MALICIOUS

Classifications: -
Threat Names: -
Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe**
ID	#4423774
MD5	c76aecc1eb0b47fc261a80b9fc06fb75
SHA1	242f3cce8400a77ed62c99fe6f56e1d8b7cfa5b4
SHA256	3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4
File Size	844.00 KB
Report Created	2022-05-23 18:42 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (12 rules, 15 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) 3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #1) 3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 96 files by appending the extension ".wsir".			
2/5	Discovery	Reads network adapter information	2	-
	• (Process #1) 3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe queries information about the network adapters via WMI. • (Process #5) wmiprvse.exe reads the network adapters' addresses by API.			
2/5	Discovery	Executes WMI query	1	-
	• (Process #1) 3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe executes WMI query: Select MACAddress From Win32_NetworkAdapter WHERE PNPDeviceID LIKE "%PCI%" AND NetConnectionStatus =2.			
2/5	Defense Evasion	Sends control codes to connected devices	3	-
	• (Process #5) wmiprvse.exe controls device "\\.\{9E8A7ED5-49C8-421B-A782-D46C28931105}" through API DeviceIOControl. • (Process #5) wmiprvse.exe controls device "\\.\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}" through API DeviceIOControl. • (Process #5) wmiprvse.exe controls device "\\.\{E96D977E-F067-4CE9-924D-F6E0A04729E4}" through API DeviceIOControl.			
2/5	Hide Tracks	Hides files	1	-
	• (Process #1) 3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe hides the file "C:\Users\RDhJ0CNFevzX\Documents\½âÃÜÎÃ¼þ.key" by setting its "hidden" attribute.			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #1) 3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe tries to read sensitive data of ftp application "Total Commander" by file.			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #1) 3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe adds "C:\Users\RDhJ0CNFevzX\Desktop\WsIR.exe" to Windows startup via registry.			
1/5	Hide Tracks	Changes folder appearance	1	-
	• (Process #1) 3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe changes the appearance of folder "C:\Users\RDhJ0CNFevzX\Desktop".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #5) wmiprvse.exe resolves 26 API functions by name.			
1/5	System Modification	Creates an unusually large number of files	1	-
	• (Process #1) 3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe creates an above average number of files.			

Mitre ATT&CK Matrix

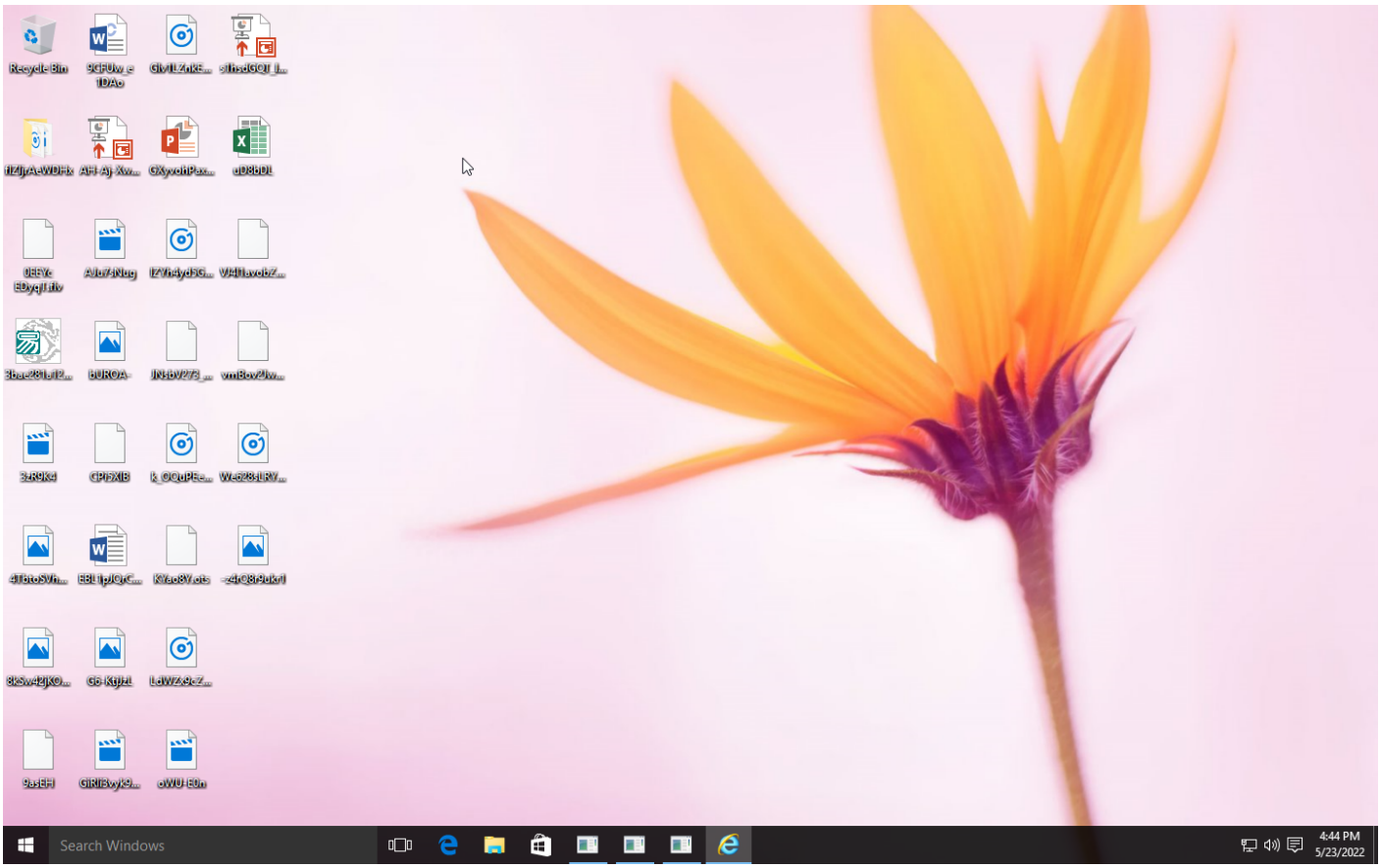
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1060 Registry Run Keys / Startup Folder		#T1112 Modify Registry	#T1081 Credentials in Files	#T1016 System Network Configuration Discovery		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
		#T1158 Hidden Files and Directories		#T1158 Hidden Files and Directories		#T1083 File and Directory Discovery		#T1005 Data from Local System			
				#T1036 Masquerading							
				#T1045 Software Packing							

