MALICIOUS

Classifications: Ransomware

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe**
ID	#9333197
MD5	c7cfaca6501361febe27a6b3e66a61bf
SHA1	55a3414b9668596e120139a059db91a306281dcc
SHA256	fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44
File Size	26.50 KB
Report Created	2023-11-21 00:28 (UTC)
Target Environment	windows 10 (64bit 20H1 -EN-) | exe

OVERVIEW

VMRay Threat Identifiers (9 rules, 9 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #1) fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe renames multiple user files.			
5/5	User Data Modification	Appends new extensions to many filenames	1	Ransomware
	• Renames 323 files by appending the extension ".rtcrypted".			
4/5	Reputation	Malicious file detected via reputation	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
3/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #1) fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe tries to detect 360TotalSecurity by file artifact.			
2/5	Discovery	Searches for sensitive browser data	1	-
	• (Process #1) fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe searches for sensitive data of web browser "Internet Explorer / Edge" by file.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe enables process privilege "SeDebugPrivilege".			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #1) fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe adds ""C: \Users\OqXZRaykm\Desktop\fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe"" to Windows startup via registry.			
1/5	Mutex	Creates mutex	1	-
	• (Process #4) openwith.exe creates mutex with name "Local\SM0:4348:120:WilError_03".			

Mitre ATT&CK Matrix

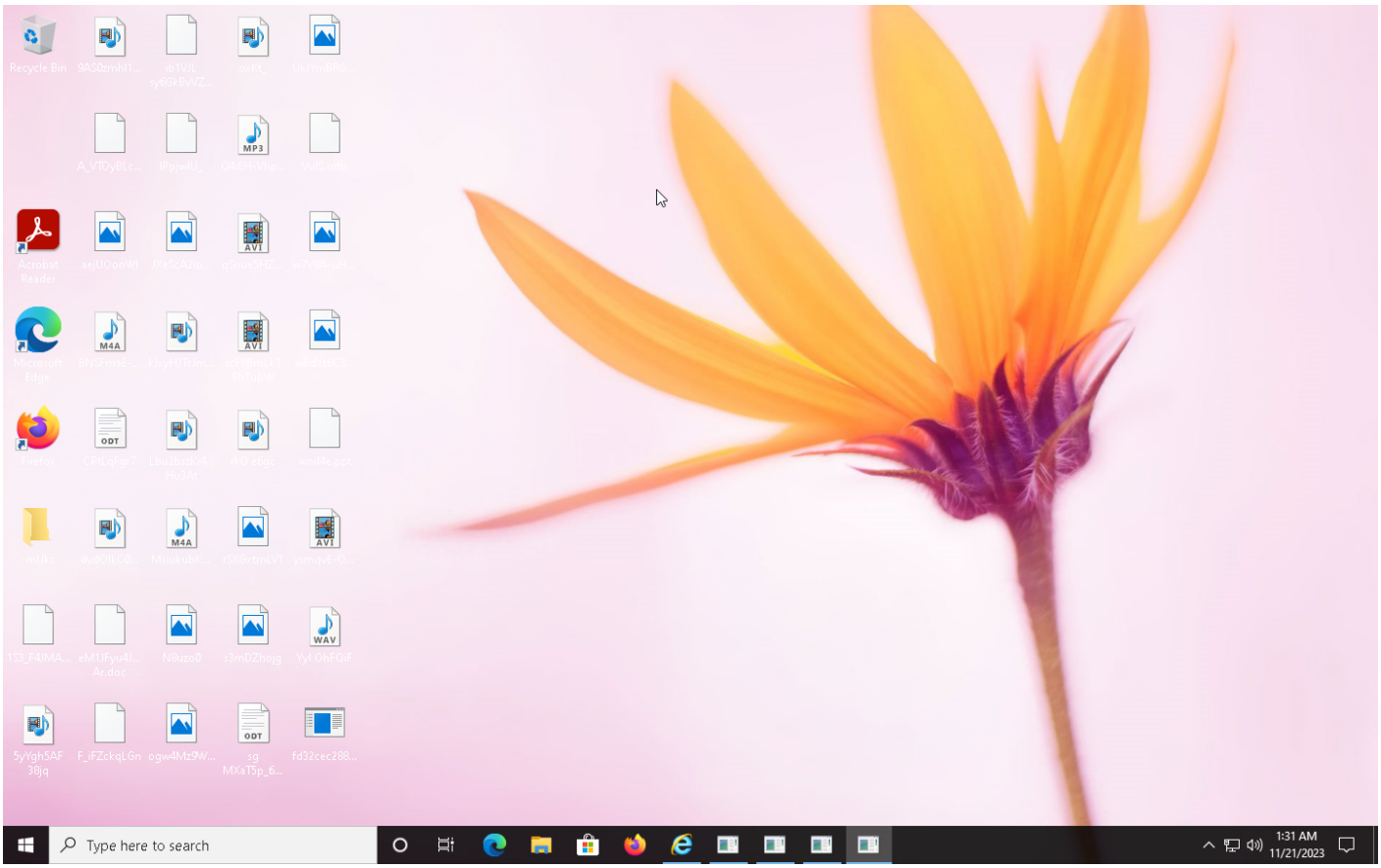
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1112 Modify Registry	#T1081 Credentials in Files	#T1063 Security Software Discovery		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
						#T1083 File and Directory Discovery		#T1005 Data from Local System			

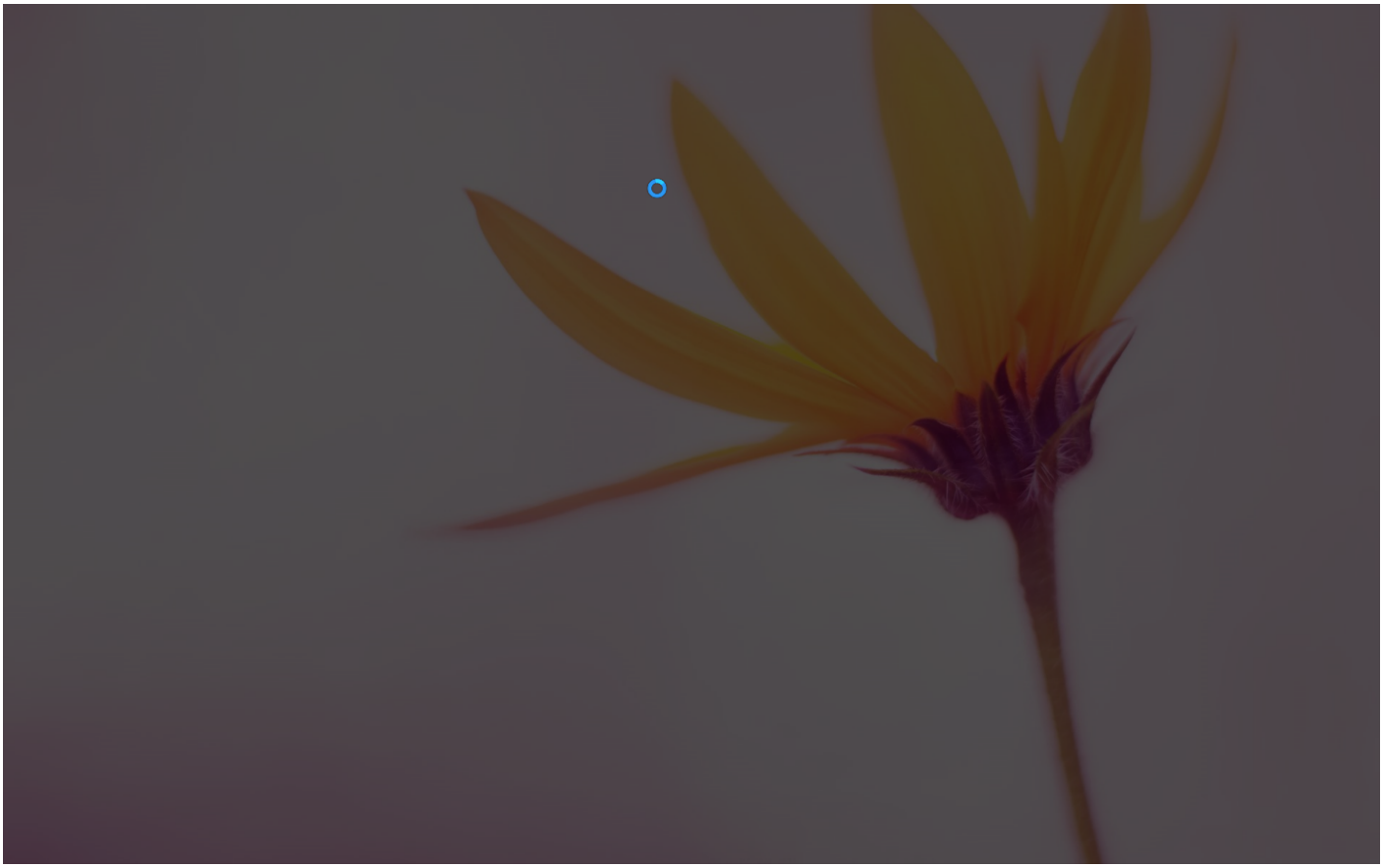
Sample Information

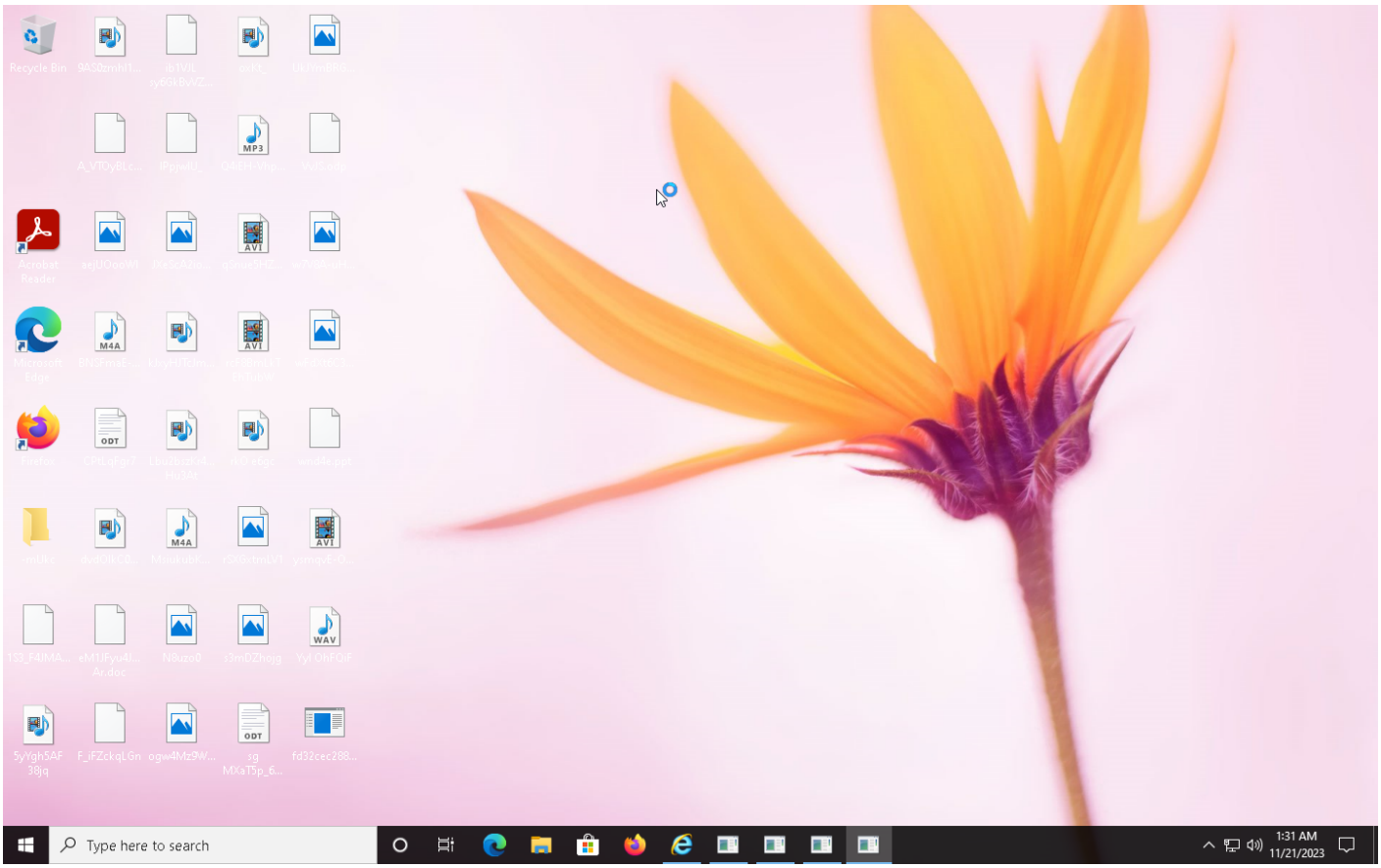
ID	#9333197
MD5	c7cfaca6501361febe27a6b3e66a61bf
SHA1	55a3414b9668596e120139a059db91a306281dcc
SHA256	fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44
SSDeep	768:57NEFbb6uTIm2IfuxvMG0HRvMG0H0uc5tunpqKYhJ:57NEwSljIyvcHRvcH0gnpqKmJ
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe
File Size	26.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

