MALICIOUS

Classifications:	Ransomware
Threat Names:	Mal/Generic-S, Mal/HTMLGen-A, Gen:Variant.Razy.326200
Verdict Reason:	-

Sample Type	**Windows Exe (x86-32)**
Sample Name	**CUsersGrujaDesktopca5751036a12d0.exe**
ID	#383975
MD5	97780c0075e7749f8880f41b91f8892f
SHA1	dfa6e362535ddfeb7df53b29cc6830617d581df1
SHA256	ca5751036a12d0a9fba5f2c6cd2bde61b9c40e1607f751c39212b9c9a94c6b5a
File Size	71.00 KB
Report Created	2021-04-18 21:44 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (13 rules, 15 matches)

Score	Category	Operation	Count	Classification
4/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) cusersgrujadesktopca5751036a12d0.exe modifies the content of multiple user files.			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected the sample itself as "Gen:Variant.Razy.326200".			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
4/5	Reputation	Contacts known malicious URL	1	-
	• Reputation analysis labels the URL "91.218.114.31/" which was contacted by (process #1) cusersgrujadesktopca5751036a12d0.exe as "Mal/HTMLGen-A".			
4/5	Reputation	Contacts known malicious IP address	1	-
	• Reputation analysis labels the contacted IP address 91.218.114.31 as "Mal/HTMLGen-A".			
3/5	User Data Modification	Possibly drops ransom note files	1	Ransomware
	• (Process #1) cusersgrujadesktopca5751036a12d0.exe possibly drops ransom note files (creates 380 instances of the file "YOUR_FILES_ARE_ENCRYPTED.HTML" in different locations).			
2/5	Discovery	Executes WMI query	1	-
	• (Process #1) cusersgrujadesktopca5751036a12d0.exe executes WMI query: select * from Win32_ShadowCopy.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #1) cusersgrujadesktopca5751036a12d0.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• (Process #1) cusersgrujadesktopca5751036a12d0.exe is possibly trying to detect a VM via rdtsc.			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) cusersgrujadesktopca5751036a12d0.exe creates mutex with name "()$&t$$""%"u$ ##)&&$t '()$pwr##(%!%p)!" u"$!! &ur$&r!!ws'")st&)r)#pt& t$&r!&t)% ".			
1/5	Hide Tracks	Changes folder appearance	1	-
	• (Process #1) cusersgrujadesktopca5751036a12d0.exe changes the appearance of folder "c:\users\rdhj0cnfevzx\searches".			
1/5	Network Connection	TOR hidden service domain embedded in document	2	-
	• URL embedded in document c:\$recycle.bin\s-1-5-18\your_files_are_encrypted.html is hosted on TOR hidden service domain nbzzb6sa6xuura2z.onion. • URL embedded in document c:\$recycle.bin\s-1-5-18\your_files_are_encrypted.html is hosted on TOR hidden service domain ebwexiymbsib4rmw.onion.			
1/5	Network Connection	All network connection attempts failed	2	-
	• Host "91.218.114.31" is unavailable. • Host "91.218.114.30" is unavailable.			

Mitre ATT&CK Matrix

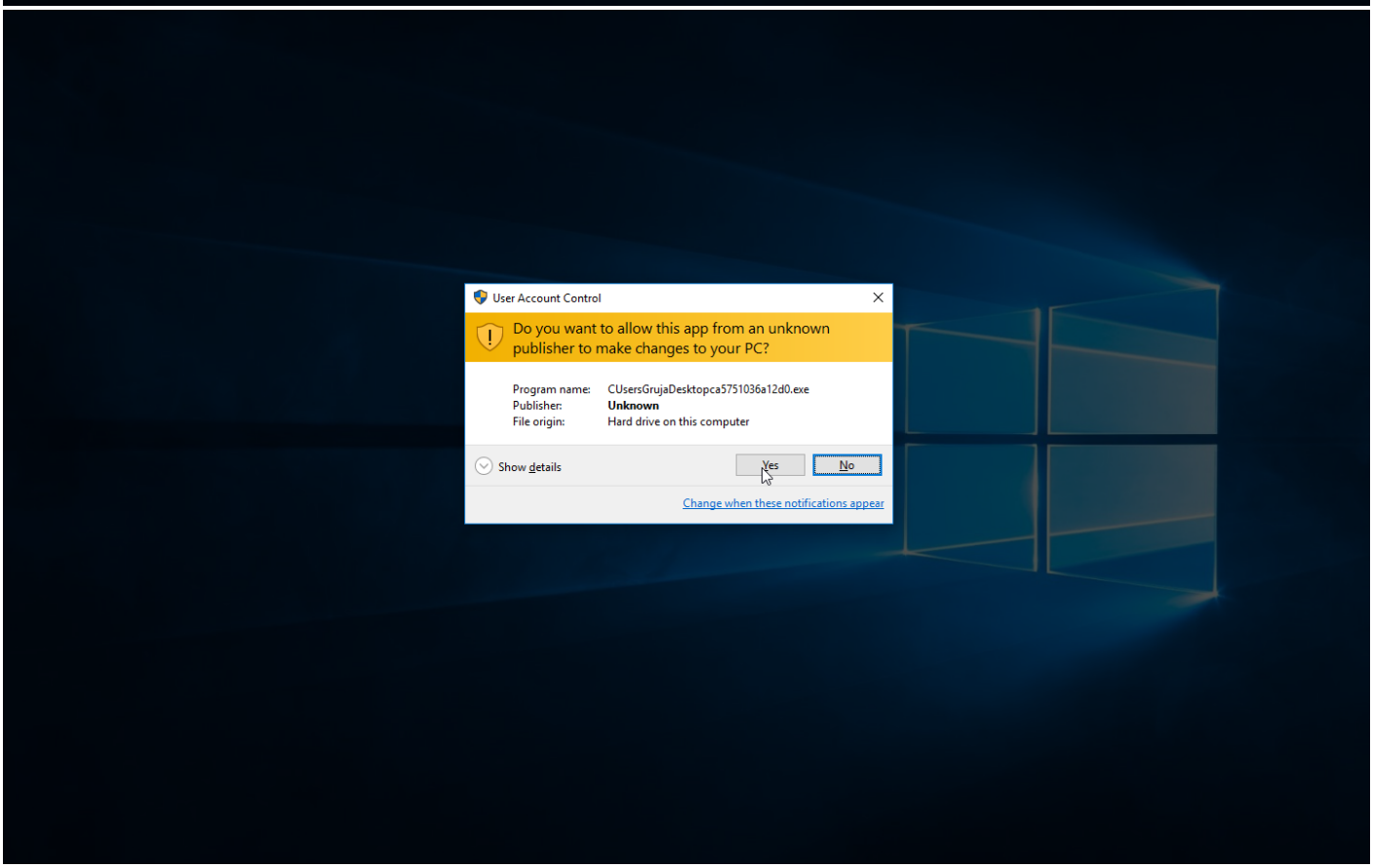
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
-	#T1047 Windows Management Instrumentation	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	#T1119 Automated Collection	-	-	-
-	-	-	-	-	#T1081 Credentials in Files	-	-	-	-	-	-
-	-	-	-	-	-	#T1083 File and Directory Discovery	-	-	-	-	-
-	-	-	-	-	-	-	-	#T1005 Data from Local System	-	-	-
-	-	-	-	-	-	-	-	-	-	-	#T1486 Data Encrypted for Impact
-	-	-	-	#T1036 Masquerading	-	-	-	-	-	-	-
-	-	-	-	#T1497 Virtualization /Sandbox Evasion	-	#T1497 Virtualization /Sandbox Evasion	-	-	-	-	-
-	-	-	-	-	-	#T1124 System Time Discovery	-	-	-	-	-
-	-	-	-	-	-	-	-	-	#T1079 Multilayer Encryption	-	-
-	-	-	-	-	-	-	-	-	#T1188 Multi-hop Proxy	-	-

