MALICIOUS

Classifications: Ransomware

Threat Names: STOP | Mal/HTMLGen-A | Djvu

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe**
ID	#5067675
MD5	5fae11a9ddb49452b6896fd3217e9665
SHA1	a642378099d0ac4e1dc3e0abe98b12bee1992e1d
SHA256	12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b
File Size	730.00 KB
Report Created	2022-08-05 14:59 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (24 rules, 146 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #11) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #11) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 220 files by appending the extension ".vvyu".			
5/5	YARA	Malicious content matched by YARA rules	100	Ransomware

- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\V89DayYK-6YpvEr4NY.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_ oxvk\61x to95hr3jmn6z\yw2t95\rnqkcz9li.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\-DwrKzsIsF2\SVKL6Wu5uab uSVqvA\Y5X8\0o41ZS\b5aBDkyBYyj.swf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E07daaq0LDB.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_ OxVk\61X TO95hR3JMn6Z\pE7_nJD0Tmm8m2VYvr.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\iudig2j9jtqfgbcv6n.docx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\pe 0cuon\jrz5y.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\ymomnephob\7q5_45ijmfp9ba_ydmbp0zwbtzu.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\tE1LWlZl-CqVZeW gL\Gpf_fTly87TJO1Dp27TE.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\appdata\locallow\microsoft\internet explorer\services\search_{0633ee93-d776-472f-a0ff-e1416b8b2e3a}.ico.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\0o41zs\lzhdqsiji02\ffcamngkkb8gmcsqdpq.mkv.vvyu".
- Rule "Djvu" from ruleset "Ransomware" has matched on a memory dump for (process #6) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe.
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\ul-Z5b.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\d7pQIdSiE6laiAyeoE\cH1Zz4OF5OqujiOEN9.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Contacts\Administrator.contact.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\azld\uhfbjiac\nooizr\rt8g.pptx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\0o41zs\235vhs8kou7y.mp4.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\favorites\links\web slice gallery.url.vvyu".
- Rule "Djvu" from ruleset "Ransomware" has matched on a memory dump for (process #2) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe.
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\ZsR7Xc26_DfdmVcahH\PRpouSq\QwaTwvQX1o7erS.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\HDnGwo1W3X7Qq9.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\vzsbld-s6.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\AzlD\PeBfuwtoR 4_wgbJ2d7Z.csv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\bnbjzezhttp-mha.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\7Q5_45ijmfP9bA\iJwMptujDhUTwyI.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\ymomnephob\e5ucc4gr1z tmgype\qjvfzvvw_idbuk5j3vj1.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\qxlg6rlrsvyemxil.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\141isvJREPi.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\z6ibw svk.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\exzou4j4nw j\m5lkrrhopgpv2jhgtq-.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop_gemdk.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\gz- yqulpeghm6.odt.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\ymomnephob\7q5_45ijmfp9ba\lejzvedjk.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\7rMc5PE99.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E5UCc4GR1Z tMgYPe\k1TTTQU2.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\xc6y6diw-2mp3g1ez.mkv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\FDSFO0.avi.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\YwgWoXY4_d Sr.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\5fJKex2DUyLjzY0p.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\fmtiy2j60xys_lff.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\u7unq0 vl v.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_ oxvk\61x to95hr3jmn6z\brlu 5vgds.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\ntkcvhllb.pps.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\hstszlrr9zv1_v.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\7oqi8laykzm3pzqg.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\-DwrKzsIsF2\SVKL6Wu5uab uSVqvA\Y5X8\0o41ZS\EDTDz9.mp4.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\fuhvly4jeagwk\nfk529nzfij1e1.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\x9kn7y7cefv.xls.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\labkKD4FQA.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\a1p6lyhhe5fq5dudw9xm.rtf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_ OxVk\61X TO95hR3JMn6Z\yw2t95\rQWnqazpz-naoLL5R.wav.vvyu".

Score	Category	Operation	Count	Classification
4/5	Reputation	Known malicious file	1	-

- The sample itself is a known malicious file.

Score	Category	Operation	Count	Classification
4/5	Reputation	Contacts known malicious URL	3	-

- Reputation analysis labels the URL "http://acacaca.org/files/1/build3.exe" which was contacted by (process #6) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "http://rgyui.top/dl/build2.exe" which was contacted by (process #6) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "http://acacaca.org/test2/get.php?pid=248506A379C3838D8B1754B19D2995D3&first=true" which was contacted by (process #6) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe as Mal/HTMLGen-A.

Score	Category	Operation	Count	Classification
4/5	Reputation	Resolves known malicious domain	2	-

- Reputation analysis labels the resolved domain "acacaca.org" as Mal/HTMLGen-A.
- Reputation analysis labels the resolved domain "rgyui.top" as Mal/HTMLGen-A.

Score	Category	Operation	Count	Classification
3/5	YARA	Suspicious content matched by YARA rules	6	-

- Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR 4\tEiHH.pdf.vvyu".
- Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR 4\tEiHH.pdf.vvyu".
- Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\7bowspyroi2cx.pdf.vvyu".
- Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\7bowspyroi2cx.pdf.vvyu".
- Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "c:\users\keecfmwgj\documents\bflhqgtm.pdf.vvyu".
- Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "c:\users\keecfmwgj\documents\bflhqgtm.pdf.vvyu".

Score	Category	Operation	Count	Classification
2/5	Hide Tracks	Deletes file after execution	1	-

- (Process #2) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe deletes executed executable "C:\Users\kEecfMwgj\AppData\Local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe".

Score	Category	Operation	Count	Classification
2/5	Anti Analysis	Delays execution	1	-

- (Process #6) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe has a thread which sleeps more than 5 minutes.

Score	Category	Operation	Count	Classification
2/5	_data_collection	Reads sensitive application data	1	-

- (Process #11) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe tries to read sensitive data of application "git" by file.

Score	Category	Operation	Count	Classification
2/5	Injection	Writes into the memory of a process started from a created or modified executable	3	-

- (Process #1) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe modifies memory of (process #2) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe.
- (Process #5) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe modifies memory of (process #6) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe.
- (Process #10) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe modifies memory of (process #11) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe.

Score	Category	Operation	Count	Classification
2/5	Injection	Modifies control flow of a process started from a created or modified executable	3	-

- (Process #1) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe alters context of (process #2) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe.
- (Process #5) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe alters context of (process #6) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe.
- (Process #10) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe alters context of (process #11) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe.

Score	Category	Operation	Count	Classification
2/5	Task Scheduling	Schedules task	1	-

Score	Category	Operation	Count	Classification
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe", to be triggered by TIME. Task has been rescheduled by the analyzer.			
1/5	Obfuscation	Reads from memory of another process	3	-
	• (Process #1) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe reads from (process #1) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe. • (Process #5) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe reads from (process #5) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe. • (Process #10) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe reads from (process #10) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	3	-
	• (Process #1) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #5) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #10) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.		
1/5	Discovery	Enumerates running processes	3	-
	• (Process #2) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe enumerates running processes. • (Process #6) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe enumerates running processes. • (Process #11) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe enumerates running processes.		
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #2) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe adds ""C:\Users\kEecfMwgj\AppData\Local\11c63de0... ...8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe" --AutoStart" to Windows startup via registry.		
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #2) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe starts (process #2) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe with a hidden window.		
1/5	Mutex	Creates mutex	2	-
	• (Process #6) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe creates mutex with name "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}". • (Process #11) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe creates mutex with name "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}".		
1/5	Discovery	Tries to get network statistics	1	-
	• (Process #11) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe gets network statistics via API.		
1/5	Network Connection	Downloads file	1	-
	• (Process #6) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe downloads file via http from http://acacaca.org/test2/get.php?pid=248506A379C3838D8B1754B19D2995D3&first=true.		
1/5	Obfuscation	Resolves API functions dynamically	6	-
	• (Process #1) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe resolves 39 API functions by name. • (Process #2) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe resolves 37 API functions by name. • (Process #5) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe resolves 39 API functions by name. • (Process #6) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe resolves 37 API functions by name. • (Process #10) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe resolves 39 API functions by name. • (Process #11) 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe resolves 58 API functions by name.		

Mitre ATT&CK Matrix

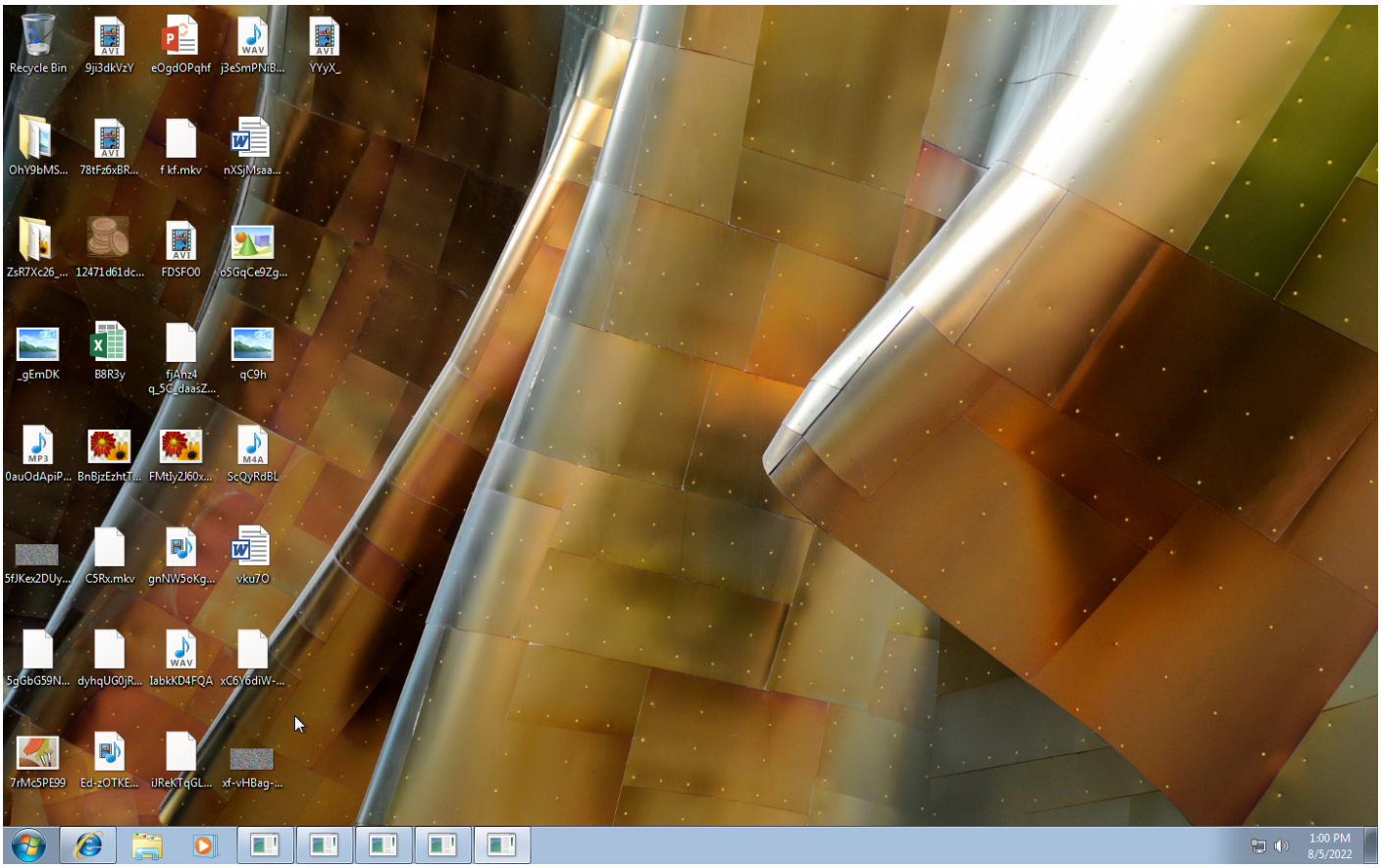
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1060 Registry Run Keys / Startup Folder	#T1053 Scheduled Task	#T1045 Software Packing	#T1081 Credentials in Files	#T1057 Process Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol		#T1486 Data Encrypted for Impact
		#T1053 Scheduled Task		#T1112 Modify Registry		#T1083 File and Directory Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
				#T1143 Hidden Window		#T1016 System Network Configuration Discovery					
						#T1049 System Network Connections Discovery					

