System	68
Module	37
Window	26
File	1572
-	10
Environment	8
-	4

Network Behavior

Type	Count
HTTPS	2
DNS	3
TCP	3

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955	C:\Users\RDhJ0CNFevzX\Desktop\66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe, C:\RDhJ0CNFevzX\Rand123\local.exe	Sample File	14.97 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	MALICIOUS
5a0f1bee7543cc12a19a01b79774ea07f1b5499823e6ccbc69f13109811f6b6b	C:\RDhJ0CNFevzX\wallpaper.jpg	Downloaded File	270.87 KB	image/jpeg	Access, Create, Write	SUSPICIOUS
9c85f1aea919253002c46a273591f78a8a96c9d14accb77d5afb0e430040c26c	C:\Users\RDhJ0CNFevzX\Documents\BS18p.pptx.paradox, c:\users\rdhj0cnfevzx\documents\bs18p.pptx.paradox	Dropped File	11.28 KB	application/octet-stream	Access, Create, Write	CLEAN
459d2439ff70d66ed0a193272d20a2663735d12462ed83e678f1b5dfce8c7092	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\afV1uedQpAS.jpg.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\ariydsq9h1hltwy2vhg\afv1uedqpas.jpg.paradox	Dropped File	8.33 KB	application/octet-stream	Access, Create, Write	CLEAN
2fd288b109d353fcb7a533e0a5f31da232a35d48eda39df0482021dc020ca046	c:\users\rdhj0cnfevzx\desktop\6gsf_oowdub.ppt.paradox, C:\Users\RDhJ0CNFevzX\Desktop\6gsF_oOWDuB.ppt.paradox	Dropped File	72.47 KB	application/octet-stream	Access, Create, Write	CLEAN
57ae662cbcf60a1d5e3bfd82a42ce12e30520edd18e72a1325d88d22322d5f76	c:\users\rdhj0cnfevzx\videos\bjumhphweyeayyo.mp4.paradox, C:\Users\RDhJ0CNFevzX\Videos\BjUmhphWyEAYYO.mp4.paradox	Dropped File	15.67 KB	application/octet-stream	Access, Create, Write	CLEAN
7d9bdc88f0e46dfcd1f8807812af009d2e4bc279e42145c657323edbbeb742a2	C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\zJcxa5nxH\NB7uoxXXE8jGPi9mjkAl\x-s1lcrQ8YRADHirKDU.mp3.paradox, c:\users\rdhj0cnfevzx\music\7kmdfrdw\zjcxa5nxh\nb7uoxxxe8jgpi9mjkal\x-s1lcrq8yradhirkdu.mp3.paradox	Dropped File	59.56 KB	application/octet-stream	Access, Create, Write	CLEAN
59488544f7c7073fa11c4a83953916430f13895280c90dec9365eeff17161401	C:\Users\RDhJ0CNFevzX\Videos\-cAxil.mp4.paradox, c:\users\rdhj0cnfevzx\videos\-caxil.mp4.paradox	Dropped File	85.98 KB	application/octet-stream	Access, Create, Write	CLEAN
dc257e671d93f00267a8b1207e6d30cedfb7ca33de2df5d0f585273ea02d1d2e	c:\users\rdhj0cnfevzx\documents\a8etnoann.pptx.paradox, C:\Users\RDhJ0CNFevzX\Documents\a8ETnoann.pptx.paradox	Dropped File	58.12 KB	application/octet-stream	Access, Create, Write	CLEAN
659f2a05ba6841e28dd5a0810a0ab6a300bef5ff51ddb224327345e69dc1aaf2	C:\Users\RDhJ0CNFevzX\Documents\bxkuQ7Rq0NwFlu_.xlsx.paradox, c:\users\rdhj0cnfevzx\documents\bxkuq7rq0nwflu_.xlsx.paradox	Dropped File	63.20 KB	application/octet-stream	Access, Create, Write	CLEAN
38416e4893e516c719afb26abfd25e3c7d8189ea6a5c2b6c97efbc9fb3bc5f9d	c:\users\rdhj0cnfevzx\desktop\wpokyx82om8q4ed.avi.paradox, C:\Users\RDhJ0CNFevzX\Desktop\WPoKyX82Om8q4Ed.avi.paradox	Dropped File	13.72 KB	application/octet-stream	Access, Create, Write	CLEAN
f5415b69e38be94519ef0a39284799e6120aa154b21f5c9660703f449555d29b	C:\Users\RDhJ0CNFevzX\Documents\mQx7YPEejtyQadEX8L.docx.paradox, c:\users\rdhj0cnfevzx\documents\mqx7ypeejtyqadex8l.docx.paradox	Dropped File	23.95 KB	application/octet-stream	Access, Create, Write	CLEAN
e031084b05c7d01d6907ba39c4404d8b1bbc19d8d6a3f1e4ee15c3bcec8b6d34	C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\QHmblmZbOvDP\mSyv2w.xls.paradox, c:\users\rdhj0cnfevzx\documents\iho0bqr\qhmblmzbo vdp\msyv2w.xls.paradox	Dropped File	3.66 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
fdd7b577b14e9ccd7b32ea9673217c34e2270c22a7bb8fd802a815662bfc654a	C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvl-CUD-ZhA-\MjBQf.csv.paradox, c:\users\rdhj0cnfevzx\documents\iho0bqr\uzvi-cud-zha-\mjbqf.csv.paradox	Dropped File	63.66 KB	application/octet-stream	Access, Create, Write	CLEAN
c6ce2208505f65aacb34ec3bd6c87467fb32e61bfa7109cab60fc7a02f65ba1	C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\zJcxa5nxH\KbKeXzFPaOL6PVtTCqk\GlHGlizt9V.mp3.paradox, c:\users\rdhj0cnfevzx\music\7kmdfrdw\zjcxa5nxh\kbkexzfpaol6pvttcqk\gihgiizt9v.mp3.paradox	Dropped File	6.50 KB	application/octet-stream	Access, Create, Write	CLEAN
cd5218ff43ed2fe83aaf014982be2eb67a8023e761ac281fd7c62fdcc1d27eb1	C:\Users\RDhJ0CNFevzX\Music\LOcciO2KhP5kfwX2op\Vxx1vR6KrqxFVGqkI.mp3.paradox, c:\users\rdhj0cnfevzx\music\loccio2khp5kfwx2op\vxx1vr6krqxfvgqki.mp3.paradox	Dropped File	8.53 KB	application/octet-stream	Access, Create, Write	CLEAN
9c9d6f0e9a82cccaffc4f90a0c27c135cfab6b765fa104544b12d549206c3eae	C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\dXYm4 e1-8H.jpg.paradox, c:\users\rdhj0cnfevzx\pictures\cdvsbna\dxym4 e1-8h.jpg.paradox	Dropped File	55.12 KB	application/octet-stream	Access, Create, Write	CLEAN
89f1cc2e3e0871de6661f823bcf41d936e70c9e4cf59d9f19c1d25f2cdfb478c	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\Tq-PzJp1KCl6Fslt9az.jpg.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\ariydsq9h1hltwy2vhg\tq-pzjp1kcl6fsit9az.jpg.paradox	Dropped File	68.33 KB	application/octet-stream	Access, Create, Write	CLEAN
0248f8454f75ce6eda9c656a5fc4acb2a4db0f91197d4257481a7c7d302e175f	C:\Users\RDhJ0CNFevzX\Videos\DJ9dTzhHBcmwI.mp4.paradox, c:\users\rdhj0cnfevzx\videos\dj9dtzhhbcmwi.mp4.paradox	Dropped File	17.16 KB	application/octet-stream	Access, Create, Write	CLEAN
bfc7390af294816a888a741b3a9b1b9c24a4362f8d7b0fa591f2db9b3a889225	C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvl-CUD-ZhA-\WrmtmocH.rtf.paradox, c:\users\rdhj0cnfevzx\documents\iho0bqr\uzvi-cud-zha-\wrmtmoch.rtf.paradox	Dropped File	20.95 KB	application/octet-stream	Access, Create, Write	CLEAN
b14e8d51807a961b080eb56c7e0651493b6677e20e9aa48ec2a89ed5938a3953	C:\Users\RDhJ0CNFevzX\Videos\BoiFgH0vw1T6k.mp4.paradox, c:\users\rdhj0cnfevzx\videos\boifgh0vw1t6k.mp4.paradox	Dropped File	45.64 KB	application/octet-stream	Access, Create, Write	CLEAN
c196b6fb25bbed289eb7d693ff6413795bae3a03132fd1c49769347b6438f7aa	c:\users\rdhj0cnfevzx\videos\2ivawd92lo3sa8a.avi.paradox, C:\Users\RDhJ0CNFevzX\Videos\2ivAWd92Lo3SA8a.avi.paradox	Dropped File	69.69 KB	application/octet-stream	Access, Create, Write	CLEAN