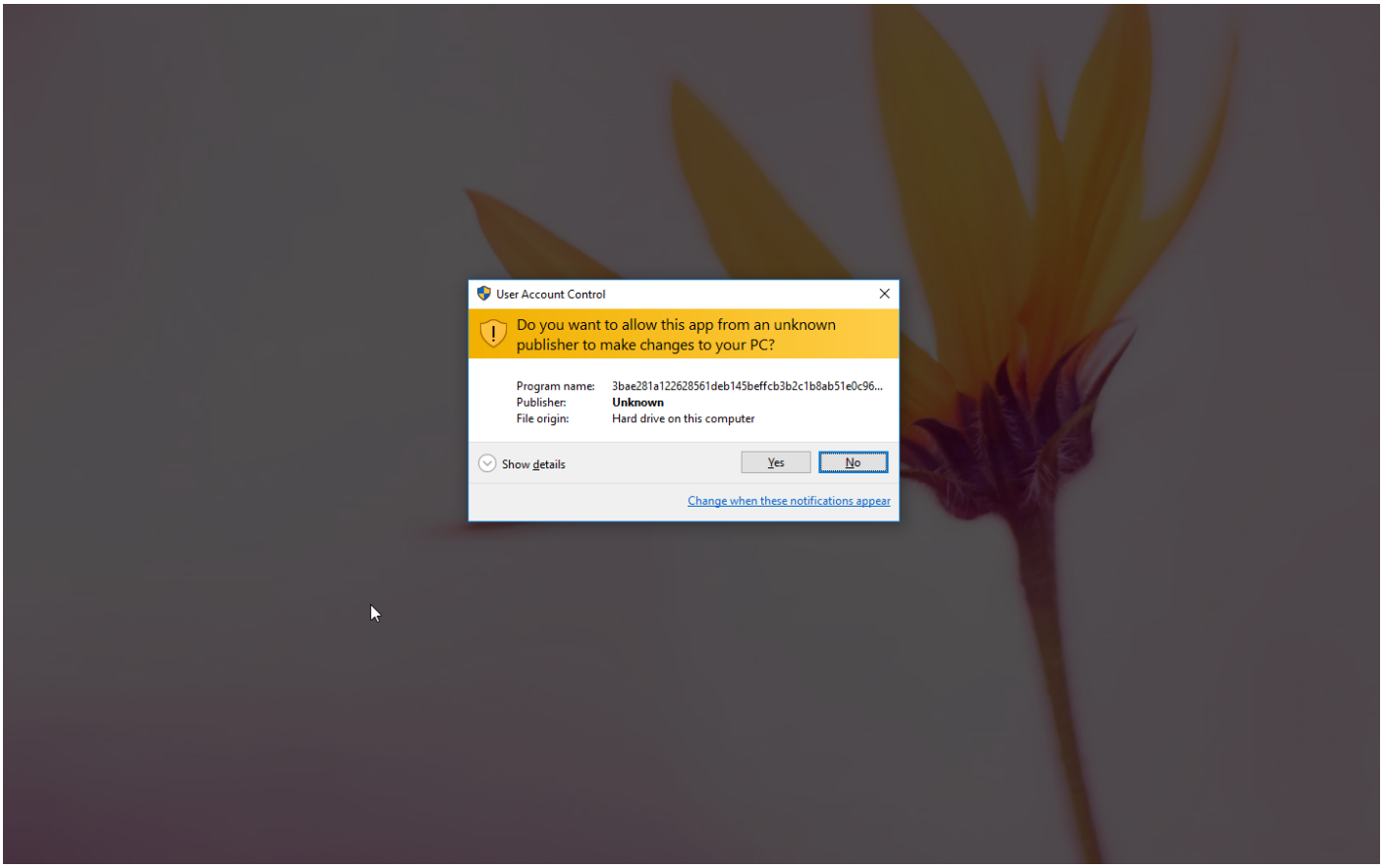
Sample Information

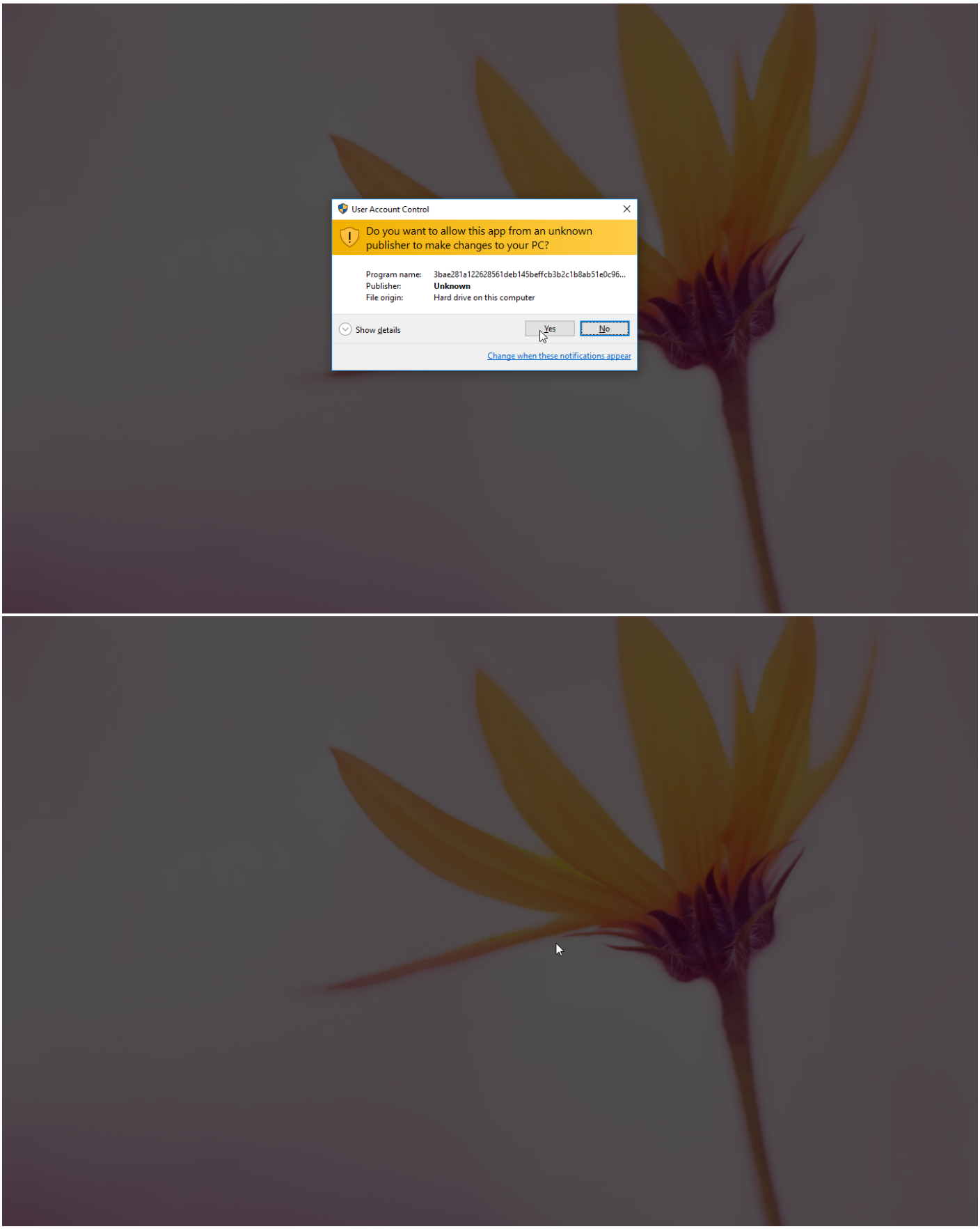
ID	#4423774
MD5	c76aecc1eb0b47fc261a80b9fc06fb75
SHA1	242f3cce8400a77ed62c99fe6f56e1d8b7cfa5b4
SHA256	3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4
SSDeep	12288:RJ7VkgeC9saHPV0rVQLL1vVM8UyztalJbuFmOOSKaBsX5:RJ7VVeC9DHdiaLJvRkmfSKaBsJ
ImpHash	4ffd26d581651ee9980129d50bc32409
File Name	3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe
File Size	844.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-05-23 18:42 (UTC+2)
Analysis Duration	00:03:57
Termination Reason	Timeout
Number of Monitored Processes	3
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Search Windows
4:44 PM
5/23/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 3bae281a122628561deb145beffcb3b2c1b8ab51e0c96...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

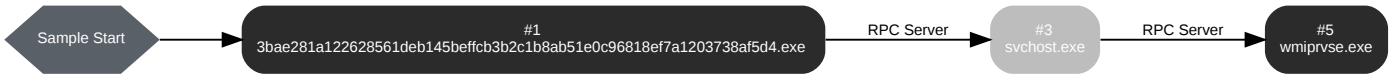
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 84753, Reason: Analysis Target
Unmonitor End Time	End Time: 310089, Reason: Terminated by timeout
Monitor duration	225.34s
Return Code	Unknown
PID	4776
Parent PID	1932
Bitness	32 Bit

Dropped Files (98)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\oWU-E0n.avi.WsIR.WsIR	49.20 KB	ab20b51509fe0a71a639d4930bee59d51f34376075def398327b0417ce2c40e9	✖
c:\users\rdhj0cnfevzx\desktop\giv1lznke-dybxmcbir3.mp3.wsir	66.18 KB	f90b5e6ce0ba3ea2bb0b4cbdbfc0e96f6ee5c4111e32906e66830b8186445a48	✖
c:\users\rdhj0cnfevzx\desktop\0eeyc edyqt.flv.wsir.wsir	60.74 KB	94118bc33f73276f4f37ddca531295dae64ad03ea0beccbcd1e2f62abd47357e	✖
c:\users\rdhj0cnfevzx\desktop\4tbtosvhwga.jpg.wsir.wsir	10.31 KB	77b03fcb452a97b90787c8778a7904b86030d27025604c4b4c90c613e8e0f2ae	✖
c:\users\rdhj0cnfevzx\desktop\0eeyc edyqt.flv.wsir.wsir	60.73 KB	dc5cc1952599b6537830a2e0bff1a4dc0b107dbfe9f0274c088843e6790d5bdb	✖
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\ke4ecUbbuT2.m4a.WsIR.WsIR	57.98 KB	51aea88962be43a95092ea370d67f7ca5d29dcf63b3c8e5e3cbcdcd2920857d4	✖
c:\users\rdhj0cnfevzx\desktop\jnsbv273_xuna9wdfumt.swf.wsir	38.20 KB	af9ec6a9825a046381aef3b18e8c27bfbdbb798f0984d484c8b76d3f00d3e055	✖
C:\Users\RDhJ0CNFevzX\Desktop\8kSw42jKOoLb1LIX.jpg.WsIR.WsIR	26.85 KB	ab34ce4228181837e1ce1c4db30ad8ebe0b78a3ab7f528665506064382ffda04	✖
c:\users\rdhj0cnfevzx\desktop\kyao8y.ots.wsir.wsir	6.72 KB	ac0bd58b9e78c379af31bfb12e294020aa48a471fe464272b7407141f06ca7c8	✖
c:\users\rdhj0cnfevzx\desktop\k_oqupeew0f6q.m4a.wsir	93.38 KB	727eebc3e97d8c941f4af8642d7c1940218230b7273530fb127bb4444e76a2c2	✖
C:\Users\RDhJ0CNFevzX\Desktop\s1hsdGQT_IQqo9A_5D_H.pps.WsIR.WsIR	85.23 KB	208db42425ba03c64766ae389d9aee26ef3f755810ad3768a61ff6b1718e443f	✖
c:\users\rdhj0cnfevzx\desktop\vj4l1avobz6t5xyoq.flv.wsir.wsir	53.88 KB	837bb7ce3a7bd05a2a13aa3dd3fa999b85b599f1eeaced9918ac4bb4ddc7b5bd	✖
C:\Users\RDhJ0CNFevzX\Desktop\EBL1pJQrCMBq.docx.WsIR.WsIR	22.44 KB	51d25f247134b03cf8911e79d23ea056594ab2a26c15e125a3b50e6bc6fc32fb	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4ut8p0tdn5vkztsh.gif.wsir	48.55 KB	51d98eddab365c7b5fd27b9efe7abb57e171292d9e665f176ab878542234d12b	✖
c:\users\rdhj0cnfevzx\desktop\g6-ktjjzl.png.wsir	25.27 KB	ce7d2771e52cd44d8ee690ea63e514da75ce9b1bd2b4393cb8a3a2ce51f43ecf	✖
c:\users\rdhj0cnfevzx\desktop\jnsbv273_xuna9wdfumt.swf.wsir	38.21 KB	8c2f9bb08027ce786c2bd0b4187a1e3983638e466ec6b83c5bc52900c7512abd	✖
c:\users\rdhj0cnfevzx\desktop\ldwzx9czy0viyiaugjtg.wav.wsir	76.44 KB	c2ee2ff47eadf1a7bc5e395c87793c6599f747ac3e8a83b6a44976eb704453a2	✖
C:\Users\RDhJ0CNFevzX\Desktop\lZYh4yd5GmG9gUQxF.m4a.WsIR	76.45 KB	dd7897d33c71d292b522dced48d8756d6138e718ed151c662061c61dff2d2280	✖