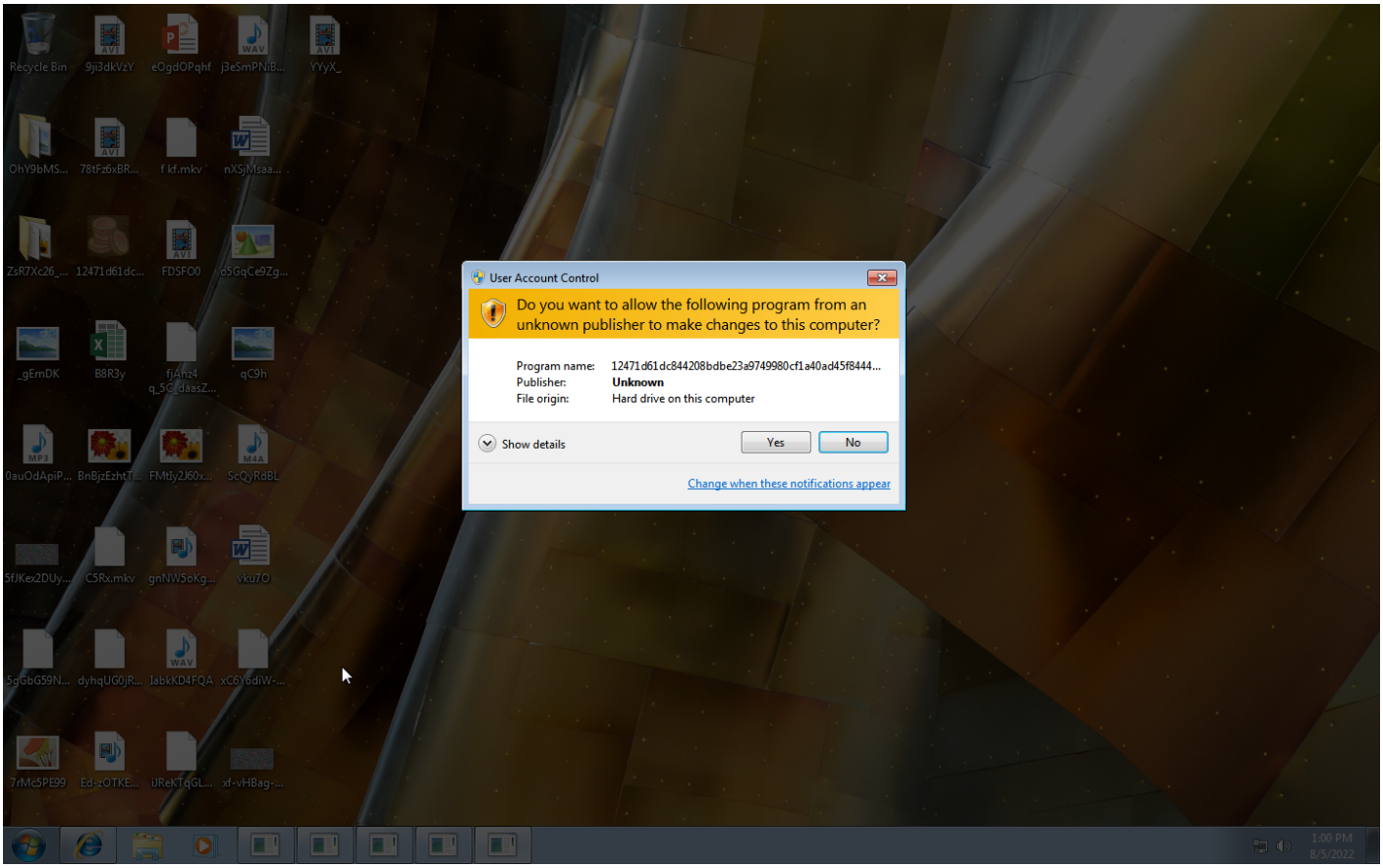
Sample Information

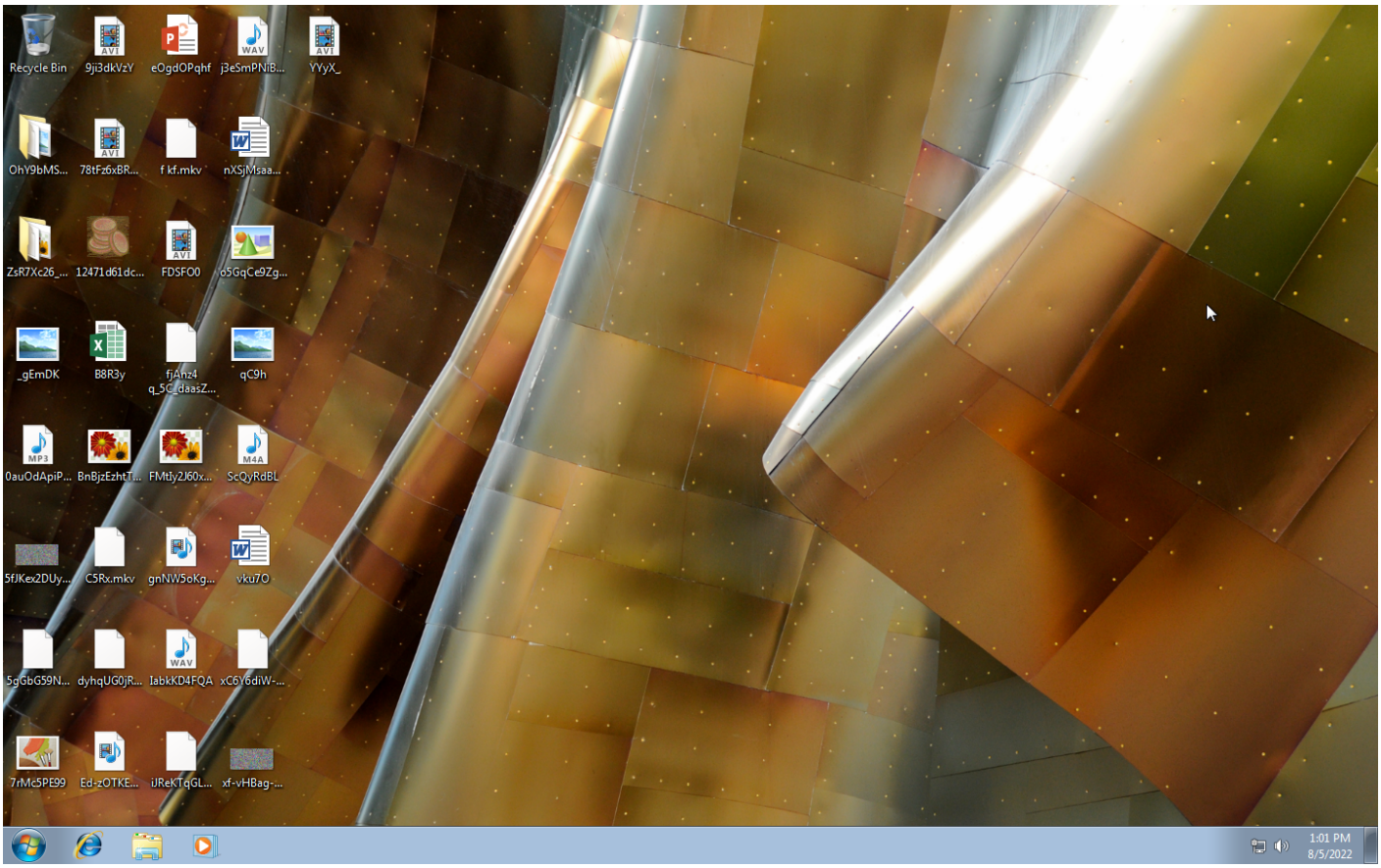
ID	#5067675
MD5	5fae11a9ddb49452b6896fd3217e9665
SHA1	a642378099d0ac4e1dc3e0abe98b12bee1992e1d
SHA256	12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b
SSDeep	12288:nCqmkJm0QpmFRBBAw356C94EnhtoLWBEmlCW85h1bmyA5qKyr3ty+SqOhUII84ko:n410QpmfBB5UEnhtjroWW/Hro+TICktO
ImpHash	fcbdb87c73dba6603c8b6aba49ea683b
File Name	12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe
File Size	730.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

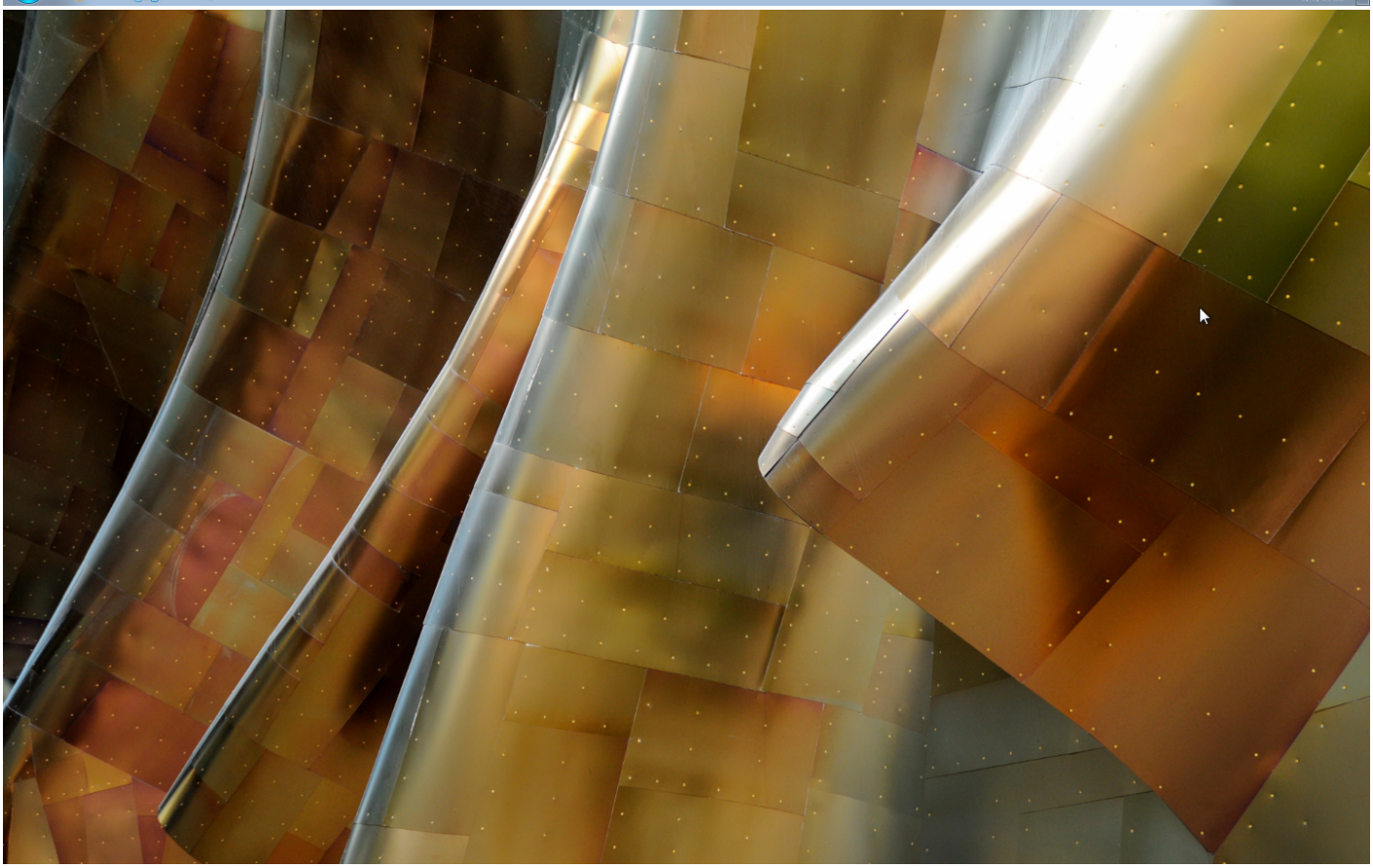
Analysis Information

Creation Time	2022-08-05 14:59 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	7
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	304




User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 12471d61dc844208bdbe23a9749980cf1a40ad45f8444...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

124.39 KB total sent

118.65 KB total received

4 ports 80, 443, 53, 445

3 contacted IP addresses

1 URLs extracted

3 files downloaded

0 malicious hosts detected

DNS

4 DNS requests for 3 domains

1 nameservers contacted

1 total requests returned errors

HTTP/S

3 URLs contacted, 2 servers

5 sessions, 3.33 KB sent, 26.13 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://rgyui.top/dl/build2.exe	-	-		0 bytes	NA
GET	http://acacaca.org/test2/get.php?pid=248506A379C3838D8B1754B19D2995D3&first=true	-	-		0 bytes	NA
GET	http://acacaca.org/files/1/build3.exe	-	-		0 bytes	NA
GET	https://api.2ip.ua/geo.json	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	acacaca.org	NO_ERROR	189.164.252.207, 190.140.99.150, 190.117.75.91, 187.170.251.250, 211.53.230.67, 190.219.54.242, 124.109.61.160, 116.121.62.237, 5.163.244.118, 110.14.121.125		NA
A	api.2ip.ua	NO_ERROR	162.0.217.254		NA
A	rgyui.top	SERV_FAIL			NA

BEHAVIOR

Process Graph

Process #1: 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 53276, Reason: Analysis Target
Unmonitor End Time	End Time: 68467, Reason: Terminated
Monitor duration	15.19s
Return Code	0
PID	3848
Parent PID	1916
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	730.00 KB	12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b	✖

Host Behavior

Type	Count
System	3
Module	52
File	6
Environment	1
Window	1
Process	1
-	3
-	9

Process #2: 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 66898, Reason: Child Process
Unmonitor End Time	End Time: 95349, Reason: Terminated
Monitor duration	28.45s
Return Code	0
PID	3872
Parent PID	3848
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf0c	0x400000(4194304)	0x400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf0c	0x401000(4198400)	0xca600	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf0c	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf0c	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf0c	0x52b000(5419008)	0x200	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf0c	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf0c	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf0c / 0xf24	0x76f101c4(1995506116)	-	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	730.00 KB	12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b	✖

Host Behavior

Type	Count
System	4
Module	47
File	6
Environment	1
Process	100
Registry	4
COM	1

Network Behavior

Type	Count
HTTPS	1

Process #4: icacls.exe

ID	4
File Name	c:\windows\syswow64\icacls.exe
Command Line	icacls "C:\Users\kEecfMwgj\AppData\Local\11c63de0-7744-463b-80d8-a375eb15d14b" /deny *S-1-1-0:(OI)(CI)(DE,DC)
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 90460, Reason: Child Process
Unmonitor End Time	End Time: 91865, Reason: Terminated
Monitor duration	1.41s
Return Code	0
PID	3912
Parent PID	3872
Bitness	32 Bit

Process #5: 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 93466, Reason: Child Process
Unmonitor End Time	End Time: 96930, Reason: Terminated
Monitor duration	3.46s
Return Code	0
PID	3928
Parent PID	3872
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	52
File	6
Environment	1
Window	1
Process	1
-	3
-	9

Process #6: 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 95364, Reason: Child Process
Unmonitor End Time	End Time: 115528, Reason: Terminated
Monitor duration	20.16s
Return Code	0
PID	3940
Parent PID	3928
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf5c	0x400000(4194304)	0x400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf5c	0x401000(4198400)	0xca600	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf5c	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf5c	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf5c	0x52b000(5419008)	0x200	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf5c	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf5c	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#5: c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0xf5c / 0xf68	0x76f101c4(1995506116)	-	✔	1

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\SystemID\PersonalID.txt	42 bytes	133276d46de8f4c5849b7ee9536406e0edfc2608134b2b0e4467d9e51c209f03	✖
C:\Users\kEecfMwgj\AppData\Local\bowsakkdestx.txt	557 bytes	3697f5de19894fd52f417f95a1eadd819359edca9b1cc944b110374bbdc821d6	✖

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

Host Behavior

Type	Count
System	4
Module	47
File	16
Environment	1
Process	98
Registry	7
COM	1
-	2
Mutex	1
User	1
Window	1
-	3

Network Behavior

Type	Count
HTTP	3
HTTPS	1
TCP	1

Process #10: 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe

ID	10
File Name	c:\users\keecfmwgj\appdata\local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe" --AutoStart
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 162434, Reason: Autostart
Unmonitor End Time	End Time: 166892, Reason: Terminated
Monitor duration	4.46s
Return Code	0
PID	1912
Parent PID	1732
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	52
File	6
Environment	1
Window	1
Process	1
-	3
-	9

Process #11: 12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe

ID	11
File Name	c:\users\keecfmwgj\appdata\local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe" --AutoStart
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 166219, Reason: Child Process
Unmonitor End Time	End Time: 199221, Reason: Terminated
Monitor duration	33.00s
Return Code	0
PID	2008
Parent PID	1912
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0x77c	0x400000(4194304)	0x400	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0x77c	0x401000(4198400)	0xca600	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0x77c	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0x77c	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0x77c	0x52b000(5419008)	0x200	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0x77c	0x52c000(5423104)	0xa400	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0x77c	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#10: c:\users\keecfmwgj\appdata\local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	0x77c / 0x7dc	0x774701c4(2001142212)	-	✔	1

Dropped Files (223)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Pictures\V89DayYK-6YpvEr4NY.gif.vvyu	57.97 KB	f02b1904b5279c9e50a252832d78819eb4883be83cd7c6dc27f51ade29c72288	✔
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipgggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\yw2t95\rnqkcz9li.mp3.vvyu	73.26 KB	5b6f6c4cae9d7470ccbb4e3ac69b8877b469e7a172d042dd5369e3e3282036da	✔
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\Y5X8\0o41ZS\b5aBDkyBYyj.swf.vvyu	76.29 KB	4bf2e089147461270f6a65e0412b862ed8a06198042a07683dcf67c85a417e8e	✔
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E07daaq0LDB.bmp.vvyu	56.61 KB	d863d924f7e7ba862654e416624d7c404749efe1b95307a4ba3c1fd3d5894837	✔
C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_ OxVk\61X TO95hR3JMn6Z\pE7_nJD0Tmm8m2VYvr.wav.vvyu	82.05 KB	d3f2bae7e647bfe7f5526820f598936224d893663e958b3c515751f38eb8fe0a	✔
c:\users\keecfmwgj\documents\iudig2j9jtqfgbcv6n.docx.vvyu	87.56 KB	47310efa770cd02ca456ec0be0a6aa41620e74bffc4a3a5e0a0d2c8a9729494e	✔
c:\users\keecfmwgj\music\pe 0cuon\jrz5y.mp3.vvyu	39.08 KB	0cce7483c297f60938fff8e1ef7a2b16dbe7bc33a94753833b9bde96a683517e	✔
c:\users\keecfmwgj\pictures\ymomnephob\7q5_45ijmfp9ba_ydmbp0zwbtzu.gif.vvyu	3.55 KB	4d5a7096b11a024cbf9be32c57231ae3aab3c9d2cafe859464b55aed8d9b6ce2	✔
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\tE1LWIZI-CqVZeWgL\Gpf_fTIy87TJO1Dp27TE.png.vvyu	20.14 KB	3727cb7a09ee05091fac7365e73d477eed533d1dde05e2c0a17f46141347b33a	✔
c:\users\keecfmwgj\appdata\locallow\microsoft\internet explorer\services\search_{0633ee93-d776-472f-a0ff-e1416b8b2e3a}.ico.vvyu	4.51 KB	330c15c54f0e83252731e6f5f820b23da10abb2bec366d32591853c58137a76d	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\y5x8\0o41zs\lzhdqsiji02\ffcamngkkb8gmcsqdpq.mkv.vvyu	73.75 KB	f9a1156e19d0529b9a9ab262624bdf84b70d70666b252121e0ba516e267548fd	✔
C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\uI-Z5b.m4a.vvyu	59.97 KB	e5d87b136c70c39ff6405b816da88aac020f352eff419e5ed5cc84eacdce35d7	✔
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\d7pQIdSiE6laiAyeoE\cH1Zz4OF5OqujiOEN9.png.vvyu	75.24 KB	49846a73c6501462096b1c21e66aa72e35f10a0c03d140bcb34554241b888453	✔
C:\Users\kEecfMwgj\Contacts\Administrator.contact.vvyu	67.11 KB	0f85ff2fffee56f6f192bfe01dfb3cd3e967697858842a02db80faaaf1456b22	✔
c:\users\keecfmwgj\documents\azld\uhfbjiac\nooizr\rt8g.pptx.vvyu	29.82 KB	e264b3e3d211e9192f546494f09aab136c24c2cab1c9fcfc212d4c2867fb370f	✔
c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe.vvyu	730.00 KB	12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b	✖
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\y5x8\0o41zs\235vhs8kou7y.mp4.vvyu	36.67 KB	3e3e3f8b29eaa006e5c80d738f5e6ebf9f17b74774dce1d2eb0c72a250796aa2	✔
c:\users\keecfmwgj\favorites\links\web slice gallery.url.vvyu	560 bytes	ff2b159f3e45375b0f330c00f525e7e8346e5ebf617d5c2922de7f1844bb8d9c	✔
C:\Users\kEecfMwgj\Desktop\ZsR7Xc26_DfdmVcahH\PRpouSq\QwaTwvQX1o7erS.mp3.vvyu	37.39 KB	50800ad30c11f75bd3d885d407e947d57a6db0f22a8d0a1c1376bcb0994f88e4	✔
C:\Users\kEecfMwgj\Videos\HDnGwo1W3X7Qq9.flv.vvyu	31.50 KB	c43abf420eeb327012e38edf4617b01764e8de8eced43f2c18aa5e416d9ff055	✔

