MALICIOUS

Classifications: Downloader | Ransomware

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

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe**
ID	#5067212
MD5	7d3324aba9cb81871405761ea678c751
SHA1	07d238ddaabe2010d5113354b5dac651c1dcf8c0
SHA256	55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c
File Size	730.00 KB
Report Created	2022-08-05 13:25 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (26 rules, 162 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #13) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #13) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 219 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\Music\zkBFKRCKZ7lX KV Wa4.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\ou84g9.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\bijamby.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\zct8oosw8v0sthu.avi.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\kq__.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\VNMhw6NdT0N.m4a.vvyu".
- Rule "Djvu" from ruleset "Ransomware" has matched on a memory dump for (process #2) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe.
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\oa7uy-r84 e\v2hz1riby\-tfbdh.mkv.vvyu".
- Rule "Djvu" from ruleset "Ransomware" has matched on a memory dump for (process #6) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe.
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\xd4m_dlxrc.csv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\yxnorx1icarsuvxvr.xls.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\ckh5enz\utklaz\fzsdv9ic_tv.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\T4N8wuVG8qRit6NO.odp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\wxhzvh5geamrbckdv0bk.pptx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\ooeO67V 2A6dBdr.pps.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\VNa8b_DcXSUW mzm.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\i8vqvhtu5d8vngf1.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\56a-hqjck-6jacz_y.docx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\sovvb9YRGyMc-lzi435.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\4x6n.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\rqq-bsnksl6mhoio1.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\v2hZ1rIby\LqnhMFL0C.mkv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\rMc5RT6t.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\cs0y__wvetbw2qsiy.docx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\s12J.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\Plnb573cskZFLk.ots.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\sy7kzm.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\pd9daotni.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\3OZhLDJPo6htg3.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\ckh5enz\mgf6_dztb1f94j.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\q6aG5\M7TOG0.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\gmt4lzpnvyjn.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\jyj5.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\dHBKKyUiRLEo_ihqOR.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\nj4aq\rfdw37vjsnr.ods.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\puDbAQqOd3K9PVjvn1u.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\h6hrgnjnvqba.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\-CxO zQcq.avi.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\jpdadhjnb.mkv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\qexdtyv1z1q_cl0jaadt.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\v2hZ1rIby\2u CRZIC7nvdh_M.mkv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\oa7uy-r84 e\mhdjwhf8pwlbd.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\bojvfqm.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\SFCuO8sWL2Jsj.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\favorites\links\web slice gallery.url.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\fdd4gb84c4w3sg.mp4.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\AKXppD7.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\uomn anj\8ydbvfzvuknzyhmzsw2e.pptx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\q7szl.swf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\oa7uy-r84 e\v2hz1riby\4zazfhouywh4e77ghf.swf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\GcroBq0Ap.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\gnn Elw-bv2A ZdUCx.csv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\ckh5enz\g9op7kzr.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\ctXFDNnUwfp1foZl.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\s387k8QuDVZj.flv.vvyu".

Score	Category	Operation	Count	Classification
4/5	Reputation	Known malicious file	2	-

- The sample itself is a known malicious file.
- Reputation analysis labels embedded file "C:\Users\kEecfMwgj\AppData\Local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe" as Mal/Generic-S.

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) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "http://rgyui.top/dl/build2.exe" which was contacted by (process #6) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "http://acacaca.org/test2/get.php?pid=9663E9B9567D9A7DCED1D0F506975904&first=true" which was contacted by (process #6) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe as Mal/HTMLGen-A.

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

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

Score	Category	Operation	Count	Classification
3/5	YARA	Suspicious content matched by YARA rules	10	-

- Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\nj4aq\xq89ysrduds.pdf.vvyu".
- Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\nj4aq\xq89ysrduds.pdf.vvyu".
- Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\6e2w9YoR-8.pdf.vvyu".
- Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\6e2w9YoR-8.pdf.vvyu".
- Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "c:\users\keecfmwgj\desktop\ssz4\7qttxszlkjh_fii.pdf.vvyu".
- Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "c:\users\keecfmwgj\desktop\ssz4\7qttxszlkjh_fii.pdf.vvyu".
- Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\f1rc6EXPyfw.pdf.vvyu".
- Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\f1rc6EXPyfw.pdf.vvyu".
- Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\5kZStye71WnSS.pdf.vvyu".
- Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\5kZStye71WnSS.pdf.vvyu".

