MALICIOUS

Classifications: Ransomware | Wiper | Spyware

Threat Names: -

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe**
ID	#4181898
MD5	52e47deed3440de981bf84e22c6da710
SHA1	e11a43a223b2558d99452b2efd4e6a289855b2b8
SHA256	274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244
File Size	36.00 KB
Report Created	2022-04-24 07:40 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (12 rules, 12 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #1) 274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe modifies the content of multiple user files.			
5/5	User Data Modification	Deletes user files	1	Wiper
	• (Process #1) 274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe deletes multiple user files.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Internet Explorer / Edge, git, Total Commander, The Bat!.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
3/5	User Data Modification	Possibly drops ransom note files	1	Ransomware
	• (Process #1) 274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe possibly drops ransom note files (creates 404 instances of the file "# HELP_TO_DECRYPT_YOUR_FILES #.html" in different locations).			
2/5	Data Collection	Reads sensitive application data	1	-
	• (Process #1) 274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe tries to read sensitive data of application "git" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #1) 274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #1) 274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive ftp data	1	-
	• (Process #1) 274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe tries to read sensitive data of ftp application "Total Commander" by file.			
2/5	Anti Analysis	Tries to detect virtual machine	1	-
	• (Process #1) 274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe is possibly trying to detect a VM via rdtsc.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) 274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe enables process privilege "SeDebugPrivilege".			
1/5	System Modification	Creates an unusually large number of files	1	-
	• (Process #1) 274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe creates an above average number of files.			

Mitre ATT&CK Matrix

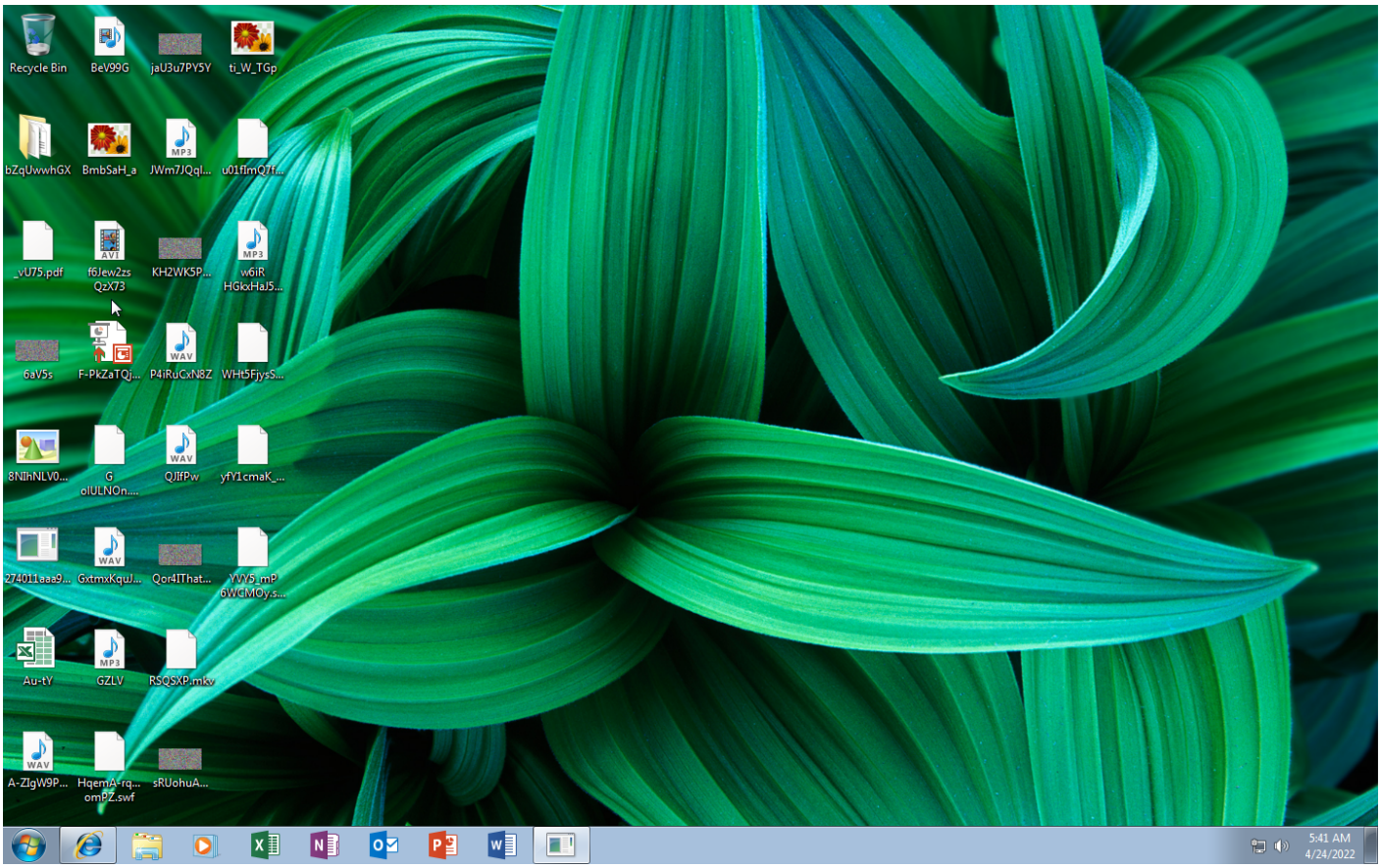
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1497 Virtualization/ Sandbox Evasion	#T1081 Credentials in Files	#T1083 File and Directory Discovery		#T1119 Automated Collection			#T1486 Data Encrypted for Impact
						#T1497 Virtualization/ Sandbox Evasion		#T1005 Data from Local System			#T1485 Data Destruction
						#T1124 System Time Discovery					