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\vzsbld-s6.bmp.vvyu	67.92 KB	d73efcc2460acfacfe99bb0e31f648fe21f34b69b3586f50172e8b8276f2ae74	✔
C:\Users\kEecfMwgj\Documents\AzlD\PeBfuwtoR4_wgbJ2d7Z.csv.vvyu	4.95 KB	f46d42ff58ca370c6629f89bfa7981f1431d69c7584920b4d8f088416920b912	✔
c:\users\keecfmwgj\desktop\bnbjzezhttp-mha.png.vvyu	31.85 KB	665c2b66c23e2f55dabe15c79c47d7578b80bea124030d2ec9d24de0dd633fcf	✔
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\7Q5_45ijmfP9bA\iJwMptujDhUTwyI.gif.vvyu	89.97 KB	350c096d17a07202e4fac1c1315b281a15277eba91f52a5c3b76257b9dc0ebb3	✔
c:\users\keecfmwgj\pictures\ymomnephob\e5ucc4gr1ztmgype\qjvfzvvw_idbuk5j3vj1.gif.vvyu	24.85 KB	aeca6a9c6ef9a0f12e6c834ea246f5d93c33be1d6f7fd27edb04d00bdc99f736	✔
c:\users\keecfmwgj\music\qxlg6rlrsvyemxil.m4a.vvyu	67.87 KB	75b19dd98d4a3bfab42f3af355bee3fa882ee536f17cb3cd06ab5b8c13164b12	✔
C:\Users\kEecfMwgj\Pictures\141isvJREPi.gif.vvyu	20.45 KB	19cdf8caba97b3b7afa1a9d2f3f680cc8132bb217a61341d072ff1b06545841e	✔
c:\users\keecfmwgj\documents\z6ibw svk.xlsx.vvyu	11.77 KB	66b85a46f946ba468b0623b24d4611603c6be4e667b2fbd0d2b8658fb6f7b1b0	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\exzou4j4nw j\m5lkrrhopgpv2jhgtq-.flv.vvyu	90.98 KB	2a441d7482f2330ecb193b7d7e56fe36d8c2e9318a947bce736150abc71dce0a	✔
c:\users\keecfmwgj\desktop_gemdk.jpg.vvyu	54.55 KB	2b8dd6407cd533cee27b868f34d37e34f3cb97dae8643d488447a183c7f3d127	✔
c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\gz-yqulpeghm6.odt.vvyu	37.36 KB	e23711b92a696bd7b023e30ef6f097781fb035c2faef4eb81ac32c3fcd239538	✔
c:\users\keecfmwgj\pictures\ymomnephob\7q5_45ijmfp9ba\lejzvedjk.gif.vvyu	15.62 KB	e24e8d6ab0a8592bdf315710f5c42d20965e9070e25943ff6f3ee817b3d05518	✔
C:\Users\kEecfMwgj\Desktop\7rMc5PE99.bmp.vvyu	15.13 KB	3308fb0e8ee3134a17ad0c43c021ad0a78459fbb21c4d4a7a8015517d3b14f03	✔
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E5UCc4GR1ZtMgYPe\k1TTTQU2.bmp.vvyu	78.29 KB	57beff21a68985a1edbbdd0ddf3cea44ebd37f295b817928b61b50d3de22f105	✔
c:\users\keecfmwgj\desktop\xc6y6diw-2mp3g1ez.mkv.vvyu	86.13 KB	8732265e1f7e02b48c6382b345171ea7e81e144f69ea7f9f8aab1351ea425727	✔
C:\Users\kEecfMwgj\Desktop\FDSFO0.avi.vvyu	65.04 KB	1bbc45862a85e6dbab93d999744601ff6b4b9ce2252dfc258711902509ea252a	✔
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\YwgWoXY4_d Sr.jpg.vvyu	98.59 KB	1d5a4c5b0e0c6ecab87ae5cdee78d774902850babd7385624cc44680363741de	✔
C:\Users\kEecfMwgj\Desktop\5fJKex2DUyLjzY0p.bmp.vvyu	50.66 KB	7bbe58971d385c76aa42b9c396adcd14fa96404e2f96dceb75aaa2d4823d97cd	✔
c:\users\keecfmwgj\desktop\fmtiy2j60xys_lff.png.vvyu	51.52 KB	54ae3f8cc3cbda628e0b9afd0d08b34c3649b5db188978fb658a613c72280e8f	✔
c:\users\keecfmwgj\videos\u7unq0 vl v.flv.vvyu	16.73 KB	f5dce59b40e7245fd54c11f9b034952c1abe27a26ead0c8c5f68bfc631b7fd8b	✔
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\brlu 5vgds.wav.vvyu	41.23 KB	2336646e50f482c8c479332c9292b0f1b0445ada546824f5b7bafdb17ba1b4d7	✔
c:\users\keecfmwgj\documents\ntkcvhllb.pps.vvyu	86.75 KB	3cb185c7c58bcdbaf6c52ab73a75db3960e9e09abd91affaf3bd10a2bbd951dc	✔
c:\users\keecfmwgj\documents\hstszlrr9zv1_v.xlsx.vvyu	40.09 KB	5d3dea242ad98e6ed353296653b80c004561814dadd0f4f0c36f2a157b829fa4	✔
C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url.vvyu	468 bytes	70a9ce1e59fcf76a1a4026d7d40a2c6e9cd0b70fe49dfac695091983ef8184e2	✔
c:\users\keecfmwgj\videos\7oqi8laykzm3pzqg.flv.vvyu	62.38 KB	702bebe1ea144f5d9bf220266ab847647de7d3fae7755e2cf12dd0774835bd3d	✔
C:\Users\kEecfMwgj\Videos\-DwrKzsIsF2\SVKL6Wu5uabuSVqvA\Y5X8\0o41ZS\EDTDz9.mp4.vvyu	30.69 KB	13f2c7008dbce22fa9928b6be897cc373a434e8c64b3d3793e99d874e2566d75	✔
c:\users\keecfmwgj\music\fuhvly4jeagwk\nfk529nzfij1e1.mp3.vvyu	55.61 KB	d5be5ba44592909b3d4b12dc923d8c7fe215f462cafeaba0c7a4a78b218d80e2	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\x9kn7y7cefv.xls.vvyu	71.28 KB	ef050899804894f9954d7acee36f4da9d858c9bd732f2853f0c0a1143814707e	✔
C:\Users\kEecfMwgj\Desktop\labkKD4FQA.wav.vvyu	43.72 KB	bc368514a63982827c829da2b35572e55cf141a03b1bebf89d88c5731702f7eb	✔
c:\users\keecfmwgj\documents\a1p6lyhhe5fq5dudw9xm.rtf.vvyu	83.07 KB	ddb98b0aac4656b576bcb113de397e0d121a6af6144582be768c008fe84db9dd	✔
C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url.vvyu	467 bytes	b9be2dbccaf3f2b8e5844d2ee8559ea677eb0793bcf12198f7d61ad2d99fdce4	✔
C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_ OxVk\61X TO95hR3JMn6Z\yw2t95\rQWnqazpz-naoLL5P.wav.vvyu	95.45 KB	cb2a82587118c4f08ed01e883c6cd84e165c136f0a029c1d763f8a3d45c92f5e	✔
c:\users\keecfmwgj\documents\-yzsadt_8t croyrko.pptx.vvyu	57.83 KB	dc9ac8be48a5de98b3a31ef404505db758957bd80e7c272a67f8a9bc0f9b85b9	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\7jjuxf5i.mp4.vvyu	31.91 KB	6db7a3c85e6330ff676d314066e65ab70f0aa7d38e0b15e49593f4effa13b09f	✔
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\Y5X8\0o41ZS\LzHDQsiji02\MQWaq1YvFIYApR.swf.vvyu	85.91 KB	b4bfe9c00914ee6e2e417ba52d8165eb22ddbfdf4ebbd3607a46c4b90e00da9b	✔
C:\Users\kEecfMwgj\Music\tRcMqrNBqTUs.mp3.vvyu	88.14 KB	ea4e84c242b75a977ff7692d60077826fbae2a9bd99e4d629a71fa6b0a636a4b	✔
C:\Users\kEecfMwgj\Documents\OkF0P0lVbo seJvjybv_.docx.vvyu	22.98 KB	dc2841c72b2b1ec5aacc78ae095ceac0025379f43a02f3a93d8b9b114b87809a	✔
c:\users\keecfmwgj\desktop\f kf.mkv.vvyu	20.96 KB	a80c45cf0892d2754bd091737513c1ce9e54fa4f20dad284d6e72a83ff125ee2	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\6cposy.swf.vvyu	4.10 KB	fc3a33814b0d6a2ac79736b54903c31940aa8c653fd61e59d04a779a13b7268c	✔
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\Y5X8\0o41ZS\Fjxa.mp4.vvyu	51.80 KB	11cedc96257ccc5792813ec4b1c077e0f200e3c7ee52bc7fee0d1511a96ad474	✔
c:\users\keecfmwgj\favorites\windows live\windows live mail.url.vvyu	467 bytes	1be6e0c185f55f20726bea3dd881f65564e02b03162f67dd5e75ec74be4fa34d	✔
c:\users\keecfmwgj\documents\yrqwfs6apmpbyvu.doc.vvyu	33.59 KB	f7d4f1a6771eeaf4b0fef37d68a0030fc1f142a6b50338ef8344420f7d36342a	✔
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\tE1LWIZl-CqVZeWgL\CfqSEGHWv8Id7U6qj5.gif.vvyu	89.31 KB	5a227aacc0a154b9269236d6fcc2944a06761c76858d1adea1c774f1b39fbeb0	✔
C:\Users\kEecfMwgj\Documents\AzID\UHfBjlaC\eE nQNbY2KI.doc.vvyu	23.81 KB	17f4783e214965c86467410b4ac705e0cfcd2afd2c09f082b15a33beb738bf0f	✔
c:\users\keecfmwgj\music\zrus.wav.vvyu	18.15 KB	54e9b79990c1d76dc6a37428f9b3e43057ff75074f1fb50249ef59143731e3c7	✔
c:\users\keecfmwgj\desktop\qc9h.jpg.vvyu	32.66 KB	d02439f8d30f64c0aef909e88d722a1f2649e9ea0ba04f727628e732c722ae51	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\qpf-r5z.mp4.vvyu	62.68 KB	121037fbf99d30d3a4c12fc5755717ae693c8fc323b1fa1156a1e02843f117e4	✔
c:\users\keecfmwgj\documents\es4lp.pptx.vvyu	13.75 KB	b34b24ced71de3f18eac20e0dd0e6af25d100ab7a242abc8f6a504c0863692e3	✔
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\F72Mw_KNQRugYJJCcBc\MSPqrTgqm.swf.vvyu	66.89 KB	2360ddfca94e2e4234e28a3d24a907ec35254aafea3eb5658500dd5f72b149a1	✔
C:\Users\kEecfMwgj\Documents\1G5yOYkuiK.docx.vvyu	95.47 KB	00d311913d06e917eeb000cf23f60012688be2577b674074a98d4eee53db47d7	✔
c:\users\keecfmwgj\desktop\5ggbg59nqgc.flv.vvyu	63.82 KB	1739db6cd80149b2f5bc58126fc3d07781a2a910141aeeefd2258b2dd173d7ba	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\0iydfpwavsjadg.mkv.vvyu	69.05 KB	5651c4c7b3488e7a061795597c502fe56c1e67cc8a06b743ad1aa925da608a49	✔
C:\Users\kEecfMwgj\Pictures\9p8OG.bmp.vvyu	91.17 KB	203222c2ba8da6533200fe080a5b9cd8e2b70a81c71d7af1844ddc1f383b5e91	✔
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\VNAR2BEit3ka1sGXw8sq.mp4.vvyu	63.73 KB	30b00c5764da1341a9c100f3a513a99c61eee165a8fe8efd223e785d6bb001f0	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\bst5msuptc.flv.vvyu	62.40 KB	7e0e063ca5c386920c63fc0c82df2ffa5ff6260689b596882bd227b55e9db872	✔

