

MALICIOUS

Classifications: Ransomware

Threat Names: -

Verdict Reason: -

Sample Type	Windows Exe (x86-32)
File Name	319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe
ID	#6454794
MD5	0a5e38ff165e9e78e58fd5b47b19b86a
SHA1	d0cccb38776b7390bf8b0fc5ebe14a75b1dfa3ef
SHA256	319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5
File Size	12.50 KB
Report Created	2022-12-27 10:17 (UTC+1)
Target Environment	win10_64_th2_en_mso2016 exe

OVERVIEW

VMRay Threat Identifiers (6 rules, 204 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
<ul style="list-style-type: none"> • (Process #1) 319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe modifies the content of multiple user files. 				
5/5	User Data Modification	Renames user files	1	Ransomware
<ul style="list-style-type: none"> • (Process #1) 319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe renames multiple user files. 				
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
<ul style="list-style-type: none"> • Renames 1944 files by appending the extension ".bd". 				
1/5	Persistence	Installs system startup script or application	1	-
<ul style="list-style-type: none"> • (Process #1) 319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe adds "C:\Users\RDHJ0C~1\AppData\Local\Temp\WU17sDZVZ12PQjL.exe" to Windows startup via registry. 				
1/5	System Modification	Modifies application directory	100	-

Score	Category	Operation	Count	Classification
1/5	System Modification	Modifies operating system directory	100	-

Score	Category	Operation	Count	Classification
-	Trusted	Known clean file	1	-

- Embedded file "" is a known clean file.

Mitre ATT&CK Matrix

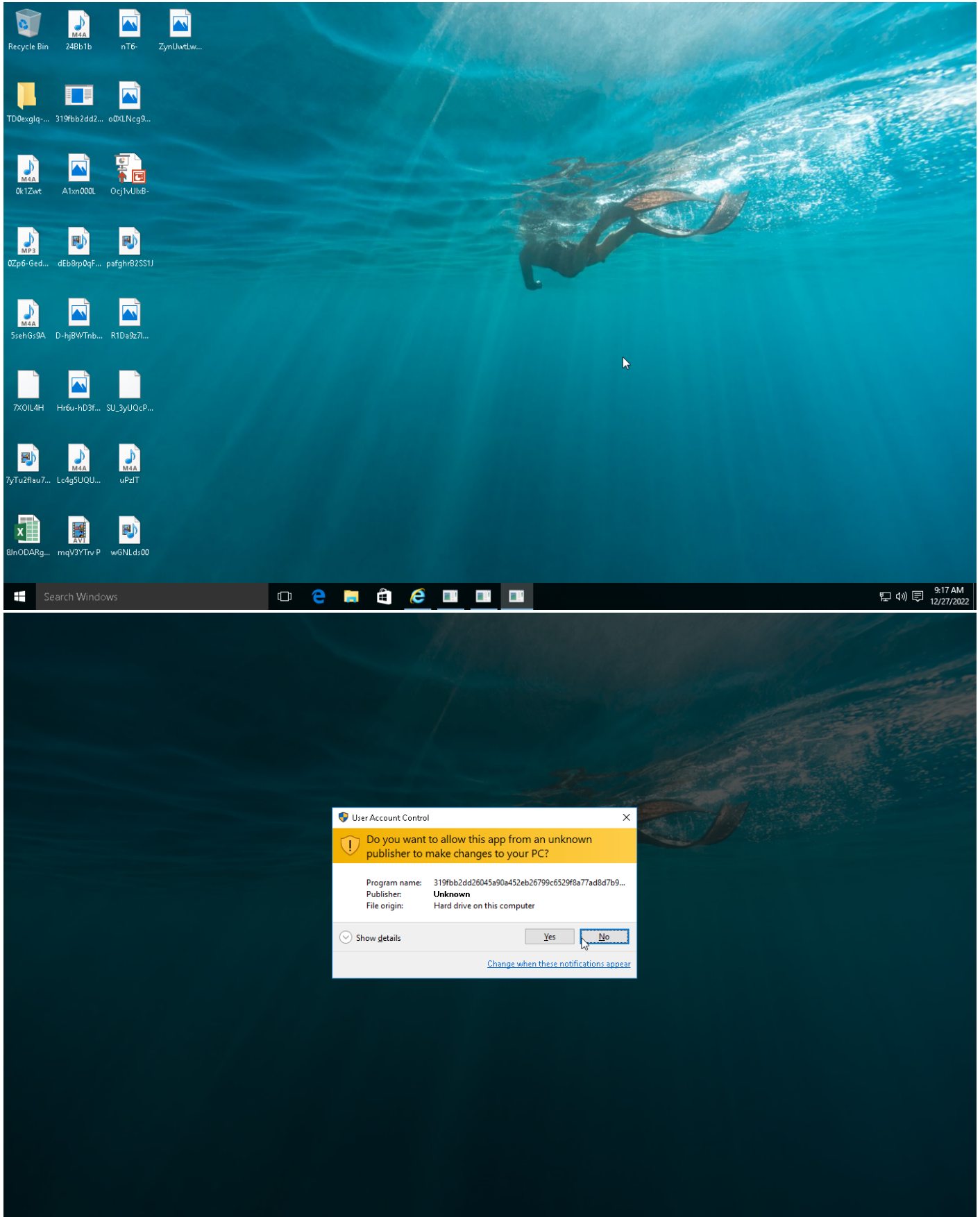
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1112 Modify Registry							#T1486 Data Encrypted for Impact

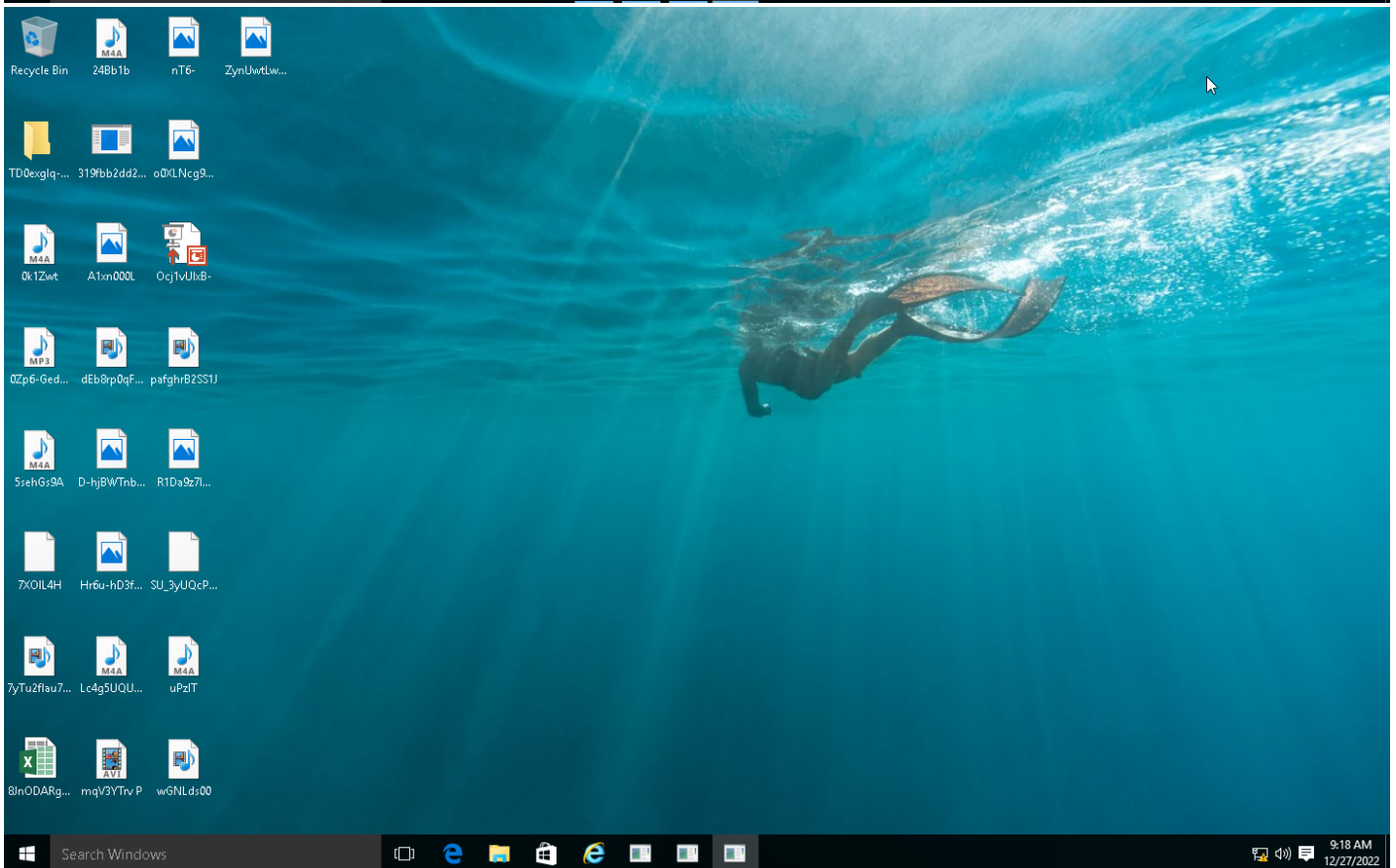
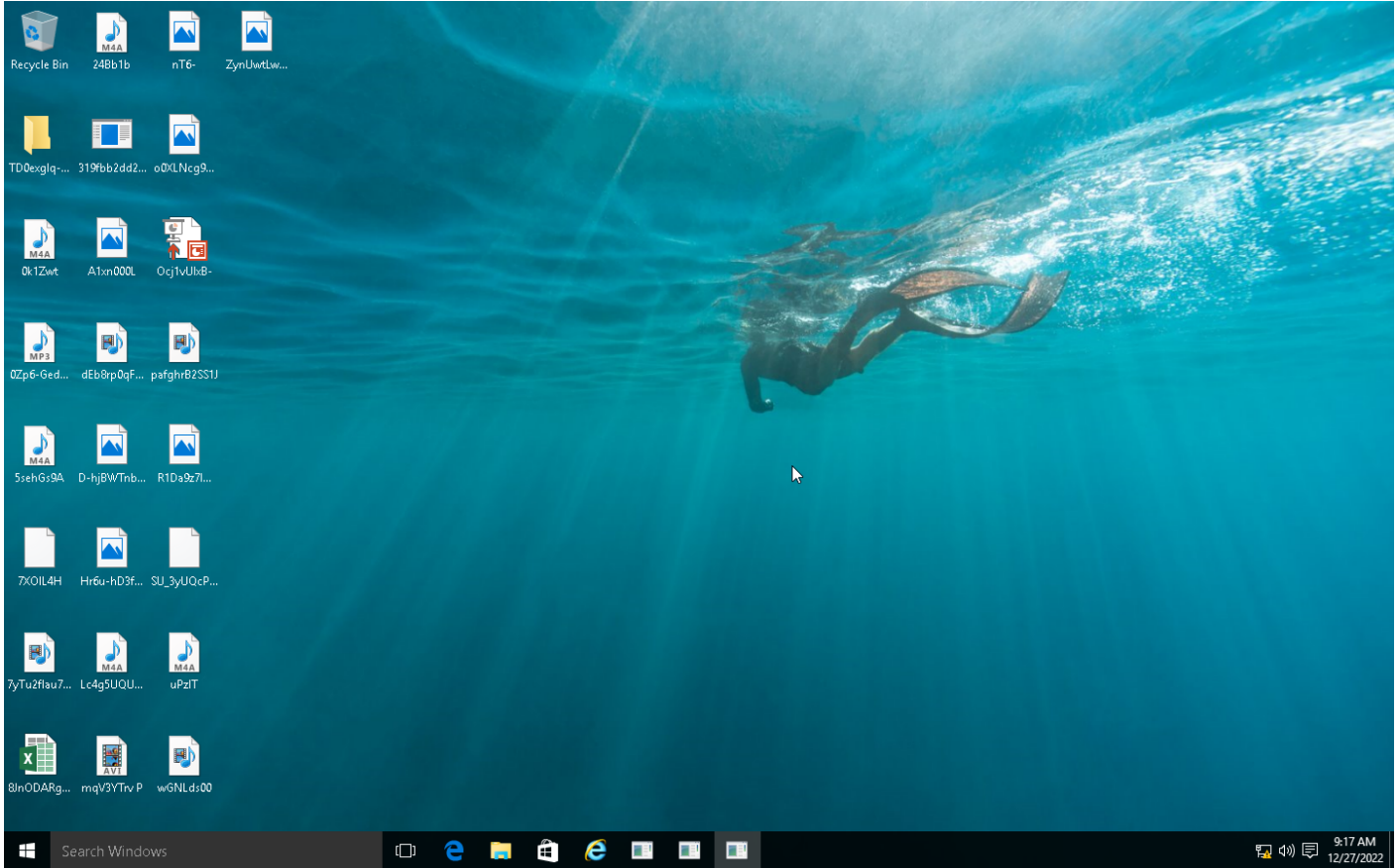
Sample Information