d2b05b1efa862f92953a0b7b96ea15adb07e7eb995c292dbf9b139dbcff138c4	C:\Users\RDhJ0CNFevzX\Documents\iBJ0lud-.docx.paradox, c:\users\rdhj0cnfevzx\documents\ibj0lud-.docx.paradox	Dropped File	38.47 KB	application/octet-stream	Access, Create, Write	CLEAN
c13c59feb5f2fb5124024e8fdec69e85f700bc46ec5eab3ca80ab0ed91043aa7	C:\Users\RDhJ0CNFevzX\Videos\51mUVK4.mkv.paradox, c:\users\rdhj0cnfevzx\videos\51muvk4.mkv.paradox	Dropped File	57.55 KB	application/octet-stream	Access, Create, Write	CLEAN
989b284a46c460ff82bed14ac1eb79a2f576846e238f204ade451311a6b8e736	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\8MdVti1_bQ.bmp.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\ariydsq9h1hltwy2vhg\8mdvti1_bq.bmp.paradox	Dropped File	31.31 KB	application/octet-stream	Access, Create, Write	CLEAN
dbc134414b67216a9781a276074dbda3f2ebd881cf9acb3eb2e531c94e83844b	C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\lnmC0XMyDQ9.jpg.paradox, c:\users\rdhj0cnfevzx\desktop\r2prf1u9fnysjo7qvmv\lnmc0xmydq9.jpg.paradox	Dropped File	84.53 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5e4f381c7a04803364125115 4bf9a1cd438855be66c1749a 7e9f932410bdc7dd	C: \Users\RDhJ0CNFevzX\Pictures\gR G40lzkz\AriYdsq9H1hLtWY2vHG\5E FkJZZxsJD.bmp.paradox, c: \users\rdhj0cnfevzx\pictures\grg40lzk z\ariydsq9h1hltwy2vhg\5efkjzzxsjd.b mp.paradox	Dropped File	53.03 KB	application/octet-stream	Access, Create, Write	CLEAN
d14ad5d2d1e9e8f758aa59ce a6257bb3852ab8b0437ca51 7fd736631ab655896	c: \users\rdhj0cnfevzx\desktop\g620ac.jp g.paradox, C: \Users\RDhJ0CNFevzX\Desktop\G62 0aC.jpg.paradox	Dropped File	72.97 KB	application/octet-stream	Access, Create, Write	CLEAN
5a65c16a50cc5beddeb97b2 a8a64f4422d6c3f96801cbc2 84ad72cc6dd0b09c8	c: \users\rdhj0cnfevzx\pictures\grg40lzk z\gj7zisxgu3qt22qtqmq3.bmp.paradox, C: \Users\RDhJ0CNFevzX\Pictures\gR G40lzkz\gJ7ZisxgU3qt22qTqMQ3.bm p.paradox	Dropped File	67.44 KB	application/octet-stream	Access, Create, Write	CLEAN
181118868111c3b2d5c0aba c1fe0d0cbe5cfe2f27ad22edf ca84c15c541d09f0	C: \Users\RDhJ0CNFevzX\Desktop\r2P Rf1U9FnysJo7qVmv\XGbXp3C5lHRk kh6wQq.png.paradox, c: \users\rdhj0cnfevzx\desktop\r2prf1u9f nysjo7qvmv\xgbxp3c5lhrkkh6wqq.png .paradox	Dropped File	15.38 KB	application/octet-stream	Access, Create, Write	CLEAN
e8a677cf242e2e3012623c30 2edbec74c4e678645f0524a1 bc09e6fccde18220	C: \Users\RDhJ0CNFevzX\Documents\ VGfbvj_4ydSGlCX-gZ2F.doc.paradox, c: \users\rdhj0cnfevzx\documents\vgfbvj _4ydsglcx-gz2f.doc.paradox	Dropped File	43.28 KB	application/octet-stream	Access, Create, Write	CLEAN
cf934a1a28bd8cba651fb722 7357f5f3ea8fee990748630703 f62de713631afa	c: \users\rdhj0cnfevzx\music\7kmdfrdw\ zjcxa5nxh\34k8hu-8.mp3.paradox, C: \Users\RDhJ0CNFevzX\Music\7Km DfrDw\zJcxa5nxH\34K8hu-8.mp3.par adox	Dropped File	83.27 KB	application/octet-stream	Access, Create, Write	CLEAN
efea52137a720b79b3de8238 729bb9e5983e1ec18858d77 3f26ade265807984c	c: \users\rdhj0cnfevzx\documents\bmrg6 ivdxlyg.docx.paradox, C: \Users\RDhJ0CNFevzX\Documents\ BMrG6iVDXlyg.docx.paradox	Dropped File	64.73 KB	application/octet-stream	Access, Create, Write	CLEAN
ec0adb4cc6de1cfab0790b86 fe2b19252c96b85cbfd1fbbff5 54ba07c5b9fb3d	C: \Users\RDhJ0CNFevzX\Pictures\CD vSbna\qmD8S.jpg.paradox, c: \users\rdhj0cnfevzx\pictures\cdvsbna\ qmd8s.jpg.paradox	Dropped File	7.05 KB	application/octet-stream	Access, Create, Write	CLEAN
083917c73ebd37f6b454ae39 e1e805a8c4cb0c9beca7f8ab 3a42b8019e62fcfe	-	Downloaded File	48.08 KB	text/html	-	CLEAN
2dca734c8344212468dc0e7 09573e30cf1c794ce62883aa 092875551df224a8d	C: \Users\RDhJ0CNFevzX\Desktop\mO 8vZJ2N.png.paradox, c: \users\rdhj0cnfevzx\desktop\mo8vzj2n .png.paradox	Dropped File	30.52 KB	application/octet-stream	Access, Create, Write	CLEAN
2945576e77b9b61fe170f40e ccec4a629ae0d6159dbd3af6 24cea4c57151f730	c: \users\rdhj0cnfevzx\documents\rbybf. xlsx.paradox, C: \Users\RDhJ0CNFevzX\Documents\r bYBf.xlsx.paradox	Dropped File	14.59 KB	application/octet-stream	Access, Create, Write	CLEAN
d2bbad53393bda1703c8e9d 4a8254cbb13b5acdcfceedd3 74ddfb15aa3bde59e	C: \Users\RDhJ0CNFevzX\Pictures\CD vSbna\w2yJe78igCw.bmp.paradox, c: \users\rdhj0cnfevzx\pictures\cdvsbna\ w2yje78igcw.bmp.paradox	Dropped File	79.64 KB	application/octet-stream	Access, Create, Write	CLEAN
f0d818c2ae2c349084a923bd cda1bdc0445fa7b82ad274dc 3fb6ed99fba8fd82	c: \users\rdhj0cnfevzx\documents\iho0bq r\yiwvx.xls.paradox, C: \Users\RDhJ0CNFevzX\Documents\I hO0bQr\yiWvX.xls.paradox	Dropped File	77.80 KB	application/octet-stream	Access, Create, Write	CLEAN
58f7526198b64699cf80985a 3797e9f8da776707985c69a9 03dc3bc095e5b1c9	c: \users\rdhj0cnfevzx\pictures\grg40lzk z\ooloeayy 74zgh4\1q19rg6lpi7qsur.jpg.paradox, C: \Users\RDhJ0CNFevzX\Pictures\gR G40lzkz\OoloEAyY 74Zgh4\1Q19rG6lPi7qsUr.jpg.paradox	Dropped File	74.00 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
019d87b7a4799be5f343b1a45f4a8a46e20c4dae7a1812868933cdd27b72d822	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\OoloEAyY74Zgh4\0gPNtabbl3ZU6Tj.png.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\ooloeayy74zgh4\0gpntabbl3zu6tj.png.paradox	Dropped File	68.98 KB	application/octet-stream	Access, Create, Write	CLEAN
c8631d245702cc73be9f22153af690b2b8fc534ef1f9d8939791109fc58d7701	C:\Users\RDhJ0CNFevzX\Videos\B7N7KqDrR.mkv.paradox, c:\users\rdhj0cnfevzx\videos\b7n7kqdrr.mkv.paradox	Dropped File	70.52 KB	application/octet-stream	Access, Create, Write	CLEAN
e2271c3ef87548f28b9e4802351d9239ddd17b6ad1480af0a95607b99439453c	c:\users\rdhj0cnfevzx\documents\jvyz5g.pptx.paradox, C:\Users\RDhJ0CNFevzX\Documents\JVYZ5G.pptx.paradox	Dropped File	79.44 KB	application/octet-stream	Access, Create, Write	CLEAN
f97c1a06dc1a2d83db3c5e90a11d0e9ad6a8f0abcc6f1a0d01a0ceb2f7a4004a	C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\gXAZTSzUcdzSa7dD9\nYbgdcIRhW1rqJ.xls.paradox, c:\users\rdhj0cnfevzx\documents\iho0bqr\uzvi-cud-zha-\gxaztszucdzsa7dd9\nybgdcirhw1rqj.xls.paradox	Dropped File	62.09 KB	application/octet-stream	Access, Create, Write	CLEAN