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Documents\AzlD\UHfBjlaC\hlTCx olpB7AQb0\S7akFO0_2kX867.ods.vvyu	20.15 KB	f29ad33e71d3b495db4faf691a85af30064a2b380b9d4834a422f6dd66b3cdc8	✔
C:\Users\kEecfMwgj\Documents\AzlD\UHfBjlaC\yEpRZCn46rxjDOAUpD\feMArPT27Tt3Vq0tfRa.odp.vvyu	31.83 KB	0b11a17ed05567cdfba68d071bfac1e4f120656375b43979f138beea3ef4758f	✔
c:\users\keecfmwgj\documents\e ri1atxotxxvz19.ppt.vvyu	54.39 KB	fb735874771f1ab94bf6be92af63acce3bc48a4333893e3539df079f8e523bfd	✔
C:\Users\kEecfMwgj\Documents\AzlD\PeBfuwtoR 4\tEiHH.pdf.vvyu	60.52 KB	87d09dcc96b9f5fe51a7d3a6df5179b0dde5790d099312776eb417f3dd86fe2a	✔
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\7Q5_45ijmfP9bA\GwAL3j0fQylFxx-jKJ.gif.vvyu	69.55 KB	835942df698062fc77ce38024245a41c3ae569831340aba92c34d6552b684372	✔
c:\users\keecfmwgj\documents\yqj5kxs1j7uvwoh.pptx.vvyu	9.83 KB	f2382a8abfe0d102eb774fdedd014290f94ec99650e7bff9534985dd7554e57c	✔
c:\users\keecfmwgj\desktop\fjanz4 q_5c_daaszw.ots.vvyu	40.34 KB	1457ef7a201dae0072c1b63cdabef8dd2dbb4002c85c599d50ffeb3673633f38	✔
c:\users\keecfmwgj\favorites\msn websites\msn autos.url.vvyu	467 bytes	e9b3f70fd0c57d38dbf1717a4da291a222a0e958651ad5b7dcd9667255664829	✔
C:\Users\kEecfMwgj\Desktop\Ed-zOTKEEUdYISk.mp4.vvyu	38.80 KB	63c48ccfb9c1c2725f75c3f43fa6fce55f2201f603580e00eb0bf68e6e8a0aed	✔
c:\users\keecfmwgj\pictures\8jmjrpib7p7v7jga.png.vvyu	84.64 KB	f9c1e3d3f15f253236e3c6371653208809bde5d790b1bc71bc0f100eed140a3f	✔
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\gFRsS2-OR13.gif.vvyu	78.58 KB	4125d609d0002358ed516dd8b4cb43e58e7a1b435e9b6ab353578eebf77b54ff	✔
C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\n3veXEkNYxTCSfl4 ofL.m4a.vvyu	69.99 KB	dcbb45df48afc4dd383ecff078decd1dc868c364af8cc256e21751a73a5f3276	✔
c:\users\keecfmwgj\pictures\ymomnephob\d7pqidsie6laiayeoe\dh_l_uel n9j1ttp1p51.gif.vvyu	61.49 KB	217ee40236447b18327eb4a334bd03d7537e7d23c5be64ec50398b5f866b69c5	✔
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\yw2t95\ia4pahu.wav.vvyu	28.16 KB	d80d53586bf7e8f2c2b2472a1fbbb7b72dd5107b63e9f9ecb4eb2ecac30ad8c8	✔
c:\users\keecfmwgj\desktop\9ji3dkvzy.avi.vvyu	41.71 KB	d8fa3f08dd3f209598e963e8b037c223a500ecc6ec487381d8db4463a1c5b6f8	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\c9qz99w\82ajw1e0_3n2yyse_.avi.vvyu	74.15 KB	26709dda24db867a0fec33f7f85be2e50e5d65b913cf4cf309c84391656a2657	✔
c:\users\keecfmwgj\desktop\zsr7xc26_dfdmvcahh\exko6hh.png.vvyu	40.30 KB	d4c4c63f26b77e471604ec7aef95bdb1ea5099afbdf57c96a7f86d8ca2539bb4	✔
C:\Users\kEecfMwgj\Documents\AzlD\EXsKx.odp.vvyu	46.84 KB	9b6a93f17fbae46a9d39f93bf0504592dce14b8cbcf62e095054a13d598ec4e8	✔
c:\users\keecfmwgj\pictures\ymomnephob\d7pqidsie6laiayeoe\k4vlze9tyd\9gfedyg-xmcwzgawdh.bmp.vvyu	63.96 KB	124cac85c7a8375d2ee6a5d2792918f9e50ea36fef645d196e2b09f46ec14a97	✔
c:\users\keecfmwgj\pictures\ymomnephob\te1lwlzl-cqvzewgl\-2okt.gif.vvyu	70.28 KB	072b03e6d6d5b5133dea0f917a209d471cc673c685d632719ccfd25676efb002	✔
c:\users\keecfmwgj\documents\azld\pebfuwtor 4\-1ots4a6s.pps.vvyu	54.39 KB	a7a0fd8f39ab20081addfbebbbbb9791bf28b00aea37ff2ce745c10d3327c1fb	✔
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\jymab2bdvruj9sv.m4a.vvyu	16.95 KB	e76ca9c6e5e874576c6cb2a13d5d52893b54450e93316d075640f25257449fbe	✔
c:\users\keecfmwgj\music\oolp hjaohulco5czcdi.mp3.vvyu	15.22 KB	7b5ca90f00d259082ce1ce3c8d9341a2deae05e7dcf760d95aeb3aad782d46d3	✔
C:\Users\kEecfMwgj\Pictures\lv6DMrgKbM_9C6x.jpg.vvyu	3.90 KB	0a2d505911e9bcae92659ea12701988c134fba11415359e5c7531fa2bf246265	✔
c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\7bowspyroi2cx.pdf.vvyu	92.35 KB	49a9102816b0bd13070c208d7eab74e0b0e2e48eba5e10b757b3b91ca2e64544	✔
C:\Users\kEecfMwgj\Documents\AzlD\PeBfuwtoR 4\ivoTJ\soMD9qxXFL8rvNP.rtf.vvyu	49.07 KB	50d40a5b742bcfe20fe56b2b2a1cf95e9a73de88d32d916870cee225a2071e09	✔
c:\users\keecfmwgj\music\pe 0cuon\i_smja7zftd 88.wav.vvyu	89.73 KB	481c458ca680433f7cd0b7f2a558ca24f75ab28d799ca5e71ce5d0700ed669c0	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\documents\azld\pebfuwtor 4\ivotj\tawx51mud\aig5nj9ziln1ciu lcka.odt.vvyu	9.54 KB	95c85188b90c8a901d9b802579144fc87ae1cb1943cc0e0cec3cd9bf85707884	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\0o41zs\lzhdqsiji02\we9tzkhspb.mp4.vvyu	12.42 KB	baa96e99d85b40ac95608fdc91f7421ddfd1c466e6260edba67d9b7a3ba505a9	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2_dei9bifvc5tqmw.flv.vvyu	49.18 KB	118d31989b101a37257f20235d9dccac8be2212f9b222a9f262318f0faac7859	✔
c:\users\keecfmwgj\documents\oo9yxvhfzy447m.docx.vvyu	81.17 KB	fd216c7d8b5bba37d789b82d076aa33ec2dbd4781bb3c0e4b3fcd1015187fbbf	✔
C:\Users\kEecfMwgj\Documents\xyVBcXoxWZOEVZ7.pptx.vvyu	32.29 KB	10bcc02e659816e174a6fc4316c010de8d2f95ea53175dd53037ed979a3b80fd	✔
c:\users\keecfmwgj\documents\azld\uhfbjiac\nooizr\vvjlrm5wps_pezl.odp.vvyu	33.47 KB	4b1fec34c68d69ceca2d8e6d30bddef31e0826ea247496b38b4100c54c41dd7a	✔
c:\users\keecfmwgj\favorites\msn websites\msn.url.vvyu	467 bytes	e32fb33afe83b74e84d7a688a9ce81bb964772c839d9a5904efbba8309da3041	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\nnzzossfvx.mp4.vvyu	65.41 KB	3a17d2f58d31c867e8e6621a0c6141f111c94921eb0ab256caf471ac9b0b06ac	✔
C:\Users\kEecfMwgj\Desktop\gnNW5oKgmW5QeElwN.mp4.vvyu	71.17 KB	349bba73483c1884679fac895993d954212046f741abc76ef471de00ec3a7d76	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\exzou4j4nw j\zwquu_bys.swf.vvyu	57.71 KB	af2268c23a12eefb64adb0e01d2229d37e8563c9ee874426f15b3371131ae75d	✔
C:\Users\kEecfMwgj\Desktop\eOgdOPqhf.odp.vvyu	43.79 KB	8059d3cbb5bf0eff05087810a8f573fd23736d08ffec4002e27cd7ba4fd550db	✔
c:\users\keecfmwgj\music\fuhvly4jeagwk\wd-bcbik6paqlyst.m4a.vvyu	26.93 KB	877c4bb6979ca315c7e84c93677b69649e22983a2ebb6eea8d2227eab42c10ac	✔
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E5UCc4GR1Z tMgYPe\4uY5fsSdcyjSgJ.jpg.vvyu	21.24 KB	4e1e6fbbfc0cdeea39f09951cbe62e8733047fff27902f2a4a7734e347c12a81	✔
c:\users\keecfmwgj\documents\outlook files\franc@gdllo.de.pst.vvyu	265.33 KB	5ff08ad47f0af066b053a886d82d9346252418ebbc71afbccf573ff1dfe8feef	✔
c:\users\keecfmwgj\documents\azld\rqz y4w0rybhq_irzd3\f4quftb6aenpm.csv.vvyu	32.15 KB	aaa3d405042df39d8a0d3265ad9d5d8fcba669ecf150e11d67c7388841a98221	✔
c:\users\keecfmwgj\desktop\yyyx_.avi.vvyu	4.62 KB	b8f4d2788cb8dd11d6c6f2737f8d5b0cf4bfb6dfbb1c04e40d818f6e5cf8c7e6	✔
c:\users\keecfmwgj\documents\bflhqgtm.pdf.vvyu	37.97 KB	72008ea37ad5a8f39172061f4bb290ff39e3c7ab17b08a5396e365d45a47b8d3	✔
C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\LNo4VDj5U-Z.wav.vvyu	81.79 KB	b65091f72d97f2e59acec22565746952aa9b99d124eebc9d271e5a69a62b00c7	✔
C:\Users\kEecfMwgj\Documents\y_n6R.xlsx.vvyu	30.35 KB	7ea10d8b6b4664fd0e4cf56da29f071d433e1f686ae856b4f37cf92f4a65d737	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\tosxrvqraigf3mknom0.avi.vvyu	65.95 KB	f1ca7ff7e133d880af610e77c788dc02048d3aa64484115ac1734e7e13455ad6	✔
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\Y5X8\wIEnhA.flv.vvyu	35.81 KB	c84ebc1aaa1d62d0098a4c9e7a6dfe4763f75fbc0c2f76ae2c69a61a694bb9e1	✔
c:\users\keecfmwgj\desktop\zsr7xc26_dfdmvcahh\kyk8l.flv.vvyu	15.39 KB	18f70f93c27e19984f27e7bac31f7e6a40df4d1b8053f156ecc0cd980be77351	✔
c:\users\keecfmwgj\desktop\c5rx.mkv.vvyu	75.66 KB	82c087708286f4d9185898d67319258a3582bd5e973f85c34cae9ef8076f4a2e	✔
c:\users\keecfmwgj\documents\azld\pebfuwtor 4\ivotj\xivbhkfoh.ppt.vvyu	19.83 KB	7ba6dec49a43959f898a28dcb710deed90aa3d641f20c180b271a451404a24db	✔
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\kf5kyh.m4a.vvyu	21.84 KB	9e324150094c29b0335eca13f2ee815887c038252b9d3651d68c2460dc01b172	✔
c:\users\keecfmwgj\pictures\ymomnephob\te1lwlzl-cqvzew gl\xgpgxl.jpg.vvyu	9.99 KB	46175ccdeb582b78cc71137335fc5aa16775e8b62a54f5f3e5f9bcedb29ccd52	✔
c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu	467 bytes	f025c3968057ff48c44b689f5bc289b348c71782350b5213f826c9dfe3136843	✔
C:\Users\kEecfMwgj\Documents\AzlD\UHfBjlaC\wzwkC7.odp.vvyu	24.75 KB	196f087b39cf4d49bd53ddeb9bfec62acf33f3e16dc55159c27cd8bc82e1a886	✔
c:\users\keecfmwgj\favorites\windows live\get windows live.url.vvyu	467 bytes	6b19d524040d4124832d7e90a7027152b549106333e6a8cff367b179df2d60de	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\desktop\ohy9bmsmlfi5\5uvlwu6-nnebg.jpg.vvyu	20.44 KB	677c7dc41a4e418122ed6cbaf8d1dac71518e217f21f3dfbd0d5018277ebcaf0	✔
C:\Users\kEecfMwgj\Desktop\OhY9bMSmLfl5\hxqHaq.mkv.vvyu	7.96 KB	5f754e82924830b4f1e544e35b5fcd196503650104b8c0eabce44ae5ee9ed4ec	✔
C:\Users\kEecfMwgj\Desktop\o5GqCe9ZgNw7JzfwVH.gif.vvyu	95.49 KB	5b577d8bb7016ed42ae9b146647417ecd1fa3b7a0ba8d099982eb890466c7f3a	✔
c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.vvyu	467 bytes	4f735a8b60601a2931dabb2311473b0220f92b792a3cbd3fd570792abd98873c	✔
c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu	467 bytes	3acf76f55cab420fef48b37dcceaeacf561a0ea274cafc60b81cb2e6d37887b0	✔
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\0o41zs\lzhdqsiji02\3exl.mkv.vvyu	82.87 KB	c5b03662e333e798a2a3e9892f0fdef122eaa40edbb8a3325bc85795b17a267a	✔
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\F72Mw_KNQRugYJJCcBc\C9Qz99w\b3JSk19CS30.avi.vvyu	93.79 KB	8d5c1468c53c57af5d92066e545a354fc9617eb93248807e28cb3a6d0effd368	✔
C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR4\XvrsId5WMhv8lJp8.ots.vvyu	32.66 KB	6d39b2fa76edba194228b842370b8a71d35e7c9e5796fbfc78c4ce4ea417a8b2	✔
C:\Users\kEecfMwgj\Desktop\xf-vHBag-ZJttfl79F6Z.bmp.vvyu	94.08 KB	ee148fc7058dac5985c98602eeea07391170ddbf65e6cf0112d3d00439c1d559	✔
c:\users\keecfmwgj\pictures\nthxrlnnkw.gif.vvyu	96.30 KB	c5600df2c43e74604428545d8936848009c31cc644b4ab15341ced9051fc3e47	✔
C:\Users\kEecfMwgj\Documents\AzID\UHfBjIaC\Z8rQUb38uy_iJ3tNKmP2.ppt.vvyu	87.98 KB	9ae8d48ff0694ac3068b063fbd26ed8d9422fa87a831f426900c7e622910812e	✔
C:\Users\kEecfMwgj\Documents\zzDsCcZ.xlsx.vvyu	1.34 KB	edb386dd3c55f95531471aff2cb6729a262e453f2c483ef37ecffd802e607b58	✔
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\d7pQIdSiE6laiAyeoE\k4vLze9TyD\hM HT 9rGnc6u.gif.vvyu	61.14 KB	7694eaf208dcac81be98be7ed791e127b8bcdc72dc18f39ac25fdf675014f3cb	✔
c:\users\keecfmwgj\documents\zsmchocwullalz-0fsrc.ots.vvyu	86.11 KB	4f6e8e38d2be9f80ec3e6bedfb6143da8f4014981c8ed48527f881fd1764bed6	✔
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\NLJO_aKDC.png.vvyu	63.38 KB	7d587a4aa691036cc9b62bb5ce20c243118cce07cc556b27bb6beeeef8f13db1	✔
c:\users\keecfmwgj\desktop\0auodapipmqwtk.mp3.vvyu	15.93 KB	b742f2270641e41ac8a22701b750cf4df11755c8396ced9f660ad702f83f719b	✔
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipgggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\yw2t95\l69lcxnvikb5vvhczyx.m4a.vvyu	33.98 KB	f9423ccceb3732c686dd203b93cd6d343ad0df1071ae4adc11e320f165f5cb77	✔
C:\Users\kEecfMwgj\Desktop\ZsR7Xc26_DfdmVcahH\PRpouSq\Yn5TngP_hrElfEBI9s.wav.vvyu	27.19 KB	771d516f5eede113b4155d0b224782dc19fe3ed979455c0fbde042b03fe74428	✔
c:\users\keecfmwgj\pictures\wzmkmopozyago-ujtdf.bmp.vvyu	45.06 KB	49a3c760926827e0755482833476d379a5b66bb21479a29aeb224cfa858b3cbf	✔

Reduced dataset

Host Behavior

Type	Count
System	295
Module	185
File	2662
Environment	1
Process	55
Registry	4
Mutex	1
User	1
Window	1