ID	#6454794
MD5	0a5e38ff165e9e78e58fd5b47b19b86a
SHA1	d0cccb38776b7390bf8b0fc5ebe14a75b1dfa3ef
SHA256	319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5
SSDeep	192:K/TrG62a6B10k3g4fXk1iTV3HGc7EkpAqEjvu2q9C/YpXnAITZfPtRMTRE4l2W:KebFNw4Pk1itKkpAjjl2YpdmToQ2W
ImpHash	0ee5d9cb6f5676c02853dce193d35794
File Name	319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe
File Size	12.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-12-27 10:17 (UTC+1)
Analysis Duration	00:02:27
Termination Reason	All processes terminated
Number of Monitored Processes	1
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✘
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0





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

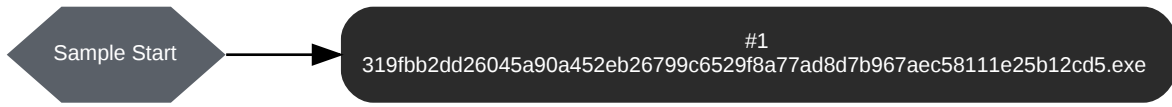
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe

ID	1
File Name	c:\users\rdhj0cnfevz\desktop\319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe
Command Line	"C:\Users\RDHJ0CNFeVz\X\Desktop\319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe"
Initial Working Directory	C:\Users\RDHJ0CNFeVz\X\Desktop\
Monitor Start Time	Start Time: 52275, Reason: Analysis Target
Unmonitor End Time	End Time: 189173, Reason: Terminated
Monitor duration	136.90s
Return Code	0
PID	4792
Parent PID	1648
Bitness	32 Bit

Dropped Files (1903)

File Name	File Size	SHA256	YARA Match
c:\program files (x86)\microsoft office\clipart\pub60cor\ph01478u.bmp.bd	31.22 KB	5f2a47685fee50e41372b38924f12535a37ff3b60b15f89e604b9d3ff803c5c	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PH0145895.JPG.BD	33.16 KB	0479e7d2e8e326200ff8e70086cc0b3e329f5a4716717ae22a63d664814149cd	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PH01213K.JPG.BD	6.19 KB	6b9d24cc7129a8b088e43b1bb6b0fc1b1ff0ae5e25628b041815070db00b6da2	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph01236u.bmp.bd	31.22 KB	42d798e2677988af98530c661a29a014b703c6f326cce3006a6ea924767dfc5b	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PH0337280.JPG.BD	12.59 KB	f5954e493262eef2b792f6a31e823678d94e20f13213479e8b60de2430c9e80	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PH0387270.JPG.BD	14.82 KB	bf110175f8f3d6240cd32c76f8c9273e8c64b00734465bd6a1c89a3f0eb8627	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PH02752G.GIF.BD	48.88 KB	db6f4dd9fc9521c810f9fca2238c382adc7f76aca30144c0ac18727d8dc3675f	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02748g.gif.bd	24.14 KB	696554e30e114b5e38f9a518fd6317a34294574d877fb2eb21ec2c8b40fd0fd	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382968.jpg.bd	109.84 KB	a9f7371977565961d72619b6d468773749cce885bbc534b1f461d2508205e67f	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PH02752U.BMP.BD	31.01 KB	c8ca73f10da0b05cefb9a4f4adf2a02f8ad1e564031f402778c3051af6fa7c ea	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0400002.png.bd	87.32 KB	4052f069d4fea46661e33e60ecc4c006e9e994a5a7e12a4d99d24b6d22610a4a	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PH0387895.JPG.BD	31.49 KB	48fad5d5e15f10ecc069e6634a1f9538b6269039b538802e20a7b872ac1dba39	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382926.jpg.bd	89.79 KB	6d7933c82f0d6fcd8b8c001ce1a9722a1e9b65caa906ee7a8c53c2122794b32	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0202045.jpg.bd	41.26 KB	30bbaa1301de4ed5653e277fb0e65f82389cca204f99eda1e4b9803a122053e3	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PH00601G.GIF.BD	1.54 KB	15039064ee52ad19d2999079f493fc9388bd34dc6823b919333598318037ffa1	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02746g.gif.bd	23.62 KB	b48ee82c746992da7b2086bfe1455ec5e3defdbd1692aed7582c9c73c7e3d7c2	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0178523.jpg.bd	23.47 KB	3527855c7c33995627197025677552b9bee1b4b6cb8dc77bc44a38f1bbc d2a54	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02291u.bmp.bd	31.43 KB	1c9d25201a0e1d1ea772e05e0847a2d7daf275202853e65590c32b6e515cf2af	✘

File Name	File Size	SHA256	YARA Match
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02736G.GIF.BD	24.90 KB	ae6180a9d8265703f63407519be638995925242dee90ce0b93123e9ac9c470b	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02743g.gif.bd	27.38 KB	0206209ccc67bfcc77ff82a1c9f287e0fcd4729f106f07241fa73d10d0b00f7e	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0141328.JPG.BD	9.96 KB	1e953cbbc613da3295d4120296b15107fe4c7c7de71315bfdeef93e90bc06838	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0101863.bmp.bd	31.43 KB	19052abcdbfec95f0835796869cddb8204297ab3a24baa181ef008c11e98cfe	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0400005.PNG.BD	93.81 KB	8c40b2a904958fd0460276b245aec330c1c9e7e43f0863e91dbc3cd1cfe865f	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02398U.BMP.BD	31.22 KB	f53535f720e495dc1be43d05bd510d973c9e9d3bcf7bb7171a81d7301a673e03	✘
c:\program files\common files\bfkeqdlno2.gif.bd	70.07 KB	709c72d51452223fda5077da1e7f62e36536fa4753fc57e4cac94ba7d3dbebf7	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0149018.JPG.BD	26.75 KB	59f55c71160f6ea6a5fc054f318e77a70ae43bfb99ba39042b65c0297a29e05	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0341559.jpg.bd	26.11 KB	0af5c0758110fd00e0c46a46f161a3072a87a22ca447f3fd72966d879a757320	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0287644.JPG.BD	16.94 KB	815a2c5608013127c6db28d30f71d590b6db45c53fd4ad1f6eb9f3af6574d90f	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02412K.JPG.BD	3.46 KB	812fc2ab0cdc3a720a4c77a3a33369a1b9849ac24dd4e0beb56cf0374e75aa	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0145669.jpg.bd	31.10 KB	6085778e35731d39f388e680175e684a9da611ffd1f6964fe5263dfe6fb20b6b	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02062U.BMP.BD	31.22 KB	5f415419e44cdd3f3d42b1b89e9308904235e4f6af1798f4fb6a0aba2c2dc660	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0227558.jpg.bd	56.73 KB	0819e1d708fb5bdb03567e62f51a76ab5657bffd9471d353a3b39c693569c68d	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0341742.JPG.BD	18.43 KB	22a0438703d4fa0031000c6bd54683cf5ba40ea2b4083d10f4be529d077d1ed	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02466u.bmp.bd	31.01 KB	5ccfbc06d4ec202e9aac86dc6bb45167ea9ceb288b5beffc59482a876dfb1962	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0321179.jpg.bd	9.21 KB	6a893ad4ac4e056f6dd3326ef871e8dee4538360f15859c908afd58eeb6d767	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0145168.jpg.bd	32.87 KB	b3e3c3abbe02278eaad798f5151c8cf0a6b1e0a8a3ddeed00b1d4e5956d05995	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02417U.BMP.BD	31.22 KB	830b68e30ffe6fdae050094ddb68616c854aad9952e84e775ed9e5f76b0d74	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382966.JPG.BD	98.13 KB	c5ee08c5ef2f5687e9f913d7d3e291e7586ffe277e93d4742e06913772612a0c	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0178348.JPG.BD	36.12 KB	922d4519a6ce0e3fafa0ce66dd92d0ab4c50b36b1b68e16895a0cb17593a8844	✘
C:\Boot\fr-FR\HOW TO DECRYPT FILES.txt	623 bytes	9bbf513c05697bf8a6a23b9015e15247b5c05039eb1f63fee5f54ee3dfec3630	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph01265u.bmp.bd	31.01 KB	4def13655fdcfca77ea145214e1f780de013017cdee85fd4ac0fcb8cb6a57	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0101866.BMP.BD	31.43 KB	4ae1622a4d1fba63f958f0cd0c07ed38d48155dbe0be1d7199e7d7a2cd5d0349	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02071U.BMP.BD	31.43 KB	ed91ceed70fd12847dbaf2cd73766bb515103c901523bf94d50858d10f047db	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0313974.JPG.BD	46.45 KB	4a627f6105550dc50656b2e533261494195c19e68fe7a2f0c739641ccf491118	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0309598.JPG.BD	32.48 KB	7552dbdb54056a101f7896e95edb468da7d3a08ad29f5a8afb72accb68a75d27	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382965.jpg.bd	110.75 KB	1c829fbc5a9608ad8443738d3cf99c37c31deef2e2936805eed1c72e21273a23	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0309664.jpg.bd	42.68 KB	79cb9edb581e5abf5bc5da6b805ebc02dab537d76015490b82d955695c38149f	✘