4a2574153b24e0ec2b3df2396e03fd4fdea2c27cba5fc74a5ebe3b4b4197e157	c:\users\rdhj0cnfevzx\documents\lqrcfpqe87lzqn.ppt.paradox, C:\Users\RDhJ0CNFevzX\Documents\lqRCFpqE87LzQN.ppt.paradox	Dropped File	74.22 KB	application/octet-stream	Access, Create, Write	CLEAN
eeeae6f8d62b264810db18bf26b1fe24b964bc570e9fad7d8c2e329ecdbee3db	c:\users\rdhj0cnfevzx\pictures\grg40lzkz\d6g892w9ejaoqh6ubp3.bmp.paradox, C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\D6g892W9EJAoQh6UBp3.bmp.paradox	Dropped File	21.09 KB	application/octet-stream	Access, Create, Write	CLEAN
d4e1561c69568c7689338105e7a64bb56ce07e5c91b692914641908b698efad6	C:\Users\RDhJ0CNFevzX\Videos\CPp1byDqsSfWme.mp4.paradox, c:\users\rdhj0cnfevzx\videos\cpp1bydqssfwme.mp4.paradox	Dropped File	15.09 KB	application/octet-stream	Access, Create, Write	CLEAN
1115f963b40d41453dbd9354d58c885d0b55dd4b72b034395f9117cb3b19b57e	c:\users\rdhj0cnfevzx\pictures\cdvsbna\uim5.png.paradox, C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\UIm5.png.paradox	Dropped File	48.95 KB	application/octet-stream	Access, Create, Write	CLEAN
080a18878545119f0939531b7724333fd0b43ff942b33f029c986810142b5bdc	C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\CdIpDdd5KAfj8fH3OK3.xls.paradox, c:\users\rdhj0cnfevzx\desktop\r2prf1u9fnysjo7qvmv\cdipddd5kafj8fh3ok3.xls.paradox	Dropped File	88.89 KB	application/octet-stream	Access, Create, Write	CLEAN
1aa9f475db6eeec39387c8eef6a2a6e0cf7bde1df16f7d4bc6fd9544f9606130	c:\users\rdhj0cnfevzx\documents\lfdjxcuknymx.ppt.paradox, C:\Users\RDhJ0CNFevzX\Documents\LfdJxcUKnYmX.ppt.paradox	Dropped File	83.58 KB	application/octet-stream	Access, Create, Write	CLEAN
636f7c42011053f3de50e8ab66435637 87ab05ca6c441114ce3bcde8702c4f42	c:\users\rdhj0cnfevzx\documents\iho0bqr\zl803n95eqjd1.doc.paradox, C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\zl803n95eQJd1.doc.paradox	Dropped File	98.61 KB	application/octet-stream	Access, Create, Write	CLEAN
d9fa129ac7725d6d37f985054cc7434c48188726baa05d71141006afd1c9e60c	C:\Users\RDhJ0CNFevzX\Desktop\READ_ME.txt	Dropped File	138 bytes	text/plain	Access, Create, Write	CLEAN
4ee1cbfb959d99bbd6e1acec88c5b50db8807f90f34af5642ed3ed66c681f51f	C:\Users\RDhJ0CNFevzX\Videos\85VAmns.avi.paradox, c:\users\rdhj0cnfevzx\videos\85vamns.avi.paradox	Dropped File	51.67 KB	application/octet-stream	Access, Create, Write	CLEAN
18b7238c671e6addce46ccc30435beaddc4490bfb171e51af00c0245f15ac67c	C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\sipKm5LRXD_iepz2cq.jpg.paradox, c:\users\rdhj0cnfevzx\pictures\cdvsbna\sipkm5lrx d_iepz2cq.jpg.paradox	Dropped File	87.58 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7d8dfb762ec845cf0b61d90788e1ab1cfee1f720b7ab51569a094fce707e7c43	c:\users\rdhj0cnfevzx\videos\a7_2itm9fk.mkv.paradox, C:\Users\RDhJ0CNFevzX\Videos\a7_2ItM9Fk.mkv.paradox	Dropped File	21.73 KB	application/octet-stream	Access, Create, Write	CLEAN
3f6c5aea0ee89e7633cc9669b4d3de76892858dc202366d71b432c69185ca211	c:\users\rdhj0cnfevzx\documents\equm7or1t3w19x6ke.docx.paradox, C:\Users\RDhJ0CNFevzX\Documents\equM7or1T3W19x6ke.docx.paradox	Dropped File	76.38 KB	application/octet-stream	Access, Create, Write	CLEAN
c286f898c2b7a6c04f33cd2da207f1e61d830cd404fea4d6611ee1d6f534705b	c:\users\rdhj0cnfevzx\documents\c9b91yr5nnhgvskp8es.pptx.paradox, C:\Users\RDhJ0CNFevzX\Documents\c9B91Yr5NnHGVSkP8ES.pptx.paradox	Dropped File	16.47 KB	application/octet-stream	Access, Create, Write	CLEAN
23140e720e5c2e69e50fdd9b242a30612b88ff7b0d876721cca103a9460ae4b6	C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\bV9qL.docx.paradox, c:\users\rdhj0cnfevzx\documents\iho0bqr\bv9ql.docx.paradox	Dropped File	66.38 KB	application/octet-stream	Access, Create, Write	CLEAN
ea7bac26ace714529e19210bac6aed42e4682a6e7af488d13b49ec945366cdb7	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\uG0XjLM.jpg.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\ariydsq9h1hltwy2vhg\ug0xjlm.jpg.paradox	Dropped File	88.77 KB	application/octet-stream	Access, Create, Write	CLEAN
8e767b2ab7ce8b1cc26238d9fb21e6cb4a5a0cab0b59665b52551929f9a9ed6c	C:\Users\RDhJ0CNFevzX\Videos\kJaRIROETbuz_IQQ.mkv.paradox, c:\users\rdhj0cnfevzx\videos\kjarlroetbuz_iqq.mkv.paradox	Dropped File	49.38 KB	application/octet-stream	Access, Create, Write	CLEAN
bc5e2372af59ee6d8deb21745a2172d61811027e7453cef1d80ec67634a58153	c:\users\rdhj0cnfevzx\desktop\g_rttfqyxs6.jpg.paradox, C:\Users\RDhJ0CNFevzX\Desktop\g_RTTfqyXS6.jpg.paradox	Dropped File	95.73 KB	application/octet-stream	Access, Create, Write	CLEAN
c04f2793884a523392493ca987384af5571f214cd7b6cbd48455e5cc299935cb	C:\Users\RDhJ0CNFevzX\Videos\KbDpI-xXRv_7VEG.mkv.paradox, c:\users\rdhj0cnfevzx\videos\kbdpi-xxrv_7veg.mkv.paradox	Dropped File	67.92 KB	application/octet-stream	Access, Create, Write	CLEAN
31fc65f844bb0d088825149c4e9695af0e4233b74c527cf6818135971604a8af	C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\lu7q0VmcZ_G6Dq.bmp.paradox, c:\users\rdhj0cnfevzx\pictures\cdvsbna\iu7q0vmc z_g6dq.bmp.paradox	Dropped File	57.45 KB	application/octet-stream	Access, Create, Write	CLEAN
73cba56ce996b4c11c51d5ae848d38cf671a6cbd8f07050e82e26d7e5578eacc	C:\Users\RDhJ0CNFevzX\Videos\zGMZOxL0WD.avi.paradox, c:\users\rdhj0cnfevzx\videos\zgmzoxl0wd.avi.paradox	Dropped File	61.11 KB	application/octet-stream	Access, Create, Write	CLEAN
3d580b9e4c277091029dfb523570a2d47f1094a2b2162b9a3183caa2bcabb881	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\OoloEAyY 74Zgh4\On_Q970XJbNE6EtRfPN.bmp.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\ooloeayy 74zgh4\on_q970xjbne6etrfpn.bmp.paradox	Dropped File	78.47 KB	application/octet-stream	Access, Create, Write	CLEAN
b8327e9e9c6c65653d1a2e4f551b8034fe35e0a4fd66d1e87424ecfcb3f1dd09	C:\Users\RDhJ0CNFevzX\Videos\23WDO ZYI.avi.paradox, c:\users\rdhj0cnfevzx\videos\23wdo zyi.avi.paradox	Dropped File	60.38 KB	application/octet-stream	Access, Create, Write	CLEAN