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

- (Process #2) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe deletes executed executable "C:\Users\kEecfMwgj\AppData\Local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe".

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

- (Process #6) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.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 #13) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.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	4	-

- (Process #1) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe modifies memory of (process #2) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe.
- (Process #5) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe modifies memory of (process #6) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe.
- (Process #7) build2.exe modifies memory of (process #8) build2.exe.
- (Process #12) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe modifies memory of (process #13) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe.

Score	Category	Operation	Count	Classification
2/5	Injection	Modifies control flow of a process started from a created or modified executable	4	-

Score	Category	Operation	Count	Classification
	• (Process #1) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe alters context of (process #2) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe. • (Process #5) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe alters context of (process #6) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe. • (Process #7) build2.exe alters context of (process #8) build2.exe. • (Process #12) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe alters context of (process #13) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe.		
2/5	Task Scheduling	Schedules task	1	-
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe", to be triggered by TIME. Task has been rescheduled by the analyzer.		
1/5	Obfuscation	Reads from memory of another process	4	-
	• (Process #1) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe reads from (process #1) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe. • (Process #5) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe reads from (process #5) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe. • (Process #7) build2.exe reads from (process #7) build2.exe. • (Process #12) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe reads from (process #12) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	4	-
	• (Process #1) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #5) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #7) build2.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #12) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.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) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe enumerates running processes. • (Process #6) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe enumerates running processes. • (Process #13) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe enumerates running processes.		
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #2) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe adds ""C:\Users\kEecfMwgj\AppData\Local\1b71cfc7... ...2-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe" --AutoStart" to Windows startup via registry.		
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #2) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe starts (process #2) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe with a hidden window.		
1/5	Mutex	Creates mutex	2	-
	• (Process #6) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe creates mutex with name "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}". • (Process #13) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe creates mutex with name "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}".		
1/5	Discovery	Reads system data	1	-
	• (Process #8) build2.exe reads the cryptographic machine GUID from registry.		
1/5	Discovery	Tries to get network statistics	1	-
	• (Process #13) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe gets network statistics via API.		
1/5	Network Connection	Downloads executable	1	Downloader

Score	Category	Operation	Count	Classification
	• (Process #6) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe downloads Windows executable via http from http://rgyui.top/dl/build2.exe.			
1/5	Network Connection	Downloads file	4	-
	• (Process #2) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe downloads file via http from https://api.2ip.ua/geo.json. • (Process #6) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe downloads file via http from http://acacaca.org/test2/get.php?pid=9663E9B9567D9A7DCED1D0F506975904&first=true. • (Process #6) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe downloads file via http from https://api.2ip.ua/geo.json. • (Process #13) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe downloads file via http from https://api.2ip.ua/geo.json.		
1/5	Obfuscation	Resolves API functions dynamically	8	-
	• (Process #1) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe resolves 39 API functions by name. • (Process #2) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe resolves 37 API functions by name. • (Process #5) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe resolves 39 API functions by name. • (Process #6) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe resolves 37 API functions by name. • (Process #7) build2.exe resolves 43 API functions by name. • (Process #8) build2.exe resolves 98 API functions by name. • (Process #12) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe resolves 39 API functions by name. • (Process #13) 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe resolves 58 API functions by name.		