File Name	File Size	SHA256	YARA Match
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0179963.JPG.BD	31.36 KB	c49290fe990d038f7d58234e3ff7d05704a4c14d7bda1f15a662c39c879956a3	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02742u.bmp.bd	31.22 KB	ee1c150ea5902bc9cd8e081681fa71a017d1dd7e52c861e976dc4f7bdacc2a0b	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0341447.jpg.bd	18.71 KB	3d794813ca0fe0bfff84efc2d54d4338c277f83b530b30147d9ba90808391a9d1	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0400001.PNG.BD	198.13 KB	1c114630ee0bb4db4cac2470861ee99aaef04e8cfd65974b3db865429dc53a5	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0287641.jpg.bd	34.41 KB	9658ae0349d3c51290aaa0c9e975fc49dc59649c467b80f65d101ee6107684e0	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382961.jpg.bd	98.69 KB	d41f309ca7118a577997f3e7944822f2579fd863da72d61212054fa0389a91ed	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382959.jpg.bd	83.88 KB	73a51b30a1cbe720bdaff16ac9a88ff734fab49b1c3bd2f4e880d6c95a9470af	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0099203.gif.bd	3.81 KB	3d8b20be89715387470fbaf14e3dc874650c2f46c03b361c6357bf9914fbc7e0	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\PH02223U.BMP.BD	31.43 KB	e5b24860b3771800b61d738f2e827e117046f7e4333a42a2c469480c22631ab	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0178459.jpg.bd	28.52 KB	343d4e09737e876e5573f502b5b6ef0657940dd8b6e136eccbb713737051f34a	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0149118.jpg.bd	63.28 KB	ceada46bd8d8081348e23eab99c2d5d0a3d1535d32c3b30fc58c7f9a30e5e326	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0177806.jpg.bd	54.25 KB	2b0c4ecd7ae3a2931c053f1d0f7a786eb23bd3aa83c679941eb4fc17f5b6d681	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382958.jpg.bd	100.98 KB	8e0323e488cb4af98c754798020e853e6598085f3dec98a9c63515155b97741b	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0148309.jpg.bd	42.65 KB	b47cc23c97737e9f8e898f92d0e99d1b7e423b8808ba512c94b151411fb2e8	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0387604.JPG.BD	46.44 KB	519077ab912cd948a7598e5929a65978e1e21cad50b7df0b51d3932cb4e905b5	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0341561.JPG.BD	41.15 KB	8441f5c9e35dc8f4d96855e02c992ced1542b8c1ac3114bfe86d530940b945dd	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0341534.JPG.BD	7.88 KB	fa9963f021800f44afc8547d398cfa1c5e93161af9b973d5a26138a41eaba9b	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0384895.JPG.BD	54.24 KB	edde04d3ac4c92beb2779d6b0747b63246e7c418d5e82226cb7ec937759c3b1b	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0144773.jpg.bd	39.29 KB	44815354c66bbe79ce5453b56408bf50c49e49c26d09021fed88d56fafdd a797	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0178460.JPG.BD	25.91 KB	3fe706f50068b6feb6fdaf3a2beaf4e4876cca815ab8241a58c84a2ecd7092d9	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0341455.JPG.BD	29.08 KB	3a696ad8106632ead89e6d498b947d9284f42477b115c8c859936a9a8dfa3ff5	✘
c:\program files\common files\7swould2wk.gif.bd	64.84 KB	d068b0744041c6c3207c5087b5f0aeea9874dfd548ef9b852a8522eca2b0e413	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382944.jpg.bd	79.53 KB	4dec080aba90d9dfa95a30a4628bdd849acf66466d7cdd7fa8e7e7c07726ed0b	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02746u.bmp.bd	31.38 KB	64449128550c1c65731e6d2a01c1b92b8409c06db3ceb83124bf443edecdc	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0148798.JPG.BD	37.34 KB	ab799123ba1bcd6481029c762614e13de145a4c402ea09eb477fd09c71558e3b	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02039u.bmp.bd	31.22 KB	d29e0b5027d9997c8ba1166cf435bfa185b5abf0304c609a248f4e5dda3bb53	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\PH01247U.BMP.BD	31.01 KB	ecd5922d0c609fa66052f310a98290857abcb7778d11f5c82ed83daf82e7e6c	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0341554.jpg.bd	27.82 KB	d8e5931279fc689b6bf73a382f81156461d8243afd7aa6b5dbac70a15d8cd3e5	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0382957.JPG.BD	106.48 KB	f0c07f14f0f1ebd329b9ad0b79c461f887a7fd12b774124e0b2e29bdb7d5a339	✘

File Name	File Size	SHA256	YARA Match
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\PH02053J.JPG.BD	26.75 KB	6da71c0221156c23a7112d94d492d9ef9a38147d702231fa804f1a8f769a8362	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0101859.bmp.bd	31.22 KB	643b239254c47e7a243cdad14c4df0c49953533430ff09184c4abd39da2c3352	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\PH01931J.JPG.BD	38.69 KB	0f6c4d348715baee5f938ba8297101a934b38c2057df48e218de318a091f3a2d	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02748u.bmp.bd	31.64 KB	3d3ce3db5a2cc08dbd70cb37296c1f1f96b032569cbaf4393c1599516eb413c8	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0341654.JPG.BD	15.37 KB	6b221f677c7b7bcf3a1f0f015b0821eff763bf893e888d1cd25c0441a2088cf	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0309585.jpg.bd	38.64 KB	010725cb3500f81227e2ccfb00a81c69e297bf3277ca63cb33a5a4692166b1d3	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0382927.JPG.BD	126.11 KB	d58d39017d19921c45adc0ad4533f1cb9ba656b0e9e54f0c17c94eed174d7ea8	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382939.jpg.bd	106.91 KB	55d576590b9ee70c4c5ce38440a06e8b6e2f8adfaa677d6782a6dcb2d601ef4	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382947.jpg.bd	84.78 KB	ae5b94a583c7b0aa11ebc27e31175deb59a65f3718f547bdc98aefba1053fe	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02069j.jpg.bd	28.65 KB	3a62c95bc24fe2a64d8d07ad96c7b16ce71c0b32d8f90af545564c05a74f6	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382948.jpg.bd	107.30 KB	968486e2a03fd8c7400516fd6a771b2fb6c40b338fb9d0142ae94690f8debfd	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0387337.JPG.BD	50.76 KB	6d0ff83ec1519599e5a57b89a9a403d32e2abf5a379ad72adaf5a78ddfc815f9	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02503u.bmp.bd	31.22 KB	ff09f2ea2266297b9eee98aa09f1a570d481c97728809f60bc6039235be9f030	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0101856.bmp.bd	76.99 KB	204d56a167167441758d5e74b108cd5acb51a7543c88ced1a7790320a726d103	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0178639.JPG.BD	31.29 KB	b91b0273613528afc5970073539284e0d30518d308c851ff4d1de6d7d0995dcc	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0145707.jpg.bd	35.96 KB	04cf8bd1245875b85cfc84c2997488de688a0249859dc34f490d601602bab8e4	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0174952.jpg.bd	24.40 KB	b4f39dd37a559ddecacac8798b2ffe617bf0edb16f51c1895b7a115195cf46f	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0384885.JPG.BD	94.87 KB	20dbc89832400adadf88d0688577aac6d554f6a1e3bf9b27e1e164456f2942a7	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02749g.gif.bd	33.90 KB	2b60dd0e7d017a387af2e507271455ccf30c8964d6cca26fa2c7a191c3db490c	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0101864.BMP.BD	31.22 KB	48f612c9bfabc43d290cad0d058f3e812db39c2a94b72637b232a88d90f9127a	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0386485.JPG.BD	14.35 KB	d6fcaae58d172bb630f09ef2582a37bb489e81d00ba67f96a024ab6f9ea5b81	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0175428.jpg.bd	14.21 KB	95cab71d98d1fe43fa6a3a28673de47c2e4fdb4141c9139a741de835a3cc319e	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph01235u.bmp.bd	31.43 KB	d348089d4c14b00b67b898111bcb70f6a271f687d592746997e01778e7e78eea	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\PH01332U.BMP.BD	31.43 KB	2d86c6055ad17e912fed0709ecb695946cb72ae5df2080a7ca990b28d9dd569	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0382967.JPG.BD	91.26 KB	d270912e8555ccc9908e19cab1d928405cecdff7e844d7c94d9203ca048c67a5	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0313965.jpg.bd	41.84 KB	45acbf0ee6644e7237b1a42c785ba1e4a274ad8e554cf886455b3d8879957e5f	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0178632.jpg.bd	22.79 KB	346a857d566fbd9c3334fad15e84ad89d14f6f8dd61eeca9cc0c40b25f103d7a	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0289430.JPG.BD	11.28 KB	1fa5960e1f26d3a13276384a823fcb613a99f420a749cfb39a3ac1b401d01342	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02740g.gif.bd	23.79 KB	f3f53d29be22f286f3e4e134ba644b57e28e9414e1babf2175bdb78a4d582141	✘

File Name	File Size	SHA256	YARA Match
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0309567.JPG.BD	21.07 KB	b2ded3778f8ca9abd499abaa1623420670283d6c8dde98b1b84e992f6c0bb2e1	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0101857.BMP.BD	31.43 KB	9db693aabfd82919a5f025e59b87667eb6c08a8b715b6de2725a1abc2db516ec	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0341499.jpg.bd	15.72 KB	fa57419659a61ee09c71b5f1a91668693d7250d0b629d91cc8ac74b82956bd87	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0309480.jpg.bd	10.44 KB	7de1d7b0ccec6b38554cc754a77a9e552fa273ced361b159b3bc3144f97a097	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0341557.jpg.bd	26.66 KB	736440bcb14fdbefb24959d861372e33bec49b8ca5e9b62fb650e1cadb16d8f	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph01562u.bmp.bd	31.43 KB	7a26d8d762cf1ff0898339304192448cbcb97871f2fd6d91c94a718701b5d9e9f	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02208u.bmp.bd	31.22 KB	8ff93c11df41b9b5783d96a3a88917dd0557600c87aa842b73dd0343f09a8462	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0099202.GIF	4.85 KB	a186570391ecb714a96da60c963bc3a6ed9cda0ca41f6c8bc3e9b4e29038ff4	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0386120.JPG.BD	30.12 KB	d840e6043627619203f5b84ec19534ca08441324e0d388b52065f3f4cf790bb2	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0145361.jpg.bd	20.63 KB	4ab0ff68b8e96d979fc9b833f259b94727941cc71318aa791e9355e4e099daa	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0182689.jpg.bd	16.23 KB	a7e9557796e8af6c61705a6d60c648230a90fd46de706e83bcaa4ef3b065c5dd	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0341344.jpg.bd	11.22 KB	bc8fa978ca6086352cfceee01acedf8884417c421422620e89b2812dd8d623b	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0341551.jpg.bd	22.58 KB	9c1fd153b21b0c7e7b62477e6137eab4fb18394840967d331322f46c8025144c	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\PH01046J.JPG.BD	132.43 KB	beee30d8f178816adea743e2761df7117c96ca51d84740263c8b725cb8071ce8	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382836.jpg.bd	66.96 KB	26d258c069bbef88772ea78652d8ba3a6eb26fb3b62ae1ccfe0719f36a2a4fa0	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382931.jpg.bd	119.82 KB	ce4b9fad7faa7ef08b69e7dce8b2903057954093b62622a4c49238014ca82eee	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0145810.jpg.bd	35.93 KB	8bb3cff4df2e47fcea762a833c841ee79f4afdad27c653de9c66fc26036c73e	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0384862.JPG.BD	100.23 KB	15be426fb1097c63f576b073d01911eafe30c75085f751860c5d0a895df3eb8	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0387591.jpg.bd	38.19 KB	d4e33ae2c70aab032c0d13b12a3f4a6c1af6046c7379caa648948948cb83a8e	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0313970.JPG.BD	32.42 KB	af724398182a8eff32aa2b7c7a6a1a546d142450dc6fe62f004cd3d18e37867a	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0145879.jpg.bd	34.59 KB	665c2831a7900dd35e66d38dd657e43e1786617d83d16de91acdf50be441175a	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0227419.JPG.BD	34.71 KB	7ccab717397c03a0be980ad4f5930d583c9ed4dd230c1943aa9be9f96a14795e	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0146142.JPG.BD	45.42 KB	31229ce3cd399835cd62bcd7716a4aab6de633494dca2b6f9819f8fde6528151	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0101865.bmp.bd	31.43 KB	85af74944f187bf02762130d1fb1653a9171fb328928e0175f6f3177d99d6658	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\PH01035U.BMP.BD	31.64 KB	ac5c263fc1f824665327085ded07422941f52b7d191adda6bdc31b78228e1a37	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382938.jpg.bd	97.21 KB	1eadb35b2d359ae8859f552730b5a0631ecd18e0936f9699333fa15a1af65b9a	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\PH02754U.BMP.BD	105.96 KB	8c109b443e983b577c62601c4dd5076f75b483d5b53968578ed35b5fb104c86f	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60C\OR\J0315580.JPG.BD	18.75 KB	756c5972a9c1959508ed4c2e07b1dfcaac276960ed1db0ebe75e7bb15e6575f	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0384888.jpg.bd	80.05 KB	4b5898a430875e8e4f875802f9016ae352db49c204d49ba03b544df5e5b12b48	✘