cfdb1fb10910b521b5630e4e47be1e1f32226bf7e6cbc95052a2c4faa5422999	C:\Users\RDhJ0CNFevzX\Music\LOcciO2KhP5kfwX 2op\bhpdCMF2_qxg\YUU6tBaYq0t.mp3.paradox, c:\users\rdhj0cnfevzx\music\loccio2khp5kfwx 2op\bhpdcmf2_qxg\yuu6tbayq0t.mp3.paradox	Dropped File	21.36 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6cd8ac5f4f81619146ace8ba383b589afbdc224d76682a355969d2d48b1fd400	C:\Users\RDhJ0CNFevzX\Documents\Axeso-6WCbUVjz.xlsx.paradox, c:\users\rdhj0cnfevzx\documents\axeso-6wcbuvjz.xlsx.paradox	Dropped File	95.50 KB	application/octet-stream	Access, Create, Write	CLEAN
2f9e7761b0790d938073bfb0ea9d4a8e9b3b18a9f8d63e67a6b1bd7ba379c592	C:\Users\RDhJ0CNFevzX\Documents\Udu1XE4Hd0l8gwhDhX2.odt.paradox, c:\users\rdhj0cnfevzx\documents\udu1xe4hd0i8gwhdhx2.odt.paradox	Dropped File	87.09 KB	application/octet-stream	Access, Create, Write	CLEAN
7252452447 85de23c24b49d981b4fdeb6c806baca19354e24442a4c095de1e7a	C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\NxW3d3OjYtrQDUX.pptx.paradox, c:\users\rdhj0cnfevzx\documents\iho0bqr\nxw3d3ojytrqdux.pptx.paradox	Dropped File	57.09 KB	application/octet-stream	Access, Create, Write	CLEAN
4d6c326972292276a4c727706a4d59aea1929a66f108412301925baa10b0c77a	c:\users\rdhj0cnfevzx\music\loccio2khp5kfwx 2op\chzujdwb.mp3.paradox, C:\Users\RDhJ0CNFevzX\Music\LOcciO2KhP5kfwX 2op\cHZujdWB.mp3.paradox	Dropped File	89.77 KB	application/octet-stream	Access, Create, Write	CLEAN
35686fdba7b521571ce0a5b39af7d3186efb74b22c220f16ce9a2fee85f8a55b	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\hD6t-A2anl.jpg.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\ariydsq9h1hltwy2vhg\hd6 t-a2anl.jpg.paradox	Dropped File	27.39 KB	application/octet-stream	Access, Create, Write	CLEAN
20cf6677a4a830a294fc9ff17b651db656149cc9d5a2b9132133e2122c84616f	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\OoloEAyY 74Zgh4\WQWnpehTBFCALVb.bmp.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\ooloeayy 74zgh4\wqwnpehtbfcalvb.bmp.paradox	Dropped File	14.80 KB	application/octet-stream	Access, Create, Write	CLEAN
168462ab9f6fadabda24cbb734766ee67d510c4f3c0160a8f4632e48851ede52	c:\users\rdhj0cnfevzx\desktop\r2prf1u9fnysjo7qvmv\ihb.mkv.paradox, C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\iHB.mkv.paradox	Dropped File	50.00 KB	application/octet-stream	Access, Create, Write	CLEAN
f049ef2889f4cc58d2f5d771e87c920322bdef7a6ee767631f75a169142db908	C:\Users\RDhJ0CNFevzX\Desktop\avNCvKlbZERjJ6.odt.paradox, c:\users\rdhj0cnfevzx\desktop\avncvkibzerjj6.odt.paradox	Dropped File	56.75 KB	application/octet-stream	Access, Create, Write	CLEAN
e871433d224d3a181fca60351a69fded476b14c1b5500f744386b9b393e562d5	C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\0ltsVjI3Z5uTF3b.mp3.paradox, c:\users\rdhj0cnfevzx\desktop\r2prf1u9fnysjo7qvmv\0itsvji3z5utf3b.mp3.paradox	Dropped File	68.02 KB	application/octet-stream	Access, Create, Write	CLEAN
94904df68c428f0a47ccf12ded46a05e1694c41d4b3adb4244e5feab897422fd	C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\zJcxa5nxH\xow2-jtbjjD9\uFm6gFL_KjdhgP.mp3.paradox, c:\users\rdhj0cnfevzx\music\7kmdfrdw\zjcxa5nxh\xow2-jtbjjd9\ufm6gfl_kjdhgp.mp3.paradox	Dropped File	68.20 KB	application/octet-stream	Access, Create, Write	CLEAN
4bf36c17e3e47cfb6b9eb27a644ed456f44b75a96a29e78bc78c56974e391c17	C:\Users\RDhJ0CNFevzX\Desktop\zSxZ4J_7Ak.ppt.paradox, c:\users\rdhj0cnfevzx\desktop\zsxz4j_7ak.ppt.paradox	Dropped File	66.83 KB	application/octet-stream	Access, Create, Write	CLEAN
8b24a1cea75cb4e7d6621f7516eaf46aae46198b064c1826cdeaf174ee6c2611	c:\users\rdhj0cnfevzx\videos\vlzh24-yjiutkgunnug.avi.paradox, C:\Users\RDhJ0CNFevzX\Videos\VLZH24-yjIUtKgUNNUg.avi.paradox	Dropped File	47.62 KB	application/octet-stream	Access, Create, Write	CLEAN
1346f74c749874146f1f4a0fbe4d4a8989e3f2f893f9cf76d9a50dad5f6f3b4d	c:\users\rdhj0cnfevzx\music\7kmdfrdw\zjcxa5nxh\nb7uoxxxe8jgpi9mjkal\buigcjetpjo.mp3.paradox, C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\zJcxa5nxH\NB7uoxXXE8jGPi9mjkAl\BuigcJeTpJO.mp3.paradox	Dropped File	87.88 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6da8d5fc30c85ef923295ba5b855ad20c525b1e87e9db7e53bde6592c43a6eaa	c:\users\rdhj0cnfevzx\pictures\ssva9xc4h39.jpg.paradox, C:\Users\RDhJ0CNFevzX\Pictures\SsvA9Xc4 h39.jpg.paradox	Dropped File	56.75 KB	application/octet-stream	Access, Create, Write	CLEAN
f8aa5e8d924bf5670dee190a44cc6bb6c22d401c08aee5983b5678f0134f8df4	C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\gXAZTSzUcdzSa7dD9\hAG8_BLENEWKevuN.pptx.paradox, c:\users\rdhj0cnfevzx\documents\iho0bqr\uzvi-cud-zha-\gxaztszucdzsa7dd9\hag8_blenewkevun.pptx.paradox	Dropped File	79.66 KB	application/octet-stream	Access, Create, Write	CLEAN
e3f6fded6759b5a1caf0231977527b94173aec748a3ecee7d4d984d2a4852e92	C:\Users\RDhJ0CNFevzX\Desktop\VHrKBoE.mkv.paradox, c:\users\rdhj0cnfevzx\desktop\vhrkboe.mkv.paradox	Dropped File	90.83 KB	application/octet-stream	Access, Create, Write	CLEAN
d59f99aee8c962f618b0bafdd07b27263cb4dd282a09634c359649c01a019610	c:\users\rdhj0cnfevzx\pictures\grg40lzkz\3 pbelo2sufc.png.paradox, C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\3 PBELo2SufC.png.paradox	Dropped File	58.14 KB	application/octet-stream	Access, Create, Write	CLEAN
6a8b51605f148496b0db99f48cb3daf3a8c6e2819c06617432be01650e2ded37	c:\users\rdhj0cnfevzx\documents_p4fctiw.xlsx.paradox, C:\Users\RDhJ0CNFevzX\Documents_p4fCTIw.xlsx.paradox	Dropped File	36.20 KB	application/octet-stream	Access, Create, Write	CLEAN
4432ac296f6497b31731a795a9327f8fb4b121a3fa30ae73578efef044bdc0d1	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\MEHNk_Kk\XzYboTZ.png.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\mehnk_kk\xzybotz.png.paradox	Dropped File	78.05 KB	application/octet-stream	Access, Create, Write	CLEAN
c81700334d04995faa698d5954baf31769e4a3712c1a403ae1339e3e1e86bbff	C:\Users\RDhJ0CNFevzX\Links\Downloads.lnk.paradox, c:\users\rdhj0cnfevzx\links\downloads.lnk.paradox	Dropped File	992 bytes	application/octet-stream	Access, Create, Write	CLEAN
70fc788511e8ee723b6f23406a2432c2af402c591ba6583cf82f918c0675c026	c:\users\rdhj0cnfevzx\pictures\cdvsbna\ysw39t6l-twgke-iut8k.jpg.paradox, C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\YsW39t6L-TWGKe-iuT8K.jpg.paradox	Dropped File	27.05 KB	application/octet-stream	Access, Create, Write	CLEAN