Mitre ATT&CK Matrix

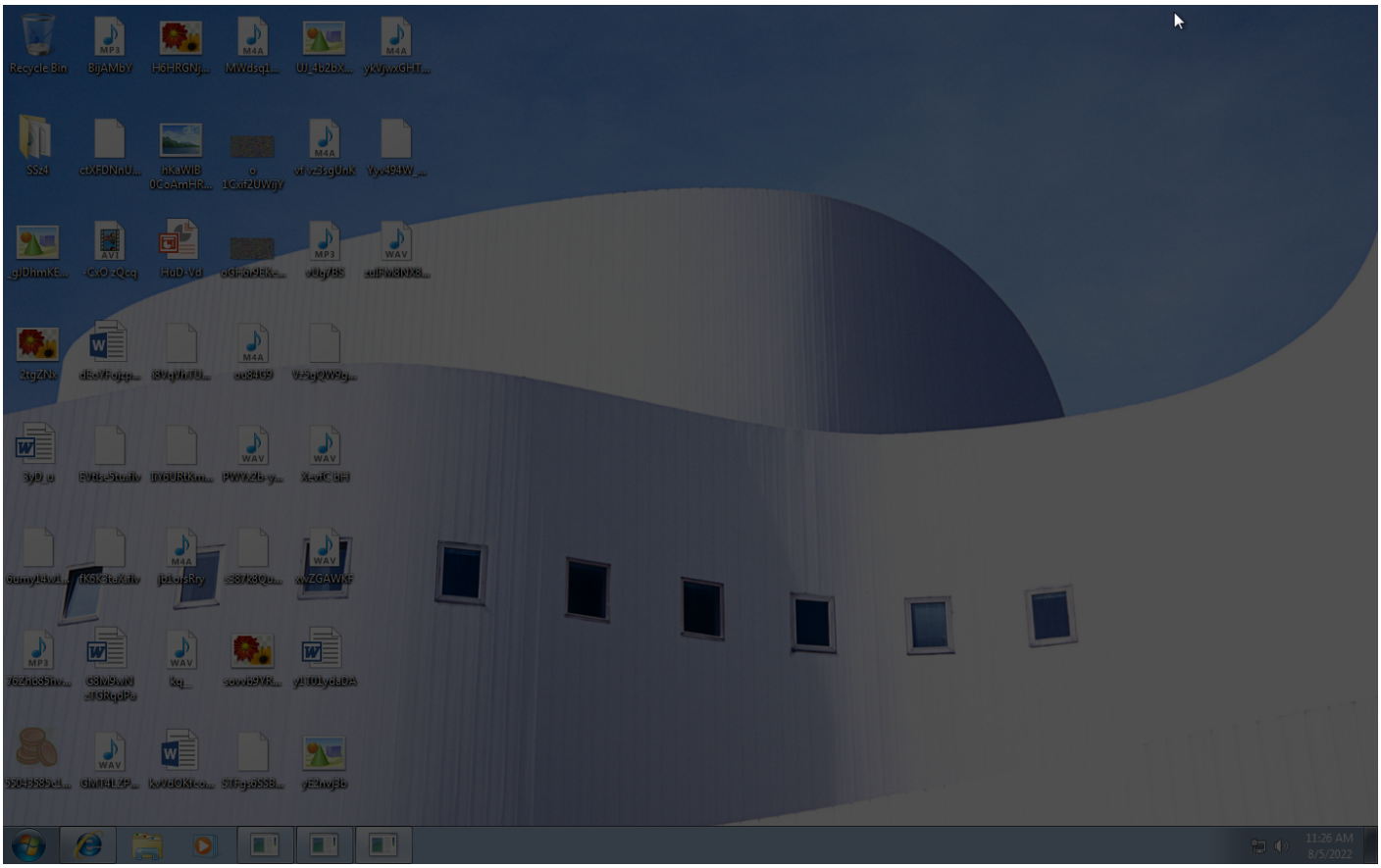
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1060 Registry Run Keys / Startup Folder	#T1053 Scheduled Task	#T1045 Software Packing	#T1081 Credentials in 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		#T1082 System Information Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
				#T1143 Hidden Window		#T1012 Query Registry					
						#T1083 File and Directory Discovery					
						#T1016 System Network Configuration Discovery					
						#T1049 System Network Connections Discovery					