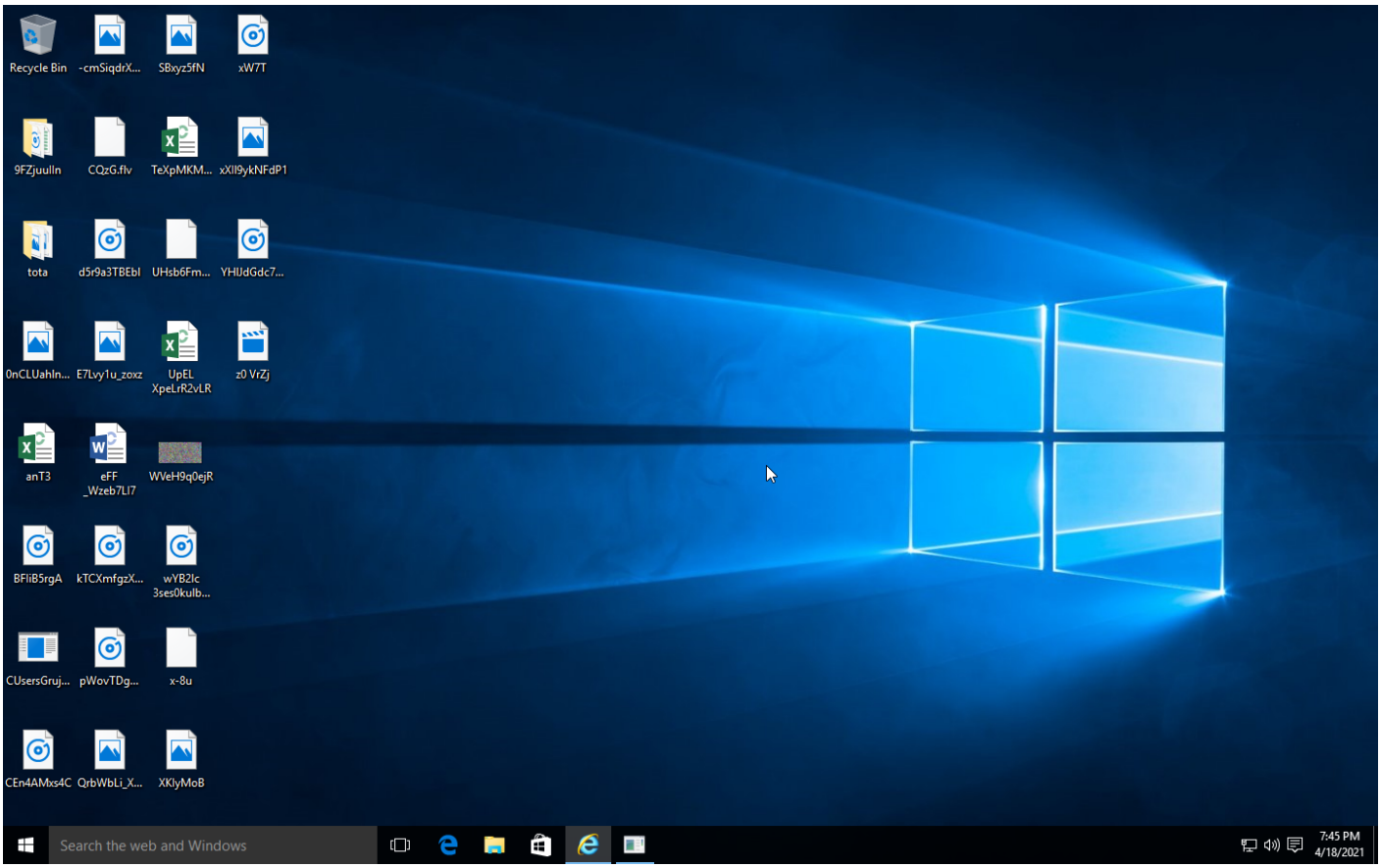
Sample Information

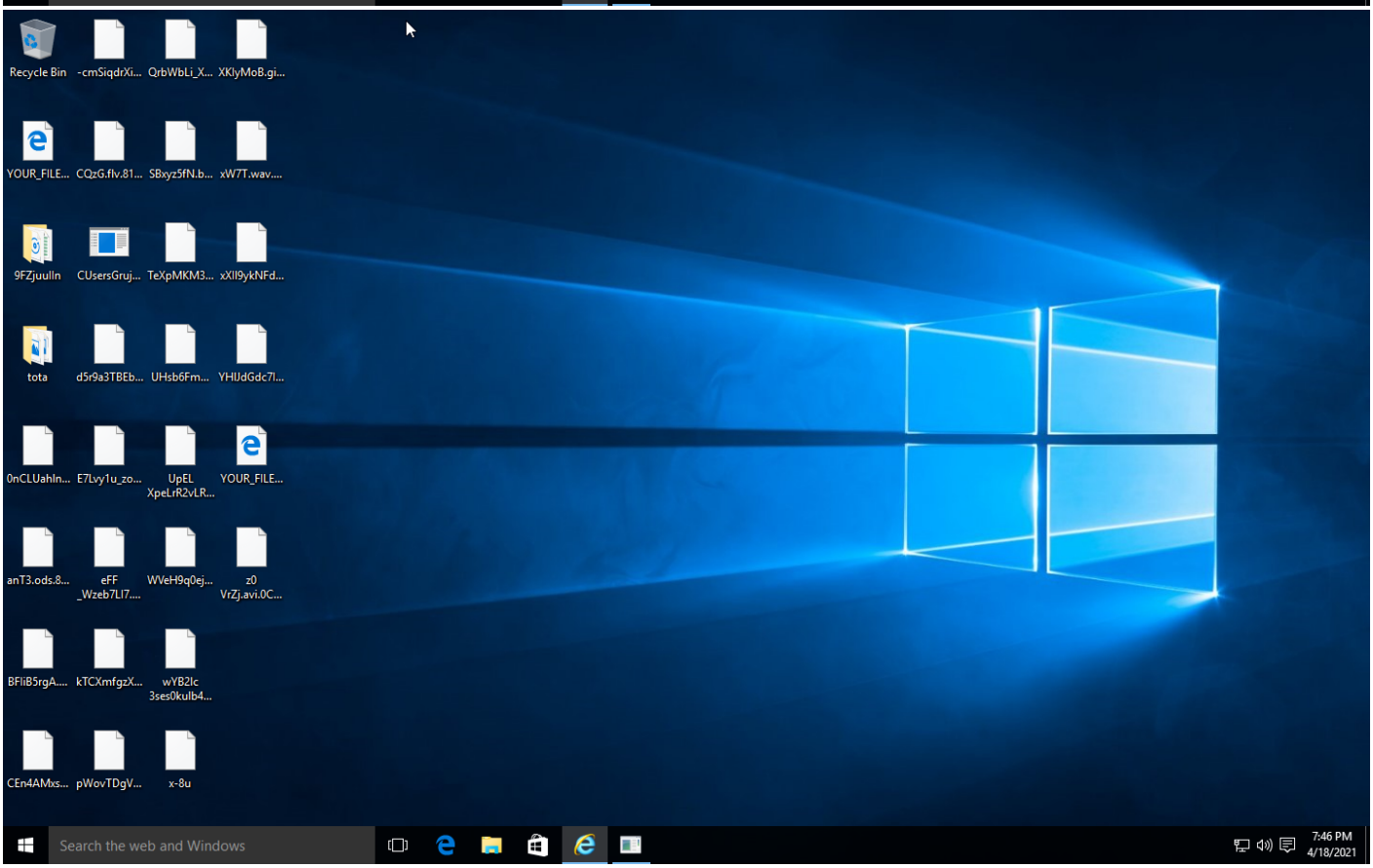
ID	1167783
MD5	97780c0075e7749f8880f41b91f8892f
SHA1	dfa6e362535ddfeb7df53b29cc6830617d581df1
SHA256	ca5751036a12d0a9fba5f2c6cd2bde61b9c40e1607f751c39212b9c9a94c6b5a
SSDeep	1536:A/6TQOU0uGYi+Zl3vjizUUYzF+R0DEOKF3BgVmVMQGr7ArwKr6D7nFkaoVNl:A/6TQO2GOvjizYQPhF3BB+bUMKsh7w
ImpHash	642af287251f2705fd4b0f565139e5a1
Filename	CUsersGrujaDesktopca5751036a12d0.exe
File Size	71.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-04-18 21:44 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	1
Execution Successfull	False
Reputation Analysis Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✓
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: CUsersGrujaDesktopca5751036a12d0.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
-cmSiqdrX...
SBxyz5fN
xW7T
9FZjuuln
CQzG.flv
TeXpMKM...
xXl9ykNFdP1
tota
d5r9a3TBEbI
UHsb6Fm...
YHlJdGdc7...
0nCLUahln...
E7Lvy1u_zoxz
UpEL XpeLrR2vLR
z0 VrZj
anT3
eFF _Wzeb7LI7
WVeH9q0ejR
BFliB5rgA
kTCXmfgzX...
wYB2Ic 3ses0kulb...
CUsersGruj...
pWovTDg...
x-8u
CEn4AMxs4C
QrbWbLi_X...
XKlyMoB
Search the web and Windows
7:45 PM
4/18/2021


Recycle Bin
-cmSiqdrXi...
QrbWbLi_X...
XKlyMoB.gi...
YOUR_FILE...
CQzG.flv.81...
SBxyz5fN.b...
xW7T.wav....
9FZjuuln
CUsersGruj...
TeXpMKM3...
xXl9ykNFd...
tota
d5r9a3TBEb...
UHsb6Fm...
YHlJdGdc7l...
0nCLUahln...
E7Lvy1u_zo...
UpEL XpeLrR2vLR...
YOUR_FILE...
anT3.ods.8...
eFF _Wzeb7LI7....
WVeH9q0ej...
z0 VrZj.avi.0C...
BFliB5rgA....
kTCXmfgzX...
wYB2Ic 3ses0kulb4...
CEn4AMxs...
pWovTDgV...
x-8u
Search the web and Windows
7:46 PM
4/18/2021

NETWORK

General

0 bytes total sent

0 bytes total received

1 ports 80

2 contacted IP addresses

2 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

2 URLs contacted, 2 servers

2 sessions, 0 bytes sent, 0 bytes recivied

DNS Requests

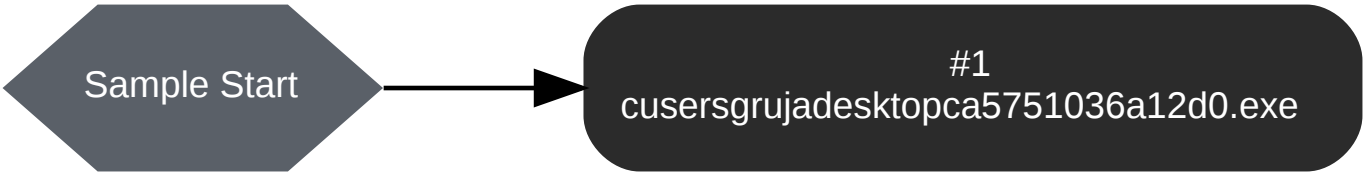
-

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://nbzzb6sa6xuura2z.onion/				0 bytes	N/A
GET	http://ebwexiymbsib4rmw.onion				0 bytes	N/A
POST	91.218.114.31/				0 bytes	N/A
POST	91.218.114.30/				0 bytes	N/A

BEHAVIOR

Process Graph



Process #1: cusersgrujadesktopca5751036a12d0.exe

ID	1
Filename	c:\users\rdhj0cnfevzx\desktop\cusersgrujadesktopca5751036a12d0.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\CUsersGrujaDesktopca5751036a12d0.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 57532, Reason: Analysis Target
Unmonitor End Time	End Time: 135513, Reason: Terminated
Monitor Duration	77.98s
Return Code	0
PID	2168
Parent PID	2104
Bitness	32 Bit

Dropped Files (134)

Filename	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✕
\\?\C:\$Recycle.Bin\S-1-5-18\YOUR_FILES_ARE_ENCRYPTED.HTML	15.00 KB	461987b667938e313358de61e8bd2df8df3252607e26c6a9e1919f432892121b	✕
-	864.46 KB	40bbbe6e0472605e0e9bae46ffe04f024a49e64a0b3e4ad6ee11074b1f4f5386	✕
-	21.85 KB	a1bd59b3e4c2a7ae707306f0890710ba1e409b1819e74e512977c74b31726aa0	✕
-	20.53 KB	5e12d340e146d4543235a81c1824398be4a36731f9ed74d0b61aa726ce168419	✕
-	3629.45 KB	173298bbb1a7ce30dddfcc7c8928e86964be65961cc4b837feb453960f931e81	✕
-	614 bytes	9c3ce8c404e8b62cb6ee9f0ea34b8cb8b0eed70ce3404d5073f6c1c5ce1d71b4	✕
-	1.35 KB	693ee2ab5b37394ebfa09050d3db63e15548c7001cf14ae5cce1dde9be0329fe	✕
-	1.93 KB	44c0558310c71fb2e1c1caa6148277cf5b2c3b53e69f50af6cf1f32382a3cd17	✕
-	4818.01 KB	9d95b0a062dcbfb639fac620d2bd6a5ffa870cdfdada96c74c403538ba4dd967	✕
-	614 bytes	9659782066faae704f6fa518551bb1b29b56cd24ba7b0943ea492b59f02eb716	✕
-	3024.26 KB	809b25871a3974202f52ff8730f6fdf637b1f3fd8f55495eed220d40fe0797c7	✕
-	37.88 KB	e58ded87e097f4fa7a9cde0e9bf20d9f9a18786f6a9b3bac309393e0c168ef32	✕
-	56.07 KB	8e589010f0c056dfacda843ae06f85c8bc75c42dfcb76e9b86692f2e58c6c8b8	✕
-	1.99 KB	bccea1ddfcb5862d41fca102910affc6cecce9bc04e4712341a14b66e32c34ce	✕
-	16.26 KB	8f0299480bf6fe3abcd1c5e1e17b6841745d7362d9529e83516c968e51d3ed40	✕
-	9.58 KB	602f67f265df27ef33520d0e680860ba650d38855d6e3413fade78401870152e	✕
-	232.30 KB	5534b54e0223286ad5126cff42fcef6c0090a5b496a38fc0dfa5799b8be37a01	✕