File Name	File Size	SHA256	YARA Match
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02750U.BMP.BD	91.81 KB	ba33f58c225730938647bb4fb33327bf6eab583ae2cfe97b4e4078af59d841b	✘
C:\Users\R\h\J\OCN\Fevz\X\Desktop\319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe	12.50 KB	319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382954.JPG.BD	86.62 KB	1e21045b8d967cbae5abee11612f67b5ee81c047c3498a71c348f709d877d9e0	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH00780U.BMP.BD	33.54 KB	39f912c86b076eeca3f0708c1cbade346ba05b68793958937e8b74ab01688304	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0287645.JPG.BD	35.38 KB	4fcb0410b111f62afde3b53d39a7b274773d66088fcb2d63aa1e7bf1d4427da	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0341448.jpg.bd	20.69 KB	282f1540055c0eb94a82251a1fd4965bc41c4bad18b8167e79cca499e941046b	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0384900.JPG.BD	69.88 KB	ba53181b840932141h29cf9755d6b67ac884400613bac61da25d7c74528eb750	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02753U.BMP.BD	105.68 KB	db069493ee1661722f6c9560f707c296f31b0f40e998126aced3f93e38c00997	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0148757.jpg.bd	65.96 KB	fea60baeef907e53821f73fe50d7a5148040cd1043c26d71b716f941722e2355	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382950.JPG.BD	94.21 KB	343b02f7f5f5e0043772f681a554757af480263a9106cb4af1a445f659b6814	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0177257.JPG.BD	44.29 KB	6978881548d968d7626e970520c26b689f16f93e016364522ab4ae9c11901772	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0341634.JPG.BD	7.62 KB	b1567d156c03f3e908b64644f30929042418929cad20cd3a3247a26f5d2b4d29	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\j0341653.jpg.bd	15.49 KB	38a1f742cd25605a7b2e6067c2abe01b2f638ecb38083de93c0f0ece4f26501f	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0178932.JPG.BD	34.51 KB	fb1d59149866b8430257e44888c334cb491d524a35e0dd4b68ec00d02c920e8b	✘
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0315612.JPG.BD	16.56 KB	1cfb828a6d179d966408a0ea88b5759f1020721987a9b92a1df881f5002c9d20	✘
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02742g.gif.bd	20.16 KB	82066fc3949119abcbe1b55c01ef6b83d98c65c672e34a341bc4f09da1c9f99e	✘