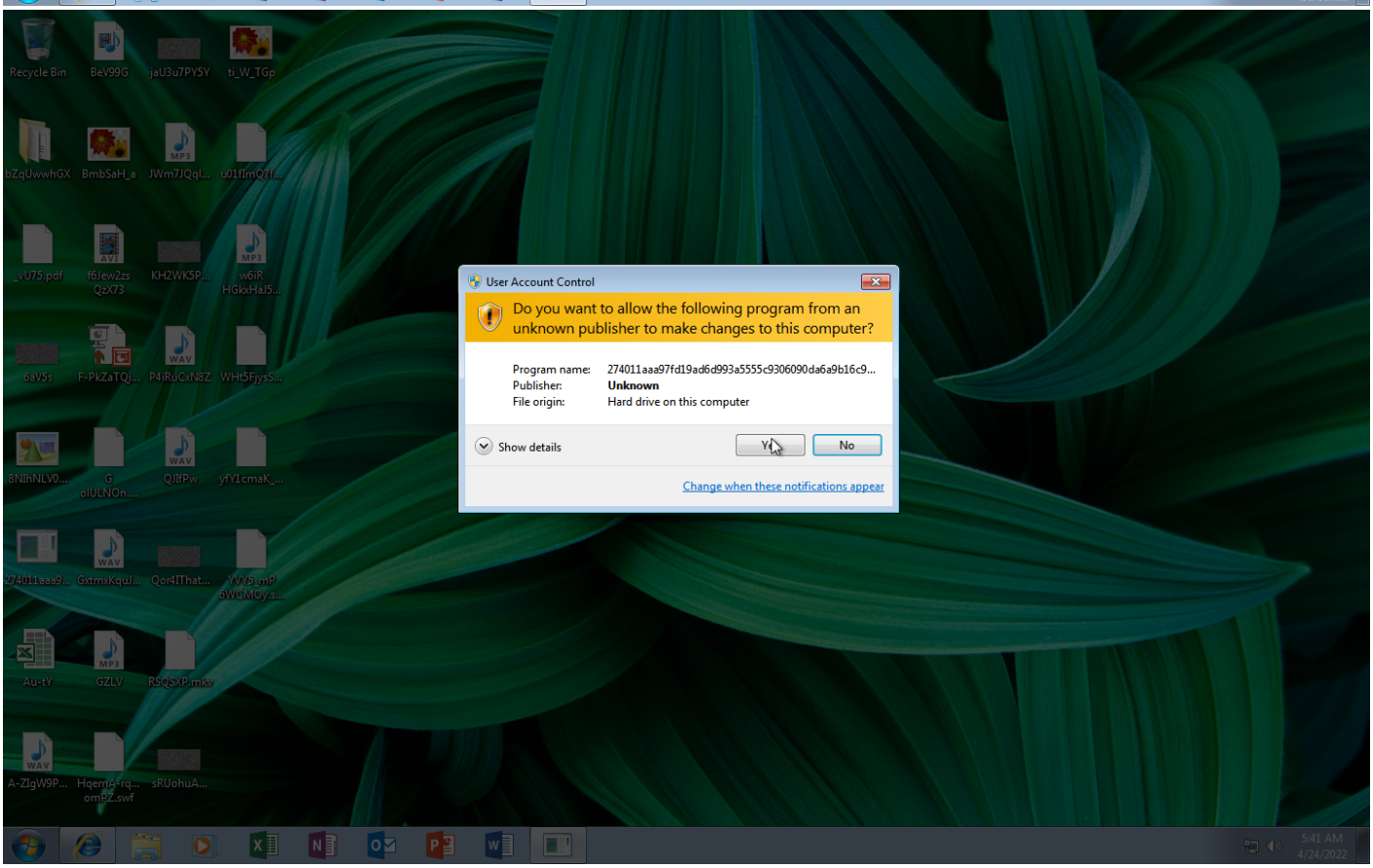
Sample Information

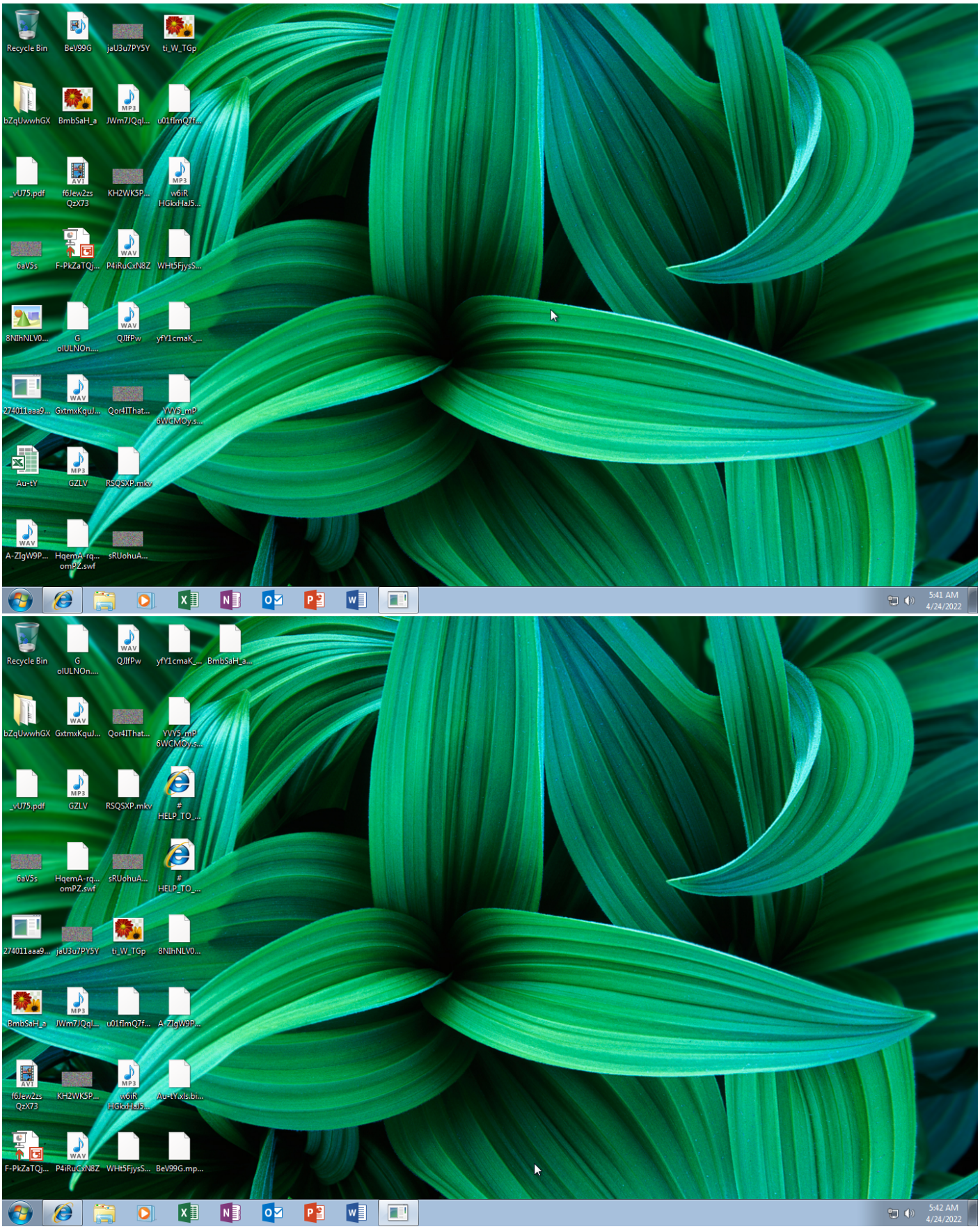
ID	#4181898
MD5	52e47deed3440de981bf84e22c6da710
SHA1	e11a43a223b2558d99452b2efd4e6a289855b2b8
SHA256	274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244
SSDeep	768:VlUgrN0sWl7V8H+xolL18mDIOfd6YgDb431QMX0nl:zPWlx8PLZfVgDb4Wl
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe
File Size	36.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2022-04-24 07:40 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	1
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✗
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
BeV99G
jaU3u7PY5Y
ti_W_TGp
bZqUwwhGX
BmbSaH_a
JWm7JQql...
u01flmQ7t...
_vU75.pdf
f6Jew2zs
QzX73
KH2WK5P...
w6iR
HGkxHaJ5...
6aV5s
F-PkZaTQj...
P4iRuCxN8Z
WHt5FjysS...
8NIhNLV0...
G
olULNOn....
QJffPw
yfV1cmaK_...
274011aaa9...
GxtmxKquJ...
Qor4IThat...
YVY5_mP
6WdMOy.s...
Au-tY
GZLV
RSQSXP.mkv
A-ZIgW9P...
HqemA-rq...
omPZ.swf
sRUohuA...
5:41 AM
4/24/2022


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 274011aaa97fd19ad6d993a5555c9306090da6a9b16c9...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

3 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

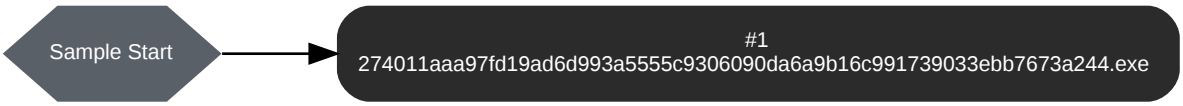
0 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	-	-		0 bytes	NA
GET	https://blockchain.com	-	-		0 bytes	NA
GET	https://localbitcoins.com/	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: 274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 42300, Reason: Analysis Target
Unmonitor End Time	End Time: 292098, Reason: Terminated by Timeout
Monitor duration	249.80s
Return Code	Unknown
PID	3580
Parent PID	1928
Bitness	32 Bit