Filename	File Size	SHA256	YARA Match
-	34.20 KB	77b2efd8459c34b2cc8ff6f3fa1d3ba76964d1075d44cc293c1e4deaeae62cbb	✗
-	35.76 KB	b1c7953437fce049a6f1f0b73e6d166b4bc5fd2e8572feeac1e87a90d438353f	✗
-	5.99 KB	f79b3ba5fd137018ef98e8aeaa2b194683cc97a4b03c6ebf420feb73ee3401ce	✗
-	22.78 KB	693380edcc483d5e7e614e50761eb80078835753e77ff5c04e8c93f5ccdc7db8	✗
-	21.44 KB	57f48823625c1a7c225d3e0d52e351d8f3d94fd3405596d9d892aa3256d54881	✗
-	1.99 KB	c2f4f6928c3f82fd9b1a1b94b86486b92785b29cecdfcac6c9bc0e87d9801058	✗
-	261.19 KB	4552d566d8b33aad769834f753b68a8e9ea02769eef0fe78907d29f30766bf5a	✗
-	87.46 KB	1dff5ae828c1b29b846fa9642e6e4cc7735666febef144dbb56cb6cf45d8612f	✗
-	104.38 KB	c10af5a9a86691bac38000735ea9330375f57acc971587d7da899635559dac4e	✗
-	1.99 KB	41d58630b35c4956e3b0238dcf009ab23fbf9b655e8c893fa6fa6dcfc55d4614	✗
-	93.70 KB	e50353624343f9e375e632f4832fe92e3e656428e77c1b01a625b4f4405879c2	✗
-	18.53 KB	f0bb000e6bdd6b168e55c19f2cfe9439c206968200b10aebbb20a096fb80893b	✗
-	1.48 KB	f8c9edf9883c04fdc32b3d82fe3688f0872837bf9b8b4b4938d694ee2c8bd8a8	✗
-	10.77 KB	196bf07c5b0c7f6c3748020a29a0c988871fc2840c95ac0f7d1b22f544c79a27	✗
-	2.24 KB	8d3aca4ef0c28e8b68364a7af323c916ecd287535ea1dccb876c70190afddf80	✗
-	9.65 KB	b22d03bec913823674ebc33585e27d194952748a3139044f50fb0d8efd234530	✗
-	91.15 KB	90764c5ece1a3ea4d4b1096b155773918988c60259acf10607384aa1f4152990	✗
-	94.19 KB	70e994d66184b068cdc82a1036f240e22f11df8a5c4402040a65fe4008a342a9	✗
-	695.23 KB	9306737e6c48629bfeb9b9921dd9c6cdcc5c6458af67d0ea5e70c7d3fbbde874	✗
-	100.36 KB	ea5ba8323386547dc3ef2dc49bab9a3e1ce246f2601efe1a8f1fbf785c83a2cd	✗
-	26.08 KB	a75fbf2fbe4694e5e337f1363e6881293172129a7b67bce3ffc5e375275961e2	✗
-	24.86 KB	c20e8bf736eaf4876da6ec7a7d61a10df9d2c13430352942196e072ddf02b8ba	✗
-	23.91 KB	65b46ce4d78f2bbedcef648a1dd4349447bf98a81b28af7938fb8a3cad798673	✗
-	23.91 KB	44c2182e56ff421b1e44f01c5c43a091ece9cbbff2e8365b46034f3ff64b15da	✗
-	1.99 KB	2b7e1b1afa7f67c8efa9608a6da53e860c5253da2ae23f50a7381a593031e4a9	✗
-	75.36 KB	cee350c6de9246486f9cf5193da281009bd1cbfd6c5dd2cd4243e484177f9caa	✗
-	13.76 KB	a6b97219ab7c1ac0f428f1693d48875e9d6eac34774840d3287f5e2b772a8248	✗
-	683.05 KB	d24c084585e6b79489a3cdf276e390b53f9b8abfdce864c7a3bf7893843998a9	✗
-	84.63 KB	b1c6faa3577b848a30068cbe8c41cae3e4c74efec0b94011049c04406f1bb596	✗

Filename	File Size	SHA256	YARA Match
-	3.17 KB	37be018c2d5858f88901edbeb8b968864981f85ff4801cf32b278e782164a4ff	✕
-	3.24 KB	cb4053b9026837b80d5870f387ddf022423870bc78a5a07b4c401256b9cb37ad	✕
-	76.03 KB	e42d07f77e1e395a67627e001a450547d176dcd11846c59f2e1bc63f4dcc99b1	✕
-	33.69 KB	d73bf6776bb585839c4af833d1b9264cfb63280dcc023521f093349fc8019300	✕
-	23.71 KB	aa7672b4af429f1b3ba4f77ea43854ac23c857a3ed3ef709b7cce78fee4ddbd6	✕
-	3.64 KB	641eec700095792ebc6789f663dbfe24a2adc151a992ea1e90743a43fe122723	✕
-	559 bytes	4576910171305b8263e3a2e3dd337fc14c95ac375d285161a5126878ff0ce06b	✕
-	1.23 KB	1b82b28548792f90656a2c811440325799b0c0156b3b020dbd2305ea19dcc0da	✕
-	5.40 KB	4157c41bcf179ac7b8971a8e82874e5a2dc6f1f75907be3815862a9d49775ec0	✕
-	6.38 KB	12d41e168dcd787bdf44a351cc4e9a4e5e13ae267920eff6ec1315f48330b0ca	✕
-	579 bytes	928b831f6643f7630f6b76813763074c944c67d2cb9d10ffc39afd79d7206461	✕
-	7.80 KB	ff225dfc318803bf275e207911d9fee80f199db0df466602f8a6b037aff780fc	✕
-	875 bytes	070aa570139043ae61f180a75f973bf767948bba9ff19d5a650cdb3afe283df6	✕
-	2.17 KB	b0e75baf8208c8b08b769c37ed833c619aeefa550a9727405ff80c8fe8de2c2b	✕
-	555 bytes	069f349e6fc4d95db5893be709d5d32c1a5e0b3b7d23a208189d7c08ee5563df	✕
-	7.17 KB	6875042b18646735ea106c7dcc7a3bde9da962b08d1c9cc2280bcdf401384854	✕
-	3.28 KB	72f0b053ff05014cbf52343038956851984 1d15c863be383b9eb45364d92ece1	✕
-	2.16 KB	abb2ae1e5e118527dfc18f9426a8a7e4474ff77f79cbf9465a828cc8aa1dab3f	✕
-	1.60 KB	bce5e29f25ba48e553ecf4bec0fd0f5c9fb6970a4237bb93ce74d32cbbd7235e	✕
-	1.78 KB	6b57aa5c0532e1e132bcd14f14f08eb1c8eb078e99e49fc2f2705c52e25a3576	✕
-	3.41 KB	a5dd6cbe9a43c943489b3b501261a02a7b4f04830c485cf9b9b1277cfa937ecc	✕
-	27.68 KB	d5bea3c2dfee2aba38cee1bbfd1cba98154656c3e1e8e6e1a32bc44ca38b26ba	✕
-	1.46 KB	2e9dc12f3d2f773cfe5f807d325c9d447c7c204c6a14ad2c256f0248949198fb	✕
-	2.35 KB	f6bda55448e20953695eb949fbf62e7d6e1872ce63ee4a5c67083df2fa8dbb67	✕
-	588.05 KB	264be192a1f63e3b381ede1f676eefdf15250ceb3d8c231c5f5b8158beaeb10e	✕
-	588.05 KB	9c214e38d96419b439da2799ac97a98c647ea0e212f56cb5672da22fc2fa923a	✕
-	5.27 KB	7e004ba7f647c917250ff11936c4ea7b0453e13fd477504b7ba7da1278de28fc	✕
-	5.27 KB	72e1286ac5b759f9e8d27fbe28af13576b1134978aae3da3dd75b0d1b9e47719	✕
-	25.18 KB	12b1b83a698bd93d7c86f90932998a66f0473d3d70d480566ca2de30c0cb7cd1	✕

Filename	File Size	SHA256	YARA Match
-	10240.00 KB	ad9957a994b7742e3a8c03ab95de1b51ac0e14f33ae95c439dd19117a6fa53fc	✗
-	1.63 KB	6e12aae48d7ab42306a981f1ae759335121b5e53ee0dc99ce52a2984ed0a605e	✗
-	36.00 KB	2e42b6f608984b9960d7d60b7fd728acdea4e0c326d9332399305f7d15d57755	✗
-	48.00 KB	9cb1da2b3466d8652726c885baca367de5ee20cc4aa1353f5dc6790256b1f229	✗
-	4.00 KB	592597a6c2381ed0834bfd208c49b82ec2ccd02d991c8536deca554a21aaed29	✗
-	4.55 KB	e04c0d166adac3d8824c8dc74acb6a6a7843ee26fc45bef839ab6b653f722d80	✗
-	5088.92 KB	8afa07c0389862d0122a30c67493c99af9683eefc923ca78dd47d31541130d50	✗
-	973.69 KB	ec7498fcef87e799b79b9b0963e43e0184a28409ff160a1e40b8b444700aa5d3	✗
-	1335.61 KB	07016764f909ebeccab7e4376a66501f70e04bd4631a8de0999c16da95d0b1a5	✗
-	5664.29 KB	3f44aa7692a02689f227f6f3b8d97ce18be91797fdbeba386510d2677e073df6	✗
-	5500.25 KB	0b74f780f578b4575685befe815cc6727efc1758704c7a71d0d2cc1c1bda1655	✗
-	5457.28 KB	90b11ecf9b7e153f1591b0d1b2bd74681a34ccdb59585ea6097e1a22952d5cf9	✗
-	1010.26 KB	48dfb90d861dc5276b80ae4e307cf17a1c4bba2537423ec2c809f375ba3d9f6a	✗
-	5033.02 KB	460288d18b225cbd0420682c0920c8e808b06d8895deca3798b2753273727474	✗
-	802.42 KB	ee67b06dabf3aacd0290ac76a5251efc6429bc485dd0c107697e2705650f14d5	✗
-	790.79 KB	91a37f6e640dc9fd419211912f8670dd025e8291357daa572308e6d393bc6695	✗
-	1473.17 KB	9829b21a6a374bfd9aed90ef443a5cdaaf786e3f8666f14d494d21ba1eb0e741	✗
-	4817.28 KB	42745f423f5d2ddc7d327bb17bc3821c33843df93b99e6258ad862d58f63ccee	✗
-	841 bytes	3d35dabef1dca85c0eb14ba6023656b141293fc1abaface5ba0c3d3a67cb9252	✗
-	1.02 KB	ea3035fc54ac9cff6d47ded10e68eeb096a166203d37745a4dcdece59e4c5714	✗
-	3072.00 KB	418af71aa144929540e9d479db04e14e428fc1417c0784ab7e2d0947893cedc1	✗
-	17.53 KB	815cecddb8c7b55c6386840c31e683b63c2dfd263d17bcb8f78784a761ec892a	✗
-	4.26 KB	fe14e4389a563b12b5df29d691c1a6842d215dca3d286b8460f8ba0328b2ab42	✗
-	4.12 KB	2d6df2c9721b57475ca4ad6b52e50f81a744a6fa0f9c360ca62f1014af6c1902	✗
-	6.42 KB	35cd16a04d1df90a88ecaf52463fe3d677252fe4fd0b6701407a40a12be0903b	✗
-	3.02 KB	1c7f35d991cb352c765c199d420bd5597b8a85198a9f7ac8f1dfb2ad908d1644	✗
-	1.27 KB	d3fe2227b2b0ca46470c4cd9498ec3074255909137485f0c424423cc0e03101d	✗
-	15.90 KB	bdbd479ed68f3df0201016e8daf91643282eb80c93c1734b6bfc04f6e161a5fa	✗
-	71.25 KB	51e7aeb0dd33470600f3c1b851af5d776496ebcd98194277155a6ddb798489ab	✗