Reduced dataset
Host Behavior

Type	Count
Module	1
System	1
File	6119
Registry	10

ARTIFACTS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5	C:\Users\RDHJ0CNFevz\X\Desktop\319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe, C:\Users\RDHJ0C~1\AppData\Local\Temp\WU17sDZVZ12PQJL.exe	Sample File	12.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
5f2a47685fee50e41372b38924f12535a37ff3b60b15f89e604b9d3ff803fc5c	c:\program files (x86)\microsoft office\clipart\pub60cor\ph01478u.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\PH01478U.BMP.BD	Dropped File	31.22 KB	image/bmp	Access, Create, Write	CLEAN
0479e7d2e8e326200ff8e70086cc0b3e329f5a4716717ae22a63d664814149cd	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0145895.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0145895.jpg.bd	Dropped File	33.16 KB	image/jpeg	Access, Create, Write	CLEAN
6b9d24cc7129a8b088e43b1bb6b0fc1b1ff0ae5e25628b041815070db00b6da2	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\PH01213K.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\ph01213k.jpg.bd	Dropped File	6.19 KB	image/jpeg	Access, Create, Write	CLEAN
42d798e2677988af98530c661a29a014b703c6f326cce3006a6ea924767dfc5b	c:\program files (x86)\microsoft office\clipart\pub60cor\ph01236u.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\PH01236U.BMP.BD	Dropped File	31.22 KB	image/bmp	Access, Create, Write	CLEAN
f5954e493262eef2b792f6a31e823678d94e20f13213479e8b60de2430c9e80	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0337280.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0337280.jpg.bd	Dropped File	12.59 KB	image/jpeg	Access, Create, Write	CLEAN
bf110175f8f3d6240cd32c76f86c382adc7f76aca30144c0a6a1c89a3f0eb8627	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0386270.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0386270.jpg.bd	Dropped File	14.82 KB	image/jpeg	Access, Create, Write	CLEAN
db6f4dd9cf9521c810f9ca2238c382adc7f76aca30144c0ac18727d8dc3675f	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\PH02752G.GIF.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\ph02752g.gif.bd	Dropped File	48.88 KB	image/gif	Access, Create, Write	CLEAN
696554e30e114b5e38f9a518fd6317a34294574d877fb2eb21ec2c8b40fd0f8d	c:\program files (x86)\microsoft office\clipart\pub60cor\ph02748g.gif.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\PH02748G.GIF.BD	Dropped File	24.14 KB	image/gif	Access, Create, Write	CLEAN
a9f7371977565961d72619b6d468773749cce885bbc534b1f461d2508205e67f	c:\program files (x86)\microsoft office\clipart\pub60cor\j0382968.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0382968.JPG.BD	Dropped File	109.84 KB	image/jpeg	Access, Create, Write	CLEAN
c8ca73f10da0b05cefb9a4f4df2a02f8ad1e564031f402778c3051af6fa7cea	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\PH02752U.BMP.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\ph02752u.bmp.bd	Dropped File	31.01 KB	image/bmp	Access, Create, Write	CLEAN
4052f069d4fea46661e33e60ecc4c006e9e994a5a7e12a4d99d24b6d22610a4a	c:\program files (x86)\microsoft office\clipart\pub60cor\j0400002.png.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0400002.PNG.BD	Dropped File	87.32 KB	image/png	Access, Create, Write	CLEAN
48fad5e15f10ecc069e6634a1f9538b6269039b538802e20a7b872ac1d1ba39	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0387895.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0387895.jpg.bd	Dropped File	31.49 KB	image/jpeg	Access, Create, Write	CLEAN
6d7933c82f0d6fcdc8bec001ce1a9722a1e9b65caa906ee7a8c53c2122794b32	c:\program files (x86)\microsoft office\clipart\pub60cor\j0382926.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0382926.JPG.BD	Dropped File	89.79 KB	image/jpeg	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
30bbaa1301de4ed5653e277f b0e65f82389cca20499eda1 e4b9803a122053e3	c:\program files (x86)\microsoft office\clipart\pub60cor\j0202045.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J020204 5.JPG.BD	Dropped File	41.26 KB	image/jpeg	Access, Create, Write	CLEAN
15039064ee52ad19d299907 9f493fc9388bd34dc6823b91 9333598318037ffa1	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH0060 1G.GIF.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\ph00601g.gif.bd	Dropped File	1.54 KB	image/gif	Access, Create, Write	CLEAN
b48ee82c746992da7b2086bf e1455ec5e3defdbd1692aed7 582c9c73c7e3d7c2	c:\program files (x86)\microsoft office\clipart\pub60cor\ph02746g.gif.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH0274 6G.GIF.BD	Dropped File	23.62 KB	image/gif	Access, Create, Write	CLEAN
3527855c7c3399562719702 5677552b9bee1b4b6cb8dc7 7bc44a38f1bbcd2a54	c:\program files (x86)\microsoft office\clipart\pub60cor\j0178523.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J017852 3.JPG.BD	Dropped File	23.47 KB	image/jpeg	Access, Create, Write	CLEAN
1c9d25201a0e1d1ea772e05 e0847a2d7daf275202853e65 590c32b6e515cf2af	c:\program files (x86)\microsoft office\clipart\pub60cor\ph02291u.bmp. bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH0229 1U.BMP.BD	Dropped File	31.43 KB	image/bmp	Access, Create, Write	CLEAN
ae6180a9d8265703f634075 19be638995925242dee90ce 0b93123e9ac9c470b	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH0273 6G.GIF.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\ph02736g.gif.bd	Dropped File	24.90 KB	image/gif	Access, Create, Write	CLEAN
0206209ccc67bfcc77ff82a1c 9f287e0fc4d729f106f07241fa 73d10d0b00f7e	c:\program files (x86)\microsoft office\clipart\pub60cor\ph02743g.gif.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH0274 3G.GIF.BD	Dropped File	27.38 KB	image/gif	Access, Create, Write	CLEAN
1e953cbcb613da3295d4120 296b15107fe4c7c7de71315b fdeef93e90bc06838	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J034132 8.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0341328.jpg.bd	Dropped File	9.96 KB	image/jpeg	Access, Create, Write	CLEAN
19052abcdbfec95f08357968 69cddb820429f7ab3a24baa1 81ef008c11e98cfe	c:\program files (x86)\microsoft office\clipart\pub60cor\j0101863.bmp.b d, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J010186 3.BMP.BD	Dropped File	31.43 KB	image/bmp	Access, Create, Write	CLEAN
8c40b2a904958fd0460276b2 45aec330c1c9e7e43cf0863e 91dbc3cd1cfe865f	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J040000 5.PNG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0400005.png.bd	Dropped File	93.81 KB	image/png	Access, Create, Write	CLEAN
f53535f720e495dc1be43d05 bd510d973c9e9d3bcf7bb717 1a81d7301a673e03	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH0239 8U.BMP.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\ph02398u.bmp. bd	Dropped File	31.22 KB	image/bmp	Access, Create, Write	CLEAN
709c72d51452223fda5077da 1e7f62e36536fa4753fc57e4c ac94ba7d3dbef7	c:\program files\common files\8fkeqdlnoz.gif.bd, C:\Program Files\Common Files\8FKeQdlnOZ.gif.BD	Dropped File	70.07 KB	image/gif	Access, Create, Write	CLEAN
59f55c71160fba6a5fc054f3 18e77a70ae43fbf99bba3904 2b65c0297a29e05	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J014901 8.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0149018.jpg.bd	Dropped File	26.75 KB	image/jpeg	Access, Create, Write	CLEAN
0af5c0758110fd00e0c46a46f 161a3072a87a22ca4473fd7 2966d879a757320	c:\program files (x86)\microsoft office\clipart\pub60cor\j0341559.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J034155 9.JPG.BD	Dropped File	26.11 KB	image/jpeg	Access, Create, Write	CLEAN
815a2c5608013127c6db28d 30f71d590b6db45c53fd4ad1f 6eb9f3af6574d90f	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J028764 4.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0287644.jpg.bd	Dropped File	16.94 KB	image/jpeg	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
812fc2ab0cdbc3a720a4c77a3a33369a1b9849ac24dd4e0beb56cf0374e75aa	C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\PH02412K.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\ph02412k.jpg.bd	Dropped File	3.46 KB	image/jpeg	Access, Create, Write	CLEAN
6085778e35731d39f388e680175e684a9da611fd1f6964fe5263dfe6fb20b6b	c:\program files (x86)\microsoft\office\clipart\pub60cor\0145669.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\J0145669.JPG.BD	Dropped File	31.10 KB	image/jpeg	Access, Create, Write	CLEAN
5f415419e44cdd3f3d42b1b89e9308904235e4f6af1798f4fb6a0aba2c2dc660	C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\PH02062U.BMP.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\ph02062u.bmp.bd	Dropped File	31.22 KB	image/bmp	Access, Create, Write	CLEAN
0819e1d708fb5bdb03567e62f51a76ab5657bbfd9471d353a3b39c693569c68d	c:\program files (x86)\microsoft\office\clipart\pub60cor\0227558.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\J0227558.JPG.BD	Dropped File	56.73 KB	image/jpeg	Access, Create, Write	CLEAN
22a0438703d4fa0031000ccb54683cfcf5ba40ea2b4083d10f4be529d077d1ed	C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\J0341742.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0341742.jpg.bd	Dropped File	18.43 KB	image/jpeg	Access, Create, Write	CLEAN
5ccfbc06d4ec202e9aac86dc6bb45167ea9ceb288b5beffc59482a876dfb1962	c:\program files (x86)\microsoft\office\clipart\pub60cor\ph02466u.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\PH02466U.BMP.BD	Dropped File	31.01 KB	image/bmp	Access, Create, Write	CLEAN
6a893ad4ac4e056f6dd3326ef71e8dee4538360f15859c908afd58eeb6d767	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0321179.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\J0321179.JPG.BD	Dropped File	9.21 KB	image/jpeg	Access, Create, Write	CLEAN
b3e3c3abbe02278eaad798f5151c8cf0a6b1e0a8a3ddeed00b1d4e5956d05995	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0145168.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\J0145168.JPG.BD	Dropped File	32.87 KB	image/jpeg	Access, Create, Write	CLEAN
830b68e30ffe6fdaae050094ddb68616c854aad99523e84e775ed9e5f76b0d74	C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\PH02417U.BMP.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\ph02417u.bmp.bd	Dropped File	31.22 KB	image/bmp	Access, Create, Write	CLEAN
c5ee08c5ef2f5687e9f913d7d3e291e7586ffe277e93d4742e06913772612a0c	C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\J0382966.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0382966.jpg.bd	Dropped File	98.13 KB	image/jpeg	Access, Create, Write	CLEAN
922d4519a6ce0e3afa0ce66dd92d0ab4c50b36b1b68e16895a0cb17593a8844	C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\J0178348.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0178348.jpg.bd	Dropped File	36.12 KB	image/jpeg	Access, Create, Write	CLEAN
9bbf513c05697bf8a6a23b9015e15247b5c05039eb1f63fe5f54ee3dfec3630	C:\Bootfr-FR\HOW TO DECRYPT FILES.txt, C:\Bootfr-CA\HOW TO DECRYPT FILES.txt, C:\Bootfr-HR\HOW TO DECRYPT FILES.txt, C:\Program... ..t, C:\MSOCache\All Users\{90160000-00A1-0409-0000-00000FF1CE}-C\HOW TO DECRYPT FILES.txt, C:\Booten-GB\HOW TO DECRYPT FILES.txt	Dropped File	623 bytes	text/plain	Access, Create, Write	CLEAN
4def1365f5dfc1ca77ea145214e1f780de013017cdee85fd4ac0fcd8cb6a57	c:\program files (x86)\microsoft\office\clipart\pub60cor\ph01265u.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\PH01265U.BMP.BD	Dropped File	31.01 KB	image/bmp	Access, Create, Write	CLEAN
4ae1622a4d1fba63f958f0cd0c07ed38d481155db0be1d7199e7d7a2cd5d0349	C:\Program Files (x86)\Microsoft Office\CLIPART\PI\PUB60COR\J0101866.BMP.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0101866.bmp.bd	Dropped File	31.43 KB	image/bmp	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ed91ceed70fd12847dbaf2cd73766bb515103cc901523bf94d50858d10f047db	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02071U.BMP.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\ph02071u.bmp.bd	Dropped File	31.43 KB	image/bmp	Access, Create, Write	CLEAN
4a627f6105550dc50656b2e533261494195c19e68fe7a2f0c739641ccf491118	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0313974.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0313974.jpg.bd	Dropped File	46.45 KB	image/jpeg	Access, Create, Write	CLEAN
7552bdbd54056a101f7896e95edb468da7d3a08ad29f5a8afb72accb68a75d27	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0309598.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0309598.jpg.bd	Dropped File	32.48 KB	image/jpeg	Access, Create, Write	CLEAN
1c829f5e5a9608ad8443738d3c199c37c31deef2e2936805eed1c72e21273a23	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0382965.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382965.JPG.BD	Dropped File	110.75 KB	image/jpeg	Access, Create, Write	CLEAN
79cb9edb581e5abf5bc5da6b805ebc02dab537d76015490b82d955695c38149f	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0309664.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0309664.JPG.BD	Dropped File	42.68 KB	image/jpeg	Access, Create, Write	CLEAN
c49290fe990d038f7d58234e3ff7d05704a4c14d7bda1f15a662c39c879956a3	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0179963.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0179963.jpg.bd	Dropped File	31.36 KB	image/jpeg	Access, Create, Write	CLEAN