Type	Count
-	4

Network Behavior

Type	Count
HTTPS	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f02b1904b5279c9e50a252832d78819eb4883be83cd7c6dc27f51ade29c72288	C:\Users\kEecfMwgj\Pictures\V89DayYK-6YpvEr4NY.gif.vvyu, c:\users\keecfmwgj\pictures\v89dayyk-6ypver4ny.gif.vvyu	Dropped File	57.97 KB	image/gif	Access, Create, Write	MALICIOUS
5b6f6c4cae9d7470ccbb4e3ac69b8877b469e7a172d042dd5369e3e3282036da	c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggquG4\psrckmpedif_oxvk\61xto95hr3jmn6z\yw2t95\rnqkcz9li.mp3.vvyu, C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_OxVk\61XTO95hR3JMn6Z\yw2t95\RNqKcz9LI.mp3.vvyu	Dropped File	73.26 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4bf2e089147461270f6a65e0412b862ed8a06198042a07683dcf67c85a417e8e	C:\Users\kEecfMwgj\Videos\-DwrKzsIsF2\SVKL6Wu5uabuSVqvA\Y5X8\0o41ZS\b5aBDkyBYyj.swf.vvyu, c:\users\keecfmwgj\videos\-dwrkzsIsf2\svkl6wu5uabusvqva\y5x8\0o41zs\b5abdkybyyj.swf.vvyu	Dropped File	76.29 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
d863d924f7e7ba862654e416624d7c404749efe1b95307a4ba3c1fd3d5894837	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E07daaq0LDB.bmp.vvyu, c:\users\keecfmwgj\pictures\ymomnephob\e07daaq0ldb.bmp.vvyu	Dropped File	56.61 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d3f2bae7e647bfe7f5526820f598936224d893663e958b3c515751f38eb8fe0a	C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_OxVk\61XTO95hR3JMn6Z\pE7_nJD0Tmm8m2VYvr.wav.vvyu, c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggquG4\psrckmpedif_oxvk\61xto95hr3jmn6z\pe7_njd0tmm8m2vyvr.wav.vvyu	Dropped File	82.05 KB	application/octet-stream	Access, Create, Write	MALICIOUS
47310efa770cd02ca456ec0be0a6aa41620e74bffc4a3a5e0a0d2c8a9729494e	c:\users\keecfmwgj\documents\iudig2j9jtqfgbcv6n.docx.vvyu, C:\Users\kEecfMwgj\Documents\iudig2j9JtQfGbCV6n.docx.vvyu	Dropped File	87.56 KB	application/zip	Access, Create, Write	MALICIOUS
0cce7483c297f60938fff8e1ef7a2b16dbe7bc33a94753833b9bde96a683517e	c:\users\keecfmwgj\music\pe0cuon\jrz5y.mp3.vvyu, C:\Users\kEecfMwgj\Music\pE0cUon\jrz5Y.mp3.vvyu	Dropped File	39.08 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4d5a7096b11a024cbf9be32c57231ae3aab3c9d2cafe859464b55aed8d9b6ce2	c:\users\keecfmwgj\pictures\ymomnephob\7q5_45ijmfp9ba_ydmbp0zwbtzu.gif.vvyu, C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\7Q5_45ijmfP9bA_yDMBp0zwbtzU.gif.vvyu	Dropped File	3.55 KB	image/gif	Access, Create, Write	MALICIOUS
3727cb7a09ee05091fac7365e73d477eed533d1dde05e2c0a17f46141347b33a	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\tE1LWIZI-CqVZeWgL\Gpf_fTIy87TJO1Dp27TE.png.vvyu, c:\users\keecfmwgj\pictures\ymomnephob\te1lwizi-cqvzewgl\gpf_ftiy87tjo1dp27te.png.vvyu	Dropped File	20.14 KB	application/octet-stream	Access, Create, Write	MALICIOUS
330c15c54f0e83252731e6f5f820b23da10abb2bec366d32591853c58137a76d	c:\users\keecfmwgj\appdata\locallow\microsoft\internet explorer\services\search_{0633ee93-d776-472f-a0ff-e1416b8b2e3a}.ico.vvyu, C:\Users\kEecfMwgj\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico.vvyu	Dropped File	4.51 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f9a1156e19d0529b9a9ab262624bdf84b70d70666b252121e0ba516e267548fd	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\y5x8\0o41zs\lzhdqsiji02\ffcamngkkb8gmcsqdpq.mkv.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\Y5X8\0o41ZS\LzHDQsiji02\ffcaMnGKKb8gMcSQDpq.mkv.vvyu	Dropped File	73.75 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e5d87b136c70c39ff6405b816da88aac020f352eff419e5ed5cc84eacdce35d7	C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\ui-Z5b.m4a.vvyu, c:\users\keecfmwgj\music\fuhvly4jeagwk\ui-z5b.m4a.vvyu	Dropped File	59.97 KB	application/octet-stream	Access, Create, Write	MALICIOUS
49846a73c6501462096b1c21e66aa72e35f10a0c03d140bcb34554241b888453	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\d7pQIdSiE6laiAyeoE\cH1Zz4OF5OqujiOEN9.png.vvyu, c:\users\keecfmwgj\pictures\ymomnephob\d7pqidsie6laiayeoe\ch1zz4of5oqujioen9.png.vvyu	Dropped File	75.24 KB	application/octet-stream	Access, Create, Write	MALICIOUS
0f85ff2fffee56f6f192bfe01dfb3cd3e967697858842a02db80faaaf1456b22	C:\Users\kEecfMwgj\Contacts\Administrator.contact.vvyu, c:\users\keecfmwgj\contacts\administrator.contact.vvyu	Dropped File	67.11 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e264b3e3d211e9192f546494f09aab136c24c2cab1c9fcfc212d4c2867fb370f	c:\users\keecfmwgj\documents\azld\uhfbjiac\nooizr\rt8g.pptx.vvyu, C:\Users\kEecfMwgj\Documents\AzlD\UHfBjIaC\noOiZR\Rt8G.pptx.vvyu	Dropped File	29.82 KB	application/octet-stream	Access, Create, Write	MALICIOUS
12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b	C:\Users\kEecfMwgj\AppData\Local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbb...\...f844449afe55fb0f1cbbda0b.exe.vvyu, C:\Users\kEecfMwgj\Desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	Sample File	730.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Read, Write	MALICIOUS
3e3e3f8b29eaa006e5c80d738f5e6ebf9f17b74774dce1d2eb0c72a250796aa2	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\y5x8\0o41zs\235vhs8kou7y.mp4.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\Y5X8\0o41ZS\235vhS8kOU7y.mp4.vvyu	Dropped File	36.67 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ff2b159f3e45375b0f330c00f525e7e8346e5ebf617d5c2922de7f1844bb8d9c	c:\users\keecfmwgj\favorites\links\webslice gallery.url.vvyu, C:\Users\kEecfMwgj\Favorites\Links\Web Slice Gallery.url.vvyu	Dropped File	560 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
50800ad30c11f75bd3d885d407e947d57a6db0f22a8d0a1c1376bcb0994f88e4	C:\Users\kEecfMwgj\Desktop\ZsR7Xc26_DfdmVcahH\PRpouSq\QwaTwvQX1o7erS.mp3.vvyu, c:\users\keecfmwgj\desktop\zsr7xc26_dfdmvcahh\prpousq\qwatwvqx1o7ers.mp3.vvyu	Dropped File	37.39 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c43abf420eeb327012e38edf4617b01764e8de8eced43f2c18aa5e416d9ff055	C:\Users\kEecfMwgj\Videos\HDnGwo1W3X7Qq9.flv.vvyu, c:\users\keecfmwgj\videos\hdngwo1w3x7qq9.flv.vvyu	Dropped File	31.50 KB	video/x-flv	Access, Create, Write	MALICIOUS
d73efcc2460acfacfe99bb0e31f648fe21f34b69b3586f50172e8b8276f2ae74	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\vzsbld-s6.bmp.vvyu, c:\users\keecfmwgj\pictures\ymomnephob\p5pcqlwf\vzsbld-s6.bmp.vvyu	Dropped File	67.92 KB	application/octet-stream	Access, Create, Write	MALICIOUS
f46d42ff58ca370c6629f89bfa7981f1431d69c7584920b4d8f088416920b912	C:\Users\kEecfMwgj\Documents\AzlD\PeBfuwtoR 4_wgbJ2d7Z.csv.vvyu, c:\users\keecfmwgj\documents\azld\pebfuwtor 4_wgbj2d7z.csv.vvyu	Dropped File	4.95 KB	application/octet-stream	Access, Create, Write	MALICIOUS
665c2b66c23e2f55dabe15c79c47d7578b80bea124030d2ec9d24de0dd633fcf	c:\users\keecfmwgj\desktop\bnbjzezhttp-mha.png.vvyu, C:\Users\kEecfMwgj\Desktop\BnBjzEzhtTp-mHA.png.vvyu	Dropped File	31.85 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
350c096d17a07202e4fac1c1315b281a15277eba91f52a5c3b76257b9dc0ebb3	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\7Q5_45ijmfP9bA\iJwMptujDhUTwyI.gif.vvyu, c:\users\keecfmwgj\pictures\ymomnephob\7q5_45ijmfp9ba\ijwmptujdhutwyi.gif.vvyu	Dropped File	89.97 KB	image/gif	Access, Create, Write	MALICIOUS
aeca6a9c6ef9a0f12e6c834ea246f5d93c33be1d6f7fd27edb04d00bdc99f736	c:\users\keecfmwgj\pictures\ymomnephob\e5ucc4gr1ztmgype\qjvfzvvw_idbuk5j3vj1.gif.vvyu, C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E5UCc4GR1ZtMgYPe\QjVfzvvW_idBuK5j3vJ1.gif.vvyu	Dropped File	24.85 KB	image/gif	Access, Create, Write	MALICIOUS
75b19dd98d4a3bfab42f3af355bee3fa882ee536f17cb3cd06ab5b8c13164b12	c:\users\keecfmwgj\music\qxlg6rlrsvyemxil.m4a.vvyu, C:\Users\kEecfMwgj\Music\qxLG6rlRsvYEmXiL.m4a.vvyu	Dropped File	67.87 KB	application/octet-stream	Access, Create, Write	MALICIOUS
19cdf8caba97b3b7afa1a9d2f3f680cc8132bb217a61341d072ff1b06545841e	C:\Users\kEecfMwgj\Pictures\141isvJREPi.gif.vvyu, c:\users\keecfmwgj\pictures\141isvjrepi.gif.vvyu	Dropped File	20.45 KB	image/gif	Access, Create, Write	MALICIOUS
66b85a46f946ba468b0623b24d4611603c6be4e667b2fbd0d2b8658fb6f7b1b0	c:\users\keecfmwgj\documents\z6ibwsvk.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\Z6ibwSvK.xlsx.vvyu	Dropped File	11.77 KB	application/octet-stream	Access, Create, Write	MALICIOUS
2a441d7482f2330ecb193b7d7e56fe36d8c2e9318a947bce736150abc71dce0a	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\exzou4j4nwj\m5lkrrhopgpv2jhgtq-.flv.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\EXZou4J4nwj\m5lKRrHOPGPv2jhgTq-.flv.vvyu	Dropped File	90.98 KB	video/x-flv	Access, Create, Write	MALICIOUS
2b8dd6407cd533cee27b868f34d37e34f3cb97dae8643d488447a183c7f3d127	c:\users\keecfmwgj\desktop_gemdk.jpg.vvyu, C:\Users\kEecfMwgj\Desktop_gEmDK.jpg.vvyu	Dropped File	54.55 KB	image/jpeg	Access, Create, Write	MALICIOUS
e23711b92a696bd7b023e30ef6f097781fb035c2faef4eb81ac32c3fcd239538	c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\gz-yqulpeghm6.odt.vvyu, C:\Users\kEecfMwgj\Documents\AzlD\UHfBjlaC\yEpRZCn46rxjDOAUpD\Gz- YQUlpeGhm6.odt.vvyu	Dropped File	37.36 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e24e8d6ab0a8592bdf315710f5c42d20965e9070e25943ff6f3ee817b3d05518	c:\users\keecfmwgj\pictures\ymomnephob\7q5_45ijmfp9ba\lejzvedjk.gif.vvyu, C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\7Q5_45ijmfP9bA\LEjZveDJk.gif.vvyu	Dropped File	15.62 KB	image/gif	Access, Create, Write	MALICIOUS
3308fb0e8ee3134a17ad0c43c021ad0a78459fbb21c4d4a7a8015517d3b14f03	C:\Users\kEecfMwgj\Desktop\7rMc5PE99.bmp.vvyu, c:\users\keecfmwgj\desktop\7rmc5pe99.bmp.vvyu	Dropped File	15.13 KB	application/octet-stream	Access, Create, Write	MALICIOUS
57beff21a68985a1edbbdd0ddf3cea44ebd37f295b817928b61b50d3de22f105	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E5UCc4GR1ZtMgYPe\k1TTTQU2.bmp.vvyu, c:\users\keecfmwgj\pictures\ymomnephob\e5ucc4gr1ztmgype\k1tttqu2.bmp.vvyu	Dropped File	78.29 KB	application/octet-stream	Access, Create, Write	MALICIOUS
8732265e1f7e02b48c6382b345171ea7e81e144f69ea7f9f8aab1351ea425727	c:\users\keecfmwgj\desktop\xc6y6diw-2mp3g1ez.mkv.vvyu, C:\Users\kEecfMwgj\Desktop\xC6Y6diW-2mP3g1eZ.mkv.vvyu	Dropped File	86.13 KB	application/octet-stream	Access, Create, Write	MALICIOUS
1bbc45862a85e6dbab93d999744601ff6b4b9ce2252dfc258711902509ea252a	C:\Users\kEecfMwgj\Desktop\FDSFO0.avi.vvyu, c:\users\keecfmwgj\desktop\fdsfo0.avi.vvyu	Dropped File	65.04 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1d5a4c5b0e0c6ecab87ae5cdee78d774902850babd7385624cc44680363741de	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\YwgWoXY4_dSr.jpg.vvyu, c:\users\keecfmwgj\pictures\ymomnephob\p5pcqlwf\ywgwoxy4_d sr.jpg.vvyu	Dropped File	98.59 KB	image/jpeg	Access, Create, Write	MALICIOUS
7bbe58971d385c76aa42b9c396adcd14fa96404e2f96dceb75aaa2d4823d97cd	C:\Users\kEecfMwgj\Desktop\5fJKex2DUyLjzY0p.bmp.vvyu, c:\users\keecfmwgj\desktop\5fjkex2duyljzy0p.bmp.vvyu	Dropped File	50.66 KB	application/octet-stream	Access, Create, Write	MALICIOUS
54ae3f8cc3cbda628e0b9afd0d08b34c3649b5db188978fb658a613c72280e8f	c:\users\keecfmwgj\desktop\fmtiy2j60xys_lff.png.vvyu, C:\Users\kEecfMwgj\Desktop\FMtIy2J60xYs_lff.png.vvyu	Dropped File	51.52 KB	application/octet-stream	Access, Create, Write	MALICIOUS
f5dce59b40e7245fd54c11f9b034952c1abe27a26ead0c8c5f68bfc631b7fd8b	c:\users\keecfmwgj\videos\u7unq0 vlv.flv.vvyu, C:\Users\kEecfMwgj\Videos\U7uNQ0 Vlv.flv.vvyu	Dropped File	16.73 KB	video/x-flv	Access, Create, Write	MALICIOUS
2336646e50f482c8c479332c9292b0f1b0445ada546824f5b7bafdb17ba1b4d7	c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_ oxvk\61xto95hr3jmn6z\brlu 5vgds.wav.vvyu, C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_OxVk\61X TO95hR3JMn6Z\brlU 5vGds.wav.vvyu	Dropped File	41.23 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3cb185c7c58bcdbaf6c52ab73a75db3960e9e09abd91affaf3bd10a2bbd951dc	c:\users\keecfmwgj\documents\ntkcvhllb.pps.vvyu, C:\Users\kEecfMwgj\Documents\nTkcVHLlB.pps.vvyu	Dropped File	86.75 KB	application/octet-stream	Access, Create, Write	MALICIOUS
5d3dea242ad98e6ed353296653b80c004561814dadd0f4f0c36f2a157b829fa4	c:\users\keecfmwgj\documents\hstszlrr9zv1_v.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\HStSZLrr9ZV1_V.xlsx.vvyu	Dropped File	40.09 KB	application/octet-stream	Access, Create, Write	MALICIOUS
70a9ce1e59fcf76a1a4026d7d40a2c6e9cd0b70fe49dfac695091983ef8184e2	C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url.vvyu, c:\users\keecfmwgj\favorites\microsoft websites\microsoft store.url.vvyu	Dropped File	468 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
702bebe1ea144f5d9bf220266ab847647de7d3fae7755e2cf12dd0774835bd3d	c:\users\keecfmwgj\videos\7oqi8laykzm3pzqg.flv.vvyu, C:\Users\kEecfMwgj\Videos\7oqi8LaYkzM3PzQg.flv.vvyu	Dropped File	62.38 KB	video/x-flv	Access, Create, Write	MALICIOUS
13f2c7008dbce22fa9928b6be897cc373a434e8c64b3d3793e99d874e2566d75	C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\Y5X8\0o41ZS\EDTDz9.mp4.vvyu, c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\y5x8\0o41zs\edtdz9.mp4.vvyu	Dropped File	30.69 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d5be5ba44592909b3d4b12dc923d8c7fe215f462cafeaba0c7a4a78b218d80e2	c:\users\keecfmwgj\music\fuhvly4jeagwk\nfk529nzfij1e1.mp3.vvyu, C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\Nfk529nzfIj1e1.mp3.vvyu	Dropped File	55.61 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ef050899804894f9954d7acee36f4da9d858c9bd732f2853f0c0a1143814707e	c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\x9kn7y7cefv.xls.vvyu, C:\Users\kEecfMwgj\Documents\AzlD\UHfBjIaC\yEpRZCn46rxjDOAUpD\X9kn7Y7ceFV.xls.vvyu	Dropped File	71.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
bc368514a63982827c829da2b35572e55cf141a03b1bebf89d88c5731702f7eb	C:\Users\kEecfMwgj\Desktop\labkKD4FQA.wav.vvyu, c:\users\keecfmwgj\desktop\iabkkd4fqa.wav.vvyu	Dropped File	43.72 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ddb98b0aac4656b576bcb113de397e0d121a6af6144582be768c008fe84db9dd	c:\users\keecfmwgj\documents\a1p6lyhhe5fq5dudw9xm.rtf.vvyu, C:\Users\kEecfMwgj\Documents\a1p6lyHhe5fq5DudW9XM.rtf.vvyu	Dropped File	83.07 KB	text/rtf	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b9be2dbccaf3f2b8e5844d2ee8559ea677eb0793bcf12198f7d61ad2d99fdce4	C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url.vvyu, c:\users\keecfmwgj\favorites\msn websites\msn money.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
cb2a82587118c4f08ed01e883c6cd84e165c136f0a029c1d763f8a3d45c92f5e	C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_OxVk\61XTO95hR3JMn6Z\yw2t95\rQWnqazpz-naoLL5P.wav.vvyu, c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggquG4\psrckmpedif_oxvk\61xto95hr3jmn6z\yw2t95\rqwnqazpz-naoll5p.wav.vvyu	Dropped File	95.45 KB	application/octet-stream	Access, Create, Write	MALICIOUS
dc9ac8be48a5de98b3a31ef404505db758957bd80e7c272a67f8a9bc0f9b85b9	c:\users\keecfmwgj\documents\-yzsadt_8t croyrko.pptx.vvyu, C:\Users\kEecfMwgj\Documents\-yzSadt_8t CRoYRKO.pptx.vvyu	Dropped File	57.83 KB	application/zip	Access, Create, Write	MALICIOUS
6db7a3c85e6330ff676d314066e65ab70f0aa7d38e0b15e49593f4effa13b09f	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\7jjuxf5i.mp4.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\F72Mw_KNQRugYJJCcBc\7jjUxF5I.mp4.vvyu	Dropped File	31.91 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b4bfe9c00914ee6e2e417ba52d8165eb22ddbfdf4ebbd3607a46c4b90e00da9b	C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\Y5X8\0o41ZS\LzHDQsiji02\MQWaq1YvFIYApR.swf.vvyu, c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\0o41zs\lzhdqsiji02\mqwaq1yvfiyapr.swf.vvyu	Dropped File	85.91 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
ea4e84c242b75a977ff7692d60077826fbae2a9bd99e4d629a71fa6b0a636a4b	C:\Users\kEecfMwgj\Music\tRcMqrNBqTUs.mp3.vvyu, c:\users\keecfmwgj\music\trcmqrnbqtus.mp3.vvyu	Dropped File	88.14 KB	application/octet-stream	Access, Create, Write	MALICIOUS
dc2841c72b2b1ec5aacc78ae095ceac0025379f43a02f3a93d8b9b114b87809a	C:\Users\kEecfMwgj\Documents\OkF0P0lVbo seJvjybv_.docx.vvyu, c:\users\keecfmwgj\documents\okf0p0lvbo sejvjybv_.docx.vvyu	Dropped File	22.98 KB	application/zip	Access, Create, Write	MALICIOUS
a80c45cf0892d2754bd091737513c1ce9e54fa4f20dad284d6e72a83ff125ee2	c:\users\keecfmwgj\desktop\fkf.mkv.vvyu, C:\Users\kEecfMwgj\Desktop\fkf.mkv.vvyu	Dropped File	20.96 KB	application/octet-stream	Access, Create, Write	MALICIOUS
fc3a33814b0d6a2ac79736b54903c31940aa8c653fd61e59d04a779a13b7268c	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\6cposy.swf.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\F72Mw_KNQRugYJJCcBc\6cPOSY.swf.vvyu	Dropped File	4.10 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
11cedc96257ccc5792813ec4b1c077e0f200e3c7ee52bc7fee0d1511a96ad474	C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\Y5X8\0o41ZS\Fjxa.mp4.vvyu, c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\0o41zs\fjxa.mp4.vvyu	Dropped File	51.80 KB	application/octet-stream	Access, Create, Write	MALICIOUS
1be6e0c185f55f20726bea3dd881f65564e02b03162f67dd5e75ec74be4fa34d	c:\users\keecfmwgj\favorites\windows live\windows live mail.url.vvyu, C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Mail.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
f7d4f1a6771eeaf4b0fef37d68a0030fc1f142a6b50338ef8344420f7d36342a	c:\users\keecfmwgj\documents\yrqwfs6apmpbyvu.doc.vvyu, C:\Users\kEecfMwgj\Documents\YrqWFs6aPMPbYVu.doc.vvyu	Dropped File	33.59 KB	application/octet-stream	Access, Create, Write	MALICIOUS
5a227aacc0a154b9269236d6fcc2944a06761c76858d1adea1c774f1b39fbeb0	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\tE1LWIZI-CqVZeWgL\CfqSEGHWv8Id7U6qj5.gif.vvyu, c:\users\keecfmwgj\pictures\ymomnephob\te1lwlzl-cqvzewgl\cfqseghwv8id7u6qj5.gif.vvyu	Dropped File	89.31 KB	image/gif	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
17f4783e214965c86467410b4ac705e0cfcd2afd2c09f082b15a33beb738bf0f	C:\Users\kEecfMwgj\Documents\AzlD\UHfBjlaC\eE nQNbY2KI.doc.vvyu, c:\users\keecfmwgj\documents\azld\uhfbjiac\ee nqnby2ki.doc.vvyu	Dropped File	23.81 KB	application/octet-stream	Access, Create, Write	MALICIOUS