Filename	File Size	SHA256	YARA Match
-	16.08 KB	f624e5e88cf80b3ab4cbbf8a4e3882b36440d3b3e101a84867758fdb6e2979bb	✗
-	16.08 KB	4eead142cfd18c80e13aac4d12aa6a38cc45870148abdde3f49fed6facb6e54e	✗
-	82.64 KB	cdc42ab7dd3219b52ba574dae3c501131a46c74195caad5a5150d390c5c25730	✗
-	75.06 KB	5d978631eb52a8a1752a1ce74d6c189f690200480891ac02085a96a7e0bd4200	✗
-	308.67 KB	e164eb8be6c58caf2415056c3151fda28f5d8c3e98e78e2f253ca6036271d86b	✗
-	16.08 KB	0abc35917e6d0ae3e06b2eec0ebd2d146aac117bd88bd6839d748a80f16dcda3	✗
-	78.44 KB	f0416cb0d3256eb9fc3ae5f815cb53d0a751ff68f7923fb86c822067c499c494	✗
-	101.96 KB	fe1aa90e8b0bd3fc8a5196e8f769dd2dd32f90ea333fa990c8e4caf5701bdd97	✗
-	845 bytes	1bc3d1a3c1ae237abf7e3e002d9bf5bc0dbd627da05d9a4b8c9f9ade90d620ca	✗
-	849 bytes	b01d1715b60075f4eeafde5e2d3cfabbb81cf68faa16fc8fc922df154767c916	✗
-	837 bytes	4a13604dacf3a8efdfe244bcc70a8142880440859529049e9adc007002645175	✗
-	849 bytes	adac671757b7801ffb4d1d598571701c962efc235fef70f87f4c22a3f040a19e	✗
-	374.24 KB	d5bb4eda48f7b2f3ad50a4da3f026f358b813460235f54862b9b65a6e304af28	✗
-	9.99 KB	debe1c6b5c2350e9998a77202f87e50b9634983dc65248f8b987b0e250d72fac	✗
-	4.56 KB	3cf02dec03b7bc10aeb961c2cbbec0372d3b661edbcf3b7d3444bdaf1d7e102e	✗
-	5.71 KB	402249c527693e5a1335682841ff87b77f096d188e2bbc598f787227323cc34c	✗
-	19.59 KB	a96f6b2f27079f33acb3b2e6fe6ae0609d732bee3f5de0fe87a1be1169361e2b	✗
-	80.19 KB	9a88a6235fdc60ee9c0b2e73d464ba40f957e72bbfd670234772cd12496c44be	✗
-	28.69 KB	8901ca24dd78f883644abb4c3e81f69056b65537bc7e543d2cf024788624aad1	✗
-	992.00 KB	cce5dfcd63ceac59cba91a5ac82f99f7d1831c9a3cada135a480be1828eeb198	✗
-	4.56 KB	a8e423084c6a51a06010706177e74b8cb8b46a28d87e65ee0f9a68e0936913fa	✗
-	374.24 KB	e8486ce47c598284a68f80c8a23c816d6643f54de2befc8201e6944e27717cea	✗
-	9.99 KB	4c47906e94271e55a3a899247e0845b26ad2007137c97884baf1612c0c80322c	✗
-	5.71 KB	a873777146bf138212f0359fd7daad43fae985999d069ea03f8cd924b0170baf	✗
-	80.19 KB	fbfbb6ae15c2aa76f964b2de5a9f420d81b936a7e8ec4eab0d5bbb6356c858eb	✗
-	28.69 KB	5a6a65d56e2cdabbb94986fc62f82bf3d7dc9d06673a2adcfb8d4676b25c7ad8	✗
-	216.69 KB	7d3b8d9815548cdd47bc74c3677a772a5e24e8c34a6644ce13d06fb331567c93	✗
-	19.59 KB	a59931a13bdcd7f82e891abf1139dec4837c294c039a3a33fc3ec11a11536166	✗
-	2614.19 KB	be57de6dfc35849a7971918b5415afae3d13c05038befe62b8a88ddc58669fb0	✗