File Name	File Size	SHA256	YARA Match
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\qhtez_bgydaj-l.png.wsir	7.05 KB	7eb68869f8afc14ddcb7d4d40dd8ced3eef7920f11430d8310fa48e7fa6ee61b	✖
C:\Users\RDhJ0CNFevzX\Desktop\vmBov2JwdPztuDyp.flv.WsIR.WsIR	47.32 KB	602b39989bc22b0ca6a8653d918205a7a41e3b6892abec5371160ed0374f8b91	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\bb7ilcqwymxeiup.xlsx.wsir	92.76 KB	0d76c8742a6e25f8722ce201796b32694be0cf3b5a49d428fef594df9b189522	✖
C:\Users\RDhJ0CNFevzX\Desktop\vmBov2JwdPztuDyp.flv.WsIR.WsIR	47.33 KB	3f569342315b09ec3294fda5e552bf1f934c2aac4adcfce09aec9da5b727a57d	✖
c:\users\rdhj0cnfevzx\desktop\9cfuw_e 1dao.odt.wsir	69.54 KB	348908fb2481a41928fceeccefd75d41be62a32ea00eb58efe64275f1b55fc36	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4ut8p0tdn5vkztsh.gif.wsir	48.56 KB	c0b8d6780381c468df8cf9d030884928b72f852a89a6c4184b1ef1158e917880	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\amb8c8tyuzftkxdd6vn.mp3.wsir.wsir	5.41 KB	8b0871e0221b74ba34377eb0d56c4749d5d1cdac8d55c0dfe9d92aa39e1663b0	✖
c:\users\rdhj0cnfevzx\desktop\we628slryqfcn.mp3.wsir	94.11 KB	f8ccfcc6fa164699825922cb69de1a27d3b380249dfcd39c44037ae802f444b2	✖
c:\users\rdhj0cnfevzx\desktop\gxyvohpaxjzlat.pptx.wsir.wsir	52.48 KB	50e66935cddad24a30fe034257e83a30e01b02e31f66903bd9042b917beb4575	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\hcsagnwcw60j2xdsh.wav.wsir.wsir	49.46 KB	623661c3419a6e08e076a30bd1d2ec8a9be57dcbab224b794ab064035760c0cd	✖
C:\Users\RDhJ0CNFevzX\Desktop\bUROA-.jpg.WsIR	78.62 KB	85cab50b809afd2a69c91d16d87dcd2a8cca38c9a87c126c14b0545bd8775818	✖
c:\users\rdhj0cnfevzx\desktop\9aseh.swf.wsir.wsir	72.12 KB	8c7432e3023de592f76b89f2a005d66cc42d8865a8100df257aacb6b10cae6d7	✖
c:\users\rdhj0cnfevzx\desktop\-z4rq8r9ukr1.jpg.wsir	88.89 KB	c8c48ef7c989b4740cb1c6abaa30e7794d4c008be6021327f7c6c051fc90d05c	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\kfprms4.mp3.wsir	25.52 KB	c73a0eeab958562d5a21b860a43a4430492c2c6484ef06c267fb22f5cca6d55a	✖
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\WpL3Kq1Gh.m4a.WsIR	79.81 KB	90942e599db941c90982d84102a973b44a94ae6216155182391 77da20c86350b	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\amb8c8tyuzftkxdd6vn.mp3.wsir.wsir	5.41 KB	e47fd48df24f1dd1235eb618f3eb77b776bb55912ee602c5cad3aaa82d980d68	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4fjcz48nwkc.mp4.wsir	74.38 KB	3d7f4dbefc9a339c60c541ae3e27a76bc613fcbff85eb29c14cd50a5212169f0	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\95o-aud3nhe9qs4eevn.mp3.wsir	70.04 KB	814dd1fcc6e4e1ee0fc46fde77c79ec10b17799890cf11d7c2b77163d40ee9c2	✖
C:\Users\RDhJ0CNFevzX\Desktop\3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe	844.00 KB	3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\12zna3pivem1wor.m4a.wsir	90.67 KB	86e0069173c821cc8806e747930831eff514f2b3e33a5c0141823a4d58e8c71e	✖
c:\users\rdhj0cnfevzx\desktop\ud8bdl.xlsx.wsir.wsir	39.11 KB	80129a359a62022d4a6e1b37081710854e09dd32c0663ec67f0f3a32c3203a1f	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\xlhkz08bi-i8drhwtenl.avi.wsir.wsir	40.20 KB	3c76d98e2cbb5af92df5f43de15b9102eb511c4e5bfd92d7748a0d3ff7be32e9	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rd18vxrba4wvaixb9.doc.wsir	67.20 KB	cd9ba2599095892e90fd2c38883780c203e9df249311dd86b25265c1d8921c4b	✖
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\faYc088QK.doc.WsIR	50.46 KB	b22ca786d02b314e856a01fd5f9c49a57b9242c6324ebd611dd625f3f18e3398	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\pv g_1cump.bmp.wsir	75.89 KB	7b59240ec3b2ceb7f97de9dd0bc10f612aca66f9fdce0c1c65afbcf82a0aeb0d	✖
C:\Users\RDhJ0CNFevzX\Documents\½âÃÜÎÄ¼þ.key	370 bytes	dbfd50014ac46c1e2bfd0111a9f7d3878beac353fea365e408d7937f0a35bf48	✖

File Name	File Size	SHA256	YARA Match
c:\users\rdhj0cnfevzx\desktop\ldwzx9czy0viyiaugjtg.wav.wsir	76.43 KB	883a9ccbb2633685a71be75ed91204642c328ac9225c6fc98c3624292b05ae9f	✖
c:\users\rdhj0cnfevzx\desktop\giv1lznke-dybxmcbir3.mp3.wsir	66.19 KB	aa0fd32e3f676bc82d16198688d7ab248ad82a602ed292bbfa85f7f5765539b2	✖
c:\users\rdhj0cnfevzx\desktop\vj4l1avobz6t5xyoq.flv.wsir.wsir	53.88 KB	ba245bc0e28e5d98a7a314c99143b200c38035fae52ebc74bb21243dae0fe79c	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4fjcz48nwkc.mp4.wsir	74.38 KB	c8d916948f8437ce159d77a7ebdc19238c8cf07f3700eb0e124f70dd85c312ae	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\12zna3pivem1wor.m4a.wsir	90.66 KB	85ce8e15b9338555d03b920f91aee9cf5bc35fc8ea4a4fd5349bb18b38eab97a	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\jpnfqkpt0lf7c.avi.wsir.wsir	37.27 KB	427c6e1109f70c169f177ffa58f2e0cc99b786783b47ad6a4c613793a072dd3c	✖
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\RbArjN3ZSZrBNDWJ1be.wav.WsIR	72.11 KB	d212873c6f5fb9575e4d3d4deb46a0a2b80aaebe2c264bab151d0518efe994ff	✖
C:\Users\RDhJ0CNFevzX\Desktop\CPi5XIB.swf.WsIR	72.88 KB	7c39f1e30da27b9b403ae8a906b430b58401e791181300cf289048c61ebfcf96	✖
C:\Users\RDhJ0CNFevzX\Desktop\EBL1pJQrCMBq.docx.WsIR.WsIR	22.43 KB	c32132dd7cf67f3e557fc7f392a5e7cdaa1bbaa77e03bfc5a9206b25dd443f50	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\pv g_1cump.bmp.wsir	75.88 KB	b6deb9cb343d557244db89d0f4aecb662ad466a8df028e4b5e70ecd257fc1009	✖
c:\users\rdhj0cnfevzx\desktop\k_oqupeew0f6q.m4a.wsir	93.38 KB	ed96d7588bea0961a5fb253c710f82c7079d249d15c9f663f894aec38d4843f6	✖
c:\users\rdhj0cnfevzx\desktop\g6-ktjjzl.png.wsir	25.26 KB	72b946683cb08c8ded60349ac2afca878139702d5671eaec6f600436788c53b2	✖
c:\users\rdhj0cnfevzx\desktop\aju7snug.mp4.wsir	80.40 KB	b1aa273a38c8d5690568fe4303996a224a8b01c83d6106cb9f0b0d51a3eaa3c4	✖
c:\users\rdhj0cnfevzx\desktop\3zr9k4.mp4.wsir.wsir	98.16 KB	437769e29e9db9a7007058aadce64e5dc70cd5469217c29a78feb99b6f5ae3df	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\bb7ilcqwymxeiup.xlsx.wsir	92.75 KB	11a4a6512424d97eb1e021dcba49444e4b2627744be2dceb30ad0c2b066f8997	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\kfprms4.mp3.wsir	25.52 KB	b075939c064ad28f97b6afce9fb74bcbcaeb4db2421f7afc149809ae59865707	✖
c:\users\rdhj0cnfevzx\desktop\-z4rq8r9ukr1.jpg.wsir	88.88 KB	cfc35162af4ac0e990bb003a14764da29ecf0e97367f800db7fb1ea4e30fda6e	✖
c:\users\rdhj0cnfevzx\desktop\gxyvohpaxjzlat.pptx.wsir.wsir	52.48 KB	5220c0b19104b840c1c9badcf00b541c634083e2784a9a0614015caf5cc5c97c	✖
C:\Users\RDhJ0CNFevzX\Desktop\s1hsdGQT_IQqo9A_5D_H.pps.WsIR.WsIR	85.23 KB	d9f56e6ad6816eeec26498838322569a3539ae11998ec7281e85567c65af6358	✖
c:\users\rdhj0cnfevzx\desktop\ah-aj-xw2l9.pps.wsir	76.67 KB	f9bba4897d498a95db58931065d58bea41592708695ba5abbbd3f0a57f6ffec5	✖
C:\Users\RDhJ0CNFevzX\Desktop\CPi5XIB.swf.WsIR	72.88 KB	dae07898b8d43df8ae7bae797a6c50f5b77d954a41af505bcc8fb1c978814555	✖
c:\users\rdhj0cnfevzx\desktop\kyao8y.ots.wsir.wsir	6.73 KB	a154dec587b3c14379c742a5f26e69a2eb5ade09cb65bc98ed54b2014cb1dc1a	✖
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\RbArjN3ZSZrBNDWJ1be.wav.WsIR	72.12 KB	7dee1e1f809e7ef7d4928961a3326e9a1eb8b0b86092faac35b802b2ab9deb29	✖
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\65OLmi32HgseAx.bmp.WsIR	54.62 KB	8cf327522b2b67aaf173a4874178e372325297d531d567aece2bf2eefbb7bdcc	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\hcsagnwcw60j2xdsh.wav.wsir.wsir	49.45 KB	af44134b31bdf860fbd1c8f521da7d0ad664a8d21e9db0c0727da660f27ba69f	✖
c:\users\rdhj0cnfevzx\desktop\ah-aj-xw2l9.pps.wsir	76.66 KB	a9615178e4a75f847ed5c475c7deb4b720893dbb08b86425cbbae3dfb08dc074	✖
C:\Users\RDhJ0CNFevzX\Desktop\IZYh4yd5GmG9gUQxF.m4a.WsIR	76.46 KB	b6a8134b1145ae502718ae5e43cc9b905f8acb0fab18067132308b23d0979e75	✖