7e27ba0d572b29543e7cc8f83154adef5ffcada5b291a4548fb52754ffa13fe8	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\xbnzj.bmp.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\ariydsq9h1hltwy2vhg\xbnzj.bmp.paradox	Dropped File	79.19 KB	application/octet-stream	Access, Create, Write	CLEAN
d8945e92a1d6731d7bec984291db328f7dcb6855b2605a6497304c22c6f691bb	c:\users\rdhj0cnfevzx\desktop\ll2mxwxrhwpc2d.jpg.paradox, C:\Users\RDhJ0CNFevzX\Desktop\Ll2MxwxRHWpc2D.jpg.paradox	Dropped File	97.44 KB	application/octet-stream	Access, Create, Write	CLEAN
50af6fe9f65721c166385fcb3ee48d34643a67ab68c7b5be272cf207940af16c	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\MEHNk_Kk\otYR0bcDOHhVdwK.jpg.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\mehnk_kk\otyr0bcdohhvdwk.jpg.paradox	Dropped File	70.80 KB	application/octet-stream	Access, Create, Write	CLEAN
d071867ccbf81309b79138af6fc9a7cc98f736c50513ad6fbee40962019a06bf	c:\users\rdhj0cnfevzx\documents\iho0bqr\uzvi-cud-zha-\gxaztszucdzsa7dd9\mousogoar.odt.paradox, C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\gXAZTSzUcdzSa7dD9\moUsOGoAr.odt.paradox	Dropped File	80.09 KB	application/octet-stream	Access, Create, Write	CLEAN
0ff7bbdd5cb87c1314e3efda75ebf9ea55eee1a67c20f7da3964df097c286de1	c:\users\rdhj0cnfevzx\pictures\qwlzs.bmp.paradox, C:\Users\RDhJ0CNFevzX\Pictures\qwlzS.bmp.paradox	Dropped File	22.83 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e729ddc5de1c41f3fc0201a279c3ca19acad69370b944a4656769826091e2b1d	C:\Users\RDhJ0CNFevzX\Videos\4DG-or0-b.avi.paradox, c:\users\rdhj0cnfevzx\videos\4dg-or0-b.avi.paradox	Dropped File	44.78 KB	application/octet-stream	Access, Create, Write	CLEAN
c8cedc88faebb214cc419584c834cd351481d50bebc1ffe4a7cbe527598ad075	C:\Users\RDhJ0CNFevzX\Videos\c_1zZ88519M.mkv.paradox, c:\users\rdhj0cnfevzx\videos\c_1zz88519m.mkv.paradox	Dropped File	13.83 KB	application/octet-stream	Access, Create, Write	CLEAN
335a457d58599725bbfd21437fe23e7dee7626bedad25d5175169229f151711b	c:\users\rdhj0cnfevzx\videos\jtmnbzore3sk2mh.mp4.paradox, C:\Users\RDhJ0CNFevzX\Videos\jTMNBZorE3Sk2mH.mp4.paradox	Dropped File	51.09 KB	application/octet-stream	Access, Create, Write	CLEAN
4c88a1be124469b26fbb8b1a40a63401cdbdf880beba32d5614fad8b5ee0f9e4	C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\8uC8KGTO2.mp3.paradox, c:\users\rdhj0cnfevzx\music\7kmdfrdw\8uc8kgto2.mp3.paradox	Dropped File	23.47 KB	application/octet-stream	Access, Create, Write	CLEAN
b3c9b0b35b02dcef8693dea8c3136e61a85028960133324963e2f39df22db600	C:\Users\RDhJ0CNFevzX\Desktop\x5SAnVmwCY.bmp.paradox, c:\users\rdhj0cnfevzx\desktop\x5sanvmwcy.bmp.paradox	Dropped File	57.55 KB	application/octet-stream	Access, Create, Write	CLEAN
e7e0d744af3a0f3ce71a55b5449ae19fd865ec1bde4606326bee2669ec1c23cc	c:\users\rdhj0cnfevzx\documents\iho0bqr\d4afyfsf.pdf.paradox, C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\D4afyfsf.pdf.paradox	Dropped File	75.48 KB	application/octet-stream	Access, Create, Write	CLEAN
450d7651105ded3a58622c19964515c92f98ffb84a1346e428bb3cc9b1645a52	C:\Users\RDhJ0CNFevzX\Desktop\p-cVbO84.doc.paradox, c:\users\rdhj0cnfevzx\desktop\p-cvbo84.doc.paradox	Dropped File	25.86 KB	application/octet-stream	Access, Create, Write	CLEAN
082d4dbc6951f8fb9b84e019657f59d8e73da61b3171eeae441b5580b5c43831	C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\LykQr.jpg.paradox, c:\users\rdhj0cnfevzx\desktop\r2prf1u9fnysjo7qvmv\lykqr.jpg.paradox	Dropped File	62.94 KB	application/octet-stream	Access, Create, Write	CLEAN
120db168df996c228b8b57c2c20dff3d84aa9064db72c6123ede86324f677489	C:\Users\RDhJ0CNFevzX\Documents\dAFINowb06QqRO4uOt.docx.paradox, c:\users\rdhj0cnfevzx\documents\dafinowb06qqro4uot.docx.paradox	Dropped File	1.80 KB	application/octet-stream	Access, Create, Write	CLEAN
ec7b9f4e7d9a0daf2988728998065fdaf5383ca9de781b3266d0b05d0d531c52	c:\users\rdhj0cnfevzx\documents\xib5.pptx.paradox, C:\Users\RDhJ0CNFevzX\Documents\XIB 5.pptx.paradox	Dropped File	24.27 KB	application/octet-stream	Access, Create, Write	CLEAN
9c5146eff3d2cfeb01456845afce842dc6c364c64a59ac0aed1ee1c7c7c3d6df	c:\users\rdhj0cnfevzx\desktop\jmlwn5tr.mp3.paradox, C:\Users\RDhJ0CNFevzX\Desktop\jmlwn5Tr.mp3.paradox	Dropped File	34.91 KB	application/octet-stream	Access, Create, Write	CLEAN
698b380664ab3f33b5d614b9a05c392801baa2020ee2238eff77e3d153888313	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\xS_92T-iMJ.bmp.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\xs_92t-imj.bmp.paradox	Dropped File	9.16 KB	application/octet-stream	Access, Create, Write	CLEAN
30852a59b57014c2dc471d79776e3456e1d41522029986f5e6f1d4b50791c208	c:\users\rdhj0cnfevzx\pictures\grg40lzkz\mehnk_kk\g-jrstvi0xfw.bmp.paradox, C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\MEHNk_Kk\g-JrStVI0xFW.bmp.paradox	Dropped File	93.56 KB	application/octet-stream	Access, Create, Write	CLEAN
a0f93220e43c84e7e51f121830e0d2eab14094a2bd533e8ca1b42aa4d035af5a	C:\Users\RDhJ0CNFevzX\Videos\Ue6Gzt3lTeB7E.mp4.paradox, c:\users\rdhj0cnfevzx\videos\ue6gzt3iteb7e.mp4.paradox	Dropped File	13.78 KB	application/octet-stream	Access, Create, Write	CLEAN
2c94e644813ee226baf70cd5d6a18184201ba1fd79b41545d2e706b62a22784e	c:\users\rdhj0cnfevzx\documents\iho0bqr\pm-yxcrz5dlv.csv.paradox, C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\Pm-YXcrz5DLV.csv.paradox	Dropped File	77.95 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5fbde2e4c61b652ff203d938fb15c8758bbe4c6334566dcc35cf8f4e3e30a9f8	C:\Users\RDhJ0CNFevzX\Videos\voHnlGNKaLfJq0z.mkv.paradox, c:\users\rdhj0cnfevzx\videos\vohnlgnkalfjq0z.mkv.paradox	Dropped File	74.05 KB	application/octet-stream	Access, Create, Write	CLEAN
de007681989f36f81abe8a692dc0ac9eb7e7b42097dfabe4e4430017161006a3	c:\users\rdhj0cnfevzx\links\desktop.lnk.paradox, C:\Users\RDhJ0CNFevzX\Links\Desktop.lnk.paradox	Dropped File	528 bytes	application/octet-stream	Access, Create, Write	CLEAN