Host Behavior

Type	Count
Module	20
System	4
Mutex	1
COM	2
-	1
File	6753
User	1

Network Behavior

Type	Count
HTTP	2
TCP	2

ARTIFACTS

File

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
ca5751036a12d0a9fba5f2c6cd2bde61b9c40e1607f751c39212b9c9a94c6b5a	C:\Users\RDhJ0CNFevzX\Desktop\CUsersGrujaDesktopca5751036a12d0.exe	Sample File	71.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
461987b667938e313358de61e8bd2df8f32526 07e26c6a9e1919f432892121b	\\?\C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\InputPersonalization\TrainedDataStore\YOUR_FILES_ARE_ENCRYPTED.HTML, \\?\C:\Prog... ...LES_ARE_ENCRYPTED.HTML, \\?\C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\17.3.5892.0626\ka\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	15.00 KB	text/html	Read, Access, Create, Write	SUSPICIOUS
40bbbe6e0472605e0e9bae46ffe04f024a49e64a0b3e4ad6ee11074b1f4f5386	c:\programdata\microsoft\clicktorun\4bad322a-c043-4ded-a97a-6fe0c4412fbe\en-us.16\stream.x86.en-us.man.dat.b52a6cc8fb7587f444c47df3b494ea273d8cb96d932f5714f89deff12500af29	Dropped File	864.46 KB	application/octet-stream		CLEAN
a1bd59b3e4c2a7ae707306f0890710ba1e409b1819e74e512977c74b31726aa0	c:\programdata\microsoft\clicktorun\4bad322a-c043-4ded-a97a-6fe0c4412fbe\en-us.16\masterdescriptor.en-us.xml.235cc25993f000e992314636c73d2f41d20d3da3eabd72395d1453bbc11f9e41	Dropped File	21.85 KB	application/octet-stream		CLEAN
5e12d340e146d4543235a81c1824398be4a36731f9ed74d0b61aa726ce168419	c:\programdata\microsoft\clicktorun\4bad322a-c043-4ded-a97a-6fe0c4412fbe\x-none.16\masterdescriptor.x-none.xml.dcff3d82d1b1ed9ba78e08c4292caff1e455c7f588d712bcdfc010adfe95300d	Dropped File	20.53 KB	application/octet-stream		CLEAN
173298bbb1a7ce30dddfcc7c8928e86964be65961cc4b837feb453960f931e81	c:\programdata\microsoft\clicktorun\4bad322a-c043-4ded-a97a-6fe0c4412fbe\x-none.16\stream.x86.x-none.man.dat.6692d2404db80b31af2521527511e37531f5a60515884abcba3b987bd9f4023e	Dropped File	3629.45 KB	application/octet-stream		CLEAN
9c3ce8c404e8b62cb6ee9f0ea34b8cb8b0eed70ce3404d5073f6c1c5ce1d71b4	c:\programdata\microsoft\clicktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b16e-646f163a08e8}\deploymentconfiguration.xml.c55c4cc3386d39ca67b7efc99f2afe6a87bb3727d6f6448ec1ee2a52f08af456	Dropped File	614 bytes	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
693ee2ab5b37394ebfa09050d3db63e15548c7001cf14ae5cce1dde9be0329fe	c:\programdata\microsoft\clicktorun\deploymentconfig.2.xml.23e6e799bc481ccb75186b6f590bcd776071f6f17ea585a13ff58529fdc5181b	Dropped File	1.35 KB	application/octet-stream		CLEAN
44c0558310c71fb2e1c1caa6148277cf5b2c3b53e69f50af6cf1f32382a3cd17	c:\programdata\microsoft\clicktorun\deploymentconfig.0.xml.c2a50e74cbbce2d28d8fe1595662eb9da2e91d1b214115e0aa3f728475c0b167	Dropped File	1.93 KB	application/octet-stream		CLEAN
9d95b0a062dcbfb639fac620d2bd6a5ffa870cdfdada96c74c403538ba4dd967	c:\programdata\microsoft\clicktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b16e-646f163a08e8}\manifest.xml.f193705816e2ae5cabaef6c93e9ed0bac5d2803827239c4815dae903ec0ce265	Dropped File	4818.01 KB	application/octet-stream		CLEAN
9659782066faae704f6fa518551bb1b29b56cd24ba7b0943ea492b59f02eb716	c:\programdata\microsoft\clicktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b16e-646f163a08e8}\userdeploymentconfiguration.xml.612c781de413ab05b13d1571d3e4db38b349472b2abe56f096b1d8fcc9a8843b	Dropped File	614 bytes	application/octet-stream		CLEAN
809b25871a3974202f52ff8730f6fdf637b1f3fd8f55495eed220d40fe0797c7	c:\programdata\microsoft\clicktorun\machinedata\catalog\packages\{9ac08e99-230b-47e8-9721-4577b7f124ea}\{1a8308c7-90d1-4200-b16e-646f163a08e8}\usermanifest.xml.983e3b788a4dd401c68d88d8b1e8a17b56c5d03a4afce882ebb6c8b091a2ff0b	Dropped File	3024.26 KB	application/octet-stream		CLEAN
e58ded87e097f4fa7a9cde0e9bf20d9f9a18786f6a9b3bac309393e0c168ef32	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.access.access.x-none.msi.16.x-none.xml.2a9c2240c096342679b02602a32dece74f3578d36dbb1ae260ce679aa85d0822	Dropped File	37.88 KB	application/octet-stream		CLEAN
8e589010f0c056dfacda843ae06f85c8bc75c42dfcb76e9b86692f2e58c6c8b8	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.accessmui.msi.16.en-us.xml.af2903751d41dd605ac38fda596c6df6dd35ec61729dc97d1b1d0214737cea63	Dropped File	56.07 KB	application/octet-stream		CLEAN
bccea1ddfcb5862d41fca102910affc6cecce9bc04e4712341a14b66e32c34ce	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.accessmuiset.msi.16.en-us.xml.4f044cad89a1720c2bbd364bfc640c46283e6f9d419fe0a6503497d594b8981f	Dropped File	1.99 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
8f0299480bf6fe3abcd1c5e1e17b6841745d7362d9529e83516c968e51d3ed40	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.dcf.dcf.x-none.msi.16.x-none.xml.05abd055f321c1f455a19fcea61c49f0f03b7e9783890e5b8b5984881e3dbc56	Dropped File	16.26 KB	application/octet-stream		CLEAN
602f67f265df27ef33520d0e680860ba650d38855d6e3413fade78401870152e	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.dcfmui.msi.16.en-us.xml.9c7c59af708a7cf4e2811d636746b9151bfab3f62a1639e894f634e643bbc829	Dropped File	9.58 KB	application/octet-stream		CLEAN
5534b54e0223286ad5126cff42fcef6c0090a5b496a38fc0dfa5799b8be37a01	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.excel.excel.x-none.msi.16.x-none.xml.590bafd8023fb2c08b6388cb451778cbfb1efa7ecf92692804b87c1e2bd8700d	Dropped File	232.30 KB	application/octet-stream		CLEAN
77b2efd8459c34b2cc8ff6f3fa1d3ba76964d1075d44cc293c1e4deaeae62cbb	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.excelmui.msi.16.en-us.xml.bc8d2d3d21cdf40a5b8e9b04479ba396ee5fdca1dfe0ea74d8d66fe1fc4ed117	Dropped File	34.20 KB	application/octet-stream		CLEAN
b1c7953437fce049a6f1f0b73e6d166b4bc5fd2e8572feeac1e87a90d438353f	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.groove.groove.x-none.msi.16.x-none.xml.91a660c1ba58544296520fa26c66c31679b68677a2bc88692825baaee991b55a	Dropped File	35.76 KB	application/octet-stream		CLEAN
f79b3ba5fd137018ef98e8aeaa2b194683cc97a4b03c6ebf420feb73ee3401ce	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.groovemui.msi.16.en-us.xml.6989212dcccacf940f0432bcd84f46751cc637bb1dc297fd8ef1cb7450ceaf58	Dropped File	5.99 KB	application/octet-stream		CLEAN
693380edcc483d5e7e614e50761eb80078835753e77ff5c04e8c93f5cccdc7db8	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.lyncmui.msi.16.en-us.xml.6c9c72a264dfe42351ff8bd45dc69b215dc711029d3433452f6c233c2943086b	Dropped File	22.78 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
57f48823625c1a7c225d3e0d52e351d8f3d94fd3405596d9d892aa3256d54881	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.office64mui.msi.16.en-us.xml.4812f047be1161911fab8137a4df6a32bf0ac27ec6fb41974189f0e250f0fd25	Dropped File	21.44 KB	application/octet-stream		CLEAN
c2f4f6928c3f82fd9b1a1b94b86486b92785b29cecdfcac6c9bc0e87d9801058	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.office64muiset.msi.16.en-us.xml.6476b1f5c9ec68fa29ec3041285cf19575a68249fa9581078af2dfb6826ac864	Dropped File	1.99 KB	application/octet-stream		CLEAN
4552d566d8b33aad769834f753b68a8e9ea02769eef0fe78907d29f30766bf5a	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.office64ww.msi.16.x-none.xml.0d912e9f3b4b905333fa9c7a2b2595bd4015d2531e6002305bae24a17276280e	Dropped File	261.19 KB	application/octet-stream		CLEAN
1dff5ae828c1b29b846fa9642e6e4cc7735666febef144dbb56cb6cf45d8612f	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.lync.lync.x-none.msi.16.x-none.xml.16f4e381e48d0162ee67461a5365ebac257148c9ddb30ee640c0b7f823854914	Dropped File	87.46 KB	application/octet-stream		CLEAN
c10af5a9a86691bac38000735ea9330375f57acc971587d7da899635559dac4e	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.officemui.msi.16.en-us.xml.a745d989dd6e2fc25a95ca19f91ab53178330d83792361ab0a827b46a46020b39	Dropped File	104.38 KB	application/octet-stream		CLEAN
41d58630b35c4956e3b0238dcf009ab23fbf9b655e8c893fa6fa6dcfc55d4614	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.officemuiset.msi.16.en-us.xml.8d9a543b57f9b91d99262495d368e23f537bcf6f72a149400d163cc63de67b4b	Dropped File	1.99 KB	application/octet-stream		CLEAN
e50353624343f9e375e632f4832fe92e3e656428e77c1b01a625b4f4405879c2	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.onenote.onenote.x-none.msi.16.x-none.xml.ca57fc1d02a891435e52e4b359361a0d9e02a777b7d8828f53ee9e6472155947	Dropped File	93.70 KB	application/octet-stream		CLEAN
f0bb000e6bdd6b168e55c19f2cfe9439c206968200b10aebbb20a096fb80893b	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.onenotemui.msi.16.en-us.xml.a8395fba273611b3dbb7295aee8b422cae600be98512484c65e089b79c19033c	Dropped File	18.53 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
f8c9edf9883c04fdc32b3d82fe3688f0872837bf9b8b4b4938d694ee2c8bd8a8	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.osm.osm.x-none.msi.16.x-none.xml.de14a6f512e6b7d0661c204b0f85acbb4c15376e9ba608b18d470d8772ae602d	Dropped File	1.48 KB	application/x-dosexec		CLEAN
196bf07c5b0c7f6c37480 20a29a0c988871fc2840c95ac0f7d1b22f544c79a27	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.osmmui.msi.16.en-us.xml.e305005790b2be59e81a8183ace8e67ba5253af8a80207c47f3f014324edb026	Dropped File	10.77 KB	application/octet-stream		CLEAN
8d3aca4ef0c28e8b68364a7af323c916ecd287535ea1dccb876c70190afddf80	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.osmux.osmux.x-none.msi.16.x-none.xml.3aa7c3f06c702f5c1ebe88ccbb16a8a3a4dc5979cf70798fca87ba6392d8542d	Dropped File	2.24 KB	application/octet-stream		CLEAN
b22d03bec913823674ebc33585e27d19495274 8a3139044f50fb0d8efd234530	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.osmuxmui.msi.16.en-us.xml.ede9707dd16e2f753267c83192ed6df43086dbf39dcfbbf303747cc7e705236a	Dropped File	9.65 KB	application/octet-stream		CLEAN
90764c5ece1a3ea4d4b1096b155773918988c60259acf10607384aa1f4152990	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.outlook.outlook.x-none.msi.16.x-none.xml.56538ccb850b5f89a694f1c43c2f98f716ea047b025b9ed24d6a55d0ec90f40f	Dropped File	91.15 KB	application/octet-stream		CLEAN
70e994d66184b068cdc82a1036f240e22f11df8a5c4402040a65fe4008a342a9	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.outlookmui.msi.16.en-us.xml.893eb23ccaf9b37c110091634df95e35230584572330b8022eeaad03fad91054	Dropped File	94.19 KB	application/octet-stream		CLEAN
9306737e6c48629bfeb9b9921dd9c6cdcc5c6458af67d0ea5e70c7d3fbbde874	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.powerpivot.powerpivot.x-none.msi.16.x-none.xml.e5889a30dd02959d351cff516a75e662aaed86dfb860c5f8d98972dbf4cc6236	Dropped File	695.23 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
ea5ba8323386547dc3ef2dc49bab9a3e1ce246f2601efe1a8f1fbf785c83a2cd	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.powerpoint.powerpoint.x-none.msi.16.x-none.xml.7b83b07f21609a71a3fd4235e905a472d194facebb3a0c15a454b45a3191817e	Dropped File	100.36 KB	application/octet-stream		CLEAN
a75fbf2fbe4694e5e337f1363e6881293172129a7b67bce3ffc5e375275961e2	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.powerpointmui.msi.16.en-us.xml.d3c8529ff6bf133eb9067bb9985d30a31728cf37e0c37803f1991ce4feda6b19	Dropped File	26.08 KB	application/octet-stream		CLEAN
c20e8bf736eaf4876da6ec7a7d61a10df9d2c134303529421 96e072ddf02b8ba	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.proof.culture.msi.16.en-us.xml.c20683c0006d2655f4257ab56ba8b0480adb8a138ccf3fd50cd0f3712dc70378	Dropped File	24.86 KB	application/octet-stream		CLEAN
65b46ce4d78f2bbedcef648a1dd4349447bf98a81b28af7938fb8a3cad798673	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.proof.culture.msi.16.es-es.xml.3ac02768eeea551ace188a88e79694b27effc72b1dd8004ee55dc60f3c5e5439	Dropped File	23.91 KB	application/octet-stream		CLEAN
44c2182e56ff421b1e44f01c5c43a091ece9cbbff2e8365b46034f3ff64b15da	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.proof.culture.msi.16.fr-fr.xml.a3d40fc656f90e65046dfc37d8cadb1300eea7404d69de8b1260ca70bdb23f24	Dropped File	23.91 KB	application/octet-stream		CLEAN
2b7e1b1afa7f67c8efa9608a6da53e860c5253da2ae23f50a7381a593031e4a9	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.proofing.msi.16.en-us.xml.8e5e7fdbdeb1019e1f1af327d35157db6b530430404bcb0ee66b08bbda398cd3f	Dropped File	1.99 KB	application/octet-stream		CLEAN
cee350c6de9246486f9cf5193da281009bd1cbfd6c5dd2cd4243e484177f9caa	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.publisher.publisher.x-none.msi.16.x-none.xml.e3f9b213894f112b0c01978ccfcdf184d4e01a29bc765ef8f5403d6f08a0087b	Dropped File	75.36 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
a6b97219ab7c1ac0f428f1693d48875e9d6eac34774840d3287f5e2b772a8248	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.publishermui.msi.16.en-us.xml.c16446b4e80f2ae98978cf024444cf109316d036d8758840ba3ef6481f259c7b	Dropped File	13.76 KB	application/octet-stream		CLEAN
d24c084585e6b79489a3cdf276e390b53f9b8abfdce864c7a3bf7893843998a9	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.shared.office.x-none.msi.16.x-none.xml.4f944e8e1926bb94c9856018047341d9f95e4edde0201794e12796a3b149ad72	Dropped File	683.05 KB	application/octet-stream		CLEAN
b1c6faa3577b848a30068cbe8c41cae3e4c74efec0b94011049c04406f1bb596	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.word.word.x-none.msi.16.x-none.xml.3934b8b27d27d3fcdb3151ac44d67db926a7b6fbe41be8629ab21c9ecfe2a735	Dropped File	84.63 KB	application/octet-stream		CLEAN
37be018c2d5858f88901edbeb8b968864981f85ff4801cf32b278e782164a4ff	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\microsoft_office_officetelemetryagentlogon2016.xml.fe211bebbdcfbcb19ed6fc1a41ad899e6c78d6e16775cac1d17fa61b0c4a9e74	Dropped File	3.17 KB	application/octet-stream		CLEAN
cb4053b9026837b80d5870f387ddf022423870bc78a5a07b4c401256b9cb37ad	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\microsoft_office_officetelemetryagentfallback2016.xml.0ffeb1c1b8d79e252d2afb77165ce2747e060017e160d17d37a0d16e33b83205	Dropped File	3.24 KB	application/octet-stream		CLEAN
e42d07f77e1e395a67627e001a450547d176dcd11846c59f2e1bc63f4dcc99b1	c:\programdata\microsoft\clicktorun\{9ac08e99-230b-47e8-9721-4577b7f124ea}\c2rmanifest.wordmui.msi.16.en-us.xml.91b947d80728256a3e2232cdb309e0088fa5a46db724dbceef51eac0d42f6c16	Dropped File	76.03 KB	application/octet-stream		CLEAN
d73bf6776bb585839c4af833d1b9264cfb63280dcc023521f093349fc8019300	c:\programdata\microsoft\identitycrl\production\ppcrlconfig600.dll.cd14c12384a0f27fad30ccea50ba446ff3b2760079076387e2a1d21f68b72900	Dropped File	33.69 KB	application/octet-stream		CLEAN
aa7672b4af429f1b3ba4f77ea43854ac23c857a3ed3ef709b7cce78fee4dbd6	c:\programdata\microsoft\identitycrl\int\ppcrlconfig600.dll.9b76d51a5e286ab163f5a241f643dfd3efb2a387f1728d50e87158ca69cf1767	Dropped File	23.71 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
641eec700095792ebc6789f663dbfe24a2adc151a992ea1e90743a43fe122723	c:\programdata\microsoft\provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\customizations.xml.e9452abce27219a7f5efa7067eabeb88371a626c6558fc4b1a0ed15b0fb8756	Dropped File	3.64 KB	application/octet-stream		CLEAN
4576910171305b8263e3a2e3dd337fc14c95ac375d285161a5126878ff0ce06b	c:\programdata\microsoft\provisioning\{18dcffd4-37d6-4bc6-87e0-4266fdbb8e49}\prov\runtime.xml.0e7a4551c407f4b9b53a3f7562f5d06c94161d2e52e85cf88476a2b8e71bc71c	Dropped File	559 bytes	application/octet-stream		CLEAN
1b82b28548792f90656a2c811440325799b0c0156b3b020dbd2305ea19dcc0da	c:\programdata\microsoft\provisioning\{1e05dd5d-a022-46c5-963c-b20de341170f}\customizations.xml.97868653c4bd6b54e148f197b536bee7f241ed3aeb0dd6e6706a99afa0011038	Dropped File	1.23 KB	application/octet-stream		CLEAN
4157c41bcf179ac7b8971a8e82874e5a2dc6f1f75907be3815862a9d49775ec0	c:\programdata\microsoft\provisioning\{23cb517f-5073-4e96-a202-7fe6122a2271}\customizations.xml.3937f94e11b3568aec37edcbcde859201ba8fa9123d01dc11b499ef133de3f3f	Dropped File	5.40 KB	application/octet-stream		CLEAN
12d41e168dcd787bdf44a351cc4e9a4e5e13ae267920eff6ec1315f48330b0ca	c:\programdata\microsoft\provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\customizations.xml.138e6cbcf435fddccd4fcfabfd8fa7f8200e39554849e0aaca98fbf772426a02	Dropped File	6.38 KB	application/octet-stream		CLEAN
928b831f6643f7630f6b76813763074c944c67d2cb9d10ffc39afd79d7206461	c:\programdata\microsoft\provisioning\{3742e5e8-6d9d-473b-99a6-8ecc0f43548a}\prov\runtime.xml.e00a73b9f049acdb9c2c2e20048a6ce8795a662ea603cdb17bc7ebf9b03c6372	Dropped File	579 bytes	application/octet-stream		CLEAN
ff225dfc318803bf275e207911d9fee80f199db0df466602f8a6b037aff780fc	c:\programdata\microsoft\provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\customizations.xml.29eef47def9fc159363b83176a127fe9d31ff7607f81e6b741670d86d4a68129	Dropped File	7.80 KB	application/octet-stream		CLEAN
070aa570139043ae61f180a75f973bf767948bba9ff19d5a650cdb3afe283df6	c:\programdata\microsoft\provisioning\{8fb7d64e-70fc-4f9d-89ee-d486817534df}\customizations.xml.24573de981c0717b812b75a2ceb24250474c6f059bd938193ed15754443d1b21	Dropped File	875 bytes	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
b0e75baf8208c8b08b769c37ed833c619aeefa550a9727405ff80c8fe8de2c2b	c:\programdata\microsoft\provisioning\{99b095d8-5959-4820-bea7-7448c8427b4e}\customizations.xml.94f5fefb71ade4e241d82cb4057f0ed268b2ec99ea6d0d9918db88393dfc8f2a	Dropped File	2.17 KB	application/octet-stream		CLEAN
069f349e6fc4d95db5893be709d5d32c1a5e0b3b7d23a208189d7c08ee5563df	c:\programdata\microsoft\provisioning\{7a30a9be-737f-47a1-a541-6e7b0761ed19}\prov\runtime.xml.6aa9d8602584e7ee923656f3ff25311fe9171749b03854a8a76c810deeeadf4c	Dropped File	555 bytes	application/octet-stream		CLEAN
6875042b18646735ea106c7dcc7a3bde9da962b08d1c9cc2280bcdf401384854	c:\programdata\microsoft\provisioning\{9aec5bda-1e87-46b3-bb96-1a01c606555e}\customizations.xml.74702a6d3cc5bfe65e66cb9f9a1d8f1061a30044752fcfd1e43eb8843a3d4f7b	Dropped File	7.17 KB	application/octet-stream		CLEAN
72f0b053ff05014cbf523430389568519841d15c863be383b9eb45364d92ece1	c:\programdata\microsoft\provisioning\{9df6a4ed-fc16-48bf-8b24-6e2ad2bfcfea}\customizations.xml.a20e1b14e1aa84c10df5703feb5bdb1146185819bbb9132d109490faab168a7c	Dropped File	3.28 KB	application/octet-stream		CLEAN