Dropped Files (69)

File Name	File Size	SHA256	YARA Match
C:\Boot\# HELP_TO_DECRYPT_YOUR_FILES #.html	3.47 KB	528bcbff16bd0df4ecfe74142d9547e4c81ec08132421f2b883ac553a45071df	✗
C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\stream.x86.en-us.man.dat.bitpy	864.48 KB	848175bb55e3190e493d0947458ae2088b5b2d76ee4c51a8ce2365c6a34f5d53	✗
C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\stream.x86.x-none.man.dat.bitpy	3629.47 KB	4d2df5bf825faaffd7c8df5d7b9e63c46cb23cb04ebf08812521467cdd5d5dff	✗
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\background.png.bitpy	126.73 KB	ea66f669d62cb4cd1a7e591ae377743af0d120796b92b48d23ec0369b2ec6bab	✗
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\device.png.bitpy	43.47 KB	2f8b4f916a5eb3f3967552170c03ef51526c77ba1b6b6160b8af8278fe960f09	✗
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\overlay.png.bitpy	28.22 KB	2cec702b344d2f9b9c277cbfdf9bd33328e3eb2ce2397c3aaefd279b4fc4cd6d	✗
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\superbar.png.bitpy	38.48 KB	58f2109cd46d0d4e2520d370f8d33535a65f1cfae8902f32c71fbbfa258e02a4	✗
C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\background.png.bitpy	126.73 KB	98eda0963ad94c2fc948dc3fa620640ef080f9b8a04824e11f949604cc751809	✗
C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\watermark.png.bitpy	28.22 KB	a619462132c230bceb5046e5411072ef9c97378f0855627d573d6abe2bd924ca	✗
C:\ProgramData\Microsoft\OfficeSoftwareProtectionPlatform\tokens.dat.bitpy	2745.84 KB	ad02551d3d8f5bed393566a2e07e983f721991c158251ca442645c3403b5ee90	✗
C:\ProgramData\Microsoft\OfficeSoftwareProtectionPlatform\Cache\cache.dat.bitpy	89.38 KB	8bc9b0d65d7d8ca3cba4ce27102daa37d217baffb504881bad131d242aeeeeb1	✗
C:\ProgramData\Microsoft\User Account Pictures\kEecfMwgj.dat.bitpy	32 bytes	ef863ae46e51e974fcac10bcfb814a4877f4665cd197c9ba33aa9dbb805d213e	✗
C:\ProgramData\Package Cache\{0FA68574-690B-4B00-89AA-B28946231449} v14.25.28508\packages\vcRuntimeAdditional_x86\cab1.cab.bitpy	5088.94 KB	87e7a4fc6943a60cfae00adbfc9082c52c4afe9e830823189910109d756b0d91	✗
C:\ProgramData\Package Cache\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E} v12.0.21005\packages\vcRuntimeMinimum_x86\cab1.cab.bitpy	973.70 KB	f60bcad669a4220fea221a51950b2303e2df0e7ee6499689dddf45a9833a8c7a	✗
C:\ProgramData\Package Cache\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2} v14.25.28508\packages\vcRuntimeMinimum_x86\cab1.cab.bitpy	1335.64 KB	6324312b83049948b1dc02e2c5a3eff1150341b4ae3cb67e4debb64618d30525	✗

File Name	File Size	SHA256	YARA Match
C:\ProgramData\Package Cache\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}v14.25.28508\packages\vcRuntimeAdditional_amd64\cab1.cab.bitpy	5500.27 KB	ef5ecab261f50785e8f1a3ab5cc1d76fdee7f914f19a5e68bf327c36ad2ef3d7	✗
C:\ProgramData\Package Cache\{929FBD26-9020-399B-9A7A-751D61F0B942}v12.0.21005\packages\vcRuntimeAdditional_amd64\cab1.cab.bitpy	5457.31 KB	e22f81f8ecc8ff1939cc54ab66481c0913c650dee268f862fff307ac9f8e695f	✗
C:\ProgramData\Package Cache\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}v12.0.21005\packages\vcRuntimeMinimum_amd64\cab1.cab.bitpy	1010.28 KB	80dea819fa7bf85eff20fc694ddea79041b14420f9c458387c89ccb5963fcf1e	✗
C:\ProgramData\Package Cache\{B175520C-86A2-35A7-8619-86DC379688B9}v11.0.61030\packages\vcRuntimeAdditional_x86\cab1.cab.bitpy	5033.05 KB	ef65e2a5eb725bfae97044b60de7709f31b8f53f3e92d540d0fb106e00741e21	✗
C:\ProgramData\Package Cache\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}v11.0.61030\packages\vcRuntimeMinimum_x86\cab1.cab.bitpy	802.45 KB	e2e8f1db49faef21519a9682a47adb7c057b29c1292901874b59f1248770ca15	✗
C:\ProgramData\Package Cache\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}v11.0.61030\packages\vcRuntimeMinimum_amd64\cab1.cab.bitpy	790.81 KB	f4ea2757fdd7b6df2e8476d8f0279f011a9d856f90f0707f86ddfbae853dce3c	✗
C:\ProgramData\Package Cache\{EEA66967-97E2-4561-A999-5C22E3CDE428}v14.25.28508\packages\vcRuntimeMinimum_amd64\cab1.cab.bitpy	1473.19 KB	7ce6e73ca75c5673edf3b9a641cd9f2e21d44c74c341ec6221ceafa4f2f36305	✗
C:\ProgramData\Package Cache\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}v12.0.21005\packages\vcRuntimeAdditional_x86\cab1.cab.bitpy	4817.31 KB	7c155fd201c29df0c7944647fb8cd64d223f025738c3a4c077c886f959c6cde1	✗
C:\Users\Default\NTUSER.DAT.LOG.bitpy	1.03 KB	3734707a4e478c6bb8e47e81b31008a047de51f567633dcc657459c6cf8725cb	✗
C:\Users\Default\AppData\Local\IconCache.db.bitpy	758.02 KB	e2413ccd3ea112070652a35597f97292fd1e1e61831b745cff41526be4e971f1	✗
C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.bak.bitpy	11.94 KB	892f061e59d65c4f480c83dccd186004a72215a99a1a54059fb515678800ff72	✗
C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.txt.bitpy	11.94 KB	be6c4e521e7cc3931376eaa5b3085509d571f172f6aa63274a5924c704a374dd	✗
C:\Users\Default\AppData\Local\Temp\FXSAPIDebugLogFile.txt.bitpy	32 bytes	72fd103ba09f2dbcf7a98e3deaed8603b4485d3a56b3e7031f852e80bf6c93c0	✗
C:\Users\kEecfMwgj\AppData\Local\IconCache.db.bitpy	1149.62 KB	3dfc9b69fc48482295633c5adab6a28f1fa3f311af9406113989c7ab506afa45	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\FORMS\FRMCACHE.DAT.bitpy	240.23 KB	337a683bf87e7f7a464e1d1eaff0ecc96ef47e1c3edcf41eab31c1fb576e251d	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\brndlog.bak.bitpy	11.94 KB	4d8001a3d22057b6ce1bcbab42e6690cd9850f1845960e3b823ac1fa16becbaf	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\brndlog.txt.bitpy	11.94 KB	4f97ec8924b09ebf03d178eacc182b89855dad95d77922f048085ddc4c125c36	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\frameiconcache.dat.bitpy	9.12 KB	ba12908f69892fa377104858fb1c6f4f41346c4adb3180a392ef304a14380f4b	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT.bitpy	16.03 KB	e866f97af740f814246ee4e62bf2ade8d1eb44c3f03dbcc717df4dd294963d90	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{8AB24C65-1C57-11EC-B986-C89F1DB658E4}.dat.bitpy	3.53 KB	ef41ad2f51b137d1d6527d0537f62c8dfcaa9cb7b33a98bc56daf71932e534a9	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\Recovery\Last Active\{CBE13020-1C57-11EC-B986-C89F1DB658E4}.dat.bitpy	19.03 KB	94791e57f87655f683a903aa92dee256ab32b07910a552cbca2eb3841d824fa5	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\OTele\{61793A19-06A8-458E-B03A-D37C5A818884} (0) - 1060 - winword.exe - OTele.dat.bitpy	304 bytes	f16dff27919d56b34b0b24e677f02bc9c5d23416a993f5a188eded4d9d8bab80	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\OTele\{61793A19-06A8-458E-B03A-D37C5A818884} (0) - 1060 - winword.exe - OTeleMediumCost.dat.bitpy	864 bytes	3ab23f6703bbfc98680eae8475fc64198dc4fa97f932dc68db19326f79995609	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\OTele\{61793A19-06A8-458E-B03A-D37C5A818884} (1) - 1060 - winword.exe - OTele.dat.bitpy	320 bytes	81cc75633dcb407474f251f765766c70b5552ac567c74217d85ef9263843ba14	✗