54e9b79990c1d76dc6a37428f9b3e43057ff75074f1fb50249ef59143731e3c7	c:\users\keecfmwgj\music\zrus.wav.vvyu, C:\Users\kEecfMwgj\Music\ZruS.wav.vvyu	Dropped File	18.15 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d02439f8d30f64c0aef909e88d722a1f2649e9ea0ba04f727628e732c722ae51	c:\users\keecfmwgj\desktop\qc9h.jpg.vvyu, C:\Users\kEecfMwgj\Desktop\qC9h.jpg.vvyu	Dropped File	32.66 KB	image/jpeg	Access, Create, Write	MALICIOUS
121037fbf99d30d3a4c12fc5755717ae693c8fc323b1fa1156a1e02843f117e4	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\qpf-r5z.mp4.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\Y5X8\qPf-R5Z.mp4.vvyu	Dropped File	62.68 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b34b24ced71de3f18eac20e0dd0e6af25d100ab7a242abc8f6a504c0863692e3	c:\users\keecfmwgj\documents\es4lp.pptx.vvyu, C:\Users\kEecfMwgj\Documents\Es4lP.pptx.vvyu	Dropped File	13.75 KB	application/octet-stream	Access, Create, Write	MALICIOUS
2360ddfca94e2e4234e28a3d24a907ec35254aafea3eb5658500dd5f72b149a1	C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\F72Mw_KNQRugYJJCcBc\MSPqrTgqm.swf.vvyu, c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\mspqrtgqm.swf.vvyu	Dropped File	66.89 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
00d311913d06e917eeb000cf23f60012688be2577b674074a98d4eee53db47d7	C:\Users\kEecfMwgj\Documents\1G5yOYkuiK.docx.vvyu, c:\users\keecfmwgj\documents\1g5yoykuik.docx.vvyu	Dropped File	95.47 KB	application/zip	Access, Create, Write	MALICIOUS
1739db6cd80149b2f5bc58126fc3d07781a2a910141aeeefd2258b2dd173d7ba	c:\users\keecfmwgj\desktop\5ggbg59nqgc.flv.vvyu, C:\Users\kEecfMwgj\Desktop\5gGbG59NQgc.flv.vvyu	Dropped File	63.82 KB	video/x-flv	Access, Create, Write	MALICIOUS
5651c4c7b3488e7a061795597c502fe56c1e67cc8a06b743ad1aa925da608a49	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\0iydfpwavsjadg.mkv.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\F72Mw_KNQRugYJJCcBc\0iyDFpwaVsJADG.mkv.vvyu	Dropped File	69.05 KB	application/octet-stream	Access, Create, Write	MALICIOUS
203222c2ba8da6533200fe080a5b9cd8e2b70a81c71d7af1844ddc1f383b5e91	C:\Users\kEecfMwgj\Pictures\9p8OG.bmp.vvyu, c:\users\keecfmwgj\pictures\9p8og.bmp.vvyu	Dropped File	91.17 KB	application/octet-stream	Access, Create, Write	MALICIOUS
30b00c5764da1341a9c100f3a513a99c61eee165a8fe8efd223e785d6bb001f0	C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\VNAR2BEit3ka1sGXw8sq.mp4.vvyu, c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\vnar2beit3ka1sgxw8sq.mp4.vvyu	Dropped File	63.73 KB	application/octet-stream	Access, Create, Write	MALICIOUS
7e0e063ca5c386920c63fc0c82df2ffa5ff6260689b596882bd227b55e9db872	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\bst5msuptc.flv.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\bsT5mSuptc.flv.vvyu	Dropped File	62.40 KB	video/x-flv	Access, Create, Write	MALICIOUS
f29ad33e71d3b495db4faf691a85af30064a2b380b9d4834a422f6dd66b3cdc8	C:\Users\kEecfMwgj\Documents\AzlD\UHfBjlaC\hlTCx olpB7AQb0\S7akFO0_2kX867.ods.vvyu, c:\users\keecfmwgj\documents\azld\uhfbjiac\hltcx olpb7aqb0\s7akfo0_2kx867.ods.vvyu	Dropped File	20.15 KB	application/zip	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0b11a17ed05567cdfba68d071bfac1e4f120656375b43979f138beea3ef4758f	C:\Users\kEecfMwgj\Documents\AzID\UHfBjIaC\yEpRZCn46rxjDOAUpD\feMArPT27Tt3Vq0tfRa.odp.vvyu, c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\femarpt27tt3vq0tfra.odp.vvyu	Dropped File	31.83 KB	application/octet-stream	Access, Create, Write	MALICIOUS
fb735874771f1ab94bf6be92af63acce3bc48a4333893e3539df079f8e523bfd	c:\users\keecfmwgj\documents\eri1atxotxxvz19.ppt.vvyu, C:\Users\kEecfMwgj\Documents\Eri1atxOTxxvZ19.ppt.vvyu	Dropped File	54.39 KB	application/octet-stream	Access, Create, Write	MALICIOUS
87d09dcc96b9f5fe51a7d3a6df5179b0dde5790d099312776eb417f3dd86fe2a	C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR 4\tEiHH.pdf.vvyu, c:\users\keecfmwgj\documents\azld\pebfuwtor 4\teihh.pdf.vvyu	Dropped File	60.52 KB	application/pdf	Access, Create, Write	MALICIOUS
835942df698062fc77ce38024245a41c3ae569831340aba92c34d6552b684372	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\7Q5_45ijmfP9bA\GwAL3j0fQyIFxx-jKJ.gif.vvyu, c:\users\keecfmwgj\pictures\ymomnephob\7q5_45ijmfp9ba\gwal3j0fqyifxx-jkj.gif.vvyu	Dropped File	69.55 KB	image/gif	Access, Create, Write	MALICIOUS
f2382a8abfe0d102eb774fded014290f94ec99650e7bff9534985dd7554e57c	c:\users\keecfmwgj\documents\yqj5kxs1j7uvwoh.pptx.vvyu, C:\Users\kEecfMwgj\Documents\Yqj5KxS1J7UVwOH.pptx.vvyu	Dropped File	9.83 KB	application/octet-stream	Access, Create, Write	MALICIOUS
1457ef7a201dae0072c1b63cdabef8dd2dbb4002c85c599d50ffeb3673633f38	c:\users\keecfmwgj\desktop\fjanz4q_5c_daaszw.ots.vvyu, C:\Users\kEecfMwgj\Desktop\fjAnz4q_5C_daasZw.ots.vvyu	Dropped File	40.34 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e9b3f70fd0c57d38dbf1717a4da291a222a0e958651ad5b7dcd9667255664829	c:\users\keecfmwgj\favorites\msn websites\msn autos.url.vvyu, C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Autos.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
63c48ccfb9c1c2725f75c3f43fa6fce55f2201f603580e00eb0bf68e6e8a0aed	C:\Users\kEecfMwgj\Desktop\Ed-zOTKEEUdYISk.mp4.vvyu, c:\users\keecfmwgj\desktop\ed-zotkeeudyisk.mp4.vvyu	Dropped File	38.80 KB	application/octet-stream	Access, Create, Write	MALICIOUS
f9c1e3d3f15f253236e3c6371653208809bde5d790b1bc71bc0f100eed140a3f	c:\users\keecfmwgj\pictures\8jmjrpib7p7v7jga.png.vvyu, C:\Users\kEecfMwgj\Pictures\8jMjrpIb7p7V7JGa.png.vvyu	Dropped File	84.64 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4125d609d0002358ed516dd8b4cb43e58e7a1b435e9b6ab353578eebf77b54ff	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\gFRsS2-OR13.gif.vvyu, c:\users\keecfmwgj\pictures\ymomnephob\gfrss2-or13.gif.vvyu	Dropped File	78.58 KB	image/gif	Access, Create, Write	MALICIOUS
dcbb45df48afc4dd383ecff078decd1dc868c364af8cc256e21751a73a5f3276	C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\n3veXEkNYxTCSfl4ofL.m4a.vvyu, c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\n3vexeknyxtcsfi4ofl.m4a.vvyu	Dropped File	69.99 KB	application/octet-stream	Access, Create, Write	MALICIOUS
217ee40236447b18327eb4a334bd03d7537e7d23c5be64ec50398b5f866b69c5	c:\users\keecfmwgj\pictures\ymomnephob\d7pqidsie6laiayeoe\dh_l_ueln9j1ttp1p51.gif.vvyu, C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\d7pQIdSiE6laiAyeoE\dH_l_Ueln9J1Ttp1P51.gif.vvyu	Dropped File	61.49 KB	image/gif	Access, Create, Write	MALICIOUS
d80d53586bf7e8f2c2b2472a1fbbb7b72dd5107b63e9f9ecb4eb2ecac30ad8c8	c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61xto95hr3jmn6z\yw2t95\ia4pahu.wav.vvyu, C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_OxVk\61XTO95hR3JMn6Z\yw2t95\ia4pAHu.wav.vvyu	Dropped File	28.16 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d8fa3f08dd3f209598e963e8b037c223a500ecc6ec487381d8db4463a1c5b6f8	c:\users\keecfmwgj\desktop\9ji3dkvzy.avi.vvyu, C:\Users\kEecfMwgj\Desktop\9ji3dkVzY.avi.vvyu	Dropped File	41.71 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
26709dda24db867a0fec33f7f85be2e50e5d65b913cf4cf309c84391656a2657	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\f72mw_knqrugyjjccbc\c9qz99w\82ajw1e0_3n2yyse_.avi.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\F72Mw_KNQRugYJJCcBc\C9Qz99w\82ajW1E0_3n2yYSE_.avi.vvyu	Dropped File	74.15 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d4c4c63f26b77e471604ec7aef95bdb1ea5099afbdf57c96a7f86d8ca2539bb4	c:\users\keecfmwgj\desktop\zsr7xc26_dfdmvcahh\exko6hh.png.vvyu, C:\Users\kEecfMwgj\Desktop\ZsR7Xc26_DfdmVcahH\Exko6hh.png.vvyu	Dropped File	40.30 KB	application/octet-stream	Access, Create, Write	MALICIOUS
9b6a93f17fbae46a9d39f93bf0504592dce14b8cbcf62e095054a13d598ec4e8	C:\Users\kEecfMwgj\Documents\AzID\EXsKx.odp.vvyu, c:\users\keecfmwgj\documents\azid\exskx.odp.vvyu	Dropped File	46.84 KB	application/octet-stream	Access, Create, Write	MALICIOUS
124cac85c7a8375d2ee6a5d2792918f9e50ea36fef645d196e2b09f46ec14a97	c:\users\keecfmwgj\pictures\ymomnephob\d7pqidsie6laiayeoe\k4vlze9tyd\9gfedyg-xmcwzgawdh.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\d7pQIdSiE6laiAyeoE\k4vLze9TyD\9GFEdyG-XmCwzgAwdH.bmp.vvyu	Dropped File	63.96 KB	application/octet-stream	Access, Create, Write	MALICIOUS
072b03e6d6d5b5133dea0f917a209d471cc673c685d632719ccfd25676efb002	c:\users\keecfmwgj\pictures\ymomnephob\te1lwlzl-cqvzewgl\-2okt.gif.vvyu, C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\tE1LWlZl-CqVZeWgL\-2oKT.gif.vvyu	Dropped File	70.28 KB	image/gif	Access, Create, Write	MALICIOUS
a7a0fd8f39ab20081addfbebbbbb9791bf28b00aea37ff2ce745c10d3327c1fb	c:\users\keecfmwgj\documents\azld\pebfuwtor 4\-1ots4a6s.pps.vvyu, C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR 4\-1Ots4A6s.pps.vvyu	Dropped File	54.39 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e76ca9c6e5e874576c6cb2a13d5d52893b54450e93316d075640f25257449fbe	c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\jymab2bdvruj9sv.m4a.vvyu, C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_OxVk\jYMAb2bdVruj9SV.m4a.vvyu	Dropped File	16.95 KB	application/octet-stream	Access, Create, Write	MALICIOUS
49a9102816b0bd13070c208d7eab74e0b0e2e48eba5e10b757b3b91ca2e64544	c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\7bowspyroi2cx.pdf.vvyu, C:\Users\kEecfMwgj\Documents\AzID\UHfBjIaC\yEpRZCn46rxjDOAUpD\7BOWSPyroI2Cx.pdf.vvyu	Dropped File	92.35 KB	application/pdf	Access, Create, Write	SUSPICIOUS
72008ea37ad5a8f39172061f4bb290ff39e3c7ab17b08a5396e365d45a47b8d3	c:\users\keecfmwgj\documents\bflhqgtm.pdf.vvyu, C:\Users\kEecfMwgj\Documents\BFlHqgTM.pdf.vvyu	Dropped File	37.97 KB	application/pdf	Access, Create, Write	SUSPICIOUS
4a1aaeed4747266983004f9fa25ff0ed024415f8232f30467b08441084b002e0	-	Web Response	554 bytes	text/html	-	CLEAN
d65eecdf981972a11ddea38b550320330f348f24d016b3b466d3523e26f64310	-	Modified File	64.00 KB	application/octet-stream	-	CLEAN
3c7d38aff2dd9e697cd3cc6c0a5d338ff2d0bdb948fb469cd21c76d8c36e53ee	-	Modified File	256.00 KB	application/octet-stream	-	CLEAN
7b5ca90f00d259082ce1ce3c8d9341a2deae05e7dcf760d95aeb3aad782d46d3	c:\users\keecfmwgj\music\oolphjaohulco5czcdi.mp3.vvyu, C:\Users\kEecfMwgj\Music\OolphJaohuLco5czCDI.mp3.vvyu	Dropped File	15.22 KB	application/octet-stream	Access, Create, Write	CLEAN
0a2d505911e9bcae92659ea12701988c134fba11415359e5c7531fa2bf246265	C:\Users\kEecfMwgj\Pictures\lv6DMrgKbM_9C6x.jpg.vvyu, c:\users\keecfmwgj\pictures\lv6dmrgkbm_9c6x.jpg.vvyu	Dropped File	3.90 KB	image/jpeg	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
50d40a5b742bcfe20fe56b2b2a1cf95e9a73de88d32d916870cee225a2071e09	C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR 4\ivoTJ\soMD9qxXFL8rvNP.rtf.vvyu, c:\users\keecfmwgj\documents\azld\pebfuwtor 4\ivotj\s omd9qxxfl8rvnp.rtf.vvyu	Dropped File	49.07 KB	text/rtf	Access, Create, Write	CLEAN
481c458ca680433f7cd0b7f2a558ca24f75ab28d799ca5e71ce5d0700ed669c0	c:\users\keecfmwgj\music\pe0cuon\i_smja7zftd 88.wav.vvyu, C:\Users\kEecfMwgj\Music\pE0cUon\I_smja7ZftD 88.wav.vvyu	Dropped File	89.73 KB	application/octet-stream	Access, Create, Write	CLEAN
6d214ad6b2cf334f0545be9f044bb26b2bd3d43dd77f5e124a5769b86c9ad995	-	Downloaded File	216 bytes	text/html	-	CLEAN
95c85188b90c8a901d9b802579144fc87ae1cb1943cc0e0cec3cd9bf85707884	c:\users\keecfmwgj\documents\azld\pebfuwtor 4\ivotj\tawx51mud\aig5nj9ziln1ciulcka.odt.vvyu, C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR 4\ivoTJ\TawX51muD\aiG5nj9ZiLn1CiuLcka.odt.vvyu	Dropped File	9.54 KB	application/octet-stream	Access, Create, Write	CLEAN
baa96e99d85b40ac95608fdc91f7421ddfd1c466e6260edba67d9b7a3ba505a9	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\0o41zs\lzhdqsiji02\we9tzkhspb.mp4.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\Y5X8\0o41ZS\LzHDQsiji02\WE9tZKhSpB.mp4.vvyu	Dropped File	12.42 KB	application/octet-stream	Access, Create, Write	CLEAN
118d31989b101a37257f20235d9dccac8be2212f9b222a9f262318f0faac7859	c:\users\keecfmwgj\videos\-dwrkzslsf2_dei9bifvc5tqmw.flv.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2_dEi9BifVC5tQMw.flv.vvyu	Dropped File	49.18 KB	video/x-flv	Access, Create, Write	CLEAN
fd216c7d8b5bba37d789b82d076aa33ec2dbd4781bb3c0e4b3fcd1015187fbbf	c:\users\keecfmwgj\documents\oo9yxvhfzy447m.docx.vvyu, C:\Users\kEecfMwgj\Documents\oO9yXvHfzy447m.docx.vvyu	Dropped File	81.17 KB	application/zip	Access, Create, Write	CLEAN
10bcc02e659816e174a6fc4316c010de8d2f95ea53175dd53037ed979a3b80fd	C:\Users\kEecfMwgj\Documents\xyVBcXoxWZOEVZ7.pptx.vvyu, c:\users\keecfmwgj\documents\xyvbcxoxwzoevz7.pptx.vvyu	Dropped File	32.29 KB	application/zip	Access, Create, Write	CLEAN
4b1fec34c68d69ceca2d8e6d30bddef31e0826ea247496b38b4100c54c41dd7a	c:\users\keecfmwgj\documents\azld\uhfbjiac\nooizr\vvjlrm5wps_pezl.odp.vvyu, C:\Users\kEecfMwgj\Documents\AzID\UHfBjIaC\noOiZR\VVjlRm5Wps_PeZL.odp.vvyu	Dropped File	33.47 KB	application/zip	Access, Create, Write	CLEAN
e32fb33afe83b74e84d7a688a9ce81bb964772c839d9a5904efbba8309da3041	c:\users\keecfmwgj\favorites\msn websites\msn.url.vvyu, C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
3a17d2f58d31c867e8e6621a0c6141f111c94921eb0ab256caf471ac9b0b06ac	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\nnzzossfvx.mp4.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\Y5X8\NNZzOSSfvX.mp4.vvyu	Dropped File	65.41 KB	application/octet-stream	Access, Create, Write	CLEAN
349bba73483c1884679fac895993d954212046f741abc76ef471de00ec3a7d76	C:\Users\kEecfMwgj\Desktop\gnNW5oKgmW5QeElwN.mp4.vvyu, c:\users\keecfmwgj\desktop\gnnw5okgmw5qeelwn.mp4.vvyu	Dropped File	71.17 KB	application/octet-stream	Access, Create, Write	CLEAN
af2268c23a12eefb64adb0e01d2229d37e8563c9ee874426f15b3371131ae75d	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\exzou4j4nw j\zwquu_bys.swf.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\EXZou4J4nw j\zwQUu_BYs.swf.vvyu	Dropped File	57.71 KB	application/x-shockwave-flash	Access, Create, Write	CLEAN
8059d3cbb5bf0eff05087810a8f573fd23736d08ffec4002e27cd7ba4fd550db	C:\Users\kEecfMwgj\Desktop\eOgdOPqhf.odp.vvyu, c:\users\keecfmwgj\desktop\eogdopqhf.odp.vvyu	Dropped File	43.79 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
877c4bb6979ca315c7e84c93677b69649e22983a2ebb6eea8d2227eab42c10ac	c:\users\keecfmwgj\music\fuhvly4jeagwk\wd-bcbik6paqlyst.m4a.vvyu, C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\wd-bCBiK6pAQlyST.m4a.vvyu	Dropped File	26.93 KB	application/octet-stream	Access, Create, Write	CLEAN
4e1e6fbbfc0cdeea39f09951cbe62e8733047fff27902f2a4a7734e347c12a81	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E5UCc4GR1ZtMgYPe\4uY5fsSdcyjSgJ.jpg.vvyu, c:\users\keecfmwgj\pictures\ymomnephob\e5ucc4gr1ztmgype\4uy5fssdcyjsgj.jpg.vvyu	Dropped File	21.24 KB	image/jpeg	Access, Create, Write	CLEAN
5ff08ad47f0af066b053a886d82d9346252418ebbc71afbccf573ff1dfe8feef	c:\users\keecfmwgj\documents\outlook files\franc@gdllo.de.pst.vvyu, C:\Users\kEecfMwgj\Documents\Outlook Files\franc@gdllo.de.pst.vvyu	Dropped File	265.33 KB	application/octet-stream	Access, Create, Write	CLEAN
aaa3d405042df39d8a0d3265ad9d5d8fcba669ecf150e11d67c7388841a98221	c:\users\keecfmwgj\documents\azld\rqzy4w0rybhq_irzd3\f4quftb6aenpm.csv.vvyu, C:\Users\kEecfMwgj\Documents\AzlD\rQzy4W0rYbhQ_iRzD3\f4quftb6AeNpM.csv.vvyu	Dropped File	32.15 KB	application/octet-stream	Access, Create, Write	CLEAN
b8f4d2788cb8dd11d6c6f2737f8d5b0cf4bfb6dfbb1c04e40d818f6e5cf8c7e6	c:\users\keecfmwgj\desktop\yyyx_.avi.vvyu, C:\Users\kEecfMwgj\Desktop\YYyX_.avi.vvyu	Dropped File	4.62 KB	application/octet-stream	Access, Create, Write	CLEAN
25824882b975d34cb5641da724c7ba14e144343247f97d0448201ccc4403819a	-	Modified File	80.00 KB	application/octet-stream	-	CLEAN
b65091f72d97f2e59acec22565746952aa9b99d124eebc9d271e5a69a62b00c7	C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\LNo4VDj5U-Z.wav.vvyu, c:\users\keecfmwgj\music\fuhvly4jeagwk\lno4vdj5u-z.wav.vvyu	Dropped File	81.79 KB	application/octet-stream	Access, Create, Write	CLEAN
7ea10d8b6b4664fd0e4cf56da29f071d433e1f686ae856b4f37cf92f4a65d737	C:\Users\kEecfMwgj\Documents\y_n6R.xlsx.vvyu, c:\users\keecfmwgj\documents\y_n6r.xlsx.vvyu	Dropped File	30.35 KB	application/octet-stream	Access, Create, Write	CLEAN
f1ca7ff7e133d880af610e77c788dc02048d3aa64484115ac1734e7e13455ad6	c:\users\keecfmwgj\videos\-dwrkzslsf2\tosxrvqraigf3mknom0.avi.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\tosxRVQralGf3MknOm0.avi.vvyu	Dropped File	65.95 KB	application/octet-stream	Access, Create, Write	CLEAN
c84ebc1aaa1d62d0098a4c9e7a6dfe4763f75fbc0c2f76ae2c69a61a694bb9e1	C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\Y5X8wIEnhA.flv.vvyu, c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\y5x8wlenha.flv.vvyu	Dropped File	35.81 KB	video/x-flv	Access, Create, Write	CLEAN
18f70f93c27e19984f27e7bac31f7e6a40df4d1b8053f156ecc0cd980be77351	c:\users\keecfmwgj\desktop\zsr7xc26_dfdmvcahh\kyk8l.flv.vvyu, C:\Users\kEecfMwgj\Desktop\ZsR7Xc26_DfdmVcahH\kyK8l.flv.vvyu	Dropped File	15.39 KB	video/x-flv	Access, Create, Write	CLEAN
82c087708286f4d9185898d67319258a3582bd5e973f85c34cae9ef8076f4a2e	c:\users\keecfmwgj\desktop\c5rx.mkv.vvyu, C:\Users\kEecfMwgj\Desktop\C5Rx.mkv.vvyu	Dropped File	75.66 KB	application/octet-stream	Access, Create, Write	CLEAN
7ba6dec49a43959f898a28dcb710deed90aa3d641f20c180b271a451404a24db	c:\users\keecfmwgj\documents\azld\pebfuwtor 4\ivotj\xivbhkfo h.ppt.vvyu, C:\Users\kEecfMwgj\Documents\AzlD\PeBfuwtoR 4\ivoTJ\XiVbHKfo h.ppt.vvyu	Dropped File	19.83 KB	application/octet-stream	Access, Create, Write	CLEAN
9e324150094c29b0335eca13f2ee815887c038252b9d3651d68c2460dc01b172	c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61xto95hr3jmn6z\kf5kyh.m4a.vvyu, C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_OxVk\61XTO95hR3JMn6Z\kf5kyH.m4a.vvyu	Dropped File	21.84 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