abb2ae1e5e118527dfc18f9426a8a7e4474ff77f79cbf9465a828cc8aa1dab3f	c:\programdata\microsoft\provisioning\{b0b9123d-7d7f-4c6b-9973-ceced46f2a09}\customizations.xml.5de914bbc4f858ba40e268dbeed7326c1eefb74f7ce073687fb876503a916c48	Dropped File	2.16 KB	application/octet-stream		CLEAN
bce5e29f25ba48e553ecf4bec0fd0f5c9fb6970a4237bb93ce74d32cbbd7235e	c:\programdata\microsoft\provisioning\{c5dc3753-b6c8-4057-b396-bf13d769311c}\customizations.xml.1a2ffef383cf6c4fa82be7ff8229eb81281cadd0e9878668836f8842302f470f	Dropped File	1.60 KB	application/octet-stream		CLEAN
6b57aa5c0532e1e132bcd14f14f08eb1c8eb078e99e49fc2f2705c52e25a3576	c:\programdata\microsoft\provisioning\{ee4aac98-c174-4941-82b1-d121e493e4fb}\customizations.xml.5a652dcbe919f507e7aa061c376886c457f27af57e0aad12a6af4ede7a11103d	Dropped File	1.78 KB	application/octet-stream		CLEAN
a5dd6cbe9a43c943489b3b501261a02a7b4f04830c485cf9b9b1277cfa937ecc	c:\programdata\microsoft\provisioning\{f11899f2-71ec-4621-9997-e17ae2f6eb26}\customizations.xml.3c3777e125ae6a2a4cc36296c2a12e42ee436c89853fc88c99b08da8cda2e24e	Dropped File	3.41 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
d5bea3c2dfee2aba38ce e1bbfd1cba98154656c3 e1e8e6e1a32bc44ca38 b26ba	c: \programdata\microsoft\ provisioning\ {fc01e91f-914c-45af-9d7 c-0b2e5fbedf62}\custom izations.xml.e817b911cf 4e9b462c2f3aa22dc733 f3e56499826724160357 a4eaefc4ca3535	Dropped File	27.68 KB	application/octet-stream		CLEAN
2e9dc12f3d2f773cfe5f8 07d325c9d447c7c204c6 a14ad2c256f024894919 8fb	c: \programdata\microsoft\ provisioning\ {fc01e91f-914c-45af-9d7 c-0b2e5fbedf62}\prov\ru ntime.xml. 2bcbe6422fdef6778dc2 ab1b655d664513b2ee5 e2f1745751dcf7d02c46 4026a	Dropped File	1.46 KB	application/octet-stream		CLEAN
f6bda55448e20953695e b949fbf62e7d6e1872ce 63ee4a5c67083df2fa8d bb67	c: \programdata\microsoft\ user account pictures\user-192.png. 6c1f84d131bf31daee64 09a8027eab66dbe635e 9a401ee46dfb60fb9a57 4e425	Dropped File	2.35 KB	application/octet-stream		CLEAN
264be192a1f63e3b381e de1f676eefdf15250ceb3 d8c231c5f5b8158beaeb 10e	c: \programdata\microsoft\ user account pictures\user.bmp. 08510f7314c2c923a183 d099e21d05c5c328240 88aed51ecd59560ba76 c32a76	Dropped File	588.05 KB	application/octet-stream		CLEAN
9c214e38d96419b439d a2799ac97a98c647ea0 e212f56cb5672da22fc2f a923a	c: \programdata\microsoft\ user account pictures\guest.bmp.c2f6 6f9290edaaa108cdcc3b 5cb4ed9540f486e1f47c 6d3947b7bc92d5f32b62	Dropped File	588.05 KB	application/octet-stream		CLEAN
7e004ba7f647c917250ff 11936c4ea7b0453e13fd 477504b7ba7da1278de 28fc	c: \programdata\microsoft\ user account pictures\guest.png. 011d5b71ce830f11a020 752fbb93997dd6b43f9fe edc842f34017a6122497 219	Dropped File	5.27 KB	application/octet-stream		CLEAN
72e1286ac5b759f9e8d2 7fbe28af13576b113497 8aae3da3dd75b0d1b9e 47719	c: \programdata\microsoft\ user account pictures\user.png. 5704c4fb9a0a8563132c 56988d69aa33f75c7e79 c3b3b12ee1815ac0222 58c69	Dropped File	5.27 KB	application/x-dosexec		CLEAN
12b1b83a698bd93d7c8 6f90932998a66f0473d3 d70d480566ca2de30c0c b7cd1	c: \programdata\microsoft\ windows defender\network inspection system\support\nislog.tx t.b824a17ccb8b0cc3265 c20d409ead7097419d2 2024a6ada953ce59e74 8dd614e	Dropped File	25.18 KB	application/octet-stream		CLEAN
ad9957a994b7742e3a8 c03ab95de1b51ac0e14f 33ae95c439dd19117a6f a53fc	c: \programdata\microsoft\ windows defender\scans\mpcach e-9899dbe4d8bb3d253e b4f285757bebaf1581b5 0f.bin. 3f22c47bd587bda83088 1836dae47518e8ae9e7 8dc24686f6632c1daf18 e2578	Dropped File	10240.00 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
6e12aae48d7ab42306a981f1ae759335121b5e53ee0dc99ce52a2984ed0a605e	c:\programdata\microsoft\windows defender\support\mplog-02112021-121950.log.1a4c5916f0518d555c60199e08b5a97240a621e94ac1fe8b301d6767a405bd1e	Dropped File	1.63 KB	application/octet-stream		CLEAN
2e42b6f608984b9960d7d60b7fd728acdea4e0c326d9332399305f7d15d57755	c:\programdata\microsoft\windows defender\support\mpwptracing-02112021-121950-00000003-ffffffff.bin.ff89eb2a750463235aca5f84805aa0fd97f8d489e6388faa8cb0f4770fe55e3d	Dropped File	36.00 KB	application/octet-stream		CLEAN
9cb1da2b3466d8652726c885baca367de5ee20cc4aa1353f5dc6790256b1f229	c:\programdata\microsoft\windows defender\support\mpwptracing-02112021-122238-00000003-ffffffff.bin.c97c08c5bda6ca20873d7eb27e5cfed4f374d9dd26c9a5a951d757782ac2c875	Dropped File	48.00 KB	application/octet-stream		CLEAN
592597a6c2381ed0834bfd208c49b82ec2ccd02d991c8536deca554a21aaed29	c:\programdata\microsoft\windows defender\support\mpwptracing-02112021-124618-00000003-ffffffff.bin.8434dbd73a6948fe33dba00a9ae02277b9ad7a898cb48318541cfc111c5f785f	Dropped File	4.00 KB	application/octet-stream		CLEAN
e04c0d166adac3d8824c8dc74acb6a6a7843ee26fc45bef839ab6b653f722d80	c:\programdata\microsoft\windows live\wlive48x48.png.0ba7776161bacf351e19eb9e8bb544cb531eac342681bd97dcc39bab5d6c6d69	Dropped File	4.55 KB	application/octet-stream		CLEAN
8afa07c0389862d0122a30c67493c99af9683eefc923ca78dd47d31541130d50	c:\programdata\packagecache\{0fa68574-690b-4b00-89aa-b28946231449}v14.25.28508\packages\vcruntimeadditional_x86\cab1.cab.1f7353b686bb3874b7dcf70d397a2d391b0ae5183f7ba5d8c07c2dcdb0caca2f	Dropped File	5088.92 KB	application/octet-stream		CLEAN
ec7498fcef87e799b79b9b0963e43e0184a28409ff160a1e40b8b444700aa5d3	c:\programdata\packagecache\{13a4ee12-23ea-3371-91ee-efb36ddfff3e}v12.0.21005\packages\vcruntimeminimum_x86\cab1.cab.8396badd3288d9fb15cea45161384fc4d4dfa16042c2b7758a8a04d31cd3ed62	Dropped File	973.69 KB	application/octet-stream		CLEAN
07016764f909ebeccab7e4376a66501f70e04bd4631a8de0999c16da95d0b1a5	c:\programdata\packagecache\{2bc3bd4d-faba-4394-93c7-9ac82a263fe2}v14.25.28508\packages\vcruntimeminimum_x86\cab1.cab.e01fda55bbdced16bde9f8cf62cbb915e0e79fd1d7f1623e421faed1ffb1d436	Dropped File	1335.61 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
3f44aa7692a02689f227f6f3b8d97ce18be91797fdbeba386510d2677e073df6	c:\programdata\packagecache\{37b8f9c7-03fb-3253-8781-2517c99d7c00}\v11.0.61030\packages\vcruntimeadditional_amd64\cab1.cab.f73c8dadc880fd3e1f1e1ef8b3dea54d938bc56f338a80bea0ab60c31fc77243	Dropped File	5664.29 KB	application/octet-stream		CLEAN
0b74f780f578b4575685befe815cc6727efc175787 04c7a71d0d2cc1c1bda1655	c:\programdata\packagecache\{7d0b74c2-c3f8-4af1-940f-cd79ab4b2dce}\v14.25.28508\packages\vcruntimeadditional_amd64\cab1.cab.70d1f2f7401e527306ec818f9ed326093c55d49b04d4a3c68b5c9fc28a951b03	Dropped File	5500.25 KB	application/octet-stream		CLEAN
90b11ecf9b7e153f1591b0d1b2bd74681a34ccdb59585ea6097e1a22952d5cf9	c:\programdata\packagecache\{929fbd26-9020-399b-9a7a-751d61f0b942}\v12.0.21005\packages\vcruntimeadditional_amd64\cab1.cab.99ed2c9fac46b8eb309bbbf1c555ed0250f019498554c787404d841e847a154a	Dropped File	5457.28 KB	application/octet-stream		CLEAN
48dfb90d861dc5276b80ae4e307cf17a1c4bba2537423ec2c809f375ba3d9f6a	c:\programdata\packagecache\{a749d8e6-b613-3be3-8f5f-045c84eba29b}\v12.0.21005\packages\vcruntimeminimum_amd64\cab1.cab.543182c5b310aabcbb8805b614e14164430caa1da63d19b807ceb35ae10de67b	Dropped File	1010.26 KB	application/octet-stream		CLEAN
460288d18b225cbd0420682c0920c8e808b06d8895deca3798b2753273727474	c:\programdata\packagecache\{b175520c-86a2-35a7-8619-86dc379688b9}\v11.0.61030\packages\vcruntimeadditional_x86\cab1.cab.e5b0ec829362a8a7929d2e88c163b79fc4e0f0e3f6630f06e2dd2ef16d672146	Dropped File	5033.02 KB	application/octet-stream		CLEAN
ee67b06dabf3aacd0290ac76a5251efc6429bc485dd0c107697e2705650f14d5	c:\programdata\packagecache\{bd95a8cd-1d9f-35ad-981a-3e7925026ebb}\v11.0.61030\packages\vcruntimeminimum_x86\cab1.cab.b52d1c80c438b58bbb8d0842a00b13fa192a823d99581f508317b2b31b31257d	Dropped File	802.42 KB	application/octet-stream		CLEAN
91a37f6e640dc9fd419211912f8670dd025e8291357daa572308e6d393bc6695	c:\programdata\packagecache\{cf2bea3c-26ea-32f8-aa9b-331f7e34ba97}\v11.0.61030\packages\vcruntimeminimum_amd64\cab1.cab.40ade269cd14f5566b1db6a7dabe010fc0a121e8df896be75978ed36b4809f0e	Dropped File	790.79 KB	application/octet-stream		CLEAN
9829b21a6a374bfd9aed90ef443a5cdaaf786e3f8666f14d494d21ba1eb0e741	c:\programdata\packagecache\{eea66967-97e2-4561-a999-5c22e3cde428}\v14.25.28508\packages\vcruntimeminimum_amd64\cab1.cab.8c2cb4e0b6fefac3bb1784c017e1373e18db85bb9214c700dfc97826c9f4e40e	Dropped File	1473.17 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
42745f423f5d2ddc7d327bb17bc3821c33843df93b99e6258ad862d58f63ccee	c:\programdata\packagecache\{f8cfeb22-a2e7-3971-9eda-4b11edefc185}v12.0.21005\packages\vcruntimeadditional_x86\cab1.cab.7eebd4de2f6238176bd6035c992fbdd08f9f5ec6f80b25a681125c2706cdcd5d	Dropped File	4817.28 KB	application/octet-stream		CLEAN
3d35dabef1dca85c0eb14ba6023656b141293fc1abaface5ba0c3d3a67cb9252	c:\programdata\usoprivate\updatestore\updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml.1a710b472d26ea7721ea0fc24883cb9acc6fd80feb948210dc4390e38861a569	Dropped File	841 bytes	application/octet-stream		CLEAN
ea3035fc54ac9cff6d47ded10e68eeb096a166203d37745a4dcdece59e4c5714	c:\recovery\windowsre\reagent.xml.7e9351c75abc89171edcac2661535183a40101c38dbca40e308f06aa72f16b45	Dropped File	1.02 KB	application/octet-stream		CLEAN
418af71aa144929540e9d479db04e14e428fc1417c0784ab7e2d0947893cedc1	c:\users\rdhj0cnfevzx\appdata\local\comms\unistoredb\usstmp.log.1ea48a96286822a552fb4f0bb2e9debc68ea719a037d250e70f634362ccd9d46	Dropped File	3072.00 KB	application/octet-stream		CLEAN
815cecddb8c7b55c6386840c31e683b63c2dfd263d17bcb8f78784a761ec892a	c:\users\rdhj0cnfevzx\appdata\local\iconcache.db.6c4ef3f63a79fecf841c1d432bbdd76f26077f23cdecf39cc98b9f6190c4486a	Dropped File	17.53 KB	application/octet-stream		CLEAN
fe14e4389a563b12b5df29d691c1a6842d215dca3d286b8460f8ba0328b2ab42	c:\users\rdhj0cnfevzx\appdata\local\microsoft\clr_v4.0\usagelogs\powershell.exe.log.bc1f46ae79d3d85cce7cdf85cbd0c51375a536c8d6494ba92f54b9a316d4bd53	Dropped File	4.26 KB	application/octet-stream		CLEAN
2d6df2c9721b57475ca4ad6b52e50f81a744a6fa0f9c360ca62f1014af6c1902	c:\users\rdhj0cnfevzx\appdata\local\microsoft\clr_v4.0_32\usagelogs\powershell.exe.log.858648c8c4db1bf3e6244d3c5620f02560cdc706e5ad53fa4bed6acc27c6c15f	Dropped File	4.12 KB	application/octet-stream		CLEAN
35cd16a04d1df90a88ecaf52463fe3d677252fe4fd0b6701407a40a12be0903b	c:\users\rdhj0cnfevzx\appdata\local\microsoft\internet explorer\brndlog.txt.e72c710c8ccad84aa1131a2a0332a4ac2b40040fd04ed6c7e3975781cdc4b94d	Dropped File	6.42 KB	application/octet-stream		CLEAN
1c7f35d991cb352c765c199d420bd5597b8a85198a9f7ac8f1dfb2ad908d1644	c:\users\rdhj0cnfevzx\appdata\local\microsoft\internet explorer\iecompatdata\iecompatdata.xml.ca74f08f019fdbe2512a43c4ba8ef92d79647233582e5a64a42b9645ac790c7d	Dropped File	3.02 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
d3fe2227b2b0ca46470c4cd9498ec3074255909137485f0c424423cc0e03101d	c:\users\rdhj0cnfevzx\appdata\local\microsoft\internet explorer\ie4uinit-userconfig.log.3a08029a2e82788d5f00470e3bb18b94791ee7b24991ad65d0ac0ca4c7963b27	Dropped File	1.27 KB	application/octet-stream		CLEAN
bdbd479ed68f3df0201016e8daf91643282eb80c93c1734b6bfc04f6e161a5fa	c:\users\rdhj0cnfevzx\appdata\local\microsoft\internet explorer\versionmanager\versionlist.xml.162099c1f493aa7e611a6d6ae7c1e8ed2addba5492506ab7f40144044f156e3d	Dropped File	15.90 KB	application/octet-stream		CLEAN
51e7aeb0dd33470600f3c1b851af5d776496ebcd98194277155a6ddb798489ab	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\16.0\msaccess.exe_rules.xml.eb24c68320bd147f7abef64f57d9d30c026cad7512037c422b777f8216131f5a	Dropped File	71.25 KB	application/octet-stream		CLEAN
f624e5e88cf80b3ab4cbbf8a4e3882b36440d3b3e101a84867758fdb6e2979bb	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\16.0\officec2rclient.exe_rules.xml.34fcb489563d3dbf4d8b74585ff0ff5d8dd9dea074ce8cf7b0e01022c2d49554	Dropped File	16.08 KB	application/octet-stream		CLEAN
4eead142cfd18c80e13aac4d12aa6a38cc45870148abdde3f49fed6facb6e54e	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\16.0\officeclicktorun.exe_rules.xml.01a4ff285ba8a6dda6129ddddeb96539d76518e76c396e248a678a68146e89d2f	Dropped File	16.08 KB	application/octet-stream		CLEAN
cdc42ab7dd3219b52ba574dae3c501131a46c74195caad5a5150d390c5c25730	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\16.0\outlook.exe_rules.xml.801fdec0b61644273809f6887baf72a0357525716d4bb5d88d7de268d24bc41a	Dropped File	82.64 KB	application/octet-stream		CLEAN
5d978631eb52a8a1752a1ce74d6c189f690200480891ac02085a96a7e0bd4200	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\16.0\powerpnt.exe_rules.xml.6354c0804f150aaccf920416ed8610fa1015a8456a191da56a57babb60bfe361	Dropped File	75.06 KB	application/octet-stream		CLEAN
e164eb8be6c58caf2415056c3151fda28f5d8c3e98e78e2f253ca6036271d86b	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\16.0\setup.exe_rules.xml.e90f43c6b7bd6398482744171df3ed365b909aa2d8c7f98fb4c9d32437c17871	Dropped File	308.67 KB	application/octet-stream		CLEAN
0abc35917e6d0ae3e06b2eec0ebd2d146aac117bd88bd6839d748a80f16dcda3	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\16.0\setup32.exe_rules.xml.666578f634783abeec6a70c047a32bbb0c2c1bcc22bbe7ab27abe7d8fc738822	Dropped File	16.08 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
f0416cb0d3256eb9fc3ae5f815cb53d0a751ff68f7923fb86c822067c499c494	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\16.0\excel.exe_rules.xml.ea75fa454e9fd85c909c1a4202ffe983acd601aa1e8a9dc03557280ecc087e24	Dropped File	78.44 KB	application/octet-stream		CLEAN
fe1aa90e8b0bd3fc8a5196e8f769dd2dd32f90ea333fa990c8e4caf5701bdd97	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\16.0\winword.exe_rules.xml.f00520072be99102d8075d7a127e439599cc485247ae3ec11e890ef8b6702120	Dropped File	101.96 KB	application/octet-stream		CLEAN
1bc3d1a3c1ae237abf7e3e002d9bf5bc0dbd627da05d9a4b8c9f9ade90d620ca	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{530fa225-a741-4103-8238-7b3d9de36f28} (0) - 3596 - winword.exe - otelemediumcost.dat.76d8f8b328e0b6b8bce1c39a30f5fe13cb5a64a62d560e2123e5715a56df8975	Dropped File	845 bytes	application/octet-stream		CLEAN
b01d1715b60075f4eeafde5e2d3cfabbb81cf68faa16fc8fc922df154767c916	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{09178d66-ba92-4de3-b96c-2b24754031bf} (0) - 1840 - msaccess.exe - otelemediumcost.dat.e543329e8e30fcbfeb127b29f50e6a0007349f3b67bdb4eebfdc24e11b628101	Dropped File	849 bytes	application/octet-stream		CLEAN
4a13604dacf3a8efdfe244bcc70a814288044085 9529049e9adc007002645175	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{c116fc9a-b698-46de-a139-0bd729ca72f1} (0) - 3756 - excel.exe - otelemediumcost.dat.6afff073814879a89fadc5e0421c75eb91ed56e3d66683af87ccaec51934970f	Dropped File	837 bytes	application/octet-stream		CLEAN
adac671757b7801ffb4d1d598571701c962efc235fef70f87f4c22a3f040a19e	c:\users\rdhj0cnfevzx\appdata\local\microsoft\office\otele\{4d44c03c-ceac-41b9-a9f9-31bd04be84b8} (0) - 540 - powerpnt.exe - otelemediumcost.dat.3efd50aab9bd29650e2b4b43f843620348edd4ea65fcf4cc19068ff0633de774	Dropped File	849 bytes	application/octet-stream		CLEAN
d5bb4eda48f7b2f3ad50a4da3f026f358b813460235f54862b9b65a6e304af28	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626\autoplayoptin.gif.19cbb8569e4470519cc469a0c7e1c838650bd5d0c89a3fdc640a062ce8d3ba2d	Dropped File	374.24 KB	application/octet-stream		CLEAN
debe1c6b5c2350e9998a77202f87e50b9634983dc65248f8b987b0e250d72fac	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626\autoplayoptin.png.ae1f0887ef2a1680493247997eb1f49fb58e53dd5e2b35d389c8c49de3bd072b	Dropped File	9.99 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
3cf02dec03b7bc10aeb961c2cbbec0372d3b661edbcf3b7d3444bdaf1d7e102e	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626\autoplaylogo.png.3369bed176cdc0ae2865f952ac52784107d9abd9448f414e613078bb6cf3f32d	Dropped File	4.56 KB	application/octet-stream		CLEAN
402249c527693e5a1335682841ff87b77f096d188e2bbc598f787227323cc34c	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626\collectonedrivelogs.bat.9540d5bd726eed8bd33a6f04eecbf9de248d9584ac335ba23d05aa8f35424821	Dropped File	5.71 KB	application/octet-stream		CLEAN
a96f6b2f27079f33acb3b2e6fe6ae0609d732bee3f5de0fe87a1be1169361e2b	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626\exclusionlist.xml.a0ad0d3da8f00b4bd56970d29632ac8f6e8ab990cc68e2083c3517d114921e18	Dropped File	19.59 KB	application/octet-stream		CLEAN
9a88a6235fdc60ee9c0b2e73d464ba40f957e72bbfd670234772cd12496c44be	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626\filesync.localizedresources.dll.943d6fb3b1e5cfcdde88298dae80fcbf95631cc38f914d48ca5272772bf34d2f	Dropped File	80.19 KB	application/octet-stream		CLEAN
8901ca24dd78f883644abb4c3e81f69056b65537bc7e543d2cf024788624aad1	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626\etwlog.dll.a431ae2ea457ebb9cdfd27af385ce2fbb0a3706ffd280e6479bb6ed6a2555577	Dropped File	28.69 KB	application/octet-stream		CLEAN
cce5dfcd63ceac59cba91a5ac82f99f7d1831c9a3cada135a480be1828eeb198	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626\filesync.resources.dll.d0a9e4bf07e5c2fa4965bf89fdf245ee4b58ca9db052cc8aab0e70c2f5e2012f	Dropped File	992.00 KB	application/octet-stream		CLEAN
a8e423084c6a51a06010706177e74b8cb8b46a28d87e65ee0f9a68e0936913fa	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_1\autoplaylogo.png.7bb716a615a0daf6f7d73a6ba6794fa8ba76523f49b97cb2bc02c63768e45310	Dropped File	4.56 KB	application/octet-stream		CLEAN
e8486ce47c598284a68f80c8a23c816d6643f54de2befc8201e6944e277177cea	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_1\autoplayoptin.gif.85f618b9046aa721673c61c07952cd7ab74912c0eaca1b5d46963f20292ca20d	Dropped File	374.24 KB	application/octet-stream		CLEAN
4c47906e94271e55a3a899247e0845b26ad2007137c97884baf1612c0c80322c	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_1\autoplayoptin.png.767d75c9248d2e28a98220017f73acc430b259fef7044d0d208154456128b3f38	Dropped File	9.99 KB	application/octet-stream		CLEAN