fa935a077b87c97d5c3c779208f40ad3d16fd934e7c4d6e2a2edcd88586d1bbc	C:\Users\RDhJ0CNFevzX\Desktop\3ALR.avi.paradox, c:\users\rdhj0cnfevzx\desktop\3alr.avi.paradox	Dropped File	97.91 KB	application/octet-stream	Access, Create, Write	CLEAN
4895e9ba2ded9ee433eb76154f92a2b2dca80c348f27eedbf6600718d60a0079	C:\Users\RDhJ0CNFevzX\Videos\W1H9qw8y.mkv.paradox, c:\users\rdhj0cnfevzx\videos\w1h9qw8y.mkv.paradox	Dropped File	35.08 KB	application/octet-stream	Access, Create, Write	CLEAN
f7bd6db8df52ba1a2cfdcc6dbd6fbd0b7fbbdc360abe3d4c3f8b2931bcae23be	C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\8 N3.docx.paradox, c:\users\rdhj0cnfevzx\documents\iho0bqr\8 n3.docx.paradox	Dropped File	24.36 KB	application/octet-stream	Access, Create, Write	CLEAN
859ec1c090b214c8eb6740a7efe4370da0c61b0407e57328f22537b4068b3002	c:\users\rdhj0cnfevzx\desktop\ofnsaydprzb46.mkv.paradox, C:\Users\RDhJ0CNFevzX\Desktop\oFnSAYDpRZb46.mkv.paradox	Dropped File	68.45 KB	application/octet-stream	Access, Create, Write	CLEAN
65dbb09bd7c4e6880c080e75c83e144835f697f9321db82968f3493ea06435f7	c:\users\rdhj0cnfevzx\desktop\r2prf1u9fnysjo7qvmv\moljpyipfv.jpg.paradox, C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\molJpyIPFV.jpg.paradox	Dropped File	61.59 KB	application/octet-stream	Access, Create, Write	CLEAN
0626213b982abfdf90dc619ae1442fbf8c6629a4cfbfb856bd62c1be873871a4	C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\93rPWrjGSl.jpg.paradox, c:\users\rdhj0cnfevzx\pictures\grg40lzkz\93rpwrjgsl.jpg.paradox	Dropped File	81.42 KB	application/octet-stream	Access, Create, Write	CLEAN
cb2ac6a1af9a572046d49e653e85196b43f19c8b690979fdcee45ea45c33aaf5	c:\users\rdhj0cnfevzx\documents\ixibdtgx.docx.paradox, C:\Users\RDhJ0CNFevzX\Documents\iXIBDT Gx.docx.paradox	Dropped File	38.33 KB	application/octet-stream	Access, Create, Write	CLEAN
b9109acade865bfeebc18315eaf188a3a911908124ad17f42bf6043ee2f2bb4a	C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\gXAZTSzUcdzSa7dD9\Fd2XhevfRzd.odt.paradox, c:\users\rdhj0cnfevzx\documents\iho0bqr\uzvi-cud-zha-\gxaztszucdzsa7dd9\fd2xhevfrzd.odt.paradox	Dropped File	15.38 KB	application/octet-stream	Access, Create, Write	CLEAN
7cf8c2e6df2d2169dfe13c2bc56f0d3c34bbbbf8a720730055df8eef40595e44	C:\Users\RDhJ0CNFevzX\Documents\DoE cR5.xlsx.paradox, c:\users\rdhj0cnfevzx\documents\doecr5.xlsx.paradox	Dropped File	39.67 KB	application/octet-stream	Access, Create, Write	CLEAN
86067e67b91c39503d370788eff82898b34a1465fbb2262313d3f398278cad0f	C:\Users\RDhJ0CNFevzX\Desktop\y-ufahLBUL h.avi.paradox, c:\users\rdhj0cnfevzx\desktop\y-ufahlbulh.avi.paradox	Dropped File	48.92 KB	application/octet-stream	Access, Create, Write	CLEAN
e5703d02884387de0a0381167499beb8781ecacd938ea8659f907683d3192497	c:\users\rdhj0cnfevzx\documents\pzrq3ttlp58bkco.docx.paradox, C:\Users\RDhJ0CNFevzX\Documents\pZRQ3ttLP58bKcO.docx.paradox	Dropped File	39.11 KB	application/octet-stream	Access, Create, Write	CLEAN
db3d36c5a38ca189f8db2a287639bcdfa8d59270eff49387f24675b37ff37db7	C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\LbG_ zixT9ffs2A.bmp.paradox, c:\users\rdhj0cnfevzx\pictures\cdvsbna\lbg_ zixt9ffs2a.bmp.paradox	Dropped File	78.45 KB	application/octet-stream	Access, Create, Write	CLEAN
7424e1e089532598d76d0a75b90293e75ef7663863452a52352187e12195510c	C:\Users\RDhJ0CNFevzX\Videos\A-MC1ceN9T2G9.mkv.paradox, c:\users\rdhj0cnfevzx\videos\a-mc1cen9t2g9.mkv.paradox	Dropped File	60.56 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2c17502ed3a6775b717898c681e20f152bbd3e668f282cfda8dee954aab21dbc	c:\users\rdhj0cnfevzx\music\loccio2khp5kfwx 2op\rez9jflaxipy.mp3.paradox, C:\Users\RDhJ0CNFevzX\Music\LOcciO2KhP5kfwX 2op\reZ9jFlAXiPY.mp3.paradox	Dropped File	58.91 KB	application/octet-stream	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\Tq-PzJp1KCl6Fslt9az.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\jmlwn5tr.mp3.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\vlzh24-yjiutkgunnug.avi.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\iho0bqr\uzvi-cud-zha-\gxaztszucdzsa7dd9\mousogoar.odt.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\LykQr.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\grg40lzkz\gj7zisxgu3qt22qtqmq3.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Links\Downloads.lnk.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\OoloEAyY 74Zgh4\On_Q970XJbNE6EtRfPN.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\23WDO ZYI.avi.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\c9b91yr5nnhgvskp8es.pptx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\WrmtmocH.rtf.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents_p4fctiw.xlsx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\voHnl GNKaLfJq0z.mkv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\xbnzj.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\x5SAnVmwCY.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\ssva9xc4 h39.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\93rPWrjGSl.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\gXAZTSzU cdzSa7dD9\hAG8_BLENEWKevuN.pptx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\p-cVbO84.doc.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\grg40lzkz\3 pbelo2sufc.png.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\iho0bqr\pm-yxcrz5dlv.csv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\VHrKBoE.mkv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\bxkuQ7Rq0NwFlu_.xlsx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\7kmdfrdw\zjcxa5nxh\nb7uoxxxe8jgpi9mjkal\buigcjetpjo.mp3.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\iBJ0lud-.docx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\hD6 t-A2anl.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\RDhJ0CNFevzX\Rand123\local.exe	Sample File, Dropped File, Accessed File, Not Extracted	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\xS_92T-iMJ.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\bmrg6ivdxlyg.docx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\Axeso-6WCbUVjz.xlsx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\IhO0bQr\8 N3.docx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\zJcxa5nxH\xow2-jtbjjD9\uFm6gFL_KjdhgP.mp3.