File Name	File Size	SHA256	YARA Match
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\xlhkz08bi-i8drhwtenl.avi.wsir.wsir	40.21 KB	8c5206f38d7627b498f6e7833a98a88041b92e6208628f61fb7a3ab6d92f7e4a	✖
C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\WpL3Kq1Gh.m4a.WsIR	79.80 KB	0fba50c651a22710736bb14d9a4c3e243043faf2a3720b9693c791538a203ff8	✖
c:\users\rdhj0cnfevzx\desktop\3zr9k4.mp4.wsir.wsir	98.16 KB	fe296dedd51b57ec45c8f8a3bcd07942d4510a3451c0db4bf83f2bfd3f3aa7b1	✖
c:\users\rdhj0cnfevzx\desktop\desktop.ini.wsir.wsir	282 bytes	4b9d687ac625690fd026ed4b236dad1cac90ef69e7ad256cc42766a065b50026	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\95o-aud3nhe9qs4eevn.mp3.wsir	70.03 KB	6af2c3bafe696655a2566dd174af7cdb6730dd7a00b8da34a7334da68edea9d4	✖
c:\users\rdhj0cnfevzx\desktop\4tbtosvhwga.jpg.wsir.wsir	10.32 KB	e79fd7d8f4a6818c8ea6d71f2851ff8865211c29ffb69cf83ab587dcbf6e810a	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\b8oqnzm.mp4.wsir	70.10 KB	a232248694e91c4b49fba8f83c2944275a3ac7c7b0f9861f8fb817cafc4ba088	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\jpnfqkpt0lf7c.avi.wsir.wsir	37.27 KB	fa543e7c74f7e918dbd2328a21ce5c5b946fd07c79434e108ba7397ee02e2a85	✖
c:\users\rdhj0cnfevzx\desktop\9cfuw_e 1dao.odt.wsir	69.55 KB	75867351a3dadace45dbb895a6cada64be013449fd0c84eff4c6044098675421	✖
c:\users\rdhj0cnfevzx\desktop\we628slryqfcn.mp3.wsir	94.10 KB	9be3d7ff692deea11addb97e4b6f06159b05b7a3d5fd306ebd87357d9fd0afee	✖
c:\users\rdhj0cnfevzx\desktop\aju7snug.mp4.wsir	80.41 KB	b1c5478c5fb05a175d9c73e9f1cf1368a6b8863f85d40a0ab755ba59929d009e	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rd18vxrba4wvaixb9.doc.wsir	67.19 KB	e4b841e3bdd09794472e5c75cc29f1e8bda7b586c5167daf81367fcaa8e3c325	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\qhtez_bgydaj-l.png.wsir	7.05 KB	28dcb9122ced25dd14c7f1363562c0d095d374a1cb3591ba8eb9239754bb87dd	✖
C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\faYc088QK.doc.WsIR	50.47 KB	58f868695cfe19bc4317de8c12a92709cee99cb68ad9daeac935f1c23d74cc75	✖
C:\Users\RDhJ0CNFevzX\Desktop\8kSw42jKOoLb1LIX.jpg.WsIR.WsIR	26.86 KB	f9b70f2060934198e02ae3cc39f0dea67d250f09795dcc3fcbf10df7dd55c39c	✖
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\b8oqnzm.mp4.wsir	70.09 KB	316706e34bfabd8f7611964a4676ae2647553e968499b5af1b8b414b4e2ae920	✖
C:\Users\RDhJ0CNFevzX\Desktop\bUROA-.jpg.WsIR	78.62 KB	50117fde03397b5892ab5a60a2bd336758edf4b4a8412887f56cac7abbe01cae	✖
C:\Users\RDhJ0CNFevzX\Desktop\oWU-E0n.avi.WsIR.WsIR	49.20 KB	f3acefd62e6299074e8cd018b72fafbc68b0bac2b69f4565796cfe16b53446fa	✖
C:\Users\RDhJ0CNFevzX\Desktop\GiRIi3vyk91ALiSqq9.mkv.WsIR	56.97 KB	f44b981e6a5bd2e3f436fe685fda51e0a7e51ba3e170ef37029fbb8a79947f40	✖
C:\Users\RDhJ0CNFevzX\Desktop\GiRIi3vyk91ALiSqq9.mkv.WsIR	56.96 KB	ea3fdd885ada0466a4cbc6ae06369115340b2183ef44f46ff40090b17572ee3c	✖
c:\users\rdhj0cnfevzx\desktop\ud8bdl.xlsx.wsir.wsir	39.12 KB	69e8917b112e80981e69de5187deb5cec80a36d890d2ceda0f09baa1782b1a34	✖
C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\65OLmi32HgseAx.bmp.WsIR	54.62 KB	6e83000b22ea30c917921a496873946d398b8874e8df347f97ff3b656db6a7b8	✖
c:\users\rdhj0cnfevzx\desktop\9aseh.swf.wsir.wsir	72.12 KB	37850a236c662458c186f213a10e6f28882264e4b323b5d296891fd7f728192a	✖
C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\ke4ecUbbuT2.m4a.WsIR.WsIR	57.98 KB	d913acaaee4348513872e9cd2b6e288cffeba8652998cb1e3d5802c202d362b1	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
C:\Users\RDhJ0CNFevzX\Desktop\3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe.WsIR	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖
c:\users\rdhj0cnfevzx\desktop\desktop.ini.wsir	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
File	712
-	1
Module	55
System	14
Registry	2
Keyboard	1
COM	1
Window	3
-	1
Environment	1

Process #3: svchost.exe

ID	3
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126719, Reason: RPC Server
Unmonitor End Time	End Time: 310089, Reason: Terminated by timeout
Monitor duration	183.37s
Return Code	Unknown
PID	868
Parent PID	4776
Bitness	64 Bit

Process #5: wmiprvse.exe

ID	5
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 126720, Reason: RPC Server
Unmonitor End Time	End Time: 310089, Reason: Terminated by timeout
Monitor duration	183.37s
Return Code	Unknown
PID	3608
Parent PID	868
Bitness	64 Bit