SHA256	Filenames	Category	Filesize	MIME Type	Operations	Verdict
a873777146bf138212f0359fd7daad43fae985999d069ea03f8cd924b0170baf	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_1\collectonedrivelogs.bat.27a1174e79f19ac8efa02aec0a385e70bff87e0556d5b7989d63ee67a3205f42	Dropped File	5.71 KB	application/octet-stream		CLEAN
fbfbb6ae15c2aa76f964b2de5a9f420d81b936a7e8ec4eab0d5bbb6356c858eb	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_1\filesync.localizedresources.dll.eccb7093e0b0c3e67b667bebddd7eb89c9de058707b074566bbd29df4d278707	Dropped File	80.19 KB	application/octet-stream		CLEAN
5a6a65d56e2cdabbb94986fc62f82bf3d7dc9d0673a2adcfb8d4676b25c7ad8	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_1\etwlog.dll.d4efa973844e6624f8bb8942af8cba161bf4c2a756509a973687397bf5a9a605	Dropped File	28.69 KB	application/octet-stream		CLEAN
7d3b8d9815548cdd47bc74c3677a772a5e24e8c34a6644ce13d06fb331567c93	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_1\filesyncapi.dll.e76705295dfe1132012760acb42cc6102f0a9d52744d6336d1a8f52d240f8929	Dropped File	216.69 KB	application/octet-stream		CLEAN
a59931a13bdcd7f82e891abf1139dec4837c294c039a3a33fc3ec11a11536166	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_1\exclusionlist.xml.5c17bc5c69ce29dbd1a6aad2e394398f310beb159ac340f413409a035172bb4d	Dropped File	19.59 KB	application/octet-stream		CLEAN
be57de6dfc35849a7971918b5415afae3d13c05038befe62b8a88ddc58669fb0	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\17.3.5892.0626_1\filesync.resources.dll.ceb77c26c2a9a4bdff1831afacddd3d7dd1b2da9d60798575ed8d1e113e0e338	Dropped File	2614.19 KB	application/octet-stream		CLEAN