ee1c150ea5902bc9cd8e081681fa71a017d1dd7e52c861e976dc4f7bdacc2a0b	c:\program files (x86)\microsoft\office\clipart\pub60cor\ph02742u.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02742U.BMP.BD	Dropped File	31.22 KB	image/bmp	Access, Create, Write	CLEAN
3d794813ca0fe0bfff84efc2d54d4338c27f783b530b30147d9ba90808391a9d1	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0341447.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0341447.JPG.BD	Dropped File	18.71 KB	image/jpeg	Access, Create, Write	CLEAN
1c114630ee0bb4db4cac2470861ee99aaef04e8ccfd65974b3db865429dc53a5	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0400001.PNG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0400001.png.bd	Dropped File	198.13 KB	image/png	Access, Create, Write	CLEAN
9658ae0349d3c51290eaa0c9e975fc49dc59649c467b80f65d101ee6107684e0	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0287641.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0287641.JPG.BD	Dropped File	34.41 KB	image/jpeg	Access, Create, Write	CLEAN
d41f309ca7118a5779973e7944822f2579fd863da72d61212054fa0389a91ed	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0382961.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382961.JPG.BD	Dropped File	98.69 KB	image/jpeg	Access, Create, Write	CLEAN
73a51b30a1cbe720bdaff16ac9a88f734fab49b1c3bd214e880d6c95a9470af	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0382959.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382959.JPG.BD	Dropped File	83.88 KB	image/jpeg	Access, Create, Write	CLEAN
3d8b20be89715387470fbaf14e3dc874650c2f46c03b361c6357bf9914fbc7e0	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0099203.gif.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0099203.GIF.BD	Dropped File	3.81 KB	image/gif	Access, Create, Write	CLEAN
e5b24860b3771800b61d738f2e827e117046ff7e4333a42a2c469480c22631ab	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02223U.BMP.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\ph02223u.bmp.bd	Dropped File	31.43 KB	image/bmp	Access, Create, Write	CLEAN
343d4e09737e876e5573f502b5b6e0f657940d8b6e136eccb713737051f34a	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0178459.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0178459.JPG.BD	Dropped File	28.52 KB	image/jpeg	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ceada46bd8d081348e23ea b99c2d5d0a3d1535d32c3b3 0fc58cf79a30e5e326	c:\program files (x86)\microsoft office\clipart\pub60cor\0149118.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\014911 8.JPG.BD	Dropped File	63.28 KB	image/jpeg	Access, Create, Write	CLEAN
2b0c4edd7ae3a2931c053f1d 0f7a786eb23bd3aa83c67994 1eb4fc17f5bd6d681	c:\program files (x86)\microsoft office\clipart\pub60cor\0177806.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\017780 6.JPG.BD	Dropped File	54.25 KB	image/jpeg	Access, Create, Write	CLEAN
8e0323e488cb4af98c754798 020e853e6598085f30dec98a9 c63515155b97741b	c:\program files (x86)\microsoft office\clipart\pub60cor\0382958.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\038295 8.JPG.BD	Dropped File	100.98 KB	image/jpeg	Access, Create, Write	CLEAN
b4a7cc23c97737e9f9be898f9 2d0e99d1b7e423b8808ba51 2c94b151411fbb2e8	c:\program files (x86)\microsoft office\clipart\pub60cor\0148309.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\014830 9.JPG.BD	Dropped File	42.65 KB	image/jpeg	Access, Create, Write	CLEAN
519077ab912cd948a7598e5 929a65978e1e21cad50b7d0 b51d3932cb4e905b5	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\038760 4.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0387604.jpg.bd	Dropped File	46.44 KB	image/jpeg	Access, Create, Write	CLEAN
8441f5c9e35dc8f4d96855e0 2c992ced1542b8c1ac3114b 1e86d530940b945dd	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\034156 1.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0341561.jpg.bd	Dropped File	41.15 KB	image/jpeg	Access, Create, Write	CLEAN
fa9963f021800f44afc8547d3 98cfa1c5e93161af9b973d5a 26138a41eaba9b	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\034153 4.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0341534.jpg.bd	Dropped File	7.88 KB	image/jpeg	Access, Create, Write	CLEAN
edde04d3ac4c92beb2779d6 b0747b63246e7c418d5e822 26cb7ec937759c3b1b	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\038489 5.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0384895.jpg.bd	Dropped File	54.24 KB	image/jpeg	Access, Create, Write	CLEAN
44815354c66bbe79ce5453b 56408bf50c49e49c26d09021 fed88d56fafdda797	c:\program files (x86)\microsoft office\clipart\pub60cor\0144773.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\014477 3.JPG.BD	Dropped File	39.29 KB	image/jpeg	Access, Create, Write	CLEAN
3fe706f50068b6f6b6fdaf3a2b eaf4e4876cca815ab8241a58 c84a2ecd7092d9	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\017846 0.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0178460.jpg.bd	Dropped File	25.91 KB	image/jpeg	Access, Create, Write	CLEAN
3a696ad8106632ead89e6d4 98b947d9284f42477b115c8c 859936a9a8dfa3ff5	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\034145 5.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0341455.jpg.bd	Dropped File	29.08 KB	image/jpeg	Access, Create, Write	CLEAN
d068b0744041c6c3207c508 7b5f0aeea9874dfd548ef9b85 2a8522eca2b0e413	c:\program files\common files\swouid\2wk.gif.bd, C:\Program Files\Common Files\swouid\2wk.gif.BD	Dropped File	64.84 KB	image/gif	Access, Create, Write	CLEAN
4dec080aba90d9dfa95a30a4 628bdd849acf66466d7cdd7f a8e7e7c07726ed0b	c:\program files (x86)\microsoft office\clipart\pub60cor\0382944.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\038294 4.JPG.BD	Dropped File	79.53 KB	image/jpeg	Access, Create, Write	CLEAN
64449128550c1c65731e6d2 a01c1b92b8409c06b3fce8b 3124bf9f443edecdc	c:\program files (x86)\microsoft office\clipart\pub60cor\ph02746u.bmp. bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH0274 6U.BMP.BD	Dropped File	31.38 KB	image/bmp	Access, Create, Write	CLEAN
ab799123ba1bcd6481029c7 62614e13de145a4c402ea09 eb477fd09c71558e3b	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\014879 8.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0148798.jpg.bd	Dropped File	37.34 KB	image/jpeg	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d29e0b5027d9997c8ba1166cf435bfa185b5abf0304c609a248f4e5dda3bbb53	c:\program files (x86)\microsoft office\clipart\pub60cor\ph02039u.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02039U.BMP.BD	Dropped File	31.22 KB	image/bmp	Access, Create, Write	CLEAN
ecd5922d0c0609fa66052f310a98290857abc7778d11f5c82ed83daf82e7e6c	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH01247U.BMP.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\ph01247u.bmp.bd	Dropped File	31.01 KB	image/bmp	Access, Create, Write	CLEAN
d8e5931279fc689b6b73a382f81156461d8243afd7aa6b5dbac70a15d8cd3e5	c:\program files (x86)\microsoft office\clipart\pub60cor\j0341554.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0341554.JPG.BD	Dropped File	27.82 KB	image/jpeg	Access, Create, Write	CLEAN
f0c07f14f0f1ebd329b9ad0b79c461f887a7fd12b774124e0b2e29bdb7d5a339	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382957.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0382957.jpg.bd	Dropped File	106.48 KB	image/jpeg	Access, Create, Write	CLEAN
6da71c0221156c23a7112d94d492d9efa938147d702231fa804f1a8f769a8362	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02053J.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\ph02053j.jpg.bd	Dropped File	26.75 KB	image/jpeg	Access, Create, Write	CLEAN
643b239254c47e7a243cdad14c4df0c49953533430f09184c4abd39da2c3352	c:\program files (x86)\microsoft office\clipart\pub60cor\j0101859.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0101859.BMP.BD	Dropped File	31.22 KB	image/bmp	Access, Create, Write	CLEAN
0f6c4d348715baee5f938ba8297101a934b38c2057df48e218de318a091f3a2d	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH01931J.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\ph01931j.jpg.bd	Dropped File	38.69 KB	image/jpeg	Access, Create, Write	CLEAN
3d3ce3db5a2cc08dbd70cb37296c1f1f96b032569cbaf4393c1599516eb413c8	c:\program files (x86)\microsoft office\clipart\pub60cor\ph02748u.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02748U.BMP.BD	Dropped File	31.64 KB	image/bmp	Access, Create, Write	CLEAN
6b221f677c7b7bcf3a1f0f015b0821eff763bf893e888d1cd25cf0441a2088cf	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0341654.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0341654.jpg.bd	Dropped File	15.37 KB	image/jpeg	Access, Create, Write	CLEAN
010725cb3500f81227e2ccfb00a81c69e297bf3277ca63cb33a5a4692166b1d3	c:\program files (x86)\microsoft office\clipart\pub60cor\j0309585.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0309585.JPG.BD	Dropped File	38.64 KB	image/jpeg	Access, Create, Write	CLEAN
d58d39017d19921c45adc0ad4533f1cb9ba656b0e8e54f0c17c94eed174d7ea8	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382927.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0382927.jpg.bd	Dropped File	126.11 KB	image/jpeg	Access, Create, Write	CLEAN
55d576590b9ee70c4c5ce38440a06e8b6e2f8adfaa677d6782a6dcba2d601ef4	c:\program files (x86)\microsoft office\clipart\pub60cor\j0382939.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382939.JPG.BD	Dropped File	106.91 KB	image/jpeg	Access, Create, Write	CLEAN
ae5b94a583c7b0aa11ebc27e31175deb59a65f53718f547bdc98aefba1053fe	c:\program files (x86)\microsoft office\clipart\pub60cor\j0382947.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382947.JPG.BD	Dropped File	84.78 KB	image/jpeg	Access, Create, Write	CLEAN
3a62c95bc24fe7e2a64d8d07ad96c7b16ce71c0b32d8f90af5455646c05a74f6	c:\program files (x86)\microsoft office\clipart\pub60cor\ph02069j.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02069J.JPG.BD	Dropped File	28.65 KB	image/jpeg	Access, Create, Write	CLEAN
968486e2a03fd8c7400516fd6a77f1b2fb6c40b338fb9d0142ae94690f8debfd	c:\program files (x86)\microsoft office\clipart\pub60cor\j0382948.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382948.JPG.BD	Dropped File	107.30 KB	image/jpeg	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6d0ff83ec1519599e5a57b89a9a403d32e2abf5a379ad72adaf5a78d5c815f9	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0387337.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0387337.jpg.bd	Dropped File	50.76 KB	image/jpeg	Access, Create, Write	CLEAN
ff09f2ea2266297b9eee98aa09f1a570d481c97728809f60bc6039235be9f030	c:\program files (x86)\microsoft\office\clipart\pub60cor\ph02503u.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\PH02503U.BMP.BD	Dropped File	31.22 KB	image/bmp	Access, Create, Write	CLEAN
204d56a167167441758d5e74b108cd5ac51a7543c88ced1a7790320a726d103	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0101856.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0101856.BMP.BD	Dropped File	76.99 KB	image/bmp	Access, Create, Write	CLEAN
b91b0273613528afc5970073539284e0d30518d308c851ff4d1de6d7d0995dccc	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0178639.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0178639.jpg.bd	Dropped File	31.29 KB	image/jpeg	Access, Create, Write	CLEAN
04cf8bd1245875b85cfc84c2997488de688a0249859dc34f490d601602bab8e4	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0145707.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0145707.JPG.BD	Dropped File	35.96 KB	image/jpeg	Access, Create, Write	CLEAN
b4f39dd37a559ddecac8798b2ffe617bf0edb16fb51c1895b7a115195cf46f	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0174952.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0174952.JPG.BD	Dropped File	24.40 KB	image/jpeg	Access, Create, Write	CLEAN
20dbc89832400adadff88d0688577aac6d554f6a1e3bf9b27e1e164456f2942a7	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0384885.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0384885.jpg.bd	Dropped File	94.87 KB	image/jpeg	Access, Create, Write	CLEAN
2b60dd0e7d017a387af2e507271455ccf30c8964d6cca26fa2c7a191c3db490c	c:\program files (x86)\microsoft\office\clipart\pub60cor\ph02749g.gif.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\PH02749G.GIF.BD	Dropped File	33.90 KB	image/gif	Access, Create, Write	CLEAN
48f612c9bfabc43d290cad0d058f3e812db39c2a94b72637b232a88d90f9127a	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0101864.BMP.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0101864.bmp.bd	Dropped File	31.22 KB	image/bmp	Access, Create, Write	CLEAN
d6fcaae5f58d172bb630f09ef2582a37fb489e81d00ba67f96a024ab6f9ea5b81	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0386485.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0386485.jpg.bd	Dropped File	14.35 KB	image/jpeg	Access, Create, Write	CLEAN
95cab71d98d1fe43fa6a3a28673de47c2eafdb4141c9139a741de835a3cc319e	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0175428.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0175428.JPG.BD	Dropped File	14.21 KB	image/jpeg	Access, Create, Write	CLEAN
d348089d4c14b00b67b898111bcb70f6a271f687d592746997e01778e7e78eea	c:\program files (x86)\microsoft\office\clipart\pub60cor\ph01235u.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\PH01235U.BMP.BD	Dropped File	31.43 KB	image/bmp	Access, Create, Write	CLEAN