Host Behavior

Type	Count
Module	4402
System	928
-	6
File	6
Registry	14

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4	C:\Users\RDhJ0CNFevzX\Desktop\3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe, C:\Users\RDhJ0CNFevzX\Desktop\...\...8af5d4.exe.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe.wsir.wsir	Sample File	844.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Read, Write	MALICIOUS
ab20b51509fe0a71a639d4930bee59d51f34376075def398327b0417ce2c40e9	C:\Users\RDhJ0CNFevzX\Desktop\oWU-E0n.avi.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\owu-e0n.avi.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\oWU-E0n.avi.WsIR, c:\users\rdhj0cnfevzx\desktop\owu-e0n.avi.wsir	Dropped File	49.20 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
f90b5e6ce0ba3ea2bb0b4cbdbfc0e96f6ee5c4111e32906e66830b8186445a48	c:\users\rdhj0cnfevzx\desktop\giv1lznke-dybxmcbir3.mp3.wsir, C:\Users\RDhJ0CNFevzX\Desktop\Glv1LZnkE-dYbxMcBir3.mp3.WsIR, c:\users\rdhj0cnfevzx\desktop\giv1lznke-dybxmcbir3.mp3.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\Glv1LZnkE-dYbxMcBir3.mp3.WsIR.WsIR	Dropped File	66.18 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
94118bc33f73276f4f37ddca531295dae64ad03ea0beccbcd1e2f62abd47357e	c:\users\rdhj0cnfevzx\desktop\0eeycedyqt.flv.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\0EEYc EDyqT.flv.WsIR.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\0EEYc EDyqT.flv.WsIR, c:\users\rdhj0cnfevzx\desktop\0eeycedyqt.flv.wsir	Dropped File	60.74 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
77b03fcb452a97b90787c8778a7904b86030d27025604c4b4c90c613e8e0f2ae	c:\users\rdhj0cnfevzx\desktop\4tbtosvhwga.jpg.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\4TbtoSVhWGA.jpg.WsIR.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\4TbtoSVhWGA.jpg.WsIR, c:\users\rdhj0cnfevzx\desktop\4tbtosvhwga.jpg.wsir	Dropped File	10.31 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
dc5cc1952599b6537830a2e0bff1a4dc0b107dbfe9f0274c088843e6790d5bdb	c:\users\rdhj0cnfevzx\desktop\0eeycedyqt.flv.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\0EEYc EDyqT.flv.WsIR.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\0EEYc EDyqT.flv.WsIR, c:\users\rdhj0cnfevzx\desktop\0eeycedyqt.flv.wsir	Dropped File	60.73 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
51aea88962be43a95092ea370d67f7ca5d29dcf63b3c8e5e3cbcdcd2920857d4	C:\Users\RDhJ0CNFevzX\Desktop\fIZIjrAeWDHx\Rkek9t3Rdv\ke4ecUbbuT2.m4a.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t...\...x\desktop\fizijraewdhx\rkek9t3rdv\ke4ecubbut2.m4a.wsir, C:\Users\RDhJ0CNFevzX\Desktop\fIZIjrAeWDHx\Rkek9t3Rdv\ke4ecUbbuT2.m4a.WsIR	Dropped File	57.98 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
af9ec6a9825a046381aef3b18e8c27bfbdbb798f0984d484c8b76d3f00d3e055	c:\users\rdhj0cnfevzx\desktop\jnsbv273_xuna9wdfumt.swf.wsir, C:\Users\RDhJ0CNFevzX\Desktop\JNsbV273_XUNA9WdFumt.swf.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\JNsbV273_XUNA9WdFumt.swf.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\jnsbv273_xuna9wdfumt.swf.wsir.wsir	Dropped File	38.20 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ab34ce4228181837e1ce1c4db30ad8ebe0b78a3ab7f528665506064382ffda04	C:\Users\RDhJ0CNFevzX\Desktop\8kSw42jKOoLb1LIX.jpg.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\8ksw42jkoolb1lix.jpg.wsir.wsir, c:\users\rdhj0cnfevzx\desktop\8ksw42jkoolb1lix.jpg.wsir, C:\Users\RDhJ0CNFevzX\Desktop\8kSw42jKOoLb1LIX.jpg.WsIR	Dropped File	26.85 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
ac0bd58b9e78c379af31bfb12e294020aa48a471fe464272b7407141f06ca7c8	c:\users\rdhj0cnfevzx\desktop\kyao8y.ots.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\KYao8Y.ots.WsIR.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\KYao8Y.ots.WsIR, c:\users\rdhj0cnfevzx\desktop\kyao8y.ots.wsir	Dropped File	6.72 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
727eebc3e97d8c941f4af8642d7c1940218230b7273530fb127bb4444e76a2c2	c:\users\rdhj0cnfevzx\desktop\k_oqupeew0f6q.m4a.wsir, C:\Users\RDhJ0CNFevzX\Desktop\k_OQuPEew0F6q.m4a.WsIR, c:\users\rdhj0cnfevzx\desktop\k_oqupeew0f6q.m4a.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\k_OQuPEew0F6q.m4a.WsIR.WsIR	Dropped File	93.38 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
208db42425ba03c64766ae389d9aee26ef3f755810ad3768a61ff6b1718e443f	C:\Users\RDhJ0CNFevzX\Desktop\s1hsdGQT_lQqo9A_5D_H.pps.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\s1hsdgqt_lqqo9a_5d_h.pps.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\s1hsdGQT_lQqo9A_5D_H.pps.WsIR, c:\users\rdhj0cnfevzx\desktop\s1hsdgqt_lqqo9a_5d_h.pps.wsir	Dropped File	85.23 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
837bb7ce3a7bd05a2a13aa3dd3fa999b85b599f1eeaced9918ac4bb4ddc7b5bd	c:\users\rdhj0cnfevzx\desktop\vj4l1avobz6t5xyoq.flv.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\VJ4l1avobZ6t5xYOQ.flv.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\vj4l1avobz6t5xyoq.flv.wsir, C:\Users\RDhJ0CNFevzX\Desktop\VJ4l1avobZ6t5xYOQ.flv.WsIR	Dropped File	53.88 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
51d25f247134b03cf8911e79d23ea056594ab2a26c15e125a3b50e6bc6fc32fb	C:\Users\RDhJ0CNFevzX\Desktop\EBL1pJQrCMBq.docx.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\ebl1pjqrcmbq.docx.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\EBL1pJQrCMBq.docx.WsIR, c:\users\rdhj0cnfevzx\desktop\ebl1pjqrcmbq.docx.wsir	Dropped File	22.44 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
51d98eddab365c7b5fd27b9efe7abb57e171292d9e665f176ab878542234d12b	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4ut8p0tdn5vkztsh.gif.wsir, C:\Users\RDhJ0CNFevzX\Desktop\fIZIjrAeWDHx\4UT8p0tDN5vkZtsh....vzx\desktop\fizijraewdhx\4ut8p0tdn5vkztsh.gif.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\fIZIjrAeWDHx\4UT8p0tDN5vkZtsh.gif.WsIR.WsIR	Dropped File	48.55 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
ce7d2771e52cd44d8ee690ea63e514da75ce9b1bd2b4393cb8a3a2ce51f43ecf	c:\users\rdhj0cnfevzx\desktop\g6-ktjjzl.png.wsir, C:\Users\RDhJ0CNFevzX\Desktop\G6-KtjJzL.png.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\G6-KtjJzL.png.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\g6-ktjjzl.png.wsir.wsir	Dropped File	25.27 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
8c2f9bb08027ce786c2bd0b4187a1e3983638e466ec6b83c5bc52900c7512abd	c:\users\rdhj0cnfevzx\desktop\jnsbv273_xuna9wdfumt.swf.wsir, C:\Users\RDhJ0CNFevzX\Desktop\JNsbV273_XUNA9WdFumt.swf.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\JNsbV273_XUNA9WdFumt.swf.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\jnsbv273_xuna9wdfumt.swf.wsir.wsir	Dropped File	38.21 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c2ee2ff47eadf1a7bc5e395c87793c6599f747ac3e8a83b6a44976eb704453a2	c:\users\rdhj0cnfevzx\desktop\ldwzx9czy0viyiaugjtg.wav.wsir, C:\Users\RDhJ0CNFevzX\Desktop\LdWZx9cZy0viyIAUgJtG.wav.WsIR, c:\users\rdhj0cnfevzx\desktop\ldwzx9czy0viyiaugjtg.wav.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\LdWZx9cZy0viyIAUgJtG.wav.WsIR.WsIR	Dropped File	76.44 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
dd7897d33c71d292b522dced48d8756d6138e718ed151c662061c61dff2d2280	C:\Users\RDhJ0CNFevzX\Desktop\lZYh4yd5GmG9gUQxF.m4a.WsIR, c:\users\rdhj0cnfevzx\desktop\izyh4yd5gmg9guqxf.m4a.wsir, c:\users\rdhj0cnfevzx\desktop\izyh4yd5gmg9guqxf.m4a.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\lZYh4yd5GmG9gUQxF.m4a.WsIR.WsIR	Dropped File	76.45 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7eb68869f8afc14ddcb7d4d40dd8ced3eef7920f11430d8310fa48e7fa6ee61b	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\qhtez_bgydaj-l.png.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\qHtez_bgyDAJ-l.png....CNFevzX\Desktop\flZIjrAeWDHx\qHtez_bgyDAJ-l.png.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\qhtez_bgydaj-l.png.wsir.wsir	Dropped File	7.05 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
602b39989bc22b0ca6a8653d918205a7a41e3b6892abec5371160ed0374f8b91	C:\Users\RDhJ0CNFevzX\Desktop\vmBov2JwdPztuDyp.flv.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\vmbov2jwdpztudyp.flv.wsir.wsir, c:\users\rdhj0cnfevzx\desktop\vmbov2jwdpztudyp.flv.wsir, C:\Users\RDhJ0CNFevzX\Desktop\vmBov2JwdPztuDyp.flv.WsIR	Dropped File	47.32 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
0d76c8742a6e25f8722ce201796b32694be0cf3b5a49d428fef594df9b189522	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\bb7ilcqwymxeiup.xlsx.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t...hx\rkek9t3rdv\bb7ilcqwymxeiup.xlsx.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\Bb7lICQwyMXEiuP.xlsx.WsIR.WsIR	Dropped File	92.76 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
3f569342315b09ec3294fda5e552bf1f934c2aac4adcfce09aec9da5b727a57d	C:\Users\RDhJ0CNFevzX\Desktop\vmBov2JwdPztuDyp.flv.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\vmbov2jwdpztudyp.flv.wsir.wsir, c:\users\rdhj0cnfevzx\desktop\vmbov2jwdpztudyp.flv.wsir, C:\Users\RDhJ0CNFevzX\Desktop\vmBov2JwdPztuDyp.flv.WsIR	Dropped File	47.33 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
348908fb2481a41928fceeccefd75d41be62a32ea00eb58efe64275f1b55fc36	c:\users\rdhj0cnfevzx\desktop\9cfuw_e1dao.odt.wsir, C:\Users\RDhJ0CNFevzX\Desktop\9CFUw_e 1DAo.odt.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\9CFUw_e 1DAo.odt.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\9cfuw_e1dao.odt.wsir.wsir	Dropped File	69.54 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
c0b8d6780381c468df8cf9d030884928b72f852a89a6c4184b1ef1158e917880	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4ut8p0tdn5vkztsh.gif.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\4UT8p0tDN5vkZtsh....vzx\desktop\fizijraewdhx\4ut8p0tdn5vkztsh.gif.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\4UT8p0tDN5vkZtsh.gif.WsIR.WsIR	Dropped File	48.56 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
8b0871e0221b74ba34377eb0d56c4749d5d1cdac8d55c0dfe9d92aa39e1663b0	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\amb8c8tyuzftkxddd6vn.mp3.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWD...wdhx\rkek9t3rdv\amb8c8tyuzftkxddd6vn.mp3.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\Amb8c8tYuZFtKXDDd6vN.mp3.WsIR	Dropped File	5.41 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f8ccfcc6fa1646998259 22cb69de1a27d3b380249dfcd39c44037ae802f444b2	c:\users\rdhj0cnfevzx\desktop\we628slryqfcn.mp3.wsir, C:\Users\RDhJ0CNFevzX\Desktop\We628sLRYqfcN.mp3.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\We628sLRYqfcN.mp3.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\we628slryqfcn.mp3.wsir.wsir	Dropped File	94.11 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
50e66935cddad24a30fe034257e83a30e01b02e31f66903bd9042b917beb4575	c:\users\rdhj0cnfevzx\desktop\gxyvohpaxjzlat.pptx.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\GXyvohPaxJZLaT.pptx.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\gxyvohpaxjzlat.pptx.wsir, C:\Users\RDhJ0CNFevzX\Desktop\GXyvohPaxJZLaT.pptx.WsIR	Dropped File	52.48 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
623661c3419a6e08e076a30bd1d2ec8a9be57dcbab224b794ab064035760c0cd	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\hcsagnwcw60j2xdsh.wav.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx... ...jraewdhx\rkek9t3rdv\hcsagnwcw60j2xdsh.wav.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\hcSAGNWCW60j2xDSH.wav.WsIR	Dropped File	49.46 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