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\OTele\{61793A19-06A8-458E-B03A-D37C5A818884} (1) - 1060 - winword.exe - OTeleMediumCost.dat.bitpy	544 bytes	69e7db20c0e1ceb61f774d4710a54b5afc360f8a2457baf13804edda38a35cc9	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\OTele\{A7D1044D-57E2-45B6-8A93-CD389A77D3AC} (0) - 2256 - winword.exe - OTele.dat.bitpy	208 bytes	38e034bd1e41dbde2893d8bd7731dcdf8252eb07e60802e67795b073e69e8378	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\AutoPlayLogo.png.bitpy	4.58 KB	9aebea41c5688eac19d9f886645e01d451475c2c5b0c719b479fbd9256837680	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\AutoPlayOptIn.gif.bitpy	374.27 KB	cec5ff383bf80823536aa589663f73a8f6b5f9d062e079d8fb49d805e5b447d6	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\AutoPlayOptIn.png.bitpy	10.02 KB	c3dbd31ecde4e5c06ad8cf395480c119fad57804b7e2be71c162649f4c0c0730	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\ScreenshotLogo.png.bitpy	4.59 KB	9cfd412f92049ca8365a8ca087c9696f4692094139e80c8b3c9a8072a2b2cecf	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\ScreenshotOptIn.png.bitpy	432.03 KB	bb0e74b204aac65e3a8e93b7ec0b8b2df1803991747024e23d89a8376b5bd434	✗
C:\temp0.bin	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Outlook\RoamCache\Stream_Calendar_2_CB55C2C1F45FED459E403036C0F2F1E7.dat.bitpy	608 bytes	45d6f81e3d01279dd9734b608e52e55b46f0d914f1ae3ea3ca3cb030dec6154b	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Outlook\RoamCache\Stream_TableViewPreviewPrefs_2_7E96CFF05AA1AB4F91E2DCF307336A81.dat.bitpy	304 bytes	587453be783d791e7a91c479b86d0f6f40c70c939308815c3f5e763718e1ed95	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Outlook\RoamCache\Stream_WorkHours_1_0B01BFE21DA49B4A926A43DB70EDB003.dat.bitpy	656 bytes	404f7516e8cb54a92088c58de2e39a2b489ea0fe6c74feb123588be91d2f336b	✗
C:\Users\kEecfMwgj\AppData\Local\Temp\lv92.xlsx.bitpy	10.56 KB	af2b19ee72eb21a60a978372ed2d4c6dc6d915b0bdc1e10c5296ab52b4183396	✗
C:\Users\kEecfMwgj\AppData\Roaming\1bVoxTN-Vw.pptx.bitpy	54.36 KB	51db55b8a0dd6df1cfee3ba4869b8304ce957eefb54cbe09d8873df4b9236392	✗
C:\Users\kEecfMwgj\AppData\Roaming\TbdxF.png.bitpy	1.22 KB	605e877c29439e5546c8cd7987a6385fd8dc87652d87234e3e795cd4f3c16668	✗
C:\Users\kEecfMwgj\AppData\Roaming\vQlzKgl0PXWpBvEU8.mp3.bitpy	63.47 KB	e81bacae1a9ca5dd35fcb5d091b891401eaa96d622bac460a6dd88a62c4b424d	✗
C:\Users\kEecfMwgj\Desktop\JWm7JQqlgRl.mp3.bitpy	93.56 KB	7b279d261470353cc1058494518a6b522710dee77dd1fa21a2526d951c76c190	✗
C:\Users\kEecfMwgj\Documents\ln7fV.pptx.bitpy	44.17 KB	440b86785d7f9b052be96984950e0550bf68bd2a6786848edb98c9dc9c471ef0	✗
C:\Users\kEecfMwgj\Documents\R8OEYg58.docx.bitpy	76.14 KB	aed40c025b1295d6d2189f09fc27a2281daa6d033968ebed83539a599b61c7b8	✗
C:\Users\kEecfMwgj\Documents\ufvNF4jQ-pQP.doc.bitpy	54.02 KB	41a396d85ec8e47489e88a60ad2f64835702b42e24e11afba491989c910713c3	✗
C:\Users\kEecfMwgj\Documents\Outlook Files\franc@gdllo.de.pst.bitpy	265.03 KB	bcf3d5896ad91b340df4cf9c081ef2bcf64aa59297c9bffd1af2c4e29e2a76b7	✗
C:\Users\kEecfMwgj\Documents\o_o-1F3TH1sB884\0pjpvs64FNx.docx.bitpy	99.11 KB	cb50f4436f8077c09b57d5d2a03b0a456d7c136fe93c343a61ebc6ecd9cdeb5c	✗
C:\Users\kEecfMwgj\Documents\yLKsNetY\MN5H2GzzCWr7.pdf.bitpy	86.09 KB	a5e9bbb108d218552b2ac1278bf1f9669b1ae7171f93b054894be69983df91bd	✗
C:\Users\kEecfMwgj\Pictures\1cWy43U6UB1yaWgds5.jpg.bitpy	95.62 KB	ebbca5fece58115c34a4f14b3b43f9e297a207d2542612b598aaaf7a62105f1e	✗
C:\Users\kEecfMwgj\Pictures\9NV7HJvRw0QQr0hlwhy.png.bitpy	8.34 KB	a007ccfae160b697caee93429c79db44da20d011f6a1df922425c7274d26b405	✗

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Pictures\c9kvkj2NGeB.png.bitpy	59.73 KB	30896086a672404c57d20a6b82dfc9cc9f804908790690904456eb80dfeed94e	✗
C:\Users\kEecfMwgj\Pictures\HKNKtQ.jpg.bitpy	60.02 KB	1009a69076c6b4727254afd09f74559528a3e19790e34afe4f1277405885e9f4	✗
C:\Users\kEecfMwgj\Pictures\kITMELnl0grVCrYTU.jpg.bitpy	92.70 KB	b053593b01e1f0d23853efef78d45378e1d0a63d053ed668620295723b45ab66	✗
C:\Users\kEecfMwgj\Pictures\rImHN1xh0sKY5.gif.bitpy	61.09 KB	0d46bfd231094488a9a291b153a49f58edabd7735a0b9a4a3dc52ca603753724	✗
C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg.bitpy	858.81 KB	a9113df7cffcc66fdf4fe55c371ade92b33d027e5998282a07b5d292877aa265	✗
C:\Users\Public\Pictures\Sample Pictures\Desert.jpg.bitpy	826.14 KB	57be857093a09f50754e8a34947641f07693c7d9310358e057a09bcfc7f74972	✗