Filename

Filename	Category	Operations	Verdict
\\?\C:\$Recycle.Bin\S-1-5-18\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	SUSPICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\CUsersGrujaDesktopca5751036a12d0.exe	Sample File	Access	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-18\desktop.ini	Accessed File	Access	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000\desktop.ini	Accessed File	Access	CLEAN
\\?\C:\$Recycle.Bin\S-1-5-21-1560258661-3990802383-1811730007-1000\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\$Recycle.Bin\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\bg-BG\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\bootvhd.dll	Accessed File	Access	CLEAN

Filename	Category	Operations	Verdict
\\?\C:\Boot\cs-CZ\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\da-DK\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\de-DE\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\el-GR\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\en-GB\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\en-US\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\es-ES\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\es-MX\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\et-EE\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\fi-FI\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\Fonts\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\fr-CA\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\fr-FR\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\hr-HR\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\hu-HU\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\it-IT\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\ja-JP\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\ko-KR\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\lt-LT\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\lv-LV\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\nb-NO\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\nl-NL\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\pl-PL\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\pt-BR\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\pt-PT\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\qps-ploc\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\Resources\bootres.dll	Accessed File	Access	CLEAN

Filename	Category	Operations	Verdict
\\?\C:\Boot\Resources\en-US\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\Resources\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\ro-RO\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\ru-RU\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\sk-SK\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\sl-SI\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\sr-Latn-CS\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\sr-Latn-RS\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\sv-SE\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\tr-TR\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\uk-UA\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\zh-CN\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\zh-HK\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\zh-TW\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\Boot\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\PerfLogs\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Comms\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\MasterDescriptor.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\stream.x86.en-us.man.dat	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\en-us.16\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\x-none.16\MasterDescriptor.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\x-none.16\stream.x86.x-none.man.dat	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\x-none.16\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN

Filename	Category	Operations	Verdict
\\?\C:\ProgramData\Microsoft\ClickToRun\4BAD322A-C043-4DED-A97A-6FE0C4412FBE\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\DeploymentConfig.0.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\DeploymentConfig.2.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\DeploymentConfiguration.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\Manifest.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\UserDeploymentConfiguration.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\UserManifest.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Integration\ShortcutBackups\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\Integration\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\MachineData\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\UserData\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Access.Access.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN

Filename	Category	Operations	Verdict
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.accessmui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.accessmuiset.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.DCF.DCF.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.dcfmui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Excel.Excel.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.excelmui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Groove.Groove.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.groovemui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Lync.Lync.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.lyncmui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64mui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64muiset.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.office64ww.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.officemui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.officemuiset.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OneNote.OneNote.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.onenotemui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN

Filename	Category	Operations	Verdict
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OSM.OSM.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.osmmui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.OSMUX.OSMUX.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.osmuxmui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Outlook.Outlook.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.outlookmui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.PowerPivot.PowerPivot.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.PowerPoint.PowerPoint.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.powerpointmui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.es-es.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Proof.Culture.msi.16.fr-fr.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.proofing.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Publisher.Publisher.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.publishermui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.shared.Office.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN

Filename	Category	Operations	Verdict
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.Word.Word.x-none.msi.16.x-none.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\C2RManifest.wordmui.msi.16.en-us.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\Microsoft_Office_OfficeTelemetryAgentFallBack2016.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\Microsoft_Office_OfficeTelemetryAgentLogOn2016.xml	Accessed File	Read, Access, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\ClickToRun\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Crypto\DSS\MachineKeys\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Crypto\DSS\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Crypto\Keys\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Crypto\PCPKSP\WindowsAIK\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Crypto\PCPKSP\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Crypto\RSA\S-1-5-18\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Crypto\RSA\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Crypto\SystemKeys\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Crypto\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\DataMart\PaidWiFi\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\DataMart\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\DeviceStage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\background.png	Accessed File	Access	CLEAN
\\?\C:\ProgramData\Microsoft\DeviceStage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\behavior.xml	Accessed File	Access	CLEAN

Filename	Category	Operations	Verdict
\\?\C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\device.png	Accessed File	Access	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\overlay.png	Accessed File	Access	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\superbar.png	Accessed File	Access	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\background.png	Accessed File	Access	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\behavior.xml	Accessed File	Access	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\watermark.png	Accessed File	Access	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Device\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\en-US\resource.xml	Accessed File	Access	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\en-US\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\resource.xml	Accessed File	Access	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\tasks.xml	Accessed File	Access	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\en-US\resource.xml	Accessed File	Access	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\en-US\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\tasks.xml	Accessed File	Access	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\Task\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Device Stage\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\DeviceSync\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN

Filename	Category	Operations	Verdict
\\?\C:\ProgramData\Microsoft\Diagnosis\AsimovUploader\YOUR_FILES_ARE_ENCRYPTED.HTML	Dropped File	Access, Create, Write	CLEAN
\\?\C:\ProgramData\Microsoft\Diagnosis\DownloadedScenarios\WINDOWS.DIAGNOSTICS.xml	Accessed File	Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://91.218.114.31		91.218.114.31		POST	MALICIOUS
http://nbzzb6sa6xuura2z.onion				GET	CLEAN
http://ebwexiymbsib4rmw.onion				GET	CLEAN
http://91.218.114.30		91.218.114.30		POST	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
nbzzb6sa6xuura2z.onion			HTTP	CLEAN
ebwexiymbsib4rmw.onion			HTTP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
91.218.114.31		Russia	HTTP, TCP	MALICIOUS
91.218.114.30		Russia	HTTP, TCP	CLEAN

Email

-

Email Address

-

Mutex

Name	Operations	Parent Process Name	Verdict
()$&t$$""%"u$ ##)&&$t '()$pwr##(%!%p)!" u"$!! &ur$&r!!ws"")st&)r)#pt& t$&r!&t)%	access	cusersgrujadesktopca5751036a12d0.exe	CLEAN

Registry

-

Process

Process Name	Commandline	Verdict
cusersgrujadesktopca5751036a12d0.exe	"C:\Users\RDhJ0CNFevzX\Desktop\CUsersGrujaDesktopca5751036a12d0.exe"	MALICIOUS

YARA / AV

Antivirus (1)

File Type	Threat Name	Filename	Verdict
SAMPLE	Gen:Variant.Razy.326200	C:\Users\RDhJ0CNFevzX\Desktop\CUsersGrujaDesktopca5751036a12d0.exe	MALICIOUS

ENVIRONMENT

Virtual Machine Information

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

Analyzer Information

Analyzer Version	4.1.1
Dynamic Engine Version	4.1.1 / 02/08/2021 15:19
Static Engine Version	1.6.0
Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (November 12, 2020)
Built-in AV Database Update Release Date	2021-04-18 17:06:45+00:00
VTI Ruleset Version	3.8
YARA Built-in Ruleset Version	1.5
Analysis Report Layout Version	10

Software Information

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