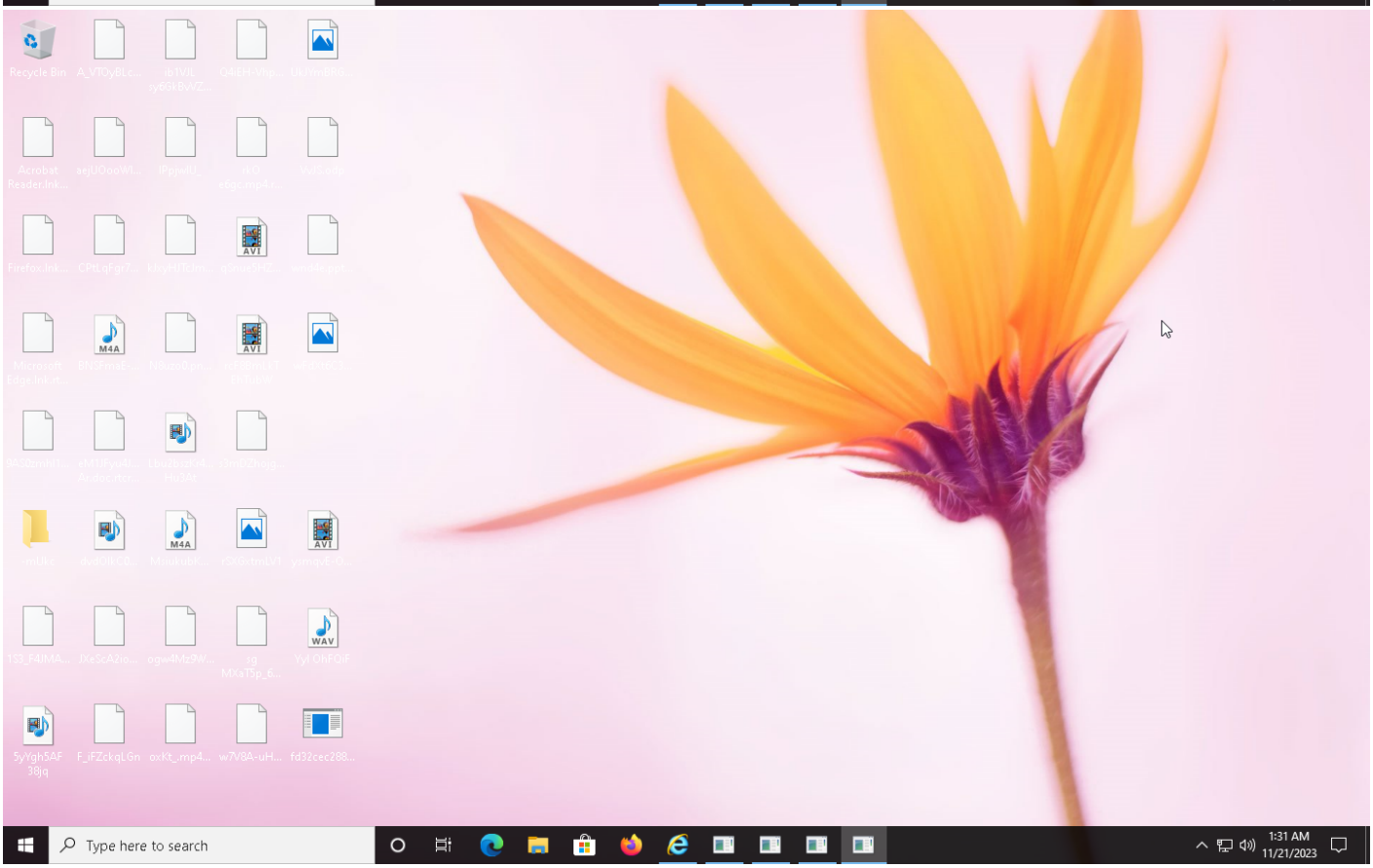
Analysis Information

Creation Time	2023-11-21 00:28 (UTC)
Analysis Duration	00:01:58
Termination Reason	Timeout
Number of Monitored Processes	2
Execution Successful	True
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
Type here to search
1:31 AM
11/21/2023







Screenshots truncated

NETWORK

General

0 bytes total sent

40 bytes total received

1 ports 445

1 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

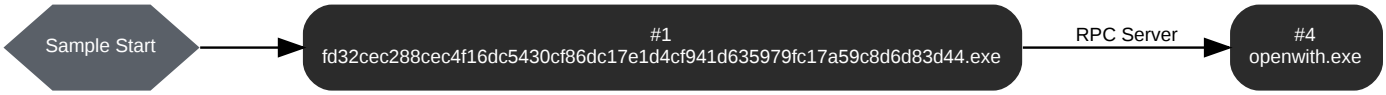
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe

ID	1
File Name	c:\users\oqxzraykm\desktop\fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe
Command Line	"C:\Users\OqXZRaykm\Desktop\fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe"
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 204220, Reason: Analysis Target
Unmonitor End Time	End Time: 321882, Reason: Terminated by timeout
Monitor duration	117.66s
Return Code	Unknown
PID	6100
Parent PID	-
Bitness	64 Bit

Dropped Files (170)

File Name	File Size	SHA256	YARA Match
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\amGLU92hTOyVS.pptx.lnk	998 bytes	7d280030dab18dddb151354e8135b1b7361ecb4d0cadc918f68ba9db26ecc266	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\ouGe8u.lnk	1.27 KB	bb6cbbfce8adbbd82e2efdae1f7cf11df9c66a9443b0bc8816bdfce41d8a8780	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\kQnlf5.lnk	874 bytes	659162fdb2cd449a4c07d6a1610af9811b81cf924f2afb48f287f29e437f0b46	✖
-	450.59 KB	f377d5088ca930e3a3968dea719d2aebdd1a52a60998c6e82530ea7e4b67809e	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\etg7nzxpzhx.lnk.rtcrypted	772 bytes	eca1e0335b6b5f1d4545a954f2edb0dc60b67817ebb99ef97b663f079dd88e50	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\bGzxP7sA1S-0PBuwA.xlsx.lnk.rtcrypted	1023 bytes	94e6632a009b6bc3a60d6f233d47a1d0e6d003e52023cf139a1df3b3bc1c1a42	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\-6jvn5s1cqngvpdy.lnk.rtcrypted	926 bytes	75e8a5c977ee2075f35a695ac0a3dde1fe79bde69356416b322a2135e272b736	✖
C:\Users\OqXZRaykm\AppData\Roaming\snzDMqSsgLa.docx	35.12 KB	c4e0ba0cc2ed43d2f1a77d6addc8a5a3d95c5e56d1afd97b9c6ac77c10dceafe	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\e_2t.lnk	951 bytes	ff0a0ee3281db4d83f0270ff68e3578d11d201ef7b164b732bc9cb222c498dda	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\167vqdu0.lnk.rtcrypted	1.05 KB	979e421d6a85e2e1d49dc2291dbc70bbec55c079a82ae093df92aff46f04c953	✖
C:\Users\OqXZRaykm\AppData\Roaming\CRk7sEcLxn.ppt.rtcrypted	41.03 KB	313b5db39565e7f8bbf2a27e36c89682a20811bb33a58989a79cefc1f13ada60	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\DMLxoOU.lnk	987 bytes	1db71acc9f77282bd85fbe8f1aef9668de7530699bfbbe2bb914f2a32ad2a0f8	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\a_vtoyblcz6nrbg97.xlsx.lnk.rtcrypted	697 bytes	71536422690d8254817541044404b1a0b07d3aaded63e91a69d99efb6377f5f9	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Chkad3-ROtdrHsoCUX.lnk	1.33 KB	227d8f204fa59bf778815c5ada66ecec770355d5e18ef0b46edecb814e82139d	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\AwXZ4sgzr.ots.lnk	999 bytes	f37a279fa170d31818d14e4a88053c16ef394becc0598c412cd830279e06cadc	✖

File Name	File Size	SHA256	YARA Match
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\fhpuak.lnk.rtcrypted	982 bytes	74a95a5497514b8e58e460fe92fd344bcd1740ee230a633523e238238c55901e	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\8gtj48.lnk.rtcrypted	1.02 KB	320ea835e4a2332ec06b5d39936f304886e566637d0feb6faa6fe24023327e63	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3ouk3xp.lnk.rtcrypted	1.05 KB	cf6294ecb50a4558e44cff57987a8ab56e9f57ea6bf646abd8f105c0956ce3dc	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aqmU9TUpYSVIUMRXMae4.lnk.rtcrypted	1.01 KB	1aa3fde7ee65319a0b2286c29e487e650c3a8ee41c0515905503ad197349389e	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\UHkhqoDlS1ZMy4YF1xN.xls.lnk	1.20 KB	e821364544bb6426a21e78e057e21e6a82738fd921ecd26a0976212d16d05692	✖
c:\users\oqxzraykm\appdata\roaming\fkijsgucmnfedtneakl.bmp.rtcrypted	72.39 KB	38ebcecf76842d75101978ec0cfdbb39e7f8391fa3f554f5e9694fc8270b9447	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\MOoazXE175u-tWOUa.lnk	1.13 KB	88623d2039ec8a1ac02d1a88f4f818a6326589b8e7bd042a0ebfd806256fbbfe	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\mL-gKRrD1UEPkt.lnk	941 bytes	53a3c5454e7933b86caba44264f36fc41db129ed87a62f4165730945d4e0d110	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\kx8a.lnk.rtcrypted	1.06 KB	8f0046e62febc82c04c6797d01f7ce246bf08fc9251075c320249e12531d3d9c	✖
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\Narrator.lnk.rtcrypted	1.08 KB	14efee845a62ee0e4482697cd2f932ff2c33c269e37b2cd059b9d92f9bc99c45	✖
C:\Users\OqXZRaykm\AppData\Roaming_tsyATtiMqRdse.mp3	99.61 KB	f10dee14acae63ddcbdddea919a2295b81d38b041956ab60b25f50cf287afe3e	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\rsxgxtmlv1.lnk.rtcrypted	657 bytes	db3449acc6a51cf410dc1a30c65cfa84c6b2f6f47e2e73c0c9827ad611bbdd2c	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\ScFVHzsefvu1Kt2J0.lnk.rtcrypted	1.67 KB	16a13d7004b0af866ebf5f1623c1ae7a4cf8a85bef62dfcefa3a95233d8a4c92	✖
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\administrative tools.lnk.rtcrypted	1.25 KB	a3a264509ca4c2867a0d92de99423a5e679ecebedfccf1c04a62800aa7c09ffc	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\oByX88izFWIaL4.lnk	1.06 KB	270731ed8ad66decb1bdb13fe35666abd9d769431e5efa9fc9b17509fd36fc77	✖
c:\users\oqxzraykm\appdata\roaming\3e8ahn.png.rtcrypted	82.82 KB	268d8c20a5ae790a2e22760c9f2bd1b5cc4ffe028b50a5bcb9c6fcf51b24e4a9	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\sgmxat5p_6ouazikq9b.lnk.rtcrypted	707 bytes	f916e7bce281cc2b25f19522d7070c4170757b54150d85446e95829e55f2cca4	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Firefox.lnk	1011 bytes	7e0a73ccb1185740778b8ea8b15a70f12641aa85d868e4ec46a6c0626e5b1260	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\oGnP UReG2.flv.lnk	955 bytes	499ea16c339667edf24d83ba4f65044b7dedc9b7fe1b7c4f18c290cf67ccafa6	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\-5Ui6BLg2cDEZ1aGZI_.lnk	1.34 KB	adc074639be96c60a97c495c221016eb405e5b4d15c902850c2b440d929a4972	✖
C:\Users\OqXZRaykm\AppData\Roaming\P4nhTG-oMiEDYv2EH.png.rtcrypted	72.83 KB	a6d791ead05c8626375b0beb4cec66946a6d82cf3af840cfa94702df35783519	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\BG-3Ru.lnk.rtcrypted	1.04 KB	9b3cee1709d6fe83ae968051bd216693151d1dac0c7a0c457a06a1b7dc405e12	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\cUOFj.lnk	850 bytes	b4be071f4cc1158a83fa3efa89ef925e00596cd983c160ad16b557c2ffbd80a3	✖
C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk	334 bytes	ebb578e0b60553ad1ab1e5bae9b501a44292f7444544aeec9e40e8b640280938	✖