Host Behavior

Type	Count
Module	7
System	5
User	1
Process	10
File	17013

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244	C:\Users\kEecfMwgj\Desktop\274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe	Sample File	36.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
528bcbff16bd0df4ecfe74142d9547e4c81ec08132421f2b883ac553a45071df	C:\Boot\zh-TW\#HELP_TO_DECRYPT_YOUR_FILES#.html, C:\Users\Default\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User ... ...CRYPT_YOUR_FILES#.html, C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\it\#HELP_TO_DECRYPT_YOUR_FILES#.html	Dropped File	3.47 KB	text/html	Create, Write, Access	SUSPICIOUS
848175bb55e3190e493d0947458ae2088b5b2d76ee4c51a8ce2365c6a34f5d53	C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\stream.x86.en-us.man.dat.bitpy	Dropped File	864.48 KB	application/octet-stream	Create, Write, Access	CLEAN
4d2df5bf825faaffd7c8df5d7b9e63c46cb23cb04ebf08812521467cdd5d5dff	C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\stream.x86.x-none.man.dat.bitpy	Dropped File	3629.47 KB	application/octet-stream	Create, Write, Access	CLEAN
ea66f669d62cb4cd1a7e591ae377743af0d120796b92b48d23ec0369b2ec6bab	C:\ProgramData\Microsoft\DeviceStage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\background.png.bitpy	Dropped File	126.73 KB	application/octet-stream	Create, Write, Access	CLEAN
2f8b4f916a5eb3f3967552170c03ef51526c77ba1b6b6160b8af8278fe960f09	C:\ProgramData\Microsoft\DeviceStage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\device.png.bitpy	Dropped File	43.47 KB	application/octet-stream	Create, Write, Access	CLEAN
2cec702b344d2f9b9c277cbfdf9bd33328e3eb2ce2397c3aaefd279b4fc4cd6d	C:\ProgramData\Microsoft\DeviceStage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\overlay.png.bitpy	Dropped File	28.22 KB	application/octet-stream	Create, Write, Access	CLEAN
58f2109cd46d0d4e2520d370f8d33535a65f1cfae8902f32c71fbbfa258e02a4	C:\ProgramData\Microsoft\DeviceStage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\superbar.png.bitpy	Dropped File	38.48 KB	application/octet-stream	Create, Access	CLEAN
98eda0963ad94c2fc948dc3fa620640ef080f9b8a04824e11f949604cc751809	C:\ProgramData\Microsoft\DeviceStage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\background.png.bitpy	Dropped File	126.73 KB	application/octet-stream	Create, Write, Access	CLEAN
a619462132c230bceb5046e5411072ef9c97378f0855627d573d6abe2bd924ca	C:\ProgramData\Microsoft\DeviceStage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\watermark.png.bitpy	Dropped File	28.22 KB	application/octet-stream	Create, Access	CLEAN
ad02551d3d8f5bed393566a2e07e983f721991c158251ca442645c3403b5ee90	C:\ProgramData\Microsoft\OfficeSoftwareProtectionPlatform\tokens.dat.bitpy	Dropped File	2745.84 KB	application/octet-stream	Create, Write, Access	CLEAN
8bc9b0d65d7d8ca3cba4ce27102daa37d217baffb504881bad131d242aeeeeb1	C:\ProgramData\Microsoft\OfficeSoftwareProtectionPlatform\Cache\cache.dat.bitpy	Dropped File	89.38 KB	application/octet-stream	Create, Write, Access	CLEAN
ef863ae46e51e974fcac10bcfb814a4877f4665cd197c9ba33aa9dbb805d213e	C:\ProgramData\Microsoft\User Account Pictures\kEecfMwgj.dat.bitpy	Dropped File	32 bytes	application/octet-stream	Create, Access	CLEAN
87e7a4fc6943a60cfae00adbfc9082c52c4afe9e830823189910109d756b0d91	C:\ProgramData\Package Cache\{0FA68574-690B-4B00-89AA-B28946231449}v14.25.28508\packages\vcRuntimeAdditional_x86\cab1.cab.bitpy	Dropped File	5088.94 KB	application/octet-stream	Create, Write, Access	CLEAN
f60bcad669a4220fea221a51950b2303e2df0e7ee6499689dddf45a9833a8c7a	C:\ProgramData\Package Cache\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}v12.0.21005\packages\vcRuntimeMinimum_x86\cab1.cab.bitpy	Dropped File	973.70 KB	application/octet-stream	Create, Access	CLEAN
6324312b83049948b1dc02e2c5a3eff1150341b4ae3cb67e4debb64618d30525	C:\ProgramData\Package Cache\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}v14.25.28508\packages\vcRuntimeMinimum_x86\cab1.cab.bitpy	Dropped File	1335.64 KB	application/octet-stream	Create, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ef5ecab261f50785e8f1a3ab5cc1d76fdee7f914f19a5e68bf327c36ad2ef3d7	C:\ProgramData\Package Cache\{7D0B74C2-C3F8-4AF1-940F-CD79AB4B2DCE}v14.25.28508\packages\vcRuntimeAdditional_amd64\cab1.cab.bitpy	Dropped File	5500.27 KB	application/octet-stream	Create, Access	CLEAN
e22f81f8ecc8ff1939cc54ab66481c0913c650dee268f862ff f307ac9f8e695f	C:\ProgramData\Package Cache\{929FBD26-9020-399B-9A7A-751D61F0B942}v12.0.21005\packages\vcRuntimeAdditional_amd64\cab1.cab.bitpy	Dropped File	5457.31 KB	application/octet-stream	Create, Access	CLEAN
80dea819fa7bf85eff20fc694ddea79041b14420f9c458387c89ccb5963fcf1e	C:\ProgramData\Package Cache\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}v12.0.21005\packages\vcRuntimeMinimum_amd64\cab1.cab.bitpy	Dropped File	1010.28 KB	application/octet-stream	Create, Write, Access	CLEAN
ef65e2a5eb725bfae97044b60de7709f31b8f53f3e92d540d0fb106e00741e21	C:\ProgramData\Package Cache\{B175520C-86A2-35A7-8619-86DC379688B9}v11.0.61030\packages\vcRuntimeAdditional_x86\cab1.cab.bitpy	Dropped File	5033.05 KB	application/octet-stream	Create, Write, Access	CLEAN
e2e8f1db49faef21519a9682a47adb7c057b29c1292901874b59f1248770ca15	C:\ProgramData\Package Cache\{BD95A8CD-1D9F-35AD-981A-3E7925026EBB}v11.0.61030\packages\vcRuntimeMinimum_x86\cab1.cab.bitpy	Dropped File	802.45 KB	application/octet-stream	Create, Access	CLEAN
f4ea2757fdd7b6df2e8476d8f0279f011a9d856f90f0707f86ddfbae853dce3c	C:\ProgramData\Package Cache\{CF2BEA3C-26EA-32F8-AA9B-331F7E34BA97}v11.0.61030\packages\vcRuntimeMinimum_amd64\cab1.cab.bitpy	Dropped File	790.81 KB	application/octet-stream	Create, Access	CLEAN
7ce6e73ca75c5673edf3b9a641cd9f2e21d44c74c341ec6221ceafa4f2f36305	C:\ProgramData\Package Cache\{EEA66967-97E2-4561-A999-5C22E3CDE428}v14.25.28508\packages\vcRuntimeMinimum_amd64\cab1.cab.bitpy	Dropped File	1473.19 KB	application/octet-stream	Create, Write, Access	CLEAN
7c155fd201c29df0c7944647fb8cd64d223f025738c3a4c077c886f959c6cde1	C:\ProgramData\Package Cache\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}v12.0.21005\packages\vcRuntimeAdditional_x86\cab1.cab.bitpy	Dropped File	4817.31 KB	application/octet-stream	Create, Write, Access	CLEAN
3734707a4e478c6bb8e47e81b31008a047de51f567633dcc657459c6cf8725cb	C:\Users\Default\NTUSER.DAT.LOG.bitpy	Dropped File	1.03 KB	application/octet-stream	Create, Access	CLEAN
e2413ccd3ea112070652a35597f97292fd1e1e61831b745cff41526be4e971f1	C:\Users\Default\AppData\Local\IconCache.db.bitpy	Dropped File	758.02 KB	application/octet-stream	Create, Write, Access	CLEAN
892f061e59d65c4f480c83dccd186004a72215a99a1a54059fb515678800ff72	C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.bak.bitpy	Dropped File	11.94 KB	application/octet-stream	Create, Access	CLEAN
be6c4e521e7cc3931376eaa5b3085509d571f172f6aa63274a5924c704a374dd	C:\Users\Default\AppData\Local\Microsoft\Internet Explorer\brndlog.txt.bitpy	Dropped File	11.94 KB	application/octet-stream	Create, Write, Access	CLEAN
72fd103ba09f2dbcf7a98e3deaed8603b4485d3a56b3e7031f852e80bf6c93c0	C:\Users\Default\AppData\Local\Temp\FXSAPIDebugLogFile.txt.bitpy	Dropped File	32 bytes	application/octet-stream	Create, Access	CLEAN
3dfc9b69fc48482295633c5adab6a28f1fa3f311af9406113989c7ab506afa45	C:\Users\kEecfMwgj\AppData\Local\IconCache.db.bitpy	Dropped File	1149.62 KB	application/octet-stream	Create, Write, Access	CLEAN
337a683bf87e7f7a464e1d1eaff0ecc96ef47e1c3edcf41eab31c1fb576e251d	C:\Users\kEecfMwgj\AppData\Local\Microsoft\FORMS\FRMCACHE.DAT.bitpy	Dropped File	240.23 KB	application/octet-stream	Create, Write, Access	CLEAN
4d8001a3d22057b6ce1bcbab42e6690cd9850f1845960e3b823ac1fa16becbaf	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\brndlog.bak.bitpy	Dropped File	11.94 KB	application/octet-stream	Create, Access	CLEAN
4f97ec8924b09ebf03d178eacc182b89855dad95d77922f048085ddc4c125c36	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\brndlog.txt.bitpy	Dropped File	11.94 KB	application/octet-stream	Create, Write, Access	CLEAN