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\ixibdt gx.docx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\4DG-or0-b.avi.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\8MdVti1_bQ.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\mO8vZJ2N.png.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\w2yJe78igCw.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\lu7q0VmcZ_G6Dq.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\jtmnbzore3sk2mh.mp4.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\3ALR.avi.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\afV1uedQpAS.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\dXYm4e1-8H.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\cdvsbna\ysw39t6l-twgke-iut8k.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\r2prf1u9fnysjo7qvmv\moljpyipfv.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Music\LOcciO2KhP5kfwX2op\bhpdCMF2_qxg\YUU6tBaYq0t.mp3.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\a7_2itm9fk.mkv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\Ue6Gzt3lTeB7E.mp4.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\5EFkJZZxsJD.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\avNCvKlbZERjJ6.odt.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\A-MC1ceN9T2G9.mkv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\g620ac.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\zJcxa5nxH\KbKeXzFPaOL6PVtTCqk\GIHGlizt9V.mp3.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\KbDpl-xXRv_7VEG.mkv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\rbybf.xlsx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\IhO0bQr\bV9qL.docx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\pictures\grg40lzkz\d6g892w9ejaoqh6ubp3.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\iho0bqr\yiwvx.xls.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\ofnsaydprzb46.mkv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\y-ufahLBUL h.avi.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\ll2mxwxrhwpc2d.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\MEHNk_Kk\otYR0bcDOHhVdwK.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\kJaRIROETbuz_IQQ.mkv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\85VAmns.avi.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\r2prf1u9fnysjo7qvmv\ihb.mkv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\qwlzs.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\XGbXp3C5lHRkkh6wQq.png.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\a8etnoann.pptx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\CdIpDdd5KAfj8fH3OK3.xls.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\InmC0XMyDQ9.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\grg40lzkz\ooloeayy74zgh4\1q19rg6lpi7qsur.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\mQx7YPEejtyQadEX8L.docx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\qmD8S.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\g_rttfqyxs6.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Music\LOcciO2KhP5kfwX2op\Vxx1vR6KrqxFVGqkI.mp3.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\lqrcfpqe87lzqn.ppt.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\51mUVK4.mkv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\B7N7KqDrR.mkv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\OoloEAyY74Zgh4\WQWnpehTBFCALVb.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\BoiFgH0vw1T6k.mp4.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\links\desktop.lnk.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\CPp1byDqsSfWme.mp4.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\dAFINowb06QqRO4uOt.docx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\AriYdsq9H1hLtWY2vHG\uG 0XjLM.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\loccio2khp5kfwx2op\rez9jflaxipy.mp3.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\Udu1XE4Hd0I8gwhDhX2.odt.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Videos\c_1zZ88519M.mkv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	Sample File, Accessed File, VM File	Access, Delete	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\W1H9qw8y.mkv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\IhO0bQr\NxW3d3OjYtrQDUX.pptx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\lfdjxcuknymx.ppt.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\LbG_zixT9ffs2A.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\BS18p.pptx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\pzrq3ttlp58bkco.docx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\7kmdfrdw\zjcxa5nxh\34k8hu-8.mp3.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\-cAxiI.mp4.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\bjumhphwyeayyo.mp4.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\zJcxa5nxH\NB7uoxXXE8jGPi9mjkAl\X-s1lcrQ8YRADHirKDU.mp3.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\zGMZOxL0WD.avi.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\zSxZ4J_7Ak.ppt.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\VGfbvj_4ydSGlCX-gZ2F.doc.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\grg40lzkz\mehnk_kk\g-jrstvi0xfw.bmp.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\IhO0bQr\uZvI-CUD-ZhA-\gXAZTSzU cdzSa7dD9\nYbgdcIRhW1rqJ.xls.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\r2PRf1U9FnysJo7qVmv\0ltsVjI3Z5uTF3b.mp3.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Videos\DJ9dTzhHBcmwI.mp4.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\wpokyx82om8q4ed.avi.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\xib 5.pptx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\equm7or1t3w19x6ke.docx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\IhO0bQr\QHmblmZbOvDP\mSyv2w.xls.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\iho0bqr\zl803n95eqjd1.doc.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\loccio2khp5kfwx2op\chzujdwb.mp3.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\iho0bqr\d4afyfsf.pdf.