46175ccdeb582b78cc71137335fc5aa16775e8b62a54f5f3e5f9bcedb29ccd52	c:\users\keecfmwgj\pictures\ymomnephob\te1lwlzl-cqvzew gl\xgpgxl.jpg.vvyu, C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\tE1LWIZl-CqVZeW gL\xGPgXL.jpg.vvyu	Dropped File	9.99 KB	image/jpeg	Access, Create, Write	CLEAN
f025c3968057ff48c44b689f5bc289b348c71782350b5213f826c9dfe3136843	c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu, C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Entertainment.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
196f087b39cf4d49bd53ddeb9bfec62acf33f3e16dc55159c27cd8bc82e1a886	C:\Users\kEecfMwgj\Documents\AzID\UHfBjlaC\wzwkC7.odp.vvyu, c:\users\keecfmwgj\documents\azid\uhfbjiac\wzwkc7.odp.vvyu	Dropped File	24.75 KB	application/octet-stream	Access, Create, Write	CLEAN
6b19d524040d4124832d7e90a7027152b549106333e6a8cff367b179df2d60de	c:\users\keecfmwgj\favorites\windows live\get windows live.url.vvyu, C:\Users\kEecfMwgj\Favorites\Windows Live\Get Windows Live.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
677c7dc41a4e418122ed6cbaf8d1dac71518e217f21f3dfbd0d5018277ebcaf0	c:\users\keecfmwgj\desktop\ohy9bmsmlfi5\5uvlwu6-nnebg.jpg.vvyu, C:\Users\kEecfMwgj\Desktop\OhY9bMSmLfI5\5UvLwu6-nNEbg.jpg.vvyu	Dropped File	20.44 KB	image/jpeg	Access, Create, Write	CLEAN
0c5cceba5c416d5424387794429f89a2456b5326e2c7e5d8d2bd67f34bb616ec	-	Modified File	32.00 KB	application/octet-stream	-	CLEAN
5f754e82924830b4f1e544e35b5fcd196503650104b8c0eabce44ae5ee9ed4ec	C:\Users\kEecfMwgj\Desktop\OhY9bMSmLfI5\hxqHaq.mkv.vvyu, c:\users\keecfmwgj\desktop\ohy9bmsmlfi5\hxqhaq.mkv.vvyu	Dropped File	7.96 KB	application/octet-stream	Access, Create, Write	CLEAN
5b577d8bb7016ed42ae9b146647417ecd1fa3b7a0ba8d099982eb890466c7f3a	C:\Users\kEecfMwgj\Desktop\o5GqCe9ZgNw7JzfwVH.gif.vvyu, c:\users\keecfmwgj\desktop\o5gqce9zgnw7jzfwvh.gif.vvyu	Dropped File	95.49 KB	image/gif	Access, Create, Write	CLEAN
4f735a8b60601a2931dabb2311473b0220f92b792a3cbd3fd570792abd98873c	c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.vvyu, C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE site on Microsoft.com.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
3acf76f55cab420fef48b37dcceaeacf561a0ea274cafc60b81cb2e6d37887b0	c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu, C:\Users\kEecfMwgj\Favorites\MSN Websites\MSNBC News.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
c5b03662e333e798a2a3e9892f0fdef122eaa40edbb8a3325bc85795b17a267a	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\0o41zs\lzhdqsiji02\3exl.mkv.vvyu, C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\Y5X8\0o41ZS\LzHDQsiji02\3Exl.mkv.vvyu	Dropped File	82.87 KB	application/octet-stream	Access, Create, Write	CLEAN
8d5c1468c53c57af5d92066e545a354fc9617eb93248807e28cb3a6d0effd368	C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\F72Mw_KNQRugYJJCcBc\C9Qz99w\b3JSk19CS30.avi.vvyu, c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\c9qz99w\b3jsk19cs30.avi.vvyu	Dropped File	93.79 KB	application/octet-stream	Access, Create, Write	CLEAN
6d39b2fa76edba194228b842370b8a71d35e7c9e5796fbfc78c4ce4ea417a8b2	C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR 4\XvrsId5WMhv8lJp8.ots.vvyu, c:\users\keecfmwgj\documents\azid\pebfuwtor 4\xvrsid5wmhv8ljp8.ots.vvyu	Dropped File	32.66 KB	application/octet-stream	Access, Create, Write	CLEAN
ee148fc7058dac5985c9860 2eeea07391170ddbf65e6cf0112d3d00439c1d559	C:\Users\kEecfMwgj\Desktop\xf-vHBag-ZJttfl79F6Z.bmp.vvyu, c:\users\keecfmwgj\desktop\xf-vhbag-zjttfi79f6z.bmp.vvyu	Dropped File	94.08 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c5600df2c43e74604428545d8936848009c31cc644b4ab15341ced9051fc3e47	c:\users\keecfmwgj\pictures\nthxrlnnkw.gif.vvyu, C:\Users\kEecfMwgj\Pictures\NThXrLNnKw.gif.vvyu	Dropped File	96.30 KB	image/gif	Access, Create, Write	CLEAN
9ae8d48ff0694ac3068b063fbd26ed8d9422fa87a831f426900c7e622910812e	C:\Users\kEecfMwgj\Documents\AzID\UHfBjIaC\Z8rQUb38uy_iJ3tNKmP2.ppt.vvyu, c:\users\keecfmwgj\documents\azid\uhfbjiac\z8rqub38uy_ij3tnkmp2.ppt.vvyu	Dropped File	87.98 KB	application/octet-stream	Access, Create, Write	CLEAN
edb386dd3c55f95531471aff2cb6729a262e453f2c483ef37ecffd802e607b58	C:\Users\kEecfMwgj\Documents\zzDsCcZ.xlsx.vvyu, c:\users\keecfmwgj\documents\zzdsccz.xlsx.vvyu	Dropped File	1.34 KB	application/octet-stream	Access, Create, Write	CLEAN
7694eaf208dcac81be98be7ed791e127b8bcdc72dc18f39ac25fdf675014f3cb	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\d7pQIdSiE6laiAyeoE\k4vLze9TyD\hM HT 9rGnc6u.gif.vvyu, c:\users\keecfmwgj\pictures\ymomnephob\d7pqidsie6laiayeoe\k4vlze9tyd\hmht 9rgnc6u.gif.vvyu	Dropped File	61.14 KB	image/gif	Access, Create, Write	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\documents\zsmchocwullalz-0fsrc.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\n3veXEkNYxTCSfl4 ofL.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\9ji3dkvzy.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\azld\rqzy4w0rybhq_irzd3\f4quftb6aenpm.csv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\y5x8\nnzzossfvx.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\zzDsCcZ.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\jymab2bdvruj9sv.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ymomnephob\d7pqidsie6laiayeoe\lbmwdokxeh2om_f.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\y5x8\0o41zs\jqftouthgp-pwfb0a.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\Y5X8\wlEnhA.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR 4\31Pg.xls.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\ScQyRdBL.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\f72mw_knqrugyjjccbc\c9qz99w\82ajw1e0_3n2yyse_.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\es4lp.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\AzID\UHfBjIaC\yEpRZCn46rxjDOAUpD\YpCtinwvv6IL210.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\eOgdOPqhf.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\wzmkmopozyago-ujtdf.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\Y5X8\0o41ZS\b5aBDkyBYyj.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\qmnc3epw1fv.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\7Q5_45ijmfP9bA\GwAL3j0fQyIFxx-jKJ.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\msn websites\msn.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\Y5X8\0o41ZS\EDTDz9.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR 4\XvrsId5WMhv8lJp8.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\azId\pebfuwtor 4\ivotj\ru0q9.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\f kf.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ncx1xStlYX_cZWb.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\vku7O.doc.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\iJReKTqGLBvZe.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\OkF0P0lVbo seJvjybv_.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\ntkcvhIlb.pps.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\d7pQIdSiE6laiAyeoE\k4vLze9TyD\hM HT 9rGnc6u.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\7q92iR26 9wIDTp.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\78tFz6xBRVYoOofh5u.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\7Q5_45ijmfP9bA\TYpweac9t_MP.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\exzou4j4nw j\m5lkrrhopgpv2jhgtq-.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\zsr7xc26_dfdmvcahh\exko6hh.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\azId\uhfbjiac\nooizr\rt8g.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\ZsR7Xc26_DfdmVcahH\PRpouSq\QwaTwvQX1o7erS.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	Dropped File, Accessed File, VM File	Access, Create, Delete, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\7pEW.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR 4_wgbJ2d7Z.csv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\Y5X8\0o41ZS\LzHDQsiji02\MQWaq1YvFIYApR.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR 4\ivoTJ\soMD9qxXFL8rvNP.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ymomnephob\e5ucc4gr1ztmgype\qjvfzvvw_idbuk5j3vj1.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\usizz5vInlecvw.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\azId\pebfuwtor 4\ivotj\jnzkj8redoajzl.xls.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\tosxrvqraigf3mknom0.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\dyhqug0jr8d4isrx0nn1.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\pictures\ymomnephob\7q5_45ijmfp9ba_ydmbp0zwbtzu.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\NLJO_aKDC.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\tu0g8bchmtwfhihtpj.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE Add-on site.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\f72mw_knqrugyjjccbc\htwdnwtyy\iricfx-m5bn.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\x9kn7y7cefv.xls.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\f72mw_knqrugyjjccbc\7jjuxf5i.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\pe 0cuon\jrz5y.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\nthxrlnnkw.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ymomnephob\d7pqidsie6laiayeoe\k4vlze9tyd\9gfedyg-xmcwzgawdh.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\azld\pebfuwtor4\a2_m3nqdrdmg.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\FDSFO0.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\Ths6OlVH\AFh4M.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ymomnephob\te1lwlzl-cqvzewgl\k4ycl.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\j3esmpnibwefl.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\yw2t95\l69lcxnvikb5vvhczyx.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\qc9h.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\OhY9bMSmLfl5\rgwTa9twwGw5.csv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\fjanz4 q_5c_daaszw.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uabuSVqvA\EXZou4J4nw j\EFsNJX_Z-O4v4Zp.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\zsr7xc26_dfdmvcahh\mpfqoqqirbvbhaaavogl.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\locallow\microsoft\internet explorer\services\search_{0633ee93-d776-472f-a0ff-e1416b8b2e3a}.ico.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Spaces.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\V89DayYK-6YpvEr4NY.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\AzlD\UHfBjlaC\eE nQNbY2Kl.doc.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\azld\uhfbjiac\nooizr\tdpk.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\-yzsadt_8t croyrko.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ymomnephob\te1lwlzl-cqvzewgl\xgpgxl.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\yrqwfs6apmpbyvu.doc.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\qpf-r5z.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\yw2t95\ia4pahu.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\yw2t95\rnqkcz9li.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\xf-vHBag-ZJttfl79F6Z.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\gnNW5oKgmW5QeElwN.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\c5rx.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\-DwrKzslsF2\SVKL6Wu5uab uSVqvA\F72Mw_KNQRugYJJCcBc\C9Qz99w\b3JSk19CS30.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\B8R3y.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\brlu 5vgds.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\tE1LWIZl-CqVZeW gL\CfqSEGHWv8ld7U6qj5.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\tkv_jmwrxlf8d6fc.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\d1e2c5.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\5ggbg59nqgc.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\azld\pebfuwtor 4\ivotj\xivbhkfo h.ppt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\BfwcyLh4.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\ztljjzckd4ecj5.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\kf5kyh.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\xyVBcXoxWZOEVZ7.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\32aCzuXFDU.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\tRcMqrNBqTUs.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_ OxVk\61X TO95hR3JMn6Z\yw2t95\ZcUZ5M4Jt.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\azld\pebfuwtor 4\ivotj\jgoljrnopieamfof-hp.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\zsr7xc26_dfdmvcahh\kyk8l.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\AzlD\PeBfuwtoR 4\tEiHH.pdf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\a8csbpx3pb.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	Sample File, Accessed File, VM File	Access, Delete, Read, Write	MALICIOUS
c:\users\keecfmwgj\music\fuhvly4jeagwk\nfk529nzfij1e1.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\yyyx_.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\documents\azld\uhfbjiac\nooizr\vvjlrm5wps_pezl.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_ OxVk\61X TO95hR3JMn6Z\pE7_nJD0Tmm8m2VYvr.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E07daaq0LDB.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\bflhqgtm.pdf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\exzou4j4nw j\zwquu_bys.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ymomnephob\te1lwlzl-cqvzewgl\-2okt.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\HDnGwo1W3X7Qq9.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipgggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\wl5kmftlwsv3.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\tE1LWlZl-CqVZeWgL\Gpf_fTIy87TJO1Dp27TE.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\J0wAvHXNsUrjj8.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_ OxVk\61X TO95hR3JMn6Z\cYVyaoVP6_8ikj.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\nifn.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\-DwrKzsIsF2\SVKL6Wu5uab uSVqvA\Y5X8\0o41ZS\Fjxa.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\ul-Z5b.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\o5GqCe9ZgNw7JzfwVH.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\gz-yqulpeghm6.odt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\vzsbld-s6.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\windows live\windows live mail.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\AzlD\EXsKx.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\0auodapipmqwtk.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\e ri1atxotxxvz19.ppt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\0o41zs\lzhdqsiji02\we9tzkhspb.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\gFRsS2-OR13.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\vpmkp.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\Ed-zOTKEEUdYISk.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\YwgWoXY4_d Sr.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\jbbjylnj 4z9k-.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\AzlD\UHfBjlaC\noOiZR\8NQv3A3MccCF.xls.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\fuhvly4jeagwk\ipgggqug4\psrckmpedif_oxvk\61x to95hr3jmn6z\x52p6pb3thpumw.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\AzlD\qGqm\B_1klj6HPFfLN8h7Oij.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\documents\yqj5kxs1j7uvwoh.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\6cposy.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\u7unq0 vl v.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\7oqi8laykzm3pzqg.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\d7pQIdSiE6laiAyeoE\cH1Zz4OF5OqujiOEN9.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\8jmjrpib7p7v7jga.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ymomnephob\7q5_45ijmfp9ba\lejzvedjk.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\microsoft websites\microsoft at home.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\0o41zs\lzhdqsiji02\3exl.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\azld\pebfuwtor 4\-1ots4a6s.pps.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\32xdz.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\fmtiy2j60xys_lff.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://acacaca.org/files/1/build3.exe	-	190.140.99.150, 189.164.252.207, 5.163.244.118, 110.14.121.125, 190.117.75.91, 190.219.54.242, 211.53.230.67, 116.121.62.237, 124.109.61.160, 187.170.251.250	-	GET	MALICIOUS
http://rgyui.top/dl/build2.exe	-	-	-	-	MALICIOUS
http://acacaca.org/test2/get.php?pid=248506A379C3838D8B1754B19D2995D3&first=true	-	190.140.99.150, 189.164.252.207, 5.163.244.118, 110.14.121.125, 190.117.75.91, 190.219.54.242, 211.53.230.67, 116.121.62.237, 124.109.61.160, 187.170.251.250	-	GET	MALICIOUS
https://api.2ip.ua/geo.json	-	162.0.217.254	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
acacaca.org	190.140.99.150, 189.164.252.207, 5.163.244.118, 110.14.121.125, 190.117.75.91, 190.219.54.242, 211.53.230.67, 116.121.62.237, 124.109.61.160, 187.170.251.250	-	TCP, HTTP, DNS	MALICIOUS
rgyui.top	-	-	-	MALICIOUS
api.2ip.ua	162.0.217.254	-	TCP, HTTPS, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
187.170.251.250	acacaca.org	Mexico	DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
116.121.62.237	acacaca.org	South Korea	DNS	CLEAN
211.53.230.67	acacaca.org	South Korea	DNS	CLEAN
190.117.75.91	acacaca.org	Peru	DNS	CLEAN
5.163.244.118	acacaca.org	Saudi Arabia	DNS	CLEAN
190.219.54.242	acacaca.org	Panama	DNS	CLEAN
162.0.217.254	api.2ip.ua	Netherlands	TCP, HTTPS, DNS	CLEAN
124.109.61.160	acacaca.org	Pakistan	DNS	CLEAN
189.164.252.207	acacaca.org	Mexico	TCP, HTTP, DNS	CLEAN
190.140.99.150	acacaca.org	Panama	DNS	CLEAN
110.14.121.125	acacaca.org	South Korea	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}	access	12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion	access	12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\SysHelper	read, access, write	12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SysHelper	read, access, write	12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	CLEAN