File Name	File Size	SHA256	YARA Match
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\n8uzo0.lnk.rtcrypted	635 bytes	3c347a9260bdf42fb8db371cd01112bb9d4107aaa0d69693e04d2f611c206bdc	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\qcpl9rrlrntbf01 0.lnk.rtcrypted	1.18 KB	5c7a02ff5fa3ab8155f8e73aa5d1e92301df8dee5250862414255fded57512d2	✖
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\accessibility\on-screen keyboard.lnk.rtcrypted	1.08 KB	53bc26fef621e405ac1f3d0b1be64ff7116e87a21b28a825bbe65607f987a9f8	✖
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell.lnk.rtcrypted	2.48 KB	437ff2eb0832ab3c081449ee7f5a54aee904ff5ccca744c226ebda56d7754452	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aXS6vb.lnk.rtcrypted	1.04 KB	36a20621ff2dff2f8536d51b989865fd16415d3a6b22244cad493ee852a6481c	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\bxOJ-KchVEH.lnk.rtcrypted	1.15 KB	b661953858cf93e94b04c41765511c794016ad3ad185dcadd69371609babaeb5	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\gMmQ7sMpVxP4WwXZrp.lnk	931 bytes	cae36c18552804d7a466f2fd1491f607d1be7eec30658fcca26057a1a0edfed1	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\MfGYDk9Y.ppt.lnk	994 bytes	a21dd4add7c4d934b8cce798edb29fde65cc74452d638392533494d304b4a9a7	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3HUK6hE8Sxy4S31RG.lnk	1.15 KB	adde9cf59bfc651ecfddb52d20a2b087ac2f8840cfe5f0a4d6e8fdd6cfc6e433	✖
C:\Users\OqXZRaykm\AppData\Roaming\DMLxoOU.bmp	73.32 KB	f113819907805d7f3de1dbf56dbc716c99bf3b394c95efaffa6912888ade25f5	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\7AZ xi 6.odp.lnk.rtcrypted	1.32 KB	787460cd38ce8fefa50db53f7cb9a13f1f2cd65b9f3e2136cbe4fd382bcf7479	✖
C:\Users\OqXZRaykm\AppData\Roaming\OTMBVrH.mp4	89.63 KB	3c609f81c1e7ec6e702da16cf0b828c85c838af8db6fea928b42ea0850793ee5	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\TL__DH.flv.lnk.rtcrypted	982 bytes	46566dddc6663331efc6ab52d6416e4ab926891e054340198405e46ca4f258e0	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Dbg3Ddy9SSgsZKwE.doc.lnk	1.10 KB	c2d659a52de629021388178b895eff6feb16945a5e09c30edbbc6237a89bb8b3	✖
C:\Users\OqXZRaykm\Music\fKXZPFzU\LUnjpDpKTSnQmwR3f6Nd\dvC8ktwxOFj7\m1FI2FSO6c8hj.mp3	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Jfz.flv.lnk	1.00 KB	32ff69472fff60f6d1690e0c554625f474e92147c7e32d5a50d743fad0750b66	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\jzacgvj_juniqbgydkt.xlsx.lnk.rtcrypted	1.20 KB	43e654e50c06e75708029cf52dfa8acc93e7bd9c8b9bea41378204758bf9cde1	✖
-	634.70 KB	81e29b7834915ef6b0502db2d60e47f09f51adcb2c6682a5856a2ecbeebac98b	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\music.lnk.rtcrypted	745 bytes	37bcd369104696341a140dedeb5ceef0d972c199f60973042b9af5d698192da7	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\PqsS9Gq RHGz.lnk.rtcrypted	981 bytes	b15517539b32849bcb29a79b640909a1a545c53281be17f601952809539aef48	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\OgZRcboo9.lnk	891 bytes	3c0c26edfdde672260b020e9a4b95970ad3720181ed69722a34098822e27e22b	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\qs6pMlaa5Rs-Y.lnk.rtcrypted	1.31 KB	7508e78e8b4a103800c01ff8f67bfe968a714c2700604ee3f1b28f22da7fd8fb	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt	80 bytes	85335d2c43c8aa0e57cb5386c31fe25dff9f3a842b088240574d7ea01f67835e	✖

File Name	File Size	SHA256	YARA Match
c:\users\oqxzraykm\appdata\roaming\microsoft\internet explorer\quick launch\user pinned\taskbar\file explorer.lnk.rtcrypted	407 bytes	c0ff9a01605662fb1f6100bacb6461b206d1b48479c40691b7a8d89eadf48957	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\snzDMqSsgLa.lnk.rtcrypted	1014 bytes	0748d3c1f8c3bf5a8f607e3e2214a5bfe3b0c1654ab05b40f96d34f6f8592835	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\s3mdzhojg.lnk.rtcrypted	652 bytes	30d775cd476794466d105c93aeef84a6bca4ccf0a805988695b2c9caec1449e5	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\mLpk6DQaJ9.lnk	1.03 KB	cfede4ed97c9a89dedabcf45012ae2c45e9413cee2ea69eda39bb6a07a504217	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\-TpGaKVbHa97zgS.ppt.lnk	1.10 KB	5e8fbe1b32c272e0ef0bcb09c1ca94e0cf9f459e6e7eeaf588996f20ce9b9dd1	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\BmJalddlQRnVT8k_d-q.lnk.rtcrypted	1.07 KB	24a0d765fac94a8daab5ef9af4d31d59bfeddfcee438d63207445f92a052dbe4	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\l_tj4.lnk.rtcrypted	1.04 KB	d51d51b246eced2359a4d95d2967f9034cd2f630196b780333e1f90340fee301	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Microsoft Edge.lnk	2.31 KB	bacfc33be3490e5d260b77149f8845de033f161e8eb9f8438300303dc45c2690	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\JxmR6v_b0d1c1TOkKn.lnk	1.67 KB	b08e94b9d09e56ab84aaf41a91df08e208af0835b7b74a79a5eee4390e852b6e	✖
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\computer.lnk.rtcrypted	335 bytes	29de2d95c0d36ebddb2f245311479317e885f97c7e1618dd90ebb29b0384d6c8	✖
C:\Recovery\WindowsRE\ReAgent.xml	1.09 KB	489539e28d4d297693db853cc320652aed70343049051f767ced1245027ffccc	✖
-	410.66 KB	4aaa22bdfdde073f9cafe10ccfe682e4fd2b911f0d9a333b01d13a5fe2494db1	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\bBT-MFL3sFb3zx-FPOy.lnk	1.14 KB	81a21384051ffc71df102d18734003d5aeff71af78c519668af275f8bd8d0663	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\CNhSRq_988nVmcAoKs l.lnk.rtcrypted	1.68 KB	00905cf0eaf1ff6bfc7300b5beda051ef5a04fab7c6a500a460c86a7cfcde384	✖
c:\users\all users\package cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe.rtcrypted	445.04 KB	0bfcfe86e4b9ec5ad003b5ddcfbb45239776007d9b4cbad93a8f8458d3c98d75	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Microsoft Edge.lnk	2.37 KB	41316b729f2338fb1c48d63ea4e599188e8db01ad2813d2e0942ed92d6d0ecb9	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\krcijzxudvtcey.doc.lnk.rtcrypted	1.28 KB	690626fac42620ba7b0b30e3d3ed96b9ca9c7ae54f5c4185e060d488a975f2ee	✖
C:\Users\OqXZRaykm\AppData\Roaming\MV73nxGICe.jpg	42.29 KB	f3cd45d46380fdb8ee44de80725d97b5d9925b7284222d5d2ec638da6920da38	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\PQbc4C6_8tW2SWaqVE.xlsx.lnk	1.00 KB	d67f0cefaf7a3a14b9604d994bc312fff2e1567f3269ec835e19ea66ea66403c	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\HP_ON6wZYt.lnk.rtcrypted	1004 bytes	a777dec328025de753cae7a127390f36a5c911e18b22e38af8bd8db0c5ebc93b	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\gmibz_0qcerv2he.lnk.rtcrypted	1008 bytes	464e9e7673d827a92d1be50f0249c653882af1b5a6a0e79b0ef5955cbe05f1ba	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\aejuooowi.lnk.rtcrypted	652 bytes	6bd9fc0d17300ac6cc4165113a15ba926bbb591e2817cc680b8ff3f933c71dde	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Roaming (2).lnk	783 bytes	cdc4ba466bef936fec87c34f9e29a41767af8d40c63a235aa477ab985f00f653	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\fenqgag3ychp.lnk.rtcrypted	1.16 KB	2f47b0025560eab963e8498c888d1e0e9b491ee60b4e60c8236e53ffabc67654	✖

File Name	File Size	SHA256	YARA Match
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\putuvkak.xlsx.lnk.rtcrypted	1.09 KB	b12cfefbb20c7bbbfff567a5a938500e7ae50ead0d92eab90b3ca5e49948d726	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\lbLbIV.lnk	1.10 KB	6d44d030a1b0c478d6d59e3cd75cb682e1101f55bcfa66e5ef69c41140baf748	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\6zSAXoBMshJ arRcZrD.lnk	1.19 KB	f1a4731b946ec88662ddddc4a06f579e66ad85f239f3ebd0d14f614accb672cd	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\hIUicmYfr BOKO-G7dUP.flv.lnk	1005 bytes	7a192c248fa58938f7fa8097ce3b810121e08a9478c3bda39abcfdf130203d1c	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\prv-43xC-PpR5k.ppt.lnk.rtcrypted	787 bytes	e8976e64811dde4ba5bfd72c9371cd0e628b903089d4cd9b9dd72b4ea52da753	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\OgZRcboo9 (2).lnk	891 bytes	e9ad432fed16c6de5c1355753015ea665a76dbdd907892b658f070d4532ff8cd	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\blfnup.lnk.rtcrypted	869 bytes	75b93c5f91c64994d136ff67e3435d6ede6267578bf4c07ea80b4f68ac202fdb	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Roaming.lnk	783 bytes	63949922f53956370dcf8b6fee8d9455800db90c7afae6d0ddb40a49bf42b796	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\AI-BTkK-C.lnk.rtcrypted	1.15 KB	6966a361ed169cdaf82e62bf4c6b43740d021e929a5771dac36f3c165adb3aa5	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\srqzB.flv.lnk	1.01 KB	c6007b718c93e84381c9c24166a04ee2a4ed544b330938c2dea60aeebb822ad9	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\ovlgxdjo_8cmq.doc.lnk.rtcrypted	1019 bytes	280779a2e750624a5d861240a9043de0dbae57e394045ab3a987b59e1f27307b	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\fKlJsgucmnFedTn EAkl.lnk	1.03 KB	dc56df790f505b6b52f72373955749e705fbb2b33448d46d0ce5becd6ec57d77	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\9bap9uzx.lnk.rtcrypted	961 bytes	eb4795b18efb317f29dfdd13f7478e43324fb5bc4dd84902151b9ea2ca138271	✖
C:\Users\OqXZRaykm\AppData\Roaming\nE3j.mp3.rtcrypted	45.75 KB	b4857813fcc38349767998900ffebb7d0e455bad69e93194ba3b697fb5295a6a	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Common Files.lnk	710 bytes	318d0921e8db06b3b65d3201c661501cec8d0406aa9bdb031b87325b56759a30	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\cYW1VXatB-JI8vQr.lnk	1019 bytes	a095b15d16f580edb05022fdbe7ec534b1c3dd00844f32074a59c8a014282fa5	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aucpxM.lnk	1.31 KB	2dcfe63e1b718b40d1fc2ee24b5252e0a35e2aa6ad66967d2dd6c1917dfc40c0	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\iku4z6njtis4ci7xut.lnk.rtcrypted	1.47 KB	76f67f8e4712027a151c2e50380994cf2c2ec19ac93824146fe52840b8a7f341	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\5jvufsxko (2).lnk.rtcrypted	1.11 KB	2e238395780b4e56cea7ad6859c70bf7748f3e796d71615913a85c5742ae499f	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\evzv9g78hf1 1b20ex.lnk.rtcrypted	1.31 KB	596663433ca3415595285471e6acfd1a95446f21808c2f5d89a6d4823f01e932	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\gDn4S0f.ppt.lnk	1.25 KB	185dfbb6c814985be8638c349fae34245cfc6e1eb21c7e7be7a6accbea82191e	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\LUnjpDpKTSnQmwR3f6Nd.lnk	1.01 KB	cef430a5fab309b4736764cd440fb5bd9023a7d4c0208637a34e9dd6c1f60bf9	✖