ba12908f69892fa377104858fb1c6f4f41346c4adb3180a392ef304a14380f4b	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\frameiconcache.dat.bitpy	Dropped File	9.12 KB	application/octet-stream	Create, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e866f97af740f814246ee4e62bf2ade8d1eb44c3f03dbcc717df4dd294963d90	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT.bitpy	Dropped File	16.03 KB	application/octet-stream	Create, Access	CLEAN
ef41ad2f51b137d1d6527d0537f62c8dfcaa9cb7b33a98bc56daf71932e534a9	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\Recovery\Last Active\RecoveryStore.{8AB24C65-1C57-11EC-B986-C89F1DB658E4}.dat.bitpy	Dropped File	3.53 KB	application/octet-stream	Create, Access	CLEAN
94791e57f87655f683a903aa92dee256ab32b07910a552cbca2eb3841d824fa5	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Internet Explorer\Recovery\Last Active\{CBE13020-1C57-11EC-B986-C89F1DB658E4}.dat.bitpy	Dropped File	19.03 KB	application/octet-stream	Create, Write, Access	CLEAN
f16dff27919d56b34b0b24e677f02bc9c5d23416a993f5a188eded4d9d8bab80	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\OTele\{61793A19-06A8-458E-B03A-D37C5A818884} (0) - 1060 - winword.exe - OTele.dat.bitpy	Dropped File	304 bytes	application/octet-stream	Create, Write, Access	CLEAN
3ab23f6703bbfc98680eae8475fc64198dc4fa97f932dc68db19326f79995609	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\OTele\{61793A19-06A8-458E-B03A-D37C5A818884} (0) - 1060 - winword.exe - OTeleMediumCost.dat.bitpy	Dropped File	864 bytes	application/octet-stream	Create, Write, Access	CLEAN
81cc75633dcb407474f251f765766c70b5552ac567c74217d85ef9263843ba14	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\OTele\{61793A19-06A8-458E-B03A-D37C5A818884} (1) - 1060 - winword.exe - OTele.dat.bitpy	Dropped File	320 bytes	application/octet-stream	Create, Access	CLEAN
69e7db20c0e1ceb61f774d4710a54b5afc360f8a2457baf13804edda38a35cc9	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\OTele\{61793A19-06A8-458E-B03A-D37C5A818884} (1) - 1060 - winword.exe - OTeleMediumCost.dat.bitpy	Dropped File	544 bytes	application/octet-stream	Create, Access	CLEAN
38e034bd1e41dbde2893d8bd7731dcdf8252eb07e60802e67795b073e69e8378	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Office\OTele\{A7D1044D-57E2-45B6-8A93-CD389A77D3AC} (0) - 2256 - winword.exe - OTele.dat.bitpy	Dropped File	208 bytes	application/octet-stream	Create, Write, Access	CLEAN
9aebea41c5688eac19d9f886645e01d451475c2c5b0c719b479fbd9256837680	C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\AutoPlayLogo.png.bitpy	Dropped File	4.58 KB	application/octet-stream	Create, Access	CLEAN
cec5ff383bf80823536aa589663f73a8f6b5f9d062e079d8fb49d805e5b447d6	C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\AutoPlayOptIn.gif.bitpy	Dropped File	374.27 KB	application/octet-stream	Create, Write, Access	CLEAN
c3dbd31ecde4e5c06ad8cf395480c119fad57804b7e2be71c162649f4c0c0730	C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\AutoPlayOptIn.png.bitpy	Dropped File	10.02 KB	application/octet-stream	Create, Access	CLEAN
9cfd412f92049ca8365a8ca087c9696f4692094139e80c8b3c9a8072a2b2cecf	C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\ScreenshotLogo.png.bitpy	Dropped File	4.59 KB	application/octet-stream	Create, Access	CLEAN
bb0e74b204aac65e3a8e93b7ec0b8b2df1803991747024e23d89a8376b5bd434	C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDrive\17.3.4604.0120\ScreenshotOptIn.png.bitpy	Dropped File	432.03 KB	application/octet-stream	Create, Write, Access	CLEAN
45d6f81e3d01279dd9734b608e52e55b46f0d914f1ae3ea3ca3cb030dec6154b	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Outlook\RoamCache\Stream_Calendar_2_CB55C2C1F45FED459E403036C0F2F1E7.dat.bitpy	Dropped File	608 bytes	application/octet-stream	Create, Access	CLEAN
587453be783d791e7a91c479b86d0f6f40c70c939308815c3f5e763718e1ed95	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Outlook\RoamCache\Stream_TableViewPreviewPrefs_2_7E96CFF05AA1AB4F91E2DCF307336A81.dat.bitpy	Dropped File	304 bytes	application/octet-stream	Create, Write, Access	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
404f7516e8cb54a92088c58de2e39a2b489ea0fe6c74feb123588be91d2f336b	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Outlook\RoamCache\Stream_WorkHours_1_0B01BFE21DA49B4A926A43DB70EDB003.dat.bitpy	Dropped File	656 bytes	application/octet-stream	Create, Write, Access	CLEAN
af2b19ee72eb21a60a978372ed2d4c6dc6d915b0bdc1e10c5296ab52b4183396	C:\Users\kEecfMwgj\AppData\Local\Temp\lv92.xlsx.bitpy	Dropped File	10.56 KB	application/octet-stream	Create, Write, Access	CLEAN
51db55b8a0dd6df1cfee3ba4869b8304ce957eefb54cbe09d8873df4b9236392	C:\Users\kEecfMwgj\AppData\Roaming\1bVoxTN-Vw.pptx.bitpy	Dropped File	54.36 KB	application/octet-stream	Create, Access	CLEAN
605e877c29439e5546c8cd7987a6385fd8dc87652d87234e3e795cd4f3c16668	C:\Users\kEecfMwgj\AppData\Roaming\TbdxF.png.bitpy	Dropped File	1.22 KB	application/octet-stream	Create, Write, Access	CLEAN
e81bacae1a9ca5dd35fcb5d091b891401eaa96d622bac460a6dd88a62c4b424d	C:\Users\kEecfMwgj\AppData\Roaming\vQlz Kgl0PXWpBvEU8.mp3.bitpy	Dropped File	63.47 KB	application/octet-stream	Create, Write, Access	CLEAN
7b279d261470353cc1058494518a6b522710dee77dd1fa21a2526d951c76c190	C:\Users\kEecfMwgj\Desktop\JWm7JQqlgRI.mp3.bitpy	Dropped File	93.56 KB	application/octet-stream	Create, Write, Access	CLEAN
440b86785d7f9b052be96984950e0550bf68bd2a6786848edb98c9dc9c471ef0	C:\Users\kEecfMwgj\Documents\In7fV.pptx.bitpy	Dropped File	44.17 KB	application/octet-stream	Create, Write, Access	CLEAN
aed40c025b1295d6d2189f09fc27a2281daa6d033968ebed83539a599b61c7b8	C:\Users\kEecfMwgj\Documents\R8OEYg58.docx.bitpy	Dropped File	76.14 KB	application/octet-stream	Create, Write, Access	CLEAN
41a396d85ec8e47489e88a60ad2f64835702b42e24e11afba491989c910713c3	C:\Users\kEecfMwgj\Documents\ufvNF4jQ-pQP.doc.bitpy	Dropped File	54.02 KB	application/octet-stream	Create, Write, Access	CLEAN
bcf3d5896ad91b340df4cf9c081ef2bcf64aa59297c9bffd1af2c4e29e2a76b7	C:\Users\kEecfMwgj\Documents\Outlook Files\franc@gdllo.de.pst.bitpy	Dropped File	265.03 KB	application/octet-stream	Create, Write, Access	CLEAN
cb50f4436f8077c09b57d5d2a03b0a456d7c136fe93c343a61ebc6ecd9cdeb5c	C:\Users\kEecfMwgj\Documents\o_o-1F3TH1sB884\0pjpvs64FNx.docx.bitpy	Dropped File	99.11 KB	application/octet-stream	Create, Write, Access	CLEAN
a5e9bbb108d218552b2ac1278bf1f9669b1ae7171f93b054894be69983df91bd	C:\Users\kEecfMwgj\Documents\yLKsNetY\MN5H2GzzCWr7.pdf.bitpy	Dropped File	86.09 KB	application/octet-stream	Create, Write, Access	CLEAN
ebbca5fece58115c34a4f14b3b43f9e297a207d2542612b598aaaf7a62105f1e	C:\Users\kEecfMwgj\Pictures\1cWy43U6UB1yaWgds5.jpg.bitpy	Dropped File	95.62 KB	application/octet-stream	Create, Write, Access	CLEAN
a007ccfae160b697caee93429c79db44da20d011f6a1df922425c7274d26b405	C:\Users\kEecfMwgj\Pictures\9NV7HJvRw0QQr0hlwhy.png.bitpy	Dropped File	8.34 KB	application/octet-stream	Create, Write, Access	CLEAN
30896086a672404c57d20a6b82dfc9cc9f804908790690904456eb80dfeed94e	C:\Users\kEecfMwgj\Pictures\c9kvkj2NGeB.png.bitpy	Dropped File	59.73 KB	application/octet-stream	Create, Access	CLEAN
1009a69076c6b4727254afd09f74559528a3e19790e34afe4f1277405885e9f4	C:\Users\kEecfMwgj\Pictures\HKNKtQ.jpg.bitpy	Dropped File	60.02 KB	application/octet-stream	Create, Write, Access	CLEAN
b053593b01e1f0d23853efef78d45378e1d0a63d053ed668620295723b45ab66	C:\Users\kEecfMwgj\Pictures\kITMELnl0grVCrYTU.jpg.bitpy	Dropped File	92.70 KB	application/octet-stream	Create, Write, Access	CLEAN
0d46bfd231094488a9a291b153a49f58edabd7735a0b9a4a3dc52ca603753724	C:\Users\kEecfMwgj\Pictures\rImHN1xh0sKY5.gif.bitpy	Dropped File	61.09 KB	application/octet-stream	Create, Write, Access	CLEAN
a9113df7cffcc66fdf4fe55c371ade92b33d027e5998282a07b5d292877aa265	C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg.bitpy	Dropped File	858.81 KB	application/octet-stream	Create, Write, Access	CLEAN
57be857093a09f50754e8a34947641f07693c7d9310358e057a09bcfc7f74972	C:\Users\Public\Pictures\Sample Pictures\Desert.jpg.bitpy	Dropped File	826.14 KB	application/octet-stream	Create, Write, Access	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Boot\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	SUSPICIOUS