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\6gsf_oowdub.ppt.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\MEHNk_Kk\XzYboTZ.png.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Music\7KmDfrDw\8uC8KGTO2.mp3.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\documents\jvyz5g.pptx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\MjBQf.csv.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\DoE cR5.xlsx.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\CDvSbna\sipKm5LRX D_iepz2cq.jpg.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\cdvsbna\uim5.png.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\lhO0bQr\uZvI-CUD-ZhA-\gXAZTSzU cdzSa7dD9\Fd2XhevfRzd.odt.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\videos\2ivawd92lo3sa8a.avi.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Pictures\gRG40lzkz\OoloEAyY 74Zgh4\0gPNtabbl3ZU6Tj.png.paradox	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Links\Downloads.lnk	Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\READ_ME.txt	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe.config	Accessed File	Access	CLEAN
C:\RDhJ0CNFevzX\Rand123	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Links\Desktop.lnk	Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\RDhJ0CNFevzX	Accessed File	Access, Create	CLEAN
C:\RDhJ0CNFevzX\wallpaper.jpg	Accessed File, Downloaded File, Extracted File	Access, Create, Write	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\READ_IT.txt.locked	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://play.google.com/?hl=de&tab=w8	-	-	-	-	CLEAN
https://www.google.de/intl/de/about/products?tab=wh	-	-	-	-	CLEAN
https://www.gstatic.com	-	-	-	-	CLEAN
https://www.google.com/setprefdomain?prefdom=DE&prev=https://www.google.de/&sig=K_ZHphx3Bg0wcMwtFW0rN51J6FWWc%3D	-	216.58.212.164	-	-	CLEAN
https://calendar.google.com/calendar?tab=wc	-	-	-	-	CLEAN
https://www.google.de/shopping?hl=de&source=og&tab=wf	-	-	-	-	CLEAN
https://mail.google.com/mail/?tab=wm	-	-	-	-	CLEAN
https://lh3.googleusercontent.com/ogw/default-user=s24	-	-	-	-	CLEAN
https://en3ez7v505kx8.x.pipedream.net	-	3.228.107.54, 23.21.95.90, 107.22.74.15, 54.174.214.98, 50.19.131.153	-	-	CLEAN
https://www.youtube.com/?tab=w1	-	-	-	-	CLEAN
https://books.google.de/?hl=de&tab=wp	-	-	-	-	CLEAN
https://www.google.com/finance?tab=we	-	216.58.212.164	-	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://blog.google/intl/de-de/produkte/suchen-entdecken/kraftstoffsparende-routen-google-maps/	-	216.58.212.164	-	-	CLEAN
https://media.threatpost.com/wp-content/uploads/sites/103/2020/01/03130357/ransomware.jpeg	-	13.226.153.2, 13.226.153.42, 13.226.153.79, 13.226.153.98	-	GET	CLEAN
https://maps.google.de/maps?hl=de&tab=wl	-	-	-	-	CLEAN
http://video.google.de/?hl=de&tab=wv	-	-	-	-	CLEAN
https://www.google.com	-	216.58.212.164	-	GET	CLEAN
https://translate.google.de/?hl=de&tab=wT	-	-	-	-	CLEAN
https://apis.google.com	-	-	-	-	CLEAN
https://accounts.google.com/ServiceLogin?hl=de&passive=true&continue=https://www.google.com/&ec=GAZAAQ	-	-	-	-	CLEAN
https://docs.google.com/document/?usp=docs_alc	-	-	-	-	CLEAN
http://www.google.de/preferences?hl=de	-	-	-	-	CLEAN
https://news.google.com/?tab=wn	-	-	-	-	CLEAN
https://www.google.de/webhp?tab=ww	-	-	-	-	CLEAN
https://lh3.googleusercontent.com/ogw/default-user=s96	-	-	-	-	CLEAN
https://www.blogger.com/?tab=wj	-	-	-	-	CLEAN
https://photos.google.com/?tab=wq&pageId=none	-	-	-	-	CLEAN
http://www.google.de/history/optout?hl=de	-	-	-	-	CLEAN
https://drive.google.com/?tab=wo	-	-	-	-	CLEAN
https://www.google.de/imghp?hl=de&tab=wi	-	-	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
accounts.google.com	-	-	-	CLEAN
www.blogger.com	-	-	-	CLEAN
en3ez7v505kx8.x.pipedream.net	3.228.107.54, 23.21.95.90, 107.22.74.15, 54.174.214.98, 50.19.131.153	-	DNS, TCP, HTTPS	CLEAN
calendar.google.com	-	-	-	CLEAN
books.google.de	-	-	-	CLEAN
news.google.com	-	-	-	CLEAN
play.google.com	-	-	-	CLEAN
www.gstatic.com	-	-	-	CLEAN
maps.google.de	-	-	-	CLEAN
www.google.de	-	-	-	CLEAN
video.google.de	-	-	-	CLEAN
d2x8sklh0hjsql.cloudfront.net	13.226.153.2, 13.226.153.42, 13.226.153.79, 13.226.153.98	-	DNS, TCP, HTTPS	CLEAN
apis.google.com	-	-	-	CLEAN
drive.google.com	-	-	-	CLEAN

Domain	IP Address	Country	Protocols	Verdict
www.google.com	216.58.212.164	-	DNS, TCP, HTTPS	CLEAN
photos.google.com	-	-	-	CLEAN
www.youtube.com	-	-	-	CLEAN
lh3.googleusercontent.com	-	-	-	CLEAN
media.threatpost.com	13.226.153.2, 13.226.153.42, 13.226.153.79, 13.226.153.98	-	DNS, TCP, HTTPS	CLEAN
translate.google.de	-	-	-	CLEAN
mail.google.com	-	-	-	CLEAN
docs.google.com	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
13.226.153.98	media.threatpost.com, d2x8sklh0hjsql.cloudfront.net	United States	DNS, TCP, HTTPS	CLEAN
13.226.153.42	media.threatpost.com, d2x8sklh0hjsql.cloudfront.net	United States	DNS	CLEAN
13.226.153.79	media.threatpost.com, d2x8sklh0hjsql.cloudfront.net	United States	DNS	CLEAN
216.58.212.164	www.google.com	United States	DNS, TCP, HTTPS	CLEAN
13.226.153.2	media.threatpost.com, d2x8sklh0hjsql.cloudfront.net	United States	DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	access, read	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	access, read	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	CLEAN

Process

Process Name	Commandline	Verdict
66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe	"C:\Users\RDhJ0CNFevzX\Desktop\66ec6a7bb5cec8d1205685833524b4f577af75570896e0b368f16e5ee0d2a955.exe"	MALICIOUS

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.2.24 / 2022-09-07 15:06:41
Link Detonation Heuristics Version	4.6.2.24 / 2022-09-07 15:06:41
Smart Memory Dumping Rules Version	4.6.2.24 / 2022-09-07 15:06:41
Config Extractors Version	4.6.2.26 / 2022-09-09 12:20:50
Signature Trust Store Version	4.6.2.24 / 2022-09-07 15:06:41
VMRay Threat Identifiers Version	4.6.2.26 / 2022-09-09 12:20:50
YARA Built-in Ruleset Version	4.6.2.26

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

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

System Root	C:\Windows