85cab50b809afd2a69c91d16d87dcd2a8cca38c9a87c126c14b0545bd8775818	C:\Users\RDhJ0CNFevzX\Desktop\bUROA-.jpg.WsIR, c:\users\rdhj0cnfevzx\desktop\buroa-.jpg.wsir, C:\Users\RDhJ0CNFevzX\Desktop\bUROA-.jpg.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\buroa-.jpg.wsir.wsir	Dropped File	78.62 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
8c7432e3023de592f76b89f2a005d66cc42d8865a8100df257aacb6b10cae6d7	c:\users\rdhj0cnfevzx\desktop\9aseh.swf.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\9asEH.swf.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\9aseh.swf.wsir, C:\Users\RDhJ0CNFevzX\Desktop\9asEH.swf.WsIR	Dropped File	72.12 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
c8c48ef7c989b4740cb1c6abaa30e7794d4c008be6021327f7c6c051fc90d05c	c:\users\rdhj0cnfevzx\desktop\-z4rq8r9ukr1.jpg.wsir, C:\Users\RDhJ0CNFevzX\Desktop\-z4rQ8r9ukr1.jpg.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\-z4rQ8r9ukr1.jpg.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\-z4rq8r9ukr1.jpg.wsir.wsir	Dropped File	88.89 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
c73a0eeab958562d5a21b860a43a4430492c2c6484ef06c267fb22f5cca6d55a	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\kfprms4.mp3.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\KfPr... ...desktop\fizijraewdhx\rkek9t3rdv\kfprms4.mp3.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\KfPrMs4.mp3.WsIR.WsIR	Dropped File	25.52 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
90942e599db941c90982d84102a973b44a94ae621615518239177da20c86350b	C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\WpL3Kq1Gh.m4a.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\wp... ...top\flZIjrAeWDHx\Rkek9t3Rdv\WpL3Kq1Gh.m4a.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\wpl3kq1gh.m4a.wsir.wsir	Dropped File	79.81 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
e47fd48df24f1dd1235eb618f3eb77b776bb55912ee602c5cad3aaa82d980d68	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\amb8c8tyuzftkxddd6vn.mp3.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWD... ...wdhx\rkek9t3rdv\amb8c8tyuzftkxddd6vn.mp3.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\Amb8c8tYuZFtKXDDd6vN.mp3.WsIR	Dropped File	5.41 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3d7f4dbefc9a339c60c541ae3e27a76bc613fcbff85eb29c14cd50a5212169f0	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4fjcz48nwkc.mp4.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\4fjcz48nwKc.mp4.WsIR, ...\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\4fjcz48nwKc.mp4.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4fjcz48nwkc.mp4.wsir.wsir	Dropped File	74.38 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
814dd1fcc6e4e1ee0fc46fde77c79ec10b17799890cf11d7c2b77163d40ee9c2	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\95o-aud3nhe9qs4eevn.mp3.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\95O-AUd3nhe9qs...sktop\fizijraewdhx\95o-aud3nhe9qs4eevn.mp3.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\95O-AUd3nhe9qs4EEVN.mp3.WsIR.WsIR	Dropped File	70.04 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
86e0069173c821cc8806e747930831eff514f2b3e33a5c0141823a4d58e8c71e	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\12zna3pivem1wor.m4a.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\12zna3plveM1woR.m4a...FevzX\Desktop\flZIjrAeWDHx\12zna3plveM1woR.m4a.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\12zna3pivem1wor.m4a.wsir.wsir	Dropped File	90.67 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
80129a359a62022d4a6e1b37081710854e09dd32c0663ec67f0f3a32c3203a1f	c:\users\rdhj0cnfevzx\desktop\ud8bdl.xlsx.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\uD8bDL.xlsx.WsIR.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\uD8bDL.xlsx.WsIR, c:\users\rdhj0cnfevzx\desktop\ud8bdl.xlsx.wsir	Dropped File	39.11 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
3c76d98e2cbb5af92df5f43de15b9102eb511c4e5bfd92d7748a0d3ff7be32e9	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\xlhkz08bi-i8drhwtenl.avi.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWD...WDHx\Rkek9t3Rdv\xlhKZ08bI-i8DrHWTeNL.avi.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\xlhkz08bi-i8drhwtenl.avi.wsir	Dropped File	40.20 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
cd9ba2599095892e90fd2c38883780c203e9df249311dd86b25265c1d8921c4b	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rd18vxrba4wvaixb9.doc.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\rD18VXRBa4WVaiXB...x\desktop\fizijraewdhx\rd18vxrba4wvaixb9.doc.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\rD18VXRBa4WVaiXB9.doc.WsIR.WsIR	Dropped File	67.20 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b22ca786d02b314e856a01fd5f9c49a57b9242c6324ebd611dd625f3f18e3398	C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\faYc088QK.doc.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\fa...top\flZIjrAeWDHx\Rkek9t3Rdv\faYc088QK.doc.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\fayc088qk.doc.wsir.wsir	Dropped File	50.46 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7b59240ec3b2ceb7f97de9dd0bc10f612aca66f9fdce0c1c65afbcf82a0aeb0d	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\pv g_1cump.bmp.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\pv G_1CuMp.bmp.WsIR, C:...rs\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\pv G_1CuMp.bmp.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\pv g_1cump.bmp.wsir.wsir	Dropped File	75.89 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
dbfd50014ac46c1e2bfd0111a9f7d3878beac353fea365e408d7937f0a35bf48	C:\Users\RDhJ0CNFevzX\Documents\½âÃÜÎÄ¼þ.key	Dropped File	370 bytes	text/plain	Access, Create, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
883a9ccbb2633685a71be75ed91204642c328ac9225c6fc98c3624292b05ae9f	c:\users\rdhj0cnfevzx\desktop\ldwzx9czy0viyiaugjtg.wav.wsir, C:\Users\RDhJ0CNFevzX\Desktop\LdWZx9cZy0viyIAUgJtG.wav.WsIR, c:\users\rdhj0cnfevzx\desktop\ldwzx9czy0viyiaugjtg.wav.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\LdWZx9cZy0viyIAUgJtG.wav.WsIR.WsIR	Dropped File	76.43 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
aa0fd32e3f676bc82d16198688d7ab248ad82a602ed292bbfa85f7f5765539b2	c:\users\rdhj0cnfevzx\desktop\giv1lznke-dybxmcbir3.mp3.wsir, C:\Users\RDhJ0CNFevzX\Desktop\Giv1LZnkE-dYbxMcBir3.mp3.WsIR, c:\users\rdhj0cnfevzx\desktop\giv1lznke-dybxmcbir3.mp3.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\Giv1LZnkE-dYbxMcBir3.mp3.WsIR.WsIR	Dropped File	66.19 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
ba245bc0e28e5d98a7a314c99143b200c38035fae52ebc74bb21243dae0fe79c	c:\users\rdhj0cnfevzx\desktop\vj4l1avobz6t5xyoq.flv.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\VJ4l1avobZ6t5xYOQ.flv.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\vj4l1avobz6t5xyoq.flv.wsir, C:\Users\RDhJ0CNFevzX\Desktop\VJ4l1avobZ6t5xYOQ.flv.WsIR	Dropped File	53.88 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
c8d916948f8437ce159d77a7ebdc19238c8cf07f3700eb0e124f70dd85c312ae	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4fjcz48nwkc.mp4.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\4fjcz48nwKc.mp4.WsIR, ...\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\4fjcz48nwKc.mp4.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4fjcz48nwkc.mp4.wsir.wsir	Dropped File	74.38 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
85ce8e15b9338555d03b920f91aee9cf5bc35fc8ea4a4fd5349bb18b38eab97a	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\12zna3pivem1wor.m4a.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\12zna3plveM1woR.m4... ...FevzX\Desktop\flZljrAeWDHx\12zna3plveM1woR.m4a.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\12zna3pivem1wor.m4a.wsir.wsir	Dropped File	90.66 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
427c6e1109f70c169f177ffa58f2e0cc99b786783b47ad6a4c613793a072dd3c	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\jpnfqkpt0lf7c.avi.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\jPnfQkpt0lf7c.a... ...\users\rdhj0cnfevzx\desktop\fizijraewdhx\jpnfqkpt0lf7c.avi.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\jPnfQkpt0lf7c.avi.WsIR	Dropped File	37.27 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
d212873c6f5fb9575e4d3d4deb46a0a2b80aaebe2c264bab151d0518efe994ff	C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\RbArjN3ZSZrBNDWJ1be.wav.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rke...k9t3Rdv\RbArjN3ZSZrBNDWJ1be.wav.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\rbarjn3zszrbndwj1be.wav.wsir.wsir	Dropped File	72.11 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7c39f1e30da27b9b403ae8a906b430b58401e791181300cf289048c61ebfcf96	C:\Users\RDhJ0CNFevzX\Desktop\CPi5XIB.swf.WsIR, c:\users\rdhj0cnfevzx\desktop\cpi5xib.swf.wsir, C:\Users\RDhJ0CNFevzX\Desktop\CPi5XIB.swf.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\cpi5xib.swf.wsir.wsir	Dropped File	72.88 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
c32132dd7cf67f3e557fc7f392a5e7cdaa1bbaa77e03bfc5a9206b25dd443f50	C:\Users\RDhJ0CNFevzX\Desktop\EBL1pJQrCMBq.docx.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\ebl1pjqrcmbq.docx.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\EBL1pJQrCMBq.docx.WsIR, c:\users\rdhj0cnfevzx\desktop\ebl1pjqrcmbq.docx.wsir	Dropped File	22.43 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b6deb9cb343d557244db89d0f4aecb662ad466a8df028e4b5e70ecd257fc1009	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\pv g_1cump.bmp.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\pv G_1CuMp.bmp.WsIR, C:... ...rs\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\pv G_1CuMp.bmp.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\pv g_1cump.bmp.wsir.wsir	Dropped File	75.88 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
ed96d7588bea0961a5fb253c710f82c7079d249d15c9f663f894aec38d4843f6	c:\users\rdhj0cnfevzx\desktop\k_oqupeew0f6q.m4a.wsir, C:\Users\RDhJ0CNFevzX\Desktop\k_OQuPEew0F6q.m4a.WsIR, c:\users\rdhj0cnfevzx\desktop\k_oqupeew0f6q.m4a.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\k_OQuPEew0F6q.m4a.WsIR.WsIR	Dropped File	93.38 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
72b946683cb08c8ded60349ac2afca878139702d5671eaec6f600436788c53b2	c:\users\rdhj0cnfevzx\desktop\g6-ktjjzl.png.wsir, C:\Users\RDhJ0CNFevzX\Desktop\G6-KtjJzL.png.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\G6-KtjJzL.png.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\g6-ktjjzl.png.wsir.wsir	Dropped File	25.26 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b1aa273a38c8d5690568fe4303996a224a8b01c83d6106cb9f0b0d51a3eaa3c4	c:\users\rdhj0cnfevzx\desktop\aju7snug.mp4.wsir, C:\Users\RDhJ0CNFevzX\Desktop\AJu7sNug.mp4.WsIR, c:\users\rdhj0cnfevzx\desktop\aju7snug.mp4.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\AJu7sNug.mp4.WsIR.WsIR	Dropped File	80.40 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
437769e29e9db9a7007058aadce64e5dc70cd5469217c29a78feb99b6f5ae3df	c:\users\rdhj0cnfevzx\desktop\3zr9k4.mp4.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\3zR9K4.mp4.WsIR.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\3zR9K4.mp4.WsIR, c:\users\rdhj0cnfevzx\desktop\3zr9k4.mp4.wsir	Dropped File	98.16 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