File Name	Category	Operations	Verdict
System Paging File	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\list.txt	Accessed File	Access	CLEAN
C:\	Accessed File	Access	CLEAN
C:\Boot\cs-CZ\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\da-DK\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\de-DE\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\el-GR\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\en-US\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\es-ES\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\fi-FI\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\Fonts\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\fr-FR\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\hu-HU\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\it-IT\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\ja-JP\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\ko-KR\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\nb-NO\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\nl-NL\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\pl-PL\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\pt-BR\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\pt-PT\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\ru-RU\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\sv-SE\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\tr-TR\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\zh-CN\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\zh-HK\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Boot\zh-TW\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\Documents and Settings\# HELP_TO_DECRYPT_YOUR_FILES #.html	Accessed File	Create, Write, Access	CLEAN
C:\PerfLogs\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\PerfLogs\Admin\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Application Data\# HELP_TO_DECRYPT_YOUR_FILES #.html	Accessed File	Create, Write, Access	CLEAN
C:\ProgramData\Desktop\# HELP_TO_DECRYPT_YOUR_FILES #.html	Accessed File	Create, Write, Access	CLEAN
C:\ProgramData\Documents\# HELP_TO_DECRYPT_YOUR_FILES #.html	Accessed File	Create, Write, Access	CLEAN
C:\ProgramData\Favorites\# HELP_TO_DECRYPT_YOUR_FILES #.html	Accessed File	Create, Write, Access	CLEAN