2d86c6055ad17e912fed0709ecb695946cb72ae5df2080a7ca990b28d9ddf569	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\PH01332U.BMP.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\ph01332u.bmp.bd	Dropped File	31.43 KB	image/bmp	Access, Create, Write	CLEAN
d270912e855ccc9908e19cab1d928405cecdf7e844d7c94d9203ca048c67a5	C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0382967.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0382967.jpg.bd	Dropped File	91.26 KB	image/jpeg	Access, Create, Write	CLEAN
45acb0ee6644e7237b1a42c785ba1e4a274ad8e554cf886455b3d8879957e5f	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0313965.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0313965.JPG.BD	Dropped File	41.84 KB	image/jpeg	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
346a857d566fbd9c3334fad15e84ad89d14f6f8dd61eeca9cc0c40b25f103d7a	c:\program files (x86)\microsoft office\clipart\pub60cor\0178632.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0178632.JPG.BD	Dropped File	22.79 KB	image/jpeg	Access, Create, Write	CLEAN
1fa5960e1f26d3a13276384a823fcb613a99f420a749cfb39a3ac1b401d01342	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0289430.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0289430.jpg.bd	Dropped File	11.28 KB	image/jpeg	Access, Create, Write	CLEAN
f3f53d29be22f286f3e4e134ba644b57e28e9414e1babf2175bdb78a4d582141	c:\program files (x86)\microsoft office\clipart\pub60cor\ph02740g.gif.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02740G.GIF.BD	Dropped File	23.79 KB	image/gif	Access, Create, Write	CLEAN
b2ded3778f8ca9abd499abaa1623420670283d6c8dde98b1b84e992f6c0bb2e1	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0309567.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0309567.jpg.bd	Dropped File	21.07 KB	image/jpeg	Access, Create, Write	CLEAN
9db693aabfd82919a5f025e59b87667eb6c08a8b715b6de2725a1abc2db516ec	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0101857.BMP.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0101857.bmp.bd	Dropped File	31.43 KB	image/bmp	Access, Create, Write	CLEAN
fa57419659a61ee09c71b5f1a91668693d7250d0b629d91cc8ac74b82956bd87	c:\program files (x86)\microsoft office\clipart\pub60cor\0341499.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0341499.JPG.BD	Dropped File	15.72 KB	image/jpeg	Access, Create, Write	CLEAN
7de1d7b0ccecb6b38554cc754a77a9e552fa273ced361b159b3bc3144f97a097	c:\program files (x86)\microsoft office\clipart\pub60cor\0309480.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0309480.JPG.BD	Dropped File	10.44 KB	image/jpeg	Access, Create, Write	CLEAN
736440bcba14dfbefb24959d8611372e33bed49b8ca5e9b62fb650e1cadb16d8f	c:\program files (x86)\microsoft office\clipart\pub60cor\0341557.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0341557.JPG.BD	Dropped File	26.66 KB	image/jpeg	Access, Create, Write	CLEAN
7a26d8d762cf1ff0898339304192448cbcb97871f2d6d91c94a718701b5d9e6f	c:\program files (x86)\microsoft office\clipart\pub60cor\ph01562u.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH01562U.BMP.BD	Dropped File	31.43 KB	image/bmp	Access, Create, Write	CLEAN
8ff93c11df41b9b5783d96a3a88917dd0557600c87aa842b73dd0343f09a8462	c:\program files (x86)\microsoft office\clipart\pub60cor\ph02208u.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH02208U.BMP.BD	Dropped File	31.22 KB	image/bmp	Access, Create, Write	CLEAN
a186570391ecb714a96da60c963bc3a6ed9cda10ca41f6c8bc3e9b4e29038ff4	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0099202.GIF, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0099202.GIF.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0099202.gif.bd	Dropped File	4.85 KB	image/gif	Access, Create, Delete, Write	CLEAN
d840e6043627619203f5b84ec19534ca08441324e0d388b52065f3f4cf790bb2	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0386120.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0386120.jpg.bd	Dropped File	30.12 KB	image/jpeg	Access, Create, Write	CLEAN
654b8fbb3beb01a6f08eb873015b728be6ac596b9d51f6c65dbf728e22441e0e	-	Extracted File	66 bytes	image/bmp	-	CLEAN
4abbff68b8e96d979f9c9b833f259bf947272941cc71318aa791e9355e4e099daa	c:\program files (x86)\microsoft office\clipart\pub60cor\0145361.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0145361.JPG.BD	Dropped File	20.63 KB	image/jpeg	Access, Create, Write	CLEAN
a7e9557796e8af6c61705a6d60c648230a90f046de706e83bcaa4ef3b065c5dd	c:\program files (x86)\microsoft office\clipart\pub60cor\0182689.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0182689.JPG.BD	Dropped File	16.23 KB	image/jpeg	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
bc8fa978ca6086352cfceee01acedf8884417c421422620e8b9b2812d8d623b	c:\program files (x86)\microsoft office\clipart\pub60cor\0341344.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0341344.JPG.BD	Dropped File	11.22 KB	image/jpeg	Access, Create, Write	CLEAN
9c1fd153b21b0c7e7b62477e6137eab4fb18394840967d331322f46c8025144c	c:\program files (x86)\microsoft office\clipart\pub60cor\0341344.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0341344.JPG.BD	Dropped File	22.58 KB	image/jpeg	Access, Create, Write	CLEAN
beee30d8f178816adea743e2761df7117c96ca51d84740263c8b725cb8071ce8	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH01046J.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\ph01046j.jpg.bd	Dropped File	132.43 KB	image/jpeg	Access, Create, Write	CLEAN
26d258c069bbeff88772ea78652d8ba3a6eb26fb3b6262ae1ccfe0719f36a2a4fa0	c:\program files (x86)\microsoft office\clipart\pub60cor\0382836.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0382836.JPG.BD	Dropped File	66.96 KB	image/jpeg	Access, Create, Write	CLEAN
ce4b9fad7faa7ef08b69e7dce8b2903057954093b62622a4c49238014ca82eeee	c:\program files (x86)\microsoft office\clipart\pub60cor\0382931.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0382931.JPG.BD	Dropped File	119.82 KB	image/jpeg	Access, Create, Write	CLEAN
8bb3c4f4df2e47fcea762a833c841ee79f4afdad27c653de9c66fc26036c73e	c:\program files (x86)\microsoft office\clipart\pub60cor\0145810.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0145810.JPG.BD	Dropped File	35.93 KB	image/jpeg	Access, Create, Write	CLEAN
15be426fb10976c63f576b073d01911eafe30c75085f751860c5d0aa95df3eb8	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0384862.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0384862.jpg.bd	Dropped File	100.23 KB	image/jpeg	Access, Create, Write	CLEAN
d4e33ae2c70aab032c0d13b12a3f4a6c1af6046c7379caa6489489948cb83a8e	c:\program files (x86)\microsoft office\clipart\pub60cor\0387591.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0387591.JPG.BD	Dropped File	38.19 KB	image/jpeg	Access, Create, Write	CLEAN
af724398182a8eff32aa2b7c7a6a1a546d142450dc6fe62f004cd3d18e37867a	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0313970.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0313970.jpg.bd	Dropped File	32.42 KB	image/jpeg	Access, Create, Write	CLEAN
665c2831a7900dd35e66d38dd657e43e1786617d83d16de91acd50be441175a	c:\program files (x86)\microsoft office\clipart\pub60cor\0145879.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0145879.JPG.BD	Dropped File	34.59 KB	image/jpeg	Access, Create, Write	CLEAN
7ccab717397c03a0be980ad4f5930d583c9e44dd230cf943aa9be9f96a14795e	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0227419.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0227419.jpg.bd	Dropped File	34.71 KB	image/jpeg	Access, Create, Write	CLEAN
31229ce3cd399835cd62bcd7716a4aab6de633494dca2b6f9819f8fde6528151	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0146142.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\0146142.jpg.bd	Dropped File	45.42 KB	image/jpeg	Access, Create, Write	CLEAN
85af74944f187bf02762130d1fb1653a9171fb328928e0175f6f31779d96658	c:\program files (x86)\microsoft office\clipart\pub60cor\0101865.bmp.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0101865.BMP.BD	Dropped File	31.43 KB	image/bmp	Access, Create, Write	CLEAN
ac5c263fc1f824665327085ded07422941f52b7d191adka6bdc31b78228e1a37	C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH01035U.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\ph01035u.jpg.bd	Dropped File	31.64 KB	image/bmp	Access, Create, Write	CLEAN
1eadb35b2d359ae8859f552730b5a0631ec1d8e0936f9699333fa15a1af65b9a	c:\program files (x86)\microsoft office\clipart\pub60cor\0382938.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\0382938.JPG.BD	Dropped File	97.21 KB	image/jpeg	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8c109b443e983b577c62601c4dd5076f75b483d5b53968578ed35b5fb104c86f	C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\PH02754.U.BMP.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\ph02754u.bmp.bd	Dropped File	105.96 KB	image/bmp	Access, Create, Write	CLEAN
756c5972a9c1959508ed4c2e07b1dfcaac276960ed1db0ebe75e7bb15e657f5f	C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\J0315580.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0315580.jpg.bd	Dropped File	18.75 KB	image/jpeg	Access, Create, Write	CLEAN
4b5898a430875e9e4f875802f9016ae352db49c204d49ba03b544fd5e5b12b48	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0384888.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\J0384888.JPG.BD	Dropped File	80.05 KB	image/jpeg	Access, Create, Write	CLEAN
ba33f58c225730938647bb4fb3327bf6eab583ae2cffe97b4e4078af59d841b	C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\PH02750U.BMP.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\ph02750u.bmp.bd	Dropped File	91.81 KB	image/bmp	Access, Create, Write	CLEAN
1e21045b8d967cbae5abee11612f67b5ee81c047c3498a71c348f709d877d9e0	C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\J0382954.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0382954.jpg.bd	Dropped File	86.62 KB	image/jpeg	Access, Create, Write	CLEAN
39f912c86b076eeca3f0708c1cbade346ba05b68793958937e8b74ab01688304	C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\PH00780U.BMP.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\ph00780u.bmp.bd	Dropped File	33.54 KB	image/bmp	Access, Create, Write	CLEAN
4fcb0410b111f62afde3b53d39a7b274773d66088fcb2d63aa1e7bf1d4427da	C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\J0287645.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0287645.jpg.bd	Dropped File	35.38 KB	image/jpeg	Access, Create, Write	CLEAN
282f1540055c0eb94a82251a1fd4965bc41c4bad18b8167e79cca499e941046b	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0341448.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\J0341448.JPG.BD	Dropped File	20.69 KB	image/jpeg	Access, Create, Write	CLEAN
ba53181b840932141b29cf9755d6b67ac884400613bac61da25d7c74528eb750	C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\J0384900.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0384900.jpg.bd	Dropped File	69.88 KB	image/jpeg	Access, Create, Write	CLEAN
db069493ee1661722f6c9560f707c296f31b0f40e998126aced3f93e38c00997	C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\PH02753U.BMP.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\ph02753u.bmp.bd	Dropped File	105.68 KB	image/bmp	Access, Create, Write	CLEAN
fea60baeef907e53821f73fe50d7a5148040cd1043c26d71b716f941722e2355	c:\program files (x86)\microsoft\office\clipart\pub60cor\j0148757.jpg.bd, C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\J0148757.JPG.BD	Dropped File	65.96 KB	image/jpeg	Access, Create, Write	CLEAN
343b02f7f5f5e00437772f681a554757af480263a9106cb4af1a445f659b6814	C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\J0382950.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0382950.jpg.bd	Dropped File	94.21 KB	image/jpeg	Access, Create, Write	CLEAN
6978881548d968d7626e970520c26b689f16f93e016364522ab4ae9c11901772	C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\J0177257.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0177257.jpg.bd	Dropped File	44.29 KB	image/jpeg	Access, Create, Write	CLEAN
b1567d156c03f3e908b64644f30929042418929cad20cd3a3247a26f5d2b4d29	C:\Program Files (x86)\Microsoft Office\CLIPART\PIB60COR\J0341634.JPG.BD, c:\program files (x86)\microsoft\office\clipart\pub60cor\j0341634.jpg.bd	Dropped File	7.62 KB	image/jpeg	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
38a1f742cd25605a7b2e6067c2abe01b2f638ecb38083de93c0f0ece4f26501f	c:\program files (x86)\microsoft office\clipart\pub60cor\j0341653.jpg.bd, c:\program files (x86)\microsoft office\clipart\pub60cor\j0341653.JPG.BD	Dropped File	15.49 KB	image/jpeg	Access, Create, Write	CLEAN
fb1d59149966b9430257e44888c334cb491d524a35e0dd4b68ec00d02c920e9b	C:\Program Files (x86)\Microsoft Office\CLIPART\pub60cor\j0178932.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0178932.jpg.bd	Dropped File	34.51 KB	image/jpeg	Access, Create, Write	CLEAN
1cfb828a6d179d966408a0ea88b5759f1020721987a9b92a1df881f5002c9d20	C:\Program Files (x86)\Microsoft Office\CLIPART\pub60cor\j0315612.JPG.BD, c:\program files (x86)\microsoft office\clipart\pub60cor\j0315612.jpg.bd	Dropped File	16.56 KB	image/jpeg	Access, Create, Write	CLEAN