File Name	File Size	SHA256	YARA Match
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\cptlqfgr7.lnk.rtcrypted	652 bytes	e69ac6cefddb4c41ff3c31615cc339db0b279cdceacb6c30e23930be1679c2aa	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\csrpjbn.lnk.rtcrypted	994 bytes	ba7f06cde546c77b651ae5c52a522f6e1de8276c072e485297ff37366f2123ea	✖
c:\users\oqxzraykm\appdata\roaming\mfgydk9y.ppt.rtcrypted	74.84 KB	745b4958c222791a14c77c439a894b2068410b3aac0b3b3245579830af00a9e2	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3um74xQY2dRtB2 VeQ.lnk	807 bytes	f58a037b8a882d8af8cb9f985a224b811f1d1ea61908061ccf5ccff4b00be8d0	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\I-byI6.lnk	1.13 KB	87db6a84945a50185a06e6eda9b12e45eb8c784c49e8357911272b8b0bb4ee55	✖
C:\Users\OqXZRaykm\AppData\Roaming\CSRpjbn.docx	13.53 KB	ad00198d8b09bfa9f93f2eeb7964d6795d814c5cefe3c96f8f7c7883406d3db4	✖
C:\Users\OqXZRaykm\AppData\Roaming\FHPuaK.png	39.14 KB	fd5aca2b8391dfc8c13780b2d1002f101e5e012972d934f7e2da419624d57bd5	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\dvC8ktwxOFj7.lnk	1.15 KB	4c1ce0a35308fe2ded924a8fa15876c315efc15f16a3a1a9e235ce5cdfa1defc	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\em1jfyu4jyx_v ar.doc.lnk.rtcrypted	687 bytes	9efd76a13a3d2fc1f6d09d8d50ceec9dba8b2b199147655a3bb037fa419df225	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\obvxwpqybk.pptx.lnk.rtcrypted	983 bytes	53c9c8cb3e6c5241b5bae18c8a99bfa951f2ebedffe53432d4c5a9ce6063f3c8	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3mZ1.lnk	1.40 KB	24b6483b2e932a99025f6dcaf6dfe2a95fff43f7348d909757f46dede0c08452	✖
-	444.90 KB	bb5c95fb882f01a7f664f76061414e48709f57b0f1f9865c9af683fb6410ab9a	✖
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\Magnify.lnk.rtcrypted	1.08 KB	b858d03aed31262b13b66ffdd085c26b8f5f9228b0a77a6e0dbadaf667714e02	✖
-	635.32 KB	31e8568ecec6727cfc94e0a00908a41415f0ba16d48619cddae98b6ad631300c	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\LFcvTFKIe.lnk	1.34 KB	d6184f2a0deb2febaca2cd1c495cd88413765531f8552cafb31ee64afb8fa93c	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\-mUkc.lnk.rtcrypted	550 bytes	d0197e3c5bf5b741078ab696e366acd6e09c58c0db74f43e7ae4dd84ab18b464	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\61De8WLPska01oVom.lnk	1.13 KB	4257a852962e206ca35638679601012396aaed45643908000e31755d379175d4	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\40MOvGfppj4bDSgoaCIa.lnk	1.34 KB	d957c406981f8b85a5cae56701becb9c5d85d6a7729e9aacd9cdd580d0d7988a	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\2sjqfwb3sa1-ail-.lnk.rtcrypted	1.15 KB	7fadc38992fe8116c79cd7022dca4c4fce953d7ed9d0296289592c00172064c3	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\CxX 3.lnk	894 bytes	9cae94cd132202d29524373043c6a61f243e78337802c3ed77b75a3c3b118061	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3bJ1.lnk	1.11 KB	82fc8cda9c697c0e1e64160af7f7a6c668ba3a230759c856fc6d758fb0a5a6b0	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\rFTl6BSzg_.lnk.rtcrypted	891 bytes	2fd644e1d8958a6fed89fd34db260dc40cda1e64ccee8016950fb64fcb5a34eb	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\tKwoXg9sP.lnk	1.09 KB	f55db5636c177b5fd457fc6768204038175285cd654e3ba0dbe6e68781d8ea2a	✖

File Name	File Size	SHA256	YARA Match
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\GDLIsvWIqGajKiRN9dGO.pptx.lnk	1.01 KB	f13490ebd21118f2ed16cc1fd064f8a0b983c78417a502c7b87b94b6efd78920	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\smN8Rnib6nLWu.xlsx.lnk	998 bytes	f22733b5127f8f624db5c0385e2a9732776e7afe80d937c968c7f7ba887cfc39	✖
C:\Users\OqXZRaykm\AppData\Local\RansomeToad.txt	12.96 KB	eaaa86a716a867b6d4ca3da87d6217363cbd904beb15b6396c8d8d1534e15a58	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\cidai4wobarezgunw3z.xlsx.lnk.rtcrypted	1.00 KB	1899a244fc1d303e822585f29a76fbc9fd21e5c21f115231575b73c55978b3b9	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\novXISG4jJT9ZShRo.ods.lnk	1.11 KB	77797307bd4961224f28d5854e50653e311127e3ff4bd1d8300a46f214f32bf4	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\eiweexdtyapi-m.doc.lnk.rtcrypted	1.00 KB	ff93787f6a9fa04ec132a77377e9446b482aca52fd1a3e49343d3b228f9a541b	✖
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\command prompt.lnk.rtcrypted	1.12 KB	b091603e1457b90b60c512e7376efd6469730f8a91542f8acb0b32caaeb35d4f	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\UkJYmBRGn-I6870DyiLq.lnk	707 bytes	32d67fa8cfb8aa08ed3cf42dd14651a6f3d48e97ca8c426466dae72a2d14a1c4	✖
C:\Users\OqXZRaykm\AppData\Roaming\eHXp79eO.mp3	7.13 KB	43b3b9e20102b220f0d3952f9605b7b725bd1d357f1b46261c7078a3d96b7002	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3q1llb5op_qjtca2ednb.odp.lnk.rtcrypted	1.40 KB	e311261af9bcef8ad530eecb1ae25df23d4de6d3504ed679eddf2969ae82dee6	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\u7sDs2LZ.lnk	1.28 KB	64e64d50d5b1c5183a2d88248640347958094ba0860ea92dd10de31b5b57652c	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\m62mMrqX1.pptx.lnk	978 bytes	2de2974483d2c0713a7442a3347f793e6106f948115dfc2ad543f935057000730	✖
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell (x86).lnk.rtcrypted	2.48 KB	ef744e32a57d99ba8112d86f96b9d6f4111973525935efa803c4975f3ef4042c	✖
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\dy8.lnk	963 bytes	85225f7f9dbe7a18ede2fc87bc51d685fb26c0177ae77c2b5751f1427b18407f	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\7qsm7bo389nple.lnk.rtcrypted	1.00 KB	9aa0ff320166b89121c4f9a15972dcf41cdff2d85f63667c27785eb6a59bbff8	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3e8ahn.lnk.rtcrypted	982 bytes	7f6f509f29349c0d18a4a50c73b73e131a31d3b03219bd4db0fa564b33aa8232	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\fabe6lam6xetp.lnk.rtcrypted	1.01 KB	6eba24e80f7e331eda526d820e53b39cd022f677063ff0f8bb2b3f107fb93f70	✖
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\5jvufsxko.lnk.rtcrypted	1.11 KB	2d192704f17219df70ff6da8bc8270149abf57cf98fa613aba3e7405b558ced9	✖
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\run.lnk.rtcrypted	409 bytes	724169d1c2088e4aea1b5eb052ff70e6c70978b41e9e492f0ad8b2c7ce00589d	✖