File Name	Category	Operations	Verdict
C:\ProgramData\Microsoft\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Assistance\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Assistance\Client\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Assistance\Client\1.0\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Assistance\Client\1.0\en-US\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\stream.x86.en-us.man.dat	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\en-us.16\stream.x86.en-us.man.dat.bitpy	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\stream.x86.x-none.man.dat	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\E728F99D-05D1-4020-9ECE-6DE2EC414166\x-none.16\stream.x86.x-none.man.dat.bitpy	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\MachineData\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\MachineData\Catalog\Packages\{9AC08E99-230B-47E8-9721-4577B7F124EA}\{1A8308C7-90D1-4200-B16E-646F163A08E8}\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\MachineData\Integration\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\MachineData\Integration\ShortcutBackups\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\UserData\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Crypto\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Crypto\DSS\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN

File Name	Category	Operations	Verdict
C:\ProgramData\Microsoft\Crypto\DSS\MachineKeys\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Crypto\Keys\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Crypto\RSA\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\background.png	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\background.png.bitpy	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\device.png	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\device.png.bitpy	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\overlay.png	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\overlay.png.bitpy	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\superbar.png	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{113527a4-45d4-4b6f-b567-97838f1b04b0}\superbar.png.bitpy	Dropped File	Create, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\background.png	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\background.png.bitpy	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\watermark.png	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Device\{8702d817-5aad-4674-9ef3-4d3decd87120}\watermark.png.bitpy	Dropped File	Create, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Task\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Task\{07deb856-fc6e-4fb9-8add-d8f2cf8722c9}\en-US\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Device Stage\Task\{e35be42d-f742-4d96-a50a-1775fb1a7a42}\en-US\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN

File Name	Category	Operations	Verdict
C:\ProgramData\Microsoft\DeviceSync\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\DRM\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\DRM\Server\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\eHome\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\eHome\logs\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\IdentityCRL\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Media Player\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\MF\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\NetFramework\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\NetFramework\BreadcrumbStore\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Network\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Network\Connections\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Network\Downloader\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Network\Downloader\qmgr0.dat	Accessed File	Access	CLEAN
C:\ProgramData\Microsoft\Network\Downloader\qmgr1.dat	Accessed File	Access	CLEAN
C:\ProgramData\Microsoft\Office\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\OfficeSoftwareProtectionPlatform\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\OfficeSoftwareProtectionPlatform\tokens.dat	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Microsoft\OfficeSoftwareProtectionPlatform\tokens.dat.bitpy	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\OfficeSoftwareProtectionPlatform\Cache\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\OfficeSoftwareProtectionPlatform\Cache\cache.dat	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Microsoft\OfficeSoftwareProtectionPlatform\Cache\cache.dat.bitpy	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\RAC\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\RAC\Outbound\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\RAC\PublishedData\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\RAC\PublishedData\RacWmiDatabase.sdf	Accessed File	Access	CLEAN
C:\ProgramData\Microsoft\RAC\StateData\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\RAC\StateData\RacDatabase.sdf	Accessed File	Access	CLEAN
C:\ProgramData\Microsoft\RAC\StateData\RacMetaData.dat	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\ProgramData\Microsoft\RAC\Temp\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Search\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Search\Data\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Search\Data\Applications\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\Search\Data\Temp\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\User Account Pictures\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft\User Account Pictures\kEecfMwgj.dat	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Microsoft\User Account Pictures\kEecfMwgj.dat.bitpy	Dropped File	Create, Access	CLEAN
C:\ProgramData\Microsoft\User Account Pictures\Default Pictures\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Access	CLEAN
C:\ProgramData\Microsoft\Vault\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Access	CLEAN
C:\ProgramData\Microsoft\WwanSvc\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Access	CLEAN
C:\ProgramData\Microsoft\WwanSvc\Profiles\# HELP_TO_DECRYPT_YOUR_FILES #.html	Accessed File	Create, Access	CLEAN
C:\ProgramData\Microsoft OneDrive\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Microsoft OneDrive\setup\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\42D5BEC7DDFBD49E76467529CBC2868987BF8460\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\42D5BEC7DDFBD49E76467529CBC2868987BF8460\packages\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\42D5BEC7DDFBD49E76467529CBC2868987BF8460\packages\Patch\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\42D5BEC7DDFBD49E76467529CBC2868987BF8460\packages\Patch\x64\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\54050A5F8AE7F0C56E553F0090146C17A1D2BF8D\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\54050A5F8AE7F0C56E553F0090146C17A1D2BF8D\packages\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\54050A5F8AE7F0C56E553F0090146C17A1D2BF8D\packages\Patch\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\54050A5F8AE7F0C56E553F0090146C17A1D2BF8D\packages\Patch\x64\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\{0FA68574-690B-4B00-89AA-B28946231449}v14.25.28508\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\{0FA68574-690B-4B00-89AA-B28946231449}v14.25.28508\packages\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\{0FA68574-690B-4B00-89AA-B28946231449}v14.25.28508\packages\vcRuntimeAdditional_x86\# HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Write, Access	CLEAN

File Name	Category	Operations	Verdict
C:\ProgramData\Package Cache\{0FA68574-690B-4B00-89AA-B28946231449}\v14.25.28508\packages\vcRuntimeAdditional_x86\cab1.cab	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Package Cache\{0FA68574-690B-4B00-89AA-B28946231449}\v14.25.28508\packages\vcRuntimeAdditional_x86\cab1.cab.bitpy	Dropped File	Create, Write, Access	CLEAN
C:\ProgramData\Package Cache\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\v12.0.21005\packages\vcRuntimeMinimum_x86\cab1.cab	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Package Cache\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}\v12.0.21005\packages\vcRuntimeMinimum_x86\cab1.cab.bitpy	Dropped File	Create, Access	CLEAN
C:\ProgramData\Package Cache\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}v14.25.28508\#HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Access	CLEAN
C:\ProgramData\Package Cache\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}v14.25.28508\packages\#HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Access	CLEAN
C:\ProgramData\Package Cache\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\v14.25.28508\packages\vcRuntimeMinimum_x86\#HELP_TO_DECRYPT_YOUR_FILES #.html	Dropped File	Create, Access	CLEAN
C:\ProgramData\Package Cache\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\v14.25.28508\packages\vcRuntimeMinimum_x86\cab1.cab	Accessed File	Delete, Read, Access	CLEAN
C:\ProgramData\Package Cache\{2BC3BD4D-FABA-4394-93C7-9AC82A263FE2}\v14.25.28508\packages\vcRuntimeMinimum_x86\cab1.cab.bitpy	Dropped File	Create, Access	CLEAN
C:\ProgramData\Package Cache\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\v11.0.61030\packages\vcRuntimeAdditional_amd64\cab1.cab	Accessed File	Delete, Access	CLEAN

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	-	-	-	GET	CLEAN
https://blockchain.com	-	-	-	GET	CLEAN
https://localbitcoins.com	-	-	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
maxcdn.bootstrapcdn.com	-	-	HTTPS	CLEAN
blockchain.com	-	-	HTTPS	CLEAN
localbitcoins.com	-	-	HTTPS	CLEAN

Process

Process Name	Commandline	Verdict
274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe	"C:\Users\kEecfMwgj\Desktop\274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244.exe"	MALICIOUS

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.4.1
Dynamic Engine Version	4.4.1 / 01/14/2022 05:06
Static Engine Version	4.4.1.0 / 2022-01-14 04:00:58
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.16 / 2022-03-11 16:16:43
Smart Memory Dumping Rules Version	4.4.1.6 / 2021-12-14 15:06:27
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.19 / 2022-03-31 10:55:59
YARA Built-in Ruleset Version	4.4.1.19

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp
System Root	C:\Windows