Reduced dataset

Filename	Category	Operations	Verdict
c:\users\rldhj0cnfevzx\appdata\local\packages\microsoft.windows.cortana_cw5n1h2xyewy\localstate\device\searchcache\appcache\133040061618385022.txt.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\MEDIA\ALYNC_secondcall.wav.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rldhj0cnfevzx\music\ejer4nhkhrs6\vmth6\jxogm\cn5f\wcvj\jd85\78qvagma9\fpchsf1.wav.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\programdata\microsoft\windows\start menu\programs\system tools\windows defender\lnk.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Windows\WinSxS\wow64_microsoft-windows-m...-odbc-administrator_31bf3856ad364e35_10.0.10586.0_none_db2a2a091c6f0159\ODBC Data Sources (32-bit).lnk.BD	Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RdHj0CNFevzX\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2xyewy\LocalState\DeviceSearchCache\AppCache\133040061328914220.txt.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\1033\PROTTPLV.XLS.BD	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ASP.NETWebAdminFiles\Images\selectedTab_1x1.gif.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Logo\images\FirstRunLogo.contrast-white_scale-100.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\PAPYRUS\THMBNAIL.PNG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\ph01179j.jpg.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Groove\Sounds\People\Whistling.wav.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Logo\images\MSPubLogo.contrast-white_scale-140.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Stationery\1033\DADSHIRT.GIF.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\RdHj0CNFevzX\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2xyewy\LocalState\DeviceSearchCache\AppCache\133039039768590531.txt.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ASP.NETWebAdminFiles\Images\darkBlue_GRAD.jpg.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Common Files\Microsoft Shared\Smart Tag\1033\MCABOUT.HTM.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\pub60cor\j0400005.PNG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\program files (x86)\microsoft office\clipart\pub60cor\wb01838_.gif.bd	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\publisher\backgrounds\j0143749.gif.bd	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0315580.JPG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\windows\serviceprofiles\localservice\appdata\roaming\microsoft\windows\start menu\programs\windows powershell\windows powershell (x86).lnk.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\windows\winsxs\amd64_microsoft-windows-narrator_31bf3856ad364e35_10.0.10586.0_none_4aa371494e102b6alnarrator.lnk.bd	Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\logo\images\m\spublogo.contrast-white_scale-100.png.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\publisher\backgrounds\wb02134_.gif.bd	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\G00038_.GIF.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH01239K.JPG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\r\dhj0cnfevz\l\appdata\local\temp\hq_g5gr7eygo.mp3.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\stationery\1033\pinelumb.htm.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\wb01237_.gif.bd	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\wb01734_.gif.bd	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\lag00040_.gif.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\logo\images\excel\logosmall.contrast-white_scale-180.png.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\logo\images\first\strunlogo.contrast-black_scale-180.png.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\R\DHj0CNFevz\X\AppData\Local\Microsoft\Windows\Notifications\wpnidm\179e8db5.jpg.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\r\dhj0cnfevz\l\desktop\td0exglq-mms3at\bwfq.pptx.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0382955.jpg.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382967.JPG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\WinX\Group3\04-1 - Network Connections.lnk.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\windows\winsxs\amd64_microsoft-windows-explorer-shortcuts_31bf3856ad364e35_10.0.10586.0_none_443d824ebb4341e2\01 - command prompt.lnk.bd	Accessed File	Access, Create, Write	MALICIOUS
c:\users\default\l\appdata\local\microsoft\windows\winx\group2\1-run.lnk.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0382950.JPG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02743g.gif.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes\16\ice\preview.gif.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\r\dhj0cnfevz\l\videos\vd6hd4z.avi.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\r\dhj0cnfevz\l\appdata\local\microsoft\windows\winx\group3\06-system.lnk.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Program Files (x86)\Microsoft Office\Office16\1033\PU BSPAPR\PDIR36F.GIF.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\ejer4hkhrs6\mth6jxogm\cn5\fwcvj\vmc-w0x6e6k\6bj\fhbg_q dtyxoerlj.wav.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\System Tools\Task Manager.Ink.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes16\bluecalm\preview.gif.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0145707.jpg.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\desktop\td0exglq-mms3atr0is26\ng0fcxkmuphj.avi.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\8dxcagdq.mp3.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\Run.Ink.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\ue23k.Ink.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Stationery\1033\PAWPRINT.HTM.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files\microsoft office\office16\1033\mso example intl setup file b.txt.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Music\JeR4HKhrS6LIMth6jXoGM\cn5LFWCvj\Sa5TIU\vnk\QywE29.wav.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\PU B60COR\J0313970.JPG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Windows PowerShell\Windows PowerShell ISE (x86).Ink.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Logos\images\WinProj\Logo.scale-80.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\media\ync_ringtones5.wav.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\PU B60COR\PH02810J.JPG.BD	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes16\layers\thm\bnail.png.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\music\ejer4hkhrs6\mth6jxogm\cn5\fwcvj\pcsc-4lj b0-.wav.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\windows\microsoft.net\framework\v2.0.50727\asp.netwebadmin\files\images\selectedtab_1x1.gif.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\media\ync_newim.wav.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\windows\winsxslamd64_microsoft-windows-msinfo32-exe_31bf3856ad364e35_10.0.10586.0_none_3861ff2fa4057c69\system information.Ink.bd	Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\ph02845g.gif.bd	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Logos\images\PowerPnt\LogoSmall.scale-100.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Logos\images\MSAccess\LogoSmall.contrast-white_scale-80.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\1033\PU BSPAPR\ZPDIR38F.GIF.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\ProgramData\Microsoft\User Account Pictures\user-40.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\rdhj0cnfevzx\documents\ofgxoeljvoh3fdj6xyy.pptx.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Logo\images\MSAccessLogoSmall.contrast-black_scale-80.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\PH01213K.JPG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\packages\microsoft.windows.cortana_cw5n1h2xyewy\acl\appcache\c192j4\6c__windows_systemapps_microsoft.windows.cortana_cw5n1h2xyewy_cache_desktop_18[1].txt.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\packages\microsoft.windows.cortana_cw5n1h2xyewy\localstate\device\searchcache\appcache133040064058720540.txt.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0341738.jpg.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\temp\kxxcink.flv.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\logo\images\powerpnt\logosmall.contrast-white_scale-80.png.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\lnk.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\IRIS\THMBNAIL.PNG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files\Common Files\Qxya1bDnxSO-cuS.bmp.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\media\laser.wav.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\computer.lnk.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\pictures\rnwt wtfv\mdeq6wjzb-rkl9uaup.bmp.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\1033\pubspapr\pdir47b.gif.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\logo\images\groovelogo.scale-180.png.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Groove\ToolBMPs\NotifierBackgroundRTL.jpg.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\windows\microsoft.net\framework64\v2.0.50727\asp.netwebadminfile\images\requiredbang.gif.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\1033\pubspapr\pdir8f.gif.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\RcLeo 22Fr BWUIJG.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\windows\recent\o0x\ncg9oqzlhpgjz2l.lnk.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\windows\microsoft.net\framework64\v2.0.50727\asp.netwebadminfile\images\unselectedtab_leftcorner.gif.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\logo\images\msaccesslogosmall.contrast-black_scale-100.png.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\ppd8HF5.pptx.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\lag00175_gif.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\System Tools\Command Prompt.lnk.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\programdata\microsoft\windows\start menu\programs\administrative tools\memory diagnostics tool.lnk.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft\office\clipart\pub60cor\j0144773.jpg.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Logo\images\WinWordLogoSmall.contrast-black_scale-140.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\1033\PUBSPAPR\PDIR9B.GIF.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rldhj0cnfevzx\appdata\roaming\microsoft\windows\recent\la1xn000.lnk.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Common Files\Microsoft Shared\THEMES16\SPRING\THMBNAIL.PNG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft\office\office16\logo\images\powerpnt\logosmall.contrast-black_scale-80.png.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_MoveDrop32x32.gif.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\1033\PUBSPAPR\PDIR45B.GIF.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ASP.NETWebAdminFiles\images\header\GRADIENT_Tail.gif.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\1033\PUBSPAPR\ZPDIR44F.GIF.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\Publisher\Backgrounds\J0143752.GIF.BD	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
c:\windows\serviceprofiles\networkservice\appdata\local\microsoft\windows\winx\group214 - control panel.lnk.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\windows\microsoft.net\framework\v4.0.30319\asp.netwebadminfiles\images\folder.gif.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\PUB60COR\J0287642.JPG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files\Java\jre1.8.0_171\lib\images\cursors\win32_LinkDrop32x32.gif.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Groove\ToolBMPs\NotifierDisableDownArrow.jpg.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft\office\office16\logo\images\powerpnt\logo.contrast-white_scale-140.png.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft\office\office16\logo\images\visio\logo.contrast-white_scale-80.png.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rldhj0cnfevzx\appdata\local\packages\microsoft.windows.cortana_cw5n1h2byewy\localstate\devicesearchcache\appcache133040063027496025.txt.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Windows\WinSxS\amd64_microsoft-windows-m...-odbc-administrator_31bf3856ad364e35_10.0.10596.0_none_d0d57fb6e80e3f5e\ODBC Data Sources (64-bit).lnk.BD	Accessed File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft\office\office16\logo\images\visio\logo.scale-180.png.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rldhj0cnfevzx\appdata\local\packages\microsoft.windows.cortana_cw5n1h2byewy\localstate\devicesearchcache\appcache133040063121055077.txt.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Logo\images\Visio\Logo.scale-80.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft\office\office16\groove\sounds\places\buzz.wav.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\program files (x86)\microsoft office\clipart\pub60cor\j0387591.jpg.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\logoimages\winprojlogosmall.scale-180.png.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\publisher\backgrounds\j0143750.gif.bd	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Documents\CRoelfs\Kaz4WMk6uLM4POnb.pptx.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\WB01241_GIF.BD	Accessed File, Dropped File, Modified File	Access, Create, Write	MALICIOUS
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools\Windows Firewall with Advanced Security\lnk.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\common files\microsoft shared\themes16\ricepapr\preview.gif.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\J0099187.JPG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevz\appdata\local\packages\microsoft.windows.cortana_cw5n1h2xyewy\aclappcache\c1j92j4x\2c__windows_systemapps_microsoft.windows.cortana_cw5n1h2xyewy_cache_coobe_coobe[1].html.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevz\desktop\7ytu2fiau7azd1m5.mp4.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Windows\WinSxS\amd64_microsoft-windows-explorer-shortcuts_31bf3856ad364e35_10.0.10586.0_none_443d824ebb4341e2\08 - Power Options\lnk.BD	Accessed File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\CLIPART\IPUB60COR\PH02412K.JPG.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevz\videos\1ydsml61qulzmls-z2byjaxxn.avi.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\windows\winsxs\amd64_microsoft-windows-explorer-shortcuts_31bf3856ad364e35_10.0.10586.0_none_443d824ebb4341e2\08 - homegroup\lnk.bd	Accessed File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\1033\PU\BSPAPR\PDIR\13F.GIF.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Logoimages\Visio\Logo.contrast-black_scale-80.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626_3\Screenshot\Logo.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Windows\Recent\7Dp4MNiUOFeIDoLj0syfl\lnk.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\office16\media\ync_busy.wav.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevz\appdata\local\packages\microsoft.windows.cortana_cw5n1h2xyewy\aclappcache\c1j92j4x\16c__windows_systemapps_microsoft.windows.cortana_cw5n1h2xyewy_cache_desktop_22[1].txt.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevz\appdata\local\microsoft\windows\notifications\wpnidm\ad152324.jpg.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\MEDIA\Default\Hold.wma.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\Logoimages\WinProj\LogoSmall.contrast-black_scale-140.png.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools\Security Configuration Management\lnk.BD	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\program files (x86)\microsoft office\clipart\pub60cor\j0309705.jpg.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\default\appdata\roaming\microsoft\internet explorer\quick launch\shows desktop.lnk.bd	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

Reduced dataset

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\FUOCNFJDMPZDFQ\shell\open\command	write, access, create	319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	access, create	319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Alcmeter	write, access	319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe	CLEAN
HKEY_CLASSES_ROOT\FUOCNFJDMPZDFQ\DefaultIcon	write, access, create	319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe	CLEAN
HKEY_CLASSES_ROOT\FUOCNFJDMPZDFQ	write, access, create	319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe	CLEAN
HKEY_CLASSES_ROOT\BD	write, access, create	319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe	CLEAN

Process

Process Name	Commandline	Verdict
319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe	"C:\Users\RDhJOCNFevz\X\Desktop\319fbb2dd26045a90a452eb26799c6529f8a77ad8d7b967aec58111e25b12cd5.exe"	MALICIOUS

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	4.7.1
Dynamic Engine Version	4.7.1 / 11/21/2022 04:40
Static Engine Version	4.7.1.0 / 2022-11-21 03:00:41
AV Exceptions Version	4.7.1.7 / 2022-10-27 16:01:27
Link Detonation Heuristics Version	4.7.1.8 / 2022-10-30 09:01:20
Smart Memory Dumping Rules Version	4.7.1.7 / 2022-10-27 16:01:27
Config Extractors Version	4.7.1.17 / 2022-11-29 09:09:04
Signature Trust Store Version	4.7.1.8 / 2022-10-30 09:01:20
VMRay Threat Identifiers Version	4.7.1.18 / 2022-12-05 15:00:42
YARA Built-in Ruleset Version	4.7.1.17

Software Information

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

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDhJ0C-1\AppData\Local\Temp

System Root

C:\Windows