Reduced dataset

Host Behavior

Type	Count
Environment	1
Registry	7
File	3741
User	1
System	600

Type	Count
Module	25
Window	12
-	1
Keyboard	97
Process	1

Process #4: openwith.exe

ID	4
File Name	c:\windows\system32\openwith.exe
Command Line	C:\Windows\system32\OpenWith.exe -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 254899, Reason: RPC Server
Unmonitor End Time	End Time: 321882, Reason: Terminated by timeout
Monitor duration	66.98s
Return Code	Unknown
PID	4348
Parent PID	6100
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
COM	1
Mutex	2
Module	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44	C:\Users\OqXZRaykm\Desktop\fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe	Sample File	26.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
489539e28d4d297693db853cc320652aed70343049051f767ced1245027ffccc	C:\Recovery\WindowsRE\ReAgent.xml, c:\recovery\windowsre\reagent.xml.rtcrypted, C:\Recovery\WindowsRE\ReAgent.xml.rtcrypted	Dropped File	1.09 KB	text/plain	Access, Create, Delete, Read, Write	CLEAN
4aaa22bdfdde073f9cafe10ccfe682e4fd2b911f0d9a333b01d13a5fe2494db1	C:\Users\All Users\Adobe\Setup\{AC76BA86-7AD7-FFFF-7B44-AC0F074E4100}\Setup.exe.rtcrypted, c:\users\all users\adobe\setup\{ac76ba86-7ad7-ffff-7b44-ac0f074e4100}\setup.exe.rtcrypted, c:\programdata\adobe\setup\{ac76ba86-7ad7-ffff-7b44-ac0f074e4100}\setup.exe	Dropped File	410.66 KB	application/octet-stream	Access, Create, Write	CLEAN
f377d5088ca930e3a3968dea719d2aebdd1a52a60998c6e82530ea7e4b67809e	C:\Users\All Users\Package Cache\{050d4fc8-5d48-4b8f-8972-47c82c46020f}\vcredist_x64.exe.rtcrypted, c:\users\all users\package cac... ...972-47c82c46020f}\vcredist_x64.exe.rtcrypted, c:\programdata\package cache\{050d4fc8-5d48-4b8f-8972-47c82c46020f}\vcredist_x64.exe	Dropped File	450.59 KB	application/octet-stream	Access, Create, Write	CLEAN
0bfcfe86e4b9ec5ad003b5ddcfbb45239776007d9b4cbad93a8f8458d3c98d75	c:\users\all users\package cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe.rtcrypted, C:\Users\All Users\Package Cac... ...bc1-97e33d9c2d6f}\vcredist_x86.exe.rtcrypted, c:\programdata\package cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe	Dropped File	445.04 KB	application/octet-stream	Access, Create, Write	CLEAN
81e29b7834915ef6b0502db2d60e47f09f51adcb2c6682a5856a2ecbeebac98b	C:\Users\All Users\Package Cache\{6ba9fb5e-8366-4cc4-bf65-25fe9819b2fc}\VC_redist.x86.exe.rtcrypted, c:\users\all users\package ca... ...5-25fe9819b2fc}\vc_redist.x86.exe.rtcrypted, c:\programdata\package cache\{6ba9fb5e-8366-4cc4-bf65-25fe9819b2fc}\vc_redist.x86.exe	Dropped File	634.70 KB	application/octet-stream	Access, Create, Write	CLEAN
bb5c95fb882f01a7f664f76061414e48709f57b0f1f9865c9af683fb6410ab9a	C:\Users\All Users\Package Cache\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\vcredist_x64.exe.rtcrypted, c:\users\all users\package cac... ...50c-4b9ceb6d66c6}\vcredist_x64.exe.rtcrypted, c:\programdata\package cache\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\vcredist_x64.exe	Dropped File	444.90 KB	application/octet-stream	Access, Create, Write	CLEAN
31e8568ecec6727cfc94e0a00908a41415f0ba16d48619cddae98b6ad631300c	c:\users\all users\package cache\{d4cecf3b-b68f-4995-8840-52ea0fab646e}\vc_redist.x64.exe.rtcrypted, C:\Users\All Users\Package Ca... ...0-52ea0fab646e}\VC_redist.x64.exe.rtcrypted, c:\programdata\package cache\{d4cecf3b-b68f-4995-8840-52ea0fab646e}\vc_redist.x64.exe	Dropped File	635.32 KB	application/octet-stream	Access, Create, Write	CLEAN
40394205c5c0f1bf6944cfac40d3cbb14ac2c781edc0f84a76a0efbf426956e1	C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk.rtcrypted, c:\users\default\appdata\ro... ...orer\Quick Launch\Shows Desktop.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk	Dropped File	352 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ebb578e0b60553ad1ab1e5bae9b501a44292f7444544aeec9e40e8b640280938	C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk, C:\Users\OqXZRaykm\AppData\Roaming\... ... switcher.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk.rtcrypted	Dropped File	334 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7db237ad2a225eeb7e19a09b53abe29169945c8d5279cbeb775824cf57389de0	C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Fax Recipient.lnk, C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Fax Recipient.lnk.rtcrypted, c:\users\default\appdata\roaming\microsoft\windows\sendto\fax recipient.lnk.rtcrypted	Dropped File	1.09 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b858d03aed31262b13b66ffdd085c26b8f5f9228b0a77a6e0dbadaf667714e02	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\Magnify.lnk.rtcrypted, c:\users\default\appda... ...essibility\magnify.lnk.rtcrypted, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\Magnify.lnk	Dropped File	1.08 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
14efee845a62ee0e4482697cd2f932ff2c33c269e37b2cd059b9d92f9bc99c45	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\Narrator.lnk.rtcrypted, c:\users\default\appd... ...sibility\narrator.lnk.rtcrypted, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\Narrator.lnk	Dropped File	1.08 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
53bc26fef621e405ac1f3d0b1be64ff7116e87a21b28a825bbe65607f987a9f8	c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\accessibility\on-screen keyboard.lnk.rtcrypted, C:\Users\De... ...eyboard.lnk.rtcrypted, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\On-Screen Keyboard.lnk	Dropped File	1.08 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
a3a264509ca4c2867a0d92de99423a5e679ecebedfccf1c04a62800aa7c09ffc	c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\administrative tools.lnk.rtcrypted, C:\Users\D... ... Tools.lnk.rtcrypted, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\Administrative Tools.lnk	Dropped File	1.25 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b091603e1457b90b60c512e7376efd6469730f8a91542f8acb0b32caaeb35d4f	c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\command prompt.lnk.rtcrypted, C:\Users\Default... ...mmand Prompt.lnk.rtcrypted, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\Command Prompt.lnk	Dropped File	1.12 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
29de2d95c0d36ebddb2f245311479317e885f97c7e1618dd90ebb29b0384d6c8	c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\computer.lnk.rtcrypted, C:\Users\Default\AppDa... ...tem Tools\computer.lnk.rtcrypted, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\computer.lnk	Dropped File	335 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
465dc73a1b8f53f5a122561b822d898a3e3ba6b7916bd4b039d799e30bdabb0c	C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\Control Panel.lnk.rtcrypted, c:\users\default\...\control panel.lnk.rtcrypted, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\Control Panel.lnk	Dropped File	405 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
c0ff9a01605662fb1f6100bacb6461b206d1b48479c40691b7a8d89eadf48957	c:\users\oqxzraykm\appdata\roaming\microsoft\internet explorer\quick launch\user pinned\taskbar\file explorer.lnk.rtcrypted, C:\Us...\...rer.lnk.rtcrypted, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\File Explorer.lnk.rtcrypted	Dropped File	407 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
724169d1c2088e4aea1b5eb052ff70e6c70978b41e9e492f0ad8b2c7ce00589d	c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\run.lnk.rtcrypted, C:\Users\Default\AppData\Ro...\...ograms\System Tools\Run.lnk.rtcrypted, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\Run.lnk	Dropped File	409 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
ef744e32a57d99ba8112d86f96b9d6f4111973525935efa803c4975f3ef4042c	c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell (x86).lnk.rtcrypted, ...rtcrypted, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\Windows PowerShell (x86).lnk	Dropped File	2.48 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
437ff2eb0832ab3c081449ee7f5a54aee904ff5ccca744c226ebda56d7754452	c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell.lnk.rtcrypted, C:\Use...\...ll.lnk.rtcrypted, C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\Windows PowerShell.lnk	Dropped File	2.48 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
268d8c20a5ae790a2e22760c9f2bd1b5cc4ffe028b50a5bcb9c6fcf51b24e4a9	c:\users\oqxzraykm\appdata\roaming\3e8ahn.png.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\3E8aHN.png.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\3E8aHN.png	Dropped File	82.82 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
313b5db39565e7f8bbf2a27e36c89682a20811bb33a58989a79cefc1f13ada60	C:\Users\OqXZRaykm\AppData\Roaming\CRk7sEcLxn.ppt.rtcrypted, c:\users\oqxzraykm\appdata\roaming\crk7seclxn.ppt.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\CRk7sEcLxn.ppt	Dropped File	41.03 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
ad00198d8b09bfa9f93f2eeb7964d6795d814c5cefe3c96f8f7c7883406d3db4	C:\Users\OqXZRaykm\AppData\Roaming\CSRpjbn.docx, c:\users\oqxzraykm\appdata\roaming\csrpjbn.docx.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\CSRpjbn.docx.rtcrypted	Dropped File	13.53 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
f113819907805d7f3de1dbf56dbc716c99bf3b394c95efaffa6912888ade25f5	C:\Users\OqXZRaykm\AppData\Roaming\DMLxoOU.bmp, C:\Users\OqXZRaykm\AppData\Roaming\DMLxoOU.bmp.rtcrypted, c:\users\oqxzraykm\appdata\roaming\dmlxoou.bmp.rtcrypted	Dropped File	73.32 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
43b3b9e20102b220f0d3952f9605b7b725bd1d357f1b46261c7078a3d96b7002	C:\Users\OqXZRaykm\AppData\Roaming\eHXp79eO.mp3, C:\Users\OqXZRaykm\AppData\Roaming\eHXp79eO.mp3.rtcrypted, c:\users\oqxzraykm\appdata\roaming\ehxp79eo.mp3.rtcrypted	Dropped File	7.13 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
3edec5db525b6c54cf11cab86f87665058af46913c9b0caa163a9aaeea45c7d6	c:\users\oqxzraykm\appdata\roaming\eiweexdtyapi-m.doc.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\ElweEXdtYapI-M.doc.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\ElweEXdtYapI-M.doc	Dropped File	70.91 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
fd5aca2b8391dfc8c13780b2d1002f101e5e012972d934f7e2da419624d57bd5	C:\Users\OqXZRaykm\AppData\Roaming\FHPuaK.png, c:\users\oqxzraykm\appdata\roaming\fhpuak.png.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\FHPuaK.png.rtcrypted	Dropped File	39.14 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
38ebcecf76842d75101978ec0cfdbb39e7f8391fa3f554f5e9694fc8270b9447	c:\users\oqxzraykm\appdata\roaming\fkijsgucmnfedtn eakl.bmp.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\fKIJsgucmnFedTn EAkl.bmp.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\fKIJsgucmnFedTn EAkl.bmp	Dropped File	72.39 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
2ab5bae60b63c26b772180ce34a32e2a813a927e48eb42167c886b036924c806	c:\users\oqxzraykm\appdata\roaming\g50o8m9fizrg8.mp4.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\G50O8m9fIZrG8.mp4.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\G50O8m9fIZrG8.mp4	Dropped File	73.90 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
745b4958c222791a14c77c439a894b2068410b3aac0b3b3245579830af00a9e2	c:\users\oqxzraykm\appdata\roaming\mfgydk9y.ppt.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\MfGYDk9Y.ppt.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\MfGYDk9Y.ppt	Dropped File	74.84 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
f3cd45d46380fdb8ee44de80725d97b5d9925b7284222d5d2ec638da6920da38	C:\Users\OqXZRaykm\AppData\Roaming\MV73nxGICe.jpg, C:\Users\OqXZRaykm\AppData\Roaming\MV73nxGICe.jpg.rtcrypted, c:\users\oqxzraykm\appdata\roaming\mv73nxgice.jpg.rtcrypted	Dropped File	42.29 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b4857813fcc38349767998900ffebb7d0e455bad69e93194ba3b697fb5295a6a	C:\Users\OqXZRaykm\AppData\Roaming\nE3j.mp3.rtcrypted, c:\users\oqxzraykm\appdata\roaming\ne3j.mp3.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\nE3j.mp3	Dropped File	45.75 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
3c609f81c1e7ec6e702da16cf0b828c85c838af8db6fea928b42ea0850793ee5	C:\Users\OqXZRaykm\AppData\Roaming\OTMBVrH.mp4, C:\Users\OqXZRaykm\AppData\Roaming\OTMBVrH.mp4.rtcrypted, c:\users\oqxzraykm\appdata\roaming\otmbvrh.mp4.rtcrypted	Dropped File	89.63 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
33eb593a5d3c219598db918af7ba50b427063b91346f1482ee062f8146fa985e	C:\Users\OqXZRaykm\AppData\Roaming\OvLGXdJo_8CMQ.doc, C:\Users\OqXZRaykm\AppData\Roaming\OvLGXdJo_8CMQ.doc.rtcrypted, c:\users\oqxzraykm\appdata\roaming\ovlgxdjo_8cmq.doc.rtcrypted	Dropped File	28.29 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
a6d791ead05c8626375b0beb4cec66946a6d82cf3af840cfa94702df35783519	C:\Users\OqXZRaykm\AppData\Roaming\P4nhTG-oMiEDYv2EH.png.rtcrypted, c:\users\oqxzraykm\appdata\roaming\p4nhtg-omiedyv2eh.png.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\P4nhTG-oMiEDYv2EH.png	Dropped File	72.83 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c4e0ba0cc2ed43d2f1a77d6addc8a5a3d95c5e56d1afd97b9c6ac77c10dceafe	C:\Users\OqXZRaykm\AppData\Roaming\snzDMqSsgLa.docx, C:\Users\OqXZRaykm\AppData\Roaming\snzDMqSsgLa.docx.rtcrypted, c:\users\oqxzraykm\appdata\roaming\snzdmqssgla.docx.rtcrypted	Dropped File	35.12 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
f10dee14acae63ddcbdddea919a2295b81d38b041956ab60b25f50cf287afe3e	C:\Users\OqXZRaykm\AppData\Roaming_tsyATtiMqRdse.mp3, c:\users\oqxzraykm\appdata\roaming_tsyattimqrdse.mp3.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming_tsyATtiMqRdse.mp3.rtcrypted	Dropped File	99.61 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7a920f42c5a7e848ef616272ec8c8149af553f73affc03260fe327c07131722e	C:\Users\OqXZRaykm\AppData\Roaming__elk.ppt, C:\Users\OqXZRaykm\AppData\Roaming__elk.ppt.rtcrypted, c:\users\oqxzraykm\appdata\roaming__elk.ppt.rtcrypted	Dropped File	59.38 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
bacfc33be3490e5d260b77149f8845de033f161e8eb9f8438300303dc45c2690	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Microsoft Edge.lnk, C:\Users\OqXZRaykm\AppData\Roaming... ...osoft Edge.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\internet explorer\quick launch\microsoft edge.lnk.rtcrypted	Dropped File	2.31 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7e0a73ccb1185740778b8ea8b15a70f12641aa85d868e4ec46a6c0626e5b1260	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Firefox.lnk, C:\Users\OqXZRaykm\Ap... ...k.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\internet explorer\quick launch\user pinned\taskbar\firefox.lnk.rtcrypted	Dropped File	1011 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
41316b729f2338fb1c48d63ea4e599188e8db01ad2813d2e0942ed92d6d0ecb9	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Microsoft Edge.lnk, c:\users\oqxzr... ...pted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Microsoft Edge.lnk.rtcrypted	Dropped File	2.37 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
85335d2c43c8aa0e57cb5386c31fe25dff9f3a842b088240574d7ea01f67835e	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt, c:\users\oqxzraykm\appdata\roa... ...istory.txt.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt.rtcrypted	Dropped File	80 bytes	text/plain	Access, Create, Delete, Read, Write	CLEAN
adc074639be96c60a97c495c221016eb405e5b4d15c902850c2b440d929a4972	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\-5Ui6BLg2cDEZ1aGZI_.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\... ...t\-5ui6blg2cdez1agzi_.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\-5Ui6BLg2cDEZ1aGZI_.lnk.rtcrypted	Dropped File	1.34 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
75e8a5c977ee2075f35a695ac0a3dde1fe79bde69356416b322a2135e272b736	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\-6jvn5s1cqngvpdy.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Mic... ...ft\Windows\Recent\-6JvN5S1cqNGvPDY.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\-6JvN5S1cqNGvPDY.lnk	Dropped File	926 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d0197e3c5bf5b741078ab696e366acd6e09c58c0db74f43e7ae4dd84ab18b464	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\-mUkc.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\-mukc.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\-mUkc.lnk	Dropped File	550 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
5e8fbe1b32c272e0ef0bcb09c1ca94e0cf9f459e6e7eeaf588996f20ce9b9dd1	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\-TpGaKVbHa97zgS.ppt.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\... ...t\-TpGaKVbHa97zgS.ppt.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\-tpgakvbha97zgs.ppt.lnk.rtcrypted	Dropped File	1.10 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
979e421d6a85e2e1d49dc2291dbc70bbec55c079a82ae093df92aff46f04c953	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\167vqdu0.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\167VqDu0.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\167VqDu0.lnk	Dropped File	1.05 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7fadc38992fe8116c79cd7022dca4c4fce953d7ed9d0296289592c00172064c3	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\2sjqfwb3sa1-ail-.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Mic... ...ft\Windows\Recent\2sJQfwB3SA1-ail-.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\2sJQfwB3SA1-ail-.lnk	Dropped File	1.15 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
82fc8cda9c697c0e1e64160af7f7a6c668ba3a230759c856fc6d758fb0a5a6b0	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3bJ1.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3bJ1.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3bj1.lnk.rtcrypted	Dropped File	1.11 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7f6f509f29349c0d18a4a50c73b73e131a31d3b03219bd4db0fa564b33aa8232	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3e8ahn.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3E8aHN.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3E8aHN.lnk	Dropped File	982 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
adde9cf59bfc651ecfddb52d20a2b087ac2f8840cfe5f0a4d6e8fdd6cfc6e433	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3HUK6hE8Sxy4S31RG.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\wi... ...ecent\3huk6he8sxy4s31rg.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3HUK6hE8Sxy4S31RG.lnk.rtcrypted	Dropped File	1.15 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
24b6483b2e932a99025f6dcaf6dfe2a95fff43f7348d909757f46dede0c08452	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3mZ1.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3mZ1.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3mz1.lnk.rtcrypted	Dropped File	1.40 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
cf6294ecb50a4558e44cff57987a8ab56e9f57ea6bf646abd8f105c0956ce3dc	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3ouk3xp.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3oUk3Xp.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3oUk3Xp.lnk	Dropped File	1.05 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
86b68471fc406a9091afbac6c6d18db36a486470f46309214b3b036f209db560	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3p6ohHYs9-.csv.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Wind... ...ws\Recent\3p6ohHYs9-.csv.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3p6ohhys9-.csv.lnk.rtcrypted	Dropped File	1.33 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
e311261af9bcef8ad530eecb1ae25df23d4de6d3504ed679eddf2969ae82dee6	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3q1llb5op_qjtca2ednb.odp.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roa... ...t\3q1llB5Op_QjTca2eDNb.odp.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3q1llB5Op_QjTca2eDNb.odp.lnk	Dropped File	1.40 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
f58a037b8a882d8af8cb9f985a224b811f1d1ea61908061ccf5ccff4b00be8d0	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3um74xQY2dRtB2 VeQ.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\w... ...ent\3um74xqy2drtb2veq.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3um74xQY2dRtB2 VeQ.lnk.rtcrypted	Dropped File	807 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
d957c406981f8b85a5cae56701becb9c5d85d6a7729e9aacd9cdd580d0d7988a	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\40MOvGfppj4bDSgoaCIa.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft... ...40MOvGfppj4bDSgoaCIa.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\40movgfppj4bdsgoacia.lnk.rtcrypted	Dropped File	1.34 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
2e238395780b4e56cea7ad6859c70bf7748f3e796d71615913a85c5742ae499f	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\5jvufsxko(2).lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\5JVUFsxkO (2).lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\5JVUFsxkO (2).lnk	Dropped File	1.11 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
2d192704f17219df70ff6da8bc8270149abf57cf98fa613aba3e7405b558ced9	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\5jvufsxko.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\5JVUFsxkO.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\5JVUFsxkO.lnk	Dropped File	1.11 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