11a4a6512424d97eb1e021dcba49444e4b2627744be2dceb30ad0c2b066f8997	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\bb7ilcqwymxeiup.xlsx.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t... ...hx\rkek9t3rdv\bb7ilcqwymxeiup.xlsx.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\Bb7IlCQwyMXEiuP.xlsx.WsIR.WsIR	Dropped File	92.75 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b075939c064ad28f97b6afce9fb74bcbcaeb4db2421f7afc149809ae59865707	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\kfprms4.mp3.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\KfPr... ...desktop\fizijraewdhx\rkek9t3rdv\kfprms4.mp3.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\KfPrMs4.mp3.WsIR.WsIR	Dropped File	25.52 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
cfc35162af4ac0e990bb003a14764da29ecf0e97367f800db7fb1ea4e30fda6e	c:\users\rdhj0cnfevzx\desktop\-z4rq8r9ukr1.jpg.wsir, C:\Users\RDhJ0CNFevzX\Desktop\-z4rQ8r9ukr1.jpg.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\-z4rQ8r9ukr1.jpg.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\-z4rq8r9ukr1.jpg.wsir.wsir	Dropped File	88.88 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
5220c0b19104b840c1c9badcf00b541c634083e2784a9a0614015caf5cc5c97c	c:\users\rdhj0cnfevzx\desktop\gxyvohpaxjzlat.pptx.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\GXyvohPaxJZLaT.pptx.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\gxyvohpaxjzlat.pptx.wsir, C:\Users\RDhJ0CNFevzX\Desktop\GXyvohPaxJZLaT.pptx.WsIR	Dropped File	52.48 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d9f56e6ad6816eeec26498838322569a3539ae11998ec7281e85567c65af6358	C:\Users\RDhJ0CNFevzX\Desktop\s1hsdGQT_lQqo9A_5D_H.pps.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\s1hsdgqt_lqqo9a_5d_h.pps.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\s1hsdGQT_lQqo9A_5D_H.pps.WsIR, c:\users\rdhj0cnfevzx\desktop\s1hsdgqt_lqqo9a_5d_h.pps.wsir	Dropped File	85.23 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
f9bba4897d498a95db58931065d58bea41592708695ba5abbbd3f0a57f6ffec5	c:\users\rdhj0cnfevzx\desktop\ah-aj-xw2l9.pps.wsir, C:\Users\RDhJ0CNFevzX\Desktop\AH-Aj-Xw2L9.pps.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\AH-Aj-Xw2L9.pps.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\ah-aj-xw2l9.pps.wsir.wsir	Dropped File	76.67 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
dae07898b8d43df8ae7bae797a6c50f5b77d954a41af505bcc8fb1c978814555	C:\Users\RDhJ0CNFevzX\Desktop\CPi5XlB.swf.WsIR, c:\users\rdhj0cnfevzx\desktop\cpi5xib.swf.wsir, C:\Users\RDhJ0CNFevzX\Desktop\CPi5XlB.swf.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\cpi5xib.swf.wsir.wsir	Dropped File	72.88 KB	application/zlib	Access, Create, Delete, Read, Write	CLEAN
a154dec587b3c14379c742a5f26e69a2eb5ade09cb65bc98ed54b2014cb1dc1a	c:\users\rdhj0cnfevzx\desktop\kyao8y.ots.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\KYao8Y.ots.WsIR.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\KYao8Y.ots.WsIR, c:\users\rdhj0cnfevzx\desktop\kyao8y.ots.wsir	Dropped File	6.73 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
7dee1e1f809e7ef7d4928961a3326e9a1eb8b0b86092faac35b802b2ab9deb29	C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\RbArjN3ZSZrBNDWJ1be.wav.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rke... ...k9t3Rdv\RbArjN3ZSZrBNDWJ1be.wav.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\rbarjn3zszrbndwj1be.wav.wsir.wsir	Dropped File	72.12 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
8cf327522b2b67aaf173a4874178e372325297d531d567aece2bf2eefbb7bdcc	C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\65OLmi32HgseAx.bmp.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3r... ...aewdhx\rkek9t3rdv\65olmi32hgseax.bmp.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\65OLmi32HgseAx.bmp.WsIR.WsIR	Dropped File	54.62 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
af44134b31bdf860fbd1c8f521da7d0ad664a8d21e9db0c0727da660f27ba69f	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\hcsagnwcw60j2xdsh.wav.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx... ...jraewdhx\rkek9t3rdv\hcsagnwcw60j2xdsh.wav.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\hcSAGNWCW60j2xDSH.wav.WsIR	Dropped File	49.45 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
a9615178e4a75f847ed5c475c7deb4b720893dbb08b86425cbbae3dfb08dc074	c:\users\rdhj0cnfevzx\desktop\ah-aj-xw2l9.pps.wsir, C:\Users\RDhJ0CNFevzX\Desktop\AH-Aj-Xw2L9.pps.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\AH-Aj-Xw2L9.pps.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\ah-aj-xw2l9.pps.wsir.wsir	Dropped File	76.66 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b6a8134b1145ae502718ae5e43cc9b905f8acb0fab18067132308b23d0979e75	C:\Users\RDhJ0CNFevzX\Desktop\lZYh4yd5GmG9gUQxF.m4a.WsIR, c:\users\rdhj0cnfevzx\desktop\izyh4yd5gmg9guqxf.m4a.wsir, c:\users\rdhj0cnfevzx\desktop\izyh4yd5gmg9guqxf.m4a.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\lZYh4yd5GmG9gUQxF.m4a.WsIR.WsIR	Dropped File	76.46 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8c5206f38d7627b498f6e7833a98a88041b92e6208628f61fb7a3ab6d92f7e4a	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\xlhkz08bi-i8drhwtenl.avi.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWD... ...WDHx\Rkek9t3Rdv\xlhKZ08bl-i8DrHWTeNL.avi.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\xlhkz08bi-i8drhwtenl.avi.wsir	Dropped File	40.21 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
0fba50c651a22710736bb14d9a4c3e243043faf2a3720b9693c791538a203ff8	C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\WpL3Kq1Gh.m4a.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\wp... ...top\flZIjrAeWDHx\Rkek9t3Rdv\WpL3Kq1Gh.m4a.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\wpl3kq1gh.m4a.wsir.wsir	Dropped File	79.80 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
fe296dedd51b57ec45c8f8a3bcd07942d4510a3451c0db4bf83f2bfd3f3aa7b1	c:\users\rdhj0cnfevzx\desktop\3zr9k4.mp4.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\3zR9K4.mp4.WsIR.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\3zR9K4.mp4.WsIR, c:\users\rdhj0cnfevzx\desktop\3zr9k4.mp4.wsir	Dropped File	98.16 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
4b9d687ac625690fd026ed4b236dad1cac90ef69e7ad256cc42766a065b50026	c:\users\rdhj0cnfevzx\desktop\desktop.ini.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini.WsIR.WsIR	Dropped File	282 bytes	text/plain	Access, Create, Write	CLEAN
6af2c3bafe696655a2566dd174af7cdb6730dd7a00b8da34a7334da68edea9d4	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\95o-aud3nhe9qs4eevn.mp3.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\95O-AUd3nhe9qs... ...sktop\fizijraewdhx\95o-aud3nhe9qs4eevn.mp3.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\95O-AUd3nhe9qs4EEVN.mp3.WsIR.WsIR	Dropped File	70.03 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
e79fd7d8f4a6818c8ea6d71f2851ff8865211c29ffb69cf83ab587dcbf6e810a	c:\users\rdhj0cnfevzx\desktop\4tbtosvhwga.jpg.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\4TbtoSVhWGA.jpg.WsIR.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\4TbtoSVhWGA.jpg.WsIR, c:\users\rdhj0cnfevzx\desktop\4tbtosvhwga.jpg.wsir	Dropped File	10.32 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
a232248694e91c4b49fba8f83c2944275a3ac7c7b0f9861f8fb817cafc4ba088	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\b8oqnzm.mp4.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\b8oQNZM.mp4.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\b8oqnzm.mp4.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\b8oQNZM.mp4.WsIR.WsIR	Dropped File	70.10 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
fa543e7c74f7e918dbd2328a21ce5c5b946fd07c79434e108ba7397ee02e2a85	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\jpnfqkpt0lf7c.avi.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\jPnfQkpt0lf7c.a... ... \users\rdhj0cnfevzx\desktop\fizijraewdhx\jpnfqkpt0lf7c.avi.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\jPnfQkpt0lf7c.avi.WsIR	Dropped File	37.27 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
75867351a3dadace45dbb895a6cada64be013449fd0c84eff4c6044098675421	c:\users\rdhj0cnfevzx\desktop\9cfuw_e1dao.odt.wsir, C:\Users\RDhJ0CNFevzX\Desktop\9CFUw_e 1DAo.odt.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\9CFUw_e 1DAo.odt.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\9cfuw_e1dao.odt.wsir.wsir	Dropped File	69.55 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9be3d7ff692deea11addb97e4b6f06159b05b7a3d5fd306ebd87357d9fd0afee	c:\users\rdhj0cnfevzx\desktop\we628slryqfcn.mp3.wsir, C:\Users\RDhJ0CNFevzX\Desktop\We628sLRYqfcN.mp3.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\We628sLRYqfcN.mp3.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\we628slryqfcn.mp3.wsir.wsir	Dropped File	94.10 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
b1c5478c5fb05a175d9c73e9f1cf1368a6b8863f85d40a0ab755ba59929d009e	c:\users\rdhj0cnfevzx\desktop\aju7snug.mp4.wsir, C:\Users\RDhJ0CNFevzX\Desktop\AJu7sNug.mp4.WsIR, c:\users\rdhj0cnfevzx\desktop\aju7snug.mp4.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\AJu7sNug.mp4.WsIR.WsIR	Dropped File	80.41 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
e4b841e3bdd09794472e5c75cc29f1e8bda7b586c5167daf81367fcaa8e3c325	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rd18vxrba4wvaixb9.doc.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\rD18VXRBa4WVaiXB...\...x\desktop\fizijraewdhx\rd18vxrba4wvaixb9.doc.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\rD18VXRBa4WVaiXB9.doc.WsIR.WsIR	Dropped File	67.19 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
28dcb9122ced25dd14c7f1363562c0d095d374a1cb3591ba8eb9239754bb87dd	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\qhtez_bgydaj-l.png.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\qHtez_bgyDAJ-l.png....\...CNFevzX\Desktop\flZIjrAeWDHx\qHtez_bgyDAJ-l.png.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\qhtez_bgydaj-l.png.wsir.wsir	Dropped File	7.05 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
58f868695cfe19bc4317de8c12a92709cee99cb68ad9daeac935f1c23d74cc75	C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\faYc088QK.doc.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\fa...\...top\flZIjrAeWDHx\Rkek9t3Rdv\faYc088QK.doc.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\fayc088qk.doc.wsir.wsir	Dropped File	50.47 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
f9b70f2060934198e02ae3cc39f0dea67d250f09795dcc3fcbf10df7dd55c39c	C:\Users\RDhJ0CNFevzX\Desktop\8kSw42jKOoLb1LIX.jpg.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\8ksw42jkoolb1lix.jpg.wsir.wsir, c:\users\rdhj0cnfevzx\desktop\8ksw42jkoolb1lix.jpg.wsir, C:\Users\RDhJ0CNFevzX\Desktop\8kSw42jKOoLb1LIX.jpg.WsIR	Dropped File	26.86 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
316706e34bfabd8f7611964a4676ae2647553e968499b5af1b8b414b4e2ae920	c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\b8oqnzm.mp4.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\b8oQNZM.mp4.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\b8oqnzm.mp4.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\b8oQNZM.mp4.WsIR.WsIR	Dropped File	70.09 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
50117fde03397b5892ab5a60a2bd336758edf4b4a8412887f56cac7abbe01cae	C:\Users\RDhJ0CNFevzX\Desktop\bUROA-.jpg.WsIR, c:\users\rdhj0cnfevzx\desktop\buroa-.jpg.wsir, C:\Users\RDhJ0CNFevzX\Desktop\bUROA-.jpg.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\buroa-.jpg.wsir.wsir	Dropped File	78.62 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