Process

Process Name	Commandline	Verdict
12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	"C:\Users\kEecfMwgj\Desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe"	MALICIOUS
12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	"C:\Users\kEecfMwgj\Desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe" --Admin IsNotAutoStart IsNotTask	MALICIOUS
12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	"C:\Users\kEecfMwgj\AppData\Local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe" --AutoStart	MALICIOUS
12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	"C:\Users\kEecfMwgj\Desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe"	SUSPICIOUS
12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	"C:\Users\kEecfMwgj\Desktop\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe" --Admin IsNotAutoStart IsNotTask	SUSPICIOUS
12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe	"C:\Users\kEecfMwgj\AppData\Local\11c63de0-7744-463b-80d8-a375eb15d14b\12471d61dc844208bdbe23a9749980cf1a40ad45f844449afe55fb0f1cbbda0b.exe" --AutoStart	SUSPICIOUS
icacls.exe	icacls "C:\Users\kEecfMwgj\AppData\Local\11c63de0-7744-463b-80d8-a375eb15d14b" /deny *S-1-1-0:(OI)(CI)(DE,DC)	CLEAN

YARA / AV

YARA (304)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\V89DayYK-6YpvEr4NY.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61xto95hr3jmn6z\yw2t95\rnqkcz9li.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\-DwrKzsIsF2\SVKL6Wu5uabuSVqvA\Y5X8\0o41ZS\b5aBDkyBYyj.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E07daaq0LDB.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_OxVk\61XTO95hR3JMn6Z\pE7_nJD0Tmm8m2VYvr.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\iudig2j9jtqfgbcv6n.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\pe0cuon\jrz5y.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ymomnephob\7q5_45ijmfp9ba_ydmbp0zwbtzu.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\tE1LWlZl-CqVZeWgL\Gpf_fTly87TJO1Dp27TE.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\appdata\locallow\microsoft\internet explorer\services\search_{0633ee93-d776-472f-a0ff-e1416b8b2e3a}.ico.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\y5x8\0o41zs\lzhdqsiji02\ffcamngkkb8gmcsqdpq.mkv.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\ul-Z5b.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\d7pQldSiE6laiAyeoE\cH1Zz4OF5OqujiOEN9.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Contacts\Administrator.contact.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\azld\uhfbjiac\nooizr\rt8g.pptx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\y5x8\0o41zs\235vhs8kou7y.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\links\web slice gallery.url.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\ZsR7Xc26_DfdmVcahH\PRpouSq\QwaTwvQX1o7erS.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\HDnGwo1W3X7Qq9.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\vzsbld-s6.bmp.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\AzlD\PeBfuwtoR 4_wgbJ2d7Z.csv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\bnbjzezhttp-mha.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\7Q5_45ijmfP9bA\iJwMptujDhUTwyI.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ymomnephob\e5ucc4gr1z tmgype\qjvfzvvw_idbuk5j3vj1.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\qxlg6rlrsvyemxil.m4a.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\141isvJREPi.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\z6ibwsvk.xlsx.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\exzou4j4nw j\m5lkrrhopgpv2jhgtq-.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop_gemdk.jpg.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\gz-yqulpeghm6.odt.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ymomnephob\7q5_45ijmfp9ba\lejzvedjk.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\7rMc5PE99.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E5UCc4GR1Z tMgYPe\k1TTTQU2.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\xc6y6diw-2mp3g1ez.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\FDSFO0.avi.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\P5pCqlWF\YwgWoXY4_dSr.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\5fJKex2DUyLjzY0p.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\fmtiy2j60xys_lff.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\u7unq0 vlv.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_ oxvk\61xto95hr3jmn6z\brlu 5vgds.wav.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\ntkcvhllb.pps.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\hstszlrr9zv1_v.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\7oqi8laykzm3pzqg.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\-DwrKzsIsF2\SVKL6Wu5uabuSVqvA\Y5X8\0o41ZS\EDTDz9.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\fuhvly4jeagwk\nfk529nzfij1e1.mp3.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\x9kn7y7cefv.xls.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\labkKD4FQA.wav.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\a1p6lyhhe5fq5dudw9xm.rtf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\PsRcKmPEdiF_OxVk\61XTO95hR3JMn6Z\yw2t95\rQWnqazpz-naoLL5P.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\-yzsadt_8t croyrko.pptx.vvyu	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\7jjuxf5i.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\-DwrKzsIsF2\SVKL6Wu5uab uSVqvA\Y5X8\0o41ZS\LzHDQsiji02\MQWaq1YvFIYApR.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\tRcMqrNBqTUs.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\OkF0P0lVbo seJvjybv_.docx.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\fkf.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\6cposy.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\-DwrKzsIsF2\SVKL6Wu5uab uSVqvA\Y5X8\0o41ZS\Fjxa.mp4.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\windows live\windows live mail.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\yrqwfs6apmpbyvu.doc.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\tE1LWIZl-CqVZeW gL\CfqSEGHWv8Id7U6qj5.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\AzlD\UHfBjIaC\eE nQNbY2KI.doc.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\zrus.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\qc9h.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\qpf-r5z.mp4.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\es4lp.pptx.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\-DwrKzsIsF2\SVKL6Wu5uab uSVqvA\F72Mw_KNQRugYJJCcBc\ MSPqrTgqm.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1G5y OYkuiK.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\5ggbg59nq gc.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzsIsf2\svkl6wu5uab usvqva\f72mw_knqrugyjjccbc\0iydfpw avsjadg.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\9p8OG.b mp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\-DwrKzsIsF2\SVKL6Wu5uab uSVqvA\VNAR2BEit3ka1sGXw8sq.m p4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzsIsf2\svkl6wu5uab usvqva\bst5msuptc.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\AzID\UHfBjIaC\hlTCx olpB7AQb0\S7akFO0_2kX867.ods.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\AzID\UHfBjIaC\yEpRZCn46rxjDOAUpD\feMArPT27Tt3Vq0tfRa.odp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\eri1atxotxxvz19.ppt.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\AzID\PeBfuwtoR 4\tEiHH.pdf.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\7Q5_45ijmfP9bA\GwAL3j0fQyIFxx-jKJ.gif.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\yqj5kxs1j7uvwoh.pptx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\fjanz4q_5c_daaszw.ots.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\msn websites\msn autos.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\Ed-zOTKEEUdYISk.mp4.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\8jmjrpib7p7v7jga.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\gFRsS2-OR13.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\fUhvLY4JeAGwk\iPggquG4\n3veXEkNYxTCSfl4ofL.m4a.vvyu	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ymomnephob\d7pqidsie6laiayeoe\dh_l_ueln9j1ttp1p51.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\61xto95hr3jmn6z\yw2t95\ia4pahu.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\9ji3dkvzy.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uabusvqva\f72mw_knqrugyjjccbc\c9qz99w\82ajw1e0_3n2yyse_.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\zsr7xc26_dfdmvcahh\exko6hh.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\AzlD\EXsKx.odp.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ymomnephob\d7pqidsie6laiayeoe\k4vlze9tyd\9gfedyg-xmcwzgawdh.bmp.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ymomnephob\te1lwlzl-cqvzew gl\-2okt.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\azld\pebfuwtor 4\-1ots4a6s.pps.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\fuhvly4jeagwk\ipggqug4\psrckmpedif_oxvk\jymab2bdvruj9sv.m4a.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\oolphjaohulco5czcdi.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\lv6DMrgKbM_9C6x.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\azld\uhfbjiac\yeprzcn46rxjdoaupd\7bowspyroi2cx.pdf.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\AzlD\PeBfuwtoR 4\ivoTJ\soMD9qxXFL8rvNP.rtf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\pe0cuon\i_smja7zftd 88.wav.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\azld\pebfuwtor 4\ivotj\tawx51mud\aig5nj9ziln1ciulcka.odt.vvyu	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\0o41zs\lzhdqsiji02\we9tzkhspb.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzslsf2_dei9bifvc5tqmw.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\oo9yxvhfzy447m.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\xyVBcXoxWZOEVZ7.pptx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\azId\uhfbjiac\nooizr\vvjlrm5wps_pezl.odp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\msn websites\msn.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\y5x8\nnzzossfvx.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\gnNW5oKgmW5QeElwN.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\-dwrkzslsf2\svkl6wu5uab usvqva\exzou4j4nw j\zwquu_bys.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\eOgdOPqhf.odp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\fuhvly4jeagwk\wd-bcbik6paqlyst.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\ymOmNEPhoB\E5UCc4GR1ZtMgYPe\4uY5fsSdcyjSgJ.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\outlook files\franc@gdllo.de.pst.vvyu	Ransomware	5/5

Reduced dataset

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	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.14 / 2022-08-03 12:19:21
YARA Built-in Ruleset Version	4.6.1.10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	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