4257a852962e206ca35638679601012396aaed45643908000e31755d379175d4	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\61De8WLPska01oVom.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\wi... ...ecent\61de8wlpska01ovom.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\61De8WLPska01oVom.lnk.rtcrypted	Dropped File	1.13 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f1a4731b946ec88662ddddc4a06f579e66ad85f239f3ebd0d14f614accb672cd	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\6zSAXoBMshJ arRcZrD.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\... ...t\6zSAXoBMshJ arRcZrD.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\6zsaxobmshj arrczrd.lnk.rtcrypted	Dropped File	1.19 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
787460cd38ce8fefa50db53f7cb9a13f1f2cd65b9f3e2136cbe4fd382bcf7479	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\7AZ xi 6.odp.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\7az xi 6.odp.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\7AZ xi 6.odp.lnk	Dropped File	1.32 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
9aa0ff320166b89121c4f9a15972dcf41cdff2d85f63667c27785eb6a59bbff8	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\7qsm7bo389nple.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\7QSM7Bo389nPLE.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\7QSM7Bo389nPLE.lnk	Dropped File	1.00 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
320ea835e4a2332ec06b5d39936f304886e566637d0feb6faa6fe24023327e63	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\8gtj48.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\8gTJ48.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\8gTJ48.lnk	Dropped File	1.02 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
eb4795b18efb317f29dfdd13f7478e43324fb5bc4dd84902151b9ea2ca138271	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\9bap9uzx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\9bAP9Uzx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\9bAP9Uzx.lnk	Dropped File	961 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
6bd9fc0d17300ac6cc4165113a15ba926bbb591e2817cc680b8ff3f933c71dde	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\aejuooowi.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aejUOooWI.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aejUOooWI.lnk	Dropped File	652 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
6966a361ed169cdaf82e62bf4c6b43740d021e929a5771dac36f3c165adb3aa5	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\AI-BTkK-C.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\ai-btkk-c.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\AI-BTkK-C.lnk	Dropped File	1.15 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7d280030dab18dddb151354e8135b1b7361ecb4d0cadc918f68ba9db26ecc266	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\amGLU92hTOyVS.pptx.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\w... ...ent\amglu92htoyvs.pptx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\amGLU92hTOyVS.pptx.lnk.rtcrypted	Dropped File	998 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1aa3fde7ee65319a0b2286c29e487e650c3a8ee41c0515905503ad197349389e	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aqmU9TUpYSVIUMRXMae4.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming...\...ws\recent\aqmu9tupysviumrxmae4.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aqmU9TUpYSVIUMRXMae4.lnk	Dropped File	1.01 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
2dcfe63e1b718b40d1fc2ee24b5252e0a35e2aa6ad66967d2dd6c1917dfc40c0	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aucpxM.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aucpxM.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\aucpxm.lnk.rtcrypted	Dropped File	1.31 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
f37a279fa170d31818d14e4a88053c16ef394becc0598c412cd830279e06cadc	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\AwXZ4sgzr.ots.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\awxz4sgzr.ots.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\AwXZ4sgzr.ots.lnk.rtcrypted	Dropped File	999 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
36a20621ff2dff2f8536d51b989865fd16415d3a6b22244cad493ee852a6481c	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aXS6vb.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\axs6vb.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aXS6vb.lnk	Dropped File	1.04 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7153642269 0d8254817541044404b1a0b07d3aaded63e91a69d99efb6377f5f9	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\a_vtoyblcz6nrbg97.xlsx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roami...\...ecent\A_VTOyBLcz6NRbG97.xlsx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\A_VTOyBLcz6NRbG97.xlsx.lnk	Dropped File	697 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
94e6632a009b6bc3a60d6f233d47a1d0e6d003e52023cf139a1df3b3bc1c1a42	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\bGzxP7sA1S-0PBuwA.xlsx.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roam...\...ent\bgzxp7sa1s-0pbuwa.xlsx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\bGzxP7sA1S-0PBuwA.xlsx.lnk	Dropped File	1023 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
81a21384051ffc71df102d18734003d5aeff71af78c519668af275f8bd8d0663	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\bBT-MFL3sFb3zx-FPOy.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\... ...t\bBT-MFL3sFb3zx-FPOy.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\bbt-mfl3sfb3zx-fpoy.lnk.rtcrypted	Dropped File	1.14 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
9b3cee1709d6fe83ae968051bd216693151d1dac0c7a0c457a06a1b7dc405e12	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\BG-3Ru.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\bg-3ru.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\BG-3Ru.lnk	Dropped File	1.04 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
75b93c5f91c64994d136ff67e3435d6ede6267578bf4c07ea80b4f68ac202fdb	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\blfnup.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\BlfnUP.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\BlfnUP.lnk	Dropped File	869 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
24a0d765fac94a8daab5ef9af4d31d59bfeddfcee438d63207445f92a052dbe4	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\BmJaldd lQRnVT8k_d-q.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\...dows\recent\bmjaldd lqrnvt8k_d-q.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\BmJaldd lQRnVT8k_d-q.lnk	Dropped File	1.07 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b661953858cf93e94b04c41765511c794016ad3ad185dcadd69371609babaeb5	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\bxOJ-KchVEH.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\bxoj-kchveh.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\bxOJ-KchVEH.lnk	Dropped File	1.15 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
227d8f204fa59bf778815c5ada66ecec770355d5e18ef0b46edecb814e82139d	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Chkad3-ROtdrHsoCUX.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\W... ...ent\Chkad3-ROtdrHsoCUX.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\chkad3-rotdrhsocux.lnk.rtcrypted	Dropped File	1.33 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
1899a244fc1d303e822585f29a76fbc9fd21e5c21f115231575b73c55978b3b9	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\cidai4wobarezgunw3z.xlsx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roa...t\CIdAi4WoBaReZGuNW3Z.xlsx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\CIdAi4WoBaReZGuNW3Z.xlsx.lnk	Dropped File	1.00 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
00905cf0eaf1ff6bfc7300b5beda051ef5a04fab7c6a500a460c86a7cfcde384	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\CNhSRq_988nVmcAoKs l.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming...ws\recent\cnhsrq_988nvmcaoksi.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\CNhSRq_988nVmcAoKs l.lnk	Dropped File	1.68 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
318d0921e8db06b3b65d3201c661501cec8d0406aa9bdb031b87325b56759a30	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Common Files.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Common Files.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\common files.lnk.rtcrypted	Dropped File	710 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
e69ac6cefddb4c41ff3c31615cc339db0b279cdceacb6c30e23930be1679c2aa	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\cptlqfgr7.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\CPtLqFgr7.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\CPtLqFgr7.lnk	Dropped File	652 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ba7f06cde546c77b651ae5c52a522f6e1de8276c072e485297ff37366f2123ea	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\csrpjbn.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\CSRpjbn.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\CSRpjbn.lnk	Dropped File	994 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b4be071f4cc1158a83fa3efa89ef925e00596cd983c160ad16b557c2ffbd80a3	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\cUOFj.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\cUOFj.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\cuofj.lnk.rtcrypted	Dropped File	850 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
9cae94cd132202d29524373043c6a61f243e78337802c3ed77b75a3c3b118061	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\CxX3.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\cxx3.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\CxX3.lnk.rtcrypted	Dropped File	894 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
a095b15d16f580edb05022fdbe7ec534b1c3dd00844f32074a59c8a014282fa5	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\cYW1VXatB-JI8vQr.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Win... ...\Recent\cYW1VXatB-JI8vQr.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\cyw1vxatb-ji8vqr.lnk.rtcrypted	Dropped File	1019 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
c2d659a52de629021388178b895eff6feb16945a5e09c30edbbc6237a89bb8b3	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Dbg3Ddy9SSgsZKwE.doc.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft... ...Dbg3Ddy9SSgsZKwE.doc.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\dbg3ddy9ssgszkwe.doc.lnk.rtcrypted	Dropped File	1.10 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
1db71acc9f77282bd85fbe8f1aef9668de7530699bfbbe2bb914f2a32ad2a0f8	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\DMLxoOU.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\dmlxoou.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\DMLxoOU.lnk.rtcrypted	Dropped File	987 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
4c1ce0a35308fe2ded924a8fa15876c315efc15f16a3a1a9e235ce5cdfa1defc	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\dvC8ktwxOFj7.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\dvc8ktwxofj7.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\dvC8ktwxOFj7.lnk.rtcrypted	Dropped File	1.15 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
85225f7f9dbe7a18ede2fc87bc51d685fb26c0177ae77c2b5751f1427b18407f	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\dy8.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\dy8.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\dy8.lnk.rtcrypted	Dropped File	963 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2cbe02f570546e2f0340174d1c32904e0269e7558022a02d5d2b4ce812d153ab	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\e95MKF1cwUHr.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\e95mkf1cwuhr.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\e95MKF1cwUHr.lnk.rtcrypted	Dropped File	1.10 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
ff93787f6a9fa04ec132a77377e9446b482aca52fd1a3e49343d3b228f9a541b	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\eiweexdtyapi-m.doc.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\M... ...indows\Recent\EIweEXdtYapI-M.doc.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\EIweEXdtYapI-M.doc.lnk	Dropped File	1.00 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
9efd76a13a3d2fc1f6d09d8d50ceec9dba8b2b199147655a3bb037fa419df225	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\em1jfyu4jyx_var.doc.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming... ...ws\Recent\eM1JFyu4JyX_VAr.doc.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\eM1JFyu4JyX_V Ar.doc.lnk	Dropped File	687 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
eca1e0335b6b5f1d4545a954f2edb0dc60b67817ebb99ef97b663f079dd88e50	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\etg7nzxpzhx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\eTG7NzXPZhX.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\eTG7NzXPZhX.lnk	Dropped File	772 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
596663433ca3415595285471e6acfd1a95446f21808c2f5d89a6d4823f01e932	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\evzv9g78hf11b20ex.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\M... ...indows\Recent\EVZV9g78HF11b20ex.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\EVZV9g78HF1 1b20ex.lnk	Dropped File	1.31 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
ff0a0ee3281db4d83f0270ff68e3578d11d201ef7b164b732bc9cb222c498dda	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\e_2t.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\e_2t.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\e_2t.lnk.rtcrypted	Dropped File	951 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
70484fa874774232bcc9e700fdac241f9fb1ecf9e9e7cd32662d689217d1255d	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\F5J9i2mP6f7Fg yEKZw4.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft... ...f5j9i2mp6f7fg yekzw4.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\F5J9i2mP6f7Fg yEKZw4.lnk.rtcrypted	Dropped File	1.34 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
6eba24e80f7e331eda526d820e53b39cd022f677063ff0f8bb2b3f107fb93f70	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\fabe6lam6xetp.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\fabE6LAM6xEtP.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\fabE6LAM6xEtP.lnk	Dropped File	1.01 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2f47b0025560eab963e8498c888d1e0e9b491ee60b4e60c8236e53ffabc67654	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\fenqgag3ychp.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\fenqGAG3YChp.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\fenqGAG3YChp.lnk	Dropped File	1.16 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
74a95a5497514b8e58e460fe92fd344bcd1740ee230a633523e238238c55901e	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\fhpuak.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\FHPuaK.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\FHPuaK.lnk	Dropped File	982 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
dc56df790f505b6b52f72373955749e705fbb2b33448d46d0ce5becd6ec57d77	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\fKlJsgucmnFedTn EAkl.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft... ...fKlJsgucmnFedTn EAkl.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\fkijsgucmnfedtn eakl.lnk.rtcrypted	Dropped File	1.03 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
1dd55d33ed9bd1024594c8f46610764ccfbff7f89c8f3215395d89b0a07d850d	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\gc5fqqjc4nhbm7mhv.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\M... ...indows\Recent\GC5fQQJc4NHBM7mhV.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\GC5fQQJc4NHBM7mhV.lnk	Dropped File	1023 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
f13490ebd21118f2ed16cc1fd064f8a0b983c78417a502c7b87b94b6efd78920	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\GDLIsvWIqGajKiRN9dGO.pptx.lnk, c:\users\oqxzraykm\appdata\roaming\micr... ...ajkirn9dgo.pptx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\GDLIsvWIqGajKiRN9dGO.pptx.lnk.rtcrypted	Dropped File	1.01 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
185dfbb6c814985be8638c349fae34245cfc6e1eb21c7e7be7a6accbea82191e	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\gDn4S0f.ppt.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\gdn4s0f.ppt.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\gDn4S0f.ppt.lnk.rtcrypted	Dropped File	1.25 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
464e9e7673d827a92d1be50f0249c653882af1b5a6a0e79b0ef5955cbe05f1ba	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\gmibz_0qcerv2he.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Micr... ...soft\Windows\Recent\gmIBz_0QcERv2HE.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\gmIBz_0QcERv2HE.lnk	Dropped File	1008 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
cae36c18552804d7a466f2fd1491f607d1be7eec30658fcca26057a1a0edfed1	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\gMmQ7sMpVxP4WwXZrp.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\W... ...ent\gMmQ7sMpVxP4WwXZrp.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\gmmq7smpvxp4wwxzrp.lnk.rtcrypted	Dropped File	931 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4b1bf407a7974caacfed363427e1341b908fa20e85d9d4338297f62495e2f5ab	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\goujvtdj1s18.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\goujVTDJ1s18.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\goujVTDJ1s18.lnk	Dropped File	1.64 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7a192c248fa58938f7fa8097ce3b810121e08a9478c3bda39abcfdf130203d1c	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\hIUicmYfr BOKO-G7dUP.flv.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Micro... ...r BOKO-G7dUP.flv.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\hiuicmyfr boko-g7dup.flv.lnk.rtcrypted	Dropped File	1005 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
a777dec328025de753cae7a127390f36a5c911e18b22e38af8bd8db0c5ebc93b	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\HP_ON6wZYt.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\hp_on6wzyt.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\HP_ON6wZYt.lnk	Dropped File	1004 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
87db6a84945a50185a06e6eda9b12e45eb8c784c49e8357911272b8b0bb4ee55	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\l-byl6.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\l-byl6.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\i-byl6.lnk.rtcrypted	Dropped File	1.13 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
76f67f8e4712027a151c2e50380994cf2c2ec19ac93824146fe52840b8a7f341	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\iku4z6njtis4ci7xut.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\M... ...indows\Recent\ikU4Z6NJTIS4CI7XUt.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\ikU4Z6NJTIS4CI7XUt.lnk	Dropped File	1.47 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7754977bbb61d92ef4fbd4709f3689e06df4744c508e54ba99469226e0addfca	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\J7Kz7aXvYKxh-WWyGI.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\W... ...ent\J7Kz7aXvYKxh-WWyGI.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\j7kz7axvykxh-wwygi.lnk.rtcrypted	Dropped File	1.32 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
32ff69472fff60f6d1690e0c554625f474e92147c7e32d5a50d743fad0750b66	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Jfz.flv.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Jfz.flv.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\jfz.flv.lnk.rtcrypted	Dropped File	1.00 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b08e94b9d09e56ab84aaf41a91df08e208af0835b7b74a79a5eee4390e852b6e	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\JxmR6v_b0d1c1TOkKn.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\w... ...ent\jxmr6v_b0d1c1tokkn.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\JxmR6v_b0d1c1TOkKn.lnk.rtcrypted	Dropped File	1.67 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
43e654e50c06e75708029cf52dfa8acc93e7bd9c8b9bea41378204758bf9cde1	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\jzacgvj_juniqbgydkt.xlsx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roa... ...t\jZACGvj_jUniQbGydKt.xlsx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\jZACGvj_jUniQbGydKt.xlsx.lnk	Dropped File	1.20 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
659162fdb2cd449a4c07d6a1610af9811b81cf924f2afb48f287f29e437f0b46	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\kQnlf5.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\kqnif5.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\kQnlf5.lnk.rtcrypted	Dropped File	874 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
690626fac42620ba7b0b30e3d3ed96b9ca9c7ae54f5c4185e060d488a975f2ee	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\krcijzxudvtcey.doc.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\M... ...indows\Recent\KrCIJZxudvtCeY.doc.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\KrCIJZxudvtCeY.doc.lnk	Dropped File	1.28 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