f3acefd62e6299074e8cd018b72fafbc68b0bac2b69f4565796cfe16b53446fa	C:\Users\RDhJ0CNFevzX\Desktop\oWU-E0n.avi.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\owu-e0n.avi.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\oWU-E0n.avi.WsIR, c:\users\rdhj0cnfevzx\desktop\owu-e0n.avi.wsir	Dropped File	49.20 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f44b981e6a5bd2e3f436fe685fda51e0a7e51ba3e170ef37029fbb8a79947f40	C:\Users\RDhJ0CNFevzX\Desktop\GiRli3vyk91ALiSqq9.mkv.WsIR, c:\users\rdhj0cnfevzx\desktop\girii3vyk91alisqq9.mkv.wsir, c:\users\rdhj0cnfevzx\desktop\girii3vyk91alisqq9.mkv.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\GiRli3vyk91ALiSqq9.mkv.WsIR.WsIR	Dropped File	56.97 KB	application/x-dosexec	Access, Create, Delete, Read, Write	CLEAN
ea3fdd885ada0466a4cbc6ae06369115340b2183ef44f46ff40090b17572ee3c	C:\Users\RDhJ0CNFevzX\Desktop\GiRli3vyk91ALiSqq9.mkv.WsIR, c:\users\rdhj0cnfevzx\desktop\girii3vyk91alisqq9.mkv.wsir, c:\users\rdhj0cnfevzx\desktop\girii3vyk91alisqq9.mkv.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\GiRli3vyk91ALiSqq9.mkv.WsIR.WsIR	Dropped File	56.96 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
69e8917b112e80981e69de5187deb5cec80a36d890d2ceda0f09baa1782b1a34	c:\users\rdhj0cnfevzx\desktop\ud8bdl.xlsx.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\uD8bDL.xlsx.WsIR.WsIR, C:\Users\RDhJ0CNFevzX\Desktop\uD8bDL.xlsx.WsIR, c:\users\rdhj0cnfevzx\desktop\ud8bdl.xlsx.wsir	Dropped File	39.12 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
6e83000b22ea30c917921a496873946d398b8874e8df347f97ff3b656db6a7b8	C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\65OLmi32HgseAx.bmp.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3r... ...aewdhx\rkek9t3rdv\65olmi32hgseax.bmp.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\65OLmi32HgseAx.bmp.WsIR.WsIR	Dropped File	54.62 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
37850a236c662458c186f213a10e6f28882264e4b323b5d296891fd7f728192a	c:\users\rdhj0cnfevzx\desktop\9aseh.swf.wsir.wsir, C:\Users\RDhJ0CNFevzX\Desktop\9asEH.swf.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\9aseh.swf.wsir, C:\Users\RDhJ0CNFevzX\Desktop\9asEH.swf.WsIR	Dropped File	72.12 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
d913acaaee4348513872e9cd2b6e288cffeba8652998cb1e3d5802c202d362b1	C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\ke4ecUbbuT2.m4a.WsIR.WsIR, c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t... ...x\desktop\fizijraewdhx\rkek9t3rdv\ke4ecubbut2.m4a.wsir, C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\ke4ecUbbuT2.m4a.WsIR	Dropped File	57.98 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\b8oqnzm.mp4.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\9aseh.swf.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\4fjcz48nwKc.mp4.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\qHtez_bgyDAJ-l.png.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\12zna3plveM1woR.m4a.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\kfprms4.mp3.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\giv1lznke-dybxmcbir3.mp3.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\JNsbV273_XUNA9WdFumt.swf.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\AH-Aj-Xw2L9.pps.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\aju7snug.mp4.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\CPi5XIB.swf.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4fjcz48nwkc.mp4.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\vj4l1avobz6t5xyoq.flv.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\IZYh4yd5GmG9gUQxF.m4a.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\-z4rq8r9ukr1.jpg.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\12zna3pivem1wor.m4a.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe.WsIR	Sample File, Dropped File, Accessed File, Not Extracted	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\jnsbv273_xuna9wdfumt.swf.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\gxyvohpaxjzlat.pptx.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\hcsagnwcw60j2xdsh.wav.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\GiRIi3vyk91ALiSqq9.mkv.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\amb8c8tyuzftkxddd6vn.mp3.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\xlhkz08bi-i8drhwtenl.avi.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\3zR9K4.mp4.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rd18vxrba4wvaixb9.doc.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\oWU-E0n.avi.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\faYc088QK.doc.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\95o-aud3nhe9qs4eevn.mp3.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\9aseh.swf.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\RbArjN3ZSZrBNDWJ1be.wav.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\uD8bDL.xlsx.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\9CFUw_e 1DAo.odt.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\vmbov2jwdpztudyp.flv.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\RbArjN3ZSZrBNDWJ1be.wav.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\CPi5XIB.swf.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\qhtez_bgydaj-l.png.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\k_oqupeew0f6q.m4a.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\65olmi32hgseax.bmp.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\EBL1pJQrCMBq.docx.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\xlhKZ08bl-i8DrHWTeNL.avi.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\KYao8Y.ots.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\95o-aud3nhe9qs4eevn.mp3.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\WpL3Kq1Gh.m4a.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe	Sample File, Accessed File, VM File	Access, Create, Delete, Read	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\oWU-E0n.avi.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\g6-ktjjzl.png.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\k_oqupeew0f6q.m4a.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4ut8p0tdn5vkztsh.gif.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\kyao8y.ots.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\we628slryqfcn.mp3.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\bb7ilcqwymxeiup.xlsx.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\bUROA-.jpg.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\faYc088QK.doc.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\ud8bdl.xlsx.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\ke4ecubbut2.m4a.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\0eeyc edyqt.flv.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\giv1lznke-dybxmcbir3.mp3.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\kfprms4.mp3.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\pvG_1CuMp.bmp.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\4TbtoSVhWGA.jpg.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\gxyvohpaxjzlat.pptx.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\bUROA-.jpg.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\desktop\vj4l1avobz6t5xyoq.flv.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\desktop.ini.wsir	Dropped File, Accessed File, Not Extracted	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe.WsIR.WsIR	Sample File, Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\4ut8p0tdn5vkztsh.gif.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\3zr9k4.mp4.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\vmBov2JwdPztuDyp.flv.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\amb8c8tyuzftkxddd6vn.mp3.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\ke4ecUbbuT2.m4a.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\ah-aj-xw2l9.pps.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\jpnfqkpt0lf7c.avi.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\0EEYc EDyqT.flv.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\We628sLRYqfcN.mp3.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\-z4rQ8r9ukr1.jpg.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rd18vxrba4wvaixb9.doc.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\flZIjrAeWDHx\Rkek9t3Rdv\WpL3Kq1Gh.m4a.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\9cfuw_e 1dao.odt.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\8kSw42jKOoLb1LIX.jpg.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\jpnfqkpt0lf7c.avi.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\desktop.ini.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\4tbtosvhwga.jpg.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\girii3vyk91alisqq9.mkv.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\s1hsdGQT_lQqo9A_5D_H.pps.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\EBL1pJQrCMBq.docx.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\izyh4yd5gmg9guqxf.m4a.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\b8oqnzm.mp4.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\pv g_1cump.bmp.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\8ksw42jkoolb1lix.jpg.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\flZljrAeWDHx\Rkek9t3Rdv\65OLmi32HgseAx.bmp.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\ldwzx9czy0viyiaugjtg.wav.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\s1hsdGQT_IQqo9A_5D_H.pps.WsIR	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\aju7snug.mp4.wsir.wsir	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\bb7ilcqwymxeiup.xlsx.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\G6-KtjJzL.png.WsIR.WsIR	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\fizijraewdhx\rkek9t3rdv\hcsagnwcw60j2xdsh.wav.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\ldwzx9czy0viyiaugjtg.wav.wsir	Dropped File, Accessed File	Access, Create, Delete, Read, Write	MALICIOUS
c:\output	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\WsIR.exe	-	-	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\desktop.ini	Accessed File	Access, Create, Delete, Read	CLEAN
\\.\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}	Accessed File	Access	CLEAN
\\.\{E4D2000A-6025-4C58-8789-AF7349886E11}	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Documents\½âÃÜÎÄ¼þ.key	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
\\.\{E96D977E-F067-4CE9-924D-F6E0A04729E4}	Accessed File	Access	CLEAN
\\.\{E25A642B-6CEB-4194-8F83-8BC82AF94F5A}	Accessed File	Access	CLEAN
\\.\{017EF944-8C88-42C3-8F92-C8F7B6022F8D}	Accessed File	Access	CLEAN
\\.\{9E8A7ED5-49C8-421B-A782-D46C28931105}	Accessed File	Access	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\software\microsoft\windows\CurrentVersion\Run\WsIR	write, access	3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe	CLEAN
HKEY_LOCAL_MACHINE\software\microsoft\windows\CurrentVersion\Run	access	3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe	CLEAN

Process

Process Name	Commandline	Verdict
3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe	"C:\Users\RDhJ0CNFevzX\Desktop\3bae281a122628561deb145beffcb3b2c1b8ab51e0c96818ef7a1203738af5d4.exe"	MALICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.5.1
Dynamic Engine Version	4.5.1 / 05/09/2022 04:24
Static Engine Version	4.5.1.0 / 2022-05-09 03:00:28
AV Exceptions Version	4.5.1.25 / 2022-04-28 14:12:58
Link Detonation Heuristics Version	4.5.1.26 / 2022-04-29 08:24:51
Smart Memory Dumping Rules Version	4.5.1.25 / 2022-04-28 14:12:58
Config Extractors Version	4.5.1.30 / 2022-05-16 06:57:54
Signature Trust Store Version	4.5.1.30 / 2022-05-16 06:57:54
VMRay Threat Identifiers Version	4.5.1.32 / 2022-05-17 14:24:05
YARA Built-in Ruleset Version	4.5.1.29

Software Information

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

System Information

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

System Root	C:\Windows