8f0046e62febc82c04c6797d01f7ce246bf08fc9251075c320249e12531d3d9c	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\kx8a.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Kx8A.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Kx8A.lnk	Dropped File	1.06 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
6d44d030a1b0c478d6d59e3cd75cb682e1101f55bcfa66e5ef69c41140baf748	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\lbLblV.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\lblbiv.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\lbLblV.lnk.rtcrypted	Dropped File	1.10 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
d6184f2a0deb2febaca2cd1c495cd88413765531f8552cafb31ee64afb8fa93c	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\LFcvTFKIe.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\lfcvtfkle.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\LFcvTFKIe.lnk.rtcrypted	Dropped File	1.34 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
cef430a5fab309b4736764cd440fb5bd9023a7d4c0208637a34e9dd6c1f60bf9	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\LUnjpDpKTSnQmwR3f6Nd.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft... ...LUnjpDpKTSnQmwR3f6Nd.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\lunjpdpktsnqmwr3f6nd.lnk.rtcrypted	Dropped File	1.01 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
d51d51b246eced2359a4d95d2967f9034cd2f630196b780333e1f90340fee301	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\l_tj4.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\l_tj4.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\l_tj4.lnk	Dropped File	1.04 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2de2974483d2c0713a7442a3347f793e6106f948115dfc2ad543f93505700730	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\m62mMrqX1.pptx.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\m62mmrqx1.pptx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\m62mMrqX1.pptx.lnk.rtcrypted	Dropped File	978 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
a21dd4add7c4d934b8cce798edb29fde65cc74452d638392533494d304b4a9a7	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\MfGYDk9Y.ppt.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\MfGYDk9Y.ppt.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\mfgydk9y.ppt.lnk.rtcrypted	Dropped File	994 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
53a3c5454e7933b86caba44264f36fc41db129ed87a62f4165730945d4e0d110	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\mL-gKRrD1UEPkt.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\mL-gKRrD1UEPkt.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\ml-gkrrd1uepkt.lnk.rtcrypted	Dropped File	941 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
cfede4ed97c9a89dedabcf45012ae2c45e9413cee2ea69eda39bb6a07a504217	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\mLpk6DQaJ9.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\mlpk6dqaj9.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\mLpk6DQaJ9.lnk.rtcrypted	Dropped File	1.03 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
88623d2039ec8a1ac02d1a88f4f818a6326589b8e7bd042a0ebfd806256fbbfe	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\MOoazXE175u-tWOUa.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\wi... ...ecent\mooazxe175u-twoua.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\MOoazXE175u-tWOUa.lnk.rtcrypted	Dropped File	1.13 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
37bcd369104696341a140dedeb5ceef0d972c199f60973042b9af5d698192da7	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\music.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Music.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Music.lnk	Dropped File	745 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
d420b244826cee9315b7ced67f4e007457c2037337affb006ad88fd96c453ae2	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\mv73nxgice.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\MV73nxGICe.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\MV73nxGICe.lnk	Dropped File	1004 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
3c347a9260bdf42fb8db371cd01112bb9d4107aaa0d69693e04d2f611c206bdc	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\n8uzo0.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\N8uzo0.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\N8uzo0.lnk	Dropped File	635 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
77797307bd4961224f28d5854e50653e311127e3ff4bd1d8300a46f214f32bf4	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\novXISG4jJT9ZShRo.ods.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsof...\...vXISG4jJT9ZShRo.ods.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\novxisg4jjt9zshro.ods.lnk.rtcrypted	Dropped File	1.11 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
53c9c8cb3e6c5241b5bae18c8a99bfa951f2ebedffe53432d4c5a9ce6063f3c8	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\obvxwpqybk.pptx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Micr...\...soft\Windows\Recent\oBVXWpqYBK.pptx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\oBVXWpqYBK.pptx.lnk	Dropped File	983 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
270731ed8ad66decb1bdb13fe35666abd9d769431e5efa9fc9b17509fd36fc77	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\oByX88izFWIaL4.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\obyx88izfwial4.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\oByX88izFWIaL4.lnk.rtcrypted	Dropped File	1.06 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
499ea16c339667edf24d83ba4f65044b7dedc9b7fe1b7c4f18c290cf67ccafa6	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\oGnPUReG2.flv.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\ognpureg2.flv.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\oGnPUReG2.flv.lnk.rtcrypted	Dropped File	955 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
51e4d797e12372d95f32cbde9c7efe1bdd6c154771e3a72a2f6db786fba62b43	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\ogw4Mz9WHOq.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\ogw4Mz9WHOq.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\ogw4mz9whoq.lnk.rtcrypted	Dropped File	662 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
e9ad432fed16c6de5c1355753015ea665a76dbdd907892b658f070d4532ff8cd	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\OgZRcboo9 (2).lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\OgZRcboo9 (2).lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\ogzrcboo9 (2).lnk.rtcrypted	Dropped File	891 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
3c0c26edfdde672260b020e9a4b95970ad3720181ed69722a34098822e27e22b	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\OgZRcboo9.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\OgZRcboo9.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\ogzrcboo9.lnk.rtcrypted	Dropped File	891 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
bb6cbbfce8adbbd82e2efdae1f7cf11df9c66a9443b0bc8816bdfce41d8a8780	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\ouGe8u.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\ouGe8u.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\ouge8u.lnk.rtcrypted	Dropped File	1.27 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
280779a2e750624a5d861240a9043de0dbae57e394045ab3a987b59e1f27307b	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\ovlgxdjo_8cmq.doc.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Mi... ...\Windows\Recent\OvLGXdJo_8CMQ.doc.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\OvLGXdJo_8CMQ.doc.lnk	Dropped File	1019 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
d67f0cefaf7a3a14b9604d994bc312fff2e1567f3269ec835e19ea66ea66403c	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\PQbc4C6_8tW2SWaqVE.xlsx.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Micro... ..._8tW2SWaqVE.xlsx.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\pqbc4c6_8tw2swaqve.xlsx.lnk.rtcrypted	Dropped File	1.00 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
9d39305ecd77464a7af4a1e4b53b19de164f28302f282654f4c7bca67e6c614b	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\P4nhTG-oMiEDYv2EH.lnk, c:\users\oqxzraykm\appdata\roaming\microsoft\wi... ...ecent\p4nhtg-omiedyv2eh.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\P4nhTG-oMiEDYv2EH.lnk.rtcrypted	Dropped File	1.01 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
c66cc9521f5ba1f066c8d8e1340238336b57dcd4e53407daff89819ccd95ffa1	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Pictures.lnk, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Pictures.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\pictures.lnk.rtcrypted	Dropped File	764 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b15517539b32849bcb29a79b640909a1a545c53281be17f601952809539aef48	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\PqsS9Gq RHGz.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\pqss9gq rhgz.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\PqsS9Gq RHGz.lnk	Dropped File	981 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
e8976e64811dde4ba5bfd72c9371cd0e628b903089d4cd9b9dd72b4ea52da753	C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\prv-43xC-PpR5k.ppt.lnk.rtcrypted, c:\users\oqxzraykm\appdata\roaming\m... ...indows\recent\prv-43xc-ppr5k.ppt.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\prv-43xC-PpR5k.ppt.lnk	Dropped File	787 bytes	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b12cfefbb20c7bbbfff567a5a938500e7ae50ead0d92eab90b3ca5e49948d726	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\putuvkak.xlsx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\pUTUVKAK.xlsx.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\pUTUVKAK.xlsx.lnk	Dropped File	1.09 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
5c7a02ff5fa3ab8155f8e73aa5d1e92301df8dee5250862414255fded57512d2	c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\qcpl9rrlrntbf010.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Mi... ...\Windows\Recent\QCPL9rrlRNtbF010.lnk.rtcrypted, C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\QCPL9rrlRNtbF01 0.lnk	Dropped File	1.18 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
C:\Users\OqXZRaykm\Desktop\fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe	Sample File	-	MALICIOUS
c:\recovery\windowsre\reagent.xml.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\All Users\Adobe\Setup\{AC76BA86-7AD7-FFFF-7B44-AC0F074E4100}\Setup.exe.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\All Users\Package Cache\{050d4fc8-5d48-4b8f-8972-47c82c46020f}\vcredist_x64.exe.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\all users\package cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\All Users\Package Cache\{6ba9fb5e-8366-4cc4-bf65-25fe9819b2fc}\VC_redist.x86.exe.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\All Users\Package Cache\{ca67548a-5ebe-413a-b50c-4b9ceb6d66c6}\vcredist_x64.exe.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\all users\package cache\{d4cecf3b-b68f-4995-8840-52ea0fab646e}\vc_redist.x64.exe.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Shows Desktop.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Window Switcher.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo\Fax Recipient.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\Magnify.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessibility\Narrator.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\accessibility\on-screen keyboard.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\administrative tools.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\command prompt.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\computer.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\Control Panel.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\file explorer.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\system tools\run.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell (x86).lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\default\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\3e8ahn.png.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\CRk7sEcLxn.ppt.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\csrpjbn.docx.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\DMLxoOU.bmp.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\eHXp79eO.mp3.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\eiweexdtyapi-m.doc.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\oqxzraykm\appdata\roaming\fhpuak.png.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\fkijsgucmnfedtneakl.bmp.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\g50o8m9fizrg8.mp4.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\mfgydk9y.ppt.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\MV73nxGICe.jpg.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\nE3j.mp3.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\OTMBVrH.mp4.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\OvLGXdJo_8CMQ.doc.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\P4nhTG-oMiEDYv2EH.png.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\snzDMqSsgLa.docx.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming_tsyattimqrdse.mp3.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming__elk.ppt.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\Microsoft Edge.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\internet explorer\quick launch\shows desktop.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\internet explorer\quick launch\window switcher.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\internet explorer\quick launch\user pinned\taskbar\file explorer.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Firefox.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\internet explorer\quick launch\user pinned\taskbar\microsoft edge.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\powershell\psreadline\consolehost_history.txt.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\-5ui6blg2cdez1agzi_.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\-6jvn5s1cqngvpdy.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\-mUkc.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\-TpGaKVbHa97zgS.ppt.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\167vqdu0.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\2sjqfwb3sa1-ail-.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3bJ1.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3e8ahn.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3huk6he8sxy4s31rg.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3mZ1.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3ouk3xp.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\3p6 ohHYs9-.csv.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3q1llb5op_qjtca2ednb.odp.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\3um74xqy2drtb2 veq.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\40MOvGfppj4bDSgoaCIa.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\5jvufsxko (2).lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\5jvufsxko.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\61de8wlpska01ovom.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\6zSAXoBMshJ arRcZrD.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\7AZ xi 6.odp.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\7qsm7bo389nple.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\8gtj48.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\9bap9uzx.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\aejuooowi.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Al-BTkK-C.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\amglu92htoyvs.pptx.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aqmU9TUpYSVIUMRXMae4.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aucpxM.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\awxz4sgzr.ots.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\aXS6vb.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\a_vtoyblcz6nrbg97.xlsx.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\bGzxP7sA1S-0PBuwA.xlsx.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\bBT-MFL3sFb3zx-FPOy.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\BG-3Ru.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\blfnup.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\BmJalddlQRnVT8k_d-q.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\bxOJ-KchVEH.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Chkad3-ROtdrHsoCUX.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\cidai4wobarezgunw3z.xlsx.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\CNhSRq_988nVmcAoKs I.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Common Files.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\cptlqfgr7.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\csrpjbn.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\cUOFj.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\cxx3.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\cYW1VXatB-JI8vQr.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Dbg3Ddy9SSgsZKwE.doc.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\dmlxoou.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\dvc8ktwxofj7.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\dy8.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\e95mkf1cwuhr.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\eiweexdtyapi-m.doc.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\em1jfyu4jyx_v ar.doc.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\etg7nzxpzhx.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\evzv9g78hf1 1b20ex.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\e_2t.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\f5j9i2mp6f7fg yekzw4.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\fabe6lam6xetp.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\fenqgag3ychp.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\fhpuak.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\fKlJsgucmnFedTn EAkl.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\gc5fqqjc4nhbm7mhv.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\gdlisvwiqgajkirn9dgo.pptx.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\gdn4s0f.ppt.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\gmibz_0qcerv2he.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\gMmQ7sMpVxP4WwXZrp.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\goujvtdj1s18.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\hIUicmYfr BOKO-G7dUP.flv.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\HP_ON6wZYt.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\I-byl6.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\iku4z6njtis4ci7xut.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\J7Kz7aXvYKxh-WWyGl.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Jfz.flv.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\jxmr6v_b0d1c1tokkn.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\jzacgvj_juniqbgydkt.xlsx.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\kqnif5.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\krcijzxudvtcey.doc.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\kx8a.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\lblbiv.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\lfcvtfkle.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\LUnjpDpKTSnQmwR3f6Nd.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\l_tj4.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\m62mmrqx1.pptx.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\MfGYDk9Y.ppt.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\mL-gKRrD1UEPkt.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\mlpk6dqaj9.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\mooazxe175u-twoua.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\music.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\mv73nxgice.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\n8uzo0.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\novXISG4jJT9ZShRo.ods.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\obvxwpqybk.pptx.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\obyx88izfwial4.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\ognpureg2.flv.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\ogw4Mz9WHOq.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\OgZRcboo9 (2).lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\OgZRcboo9.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\ouGe8u.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\ovlgxdjo_8cmq.doc.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\PQbc4C6_8tW2SWaqVE.xlsx.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\users\oqxzraykm\appdata\roaming\microsoft\windows\recent\p4nhtg-omiedyv2eh.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\Pictures.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\OqXZRaykm\AppData\Roaming\Microsoft\Windows\Recent\PqsS9Gq RHGz.lnk.rtcrypted	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS

Reduced dataset

Mutex

Name	Operations	Parent Process Name	Verdict
Local\SM0:4348:120:WilError_03	delete, access	openwith.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	access	fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Ransomtoad	write, read, access	fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe	CLEAN

Process

Process Name	Commandline	Verdict
fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe	"C:\Users\OqXZRaykm\Desktop\fd32cec288cec4f16dc5430cf86dc17e1d4cf941d635979fc17a59c8d6d83d44.exe"	MALICIOUS
openwith.exe	C:\Windows\system32\OpenWith.exe -Embedding	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win10_64_20h1_en_base
Description	windows 10 (64bit 20H1 -EN-)
Architecture	x86 64-bit
Operating System	Windows 10 20H1
Kernel Version	10.0.19041.208 (dc9233f8-5819-e3d0-929a-7bde0b87f0b9)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2023.4.1
Dynamic Engine Version	2023.4.1 / 11/10/2023 05:23
Static Engine Version	2023.4.1.0 / 2023-11-10 04:00:12
AV Exceptions Version	2023.4.1.4 / 2023-09-25 17:49:30
Link Detonation Heuristics Version	2023.4.1.27 / 2023-11-09 21:01:46
Smart Memory Dumping Rules Version	2023.4.1.4 / 2023-09-25 17:49:30
Config Extractors Version	2023.4.1.27 / 2023-11-09 21:01:46
Signature Trust Store Version	2023.4.1.4 / 2023-09-25 17:49:30
VMRay Threat Identifiers Version	2023.4.1.27 / 2023-11-09 21:01:46
YARA Built-in Ruleset Version	2023.4.1.27

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	Not installed
Microsoft Office Version	Not installed
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.207.19041.0
Chrome Version	Not installed
Firefox Version	108.0
Flash Version	Not installed
Java Version	8.0.3610.9

System Information

Sample Directory	C:\Users\OqXZRaykm\Desktop
Computer Name	PXTHFFRYO7
User Domain	PXTHFFRYO7
User Name	OqXZRaykm
User Profile	C:\Users\OqXZRaykm
Temp Directory	C:\Users\OQXZRA~1\AppData\Local\Temp

System Root	C:\Windows