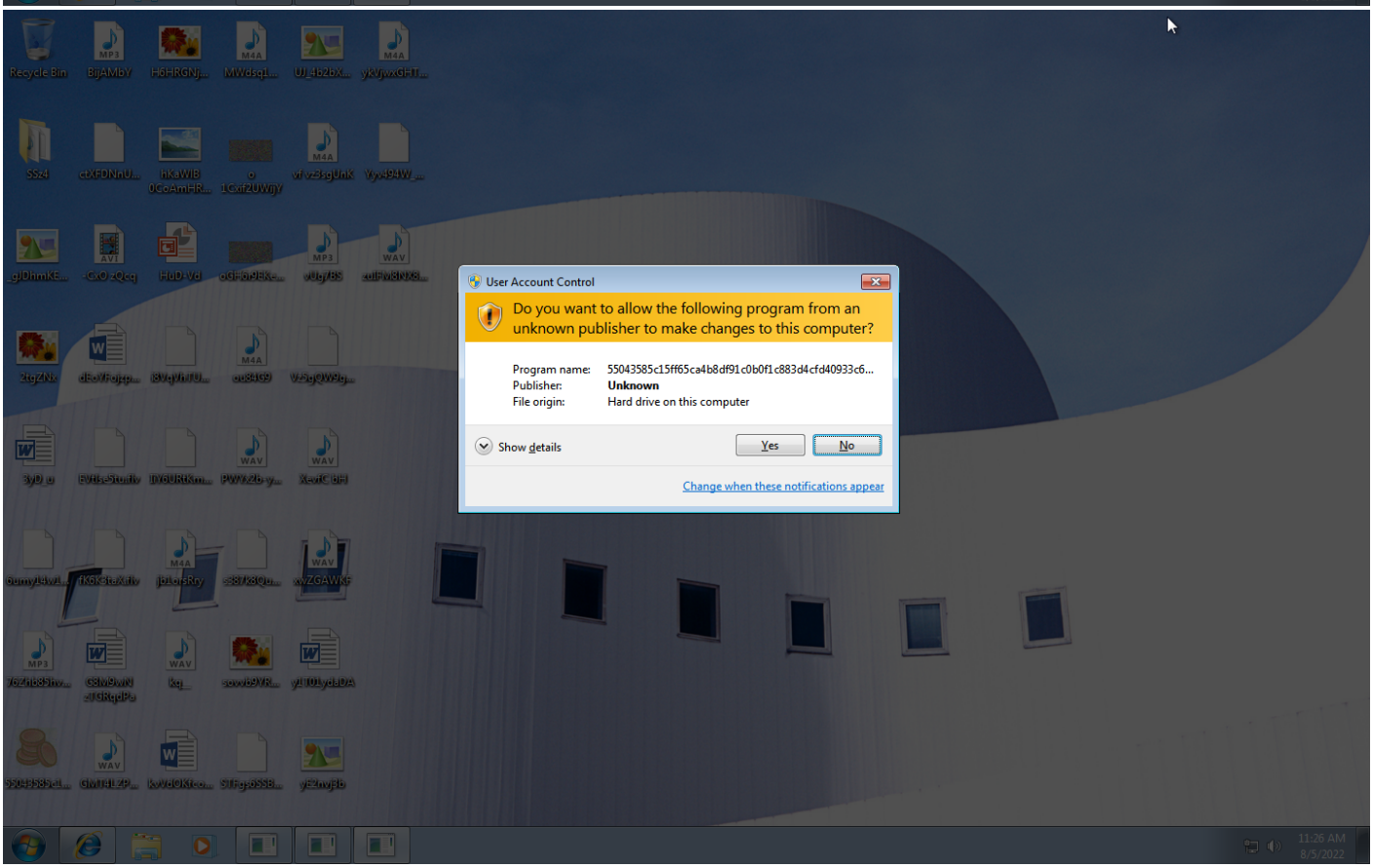
Sample Information

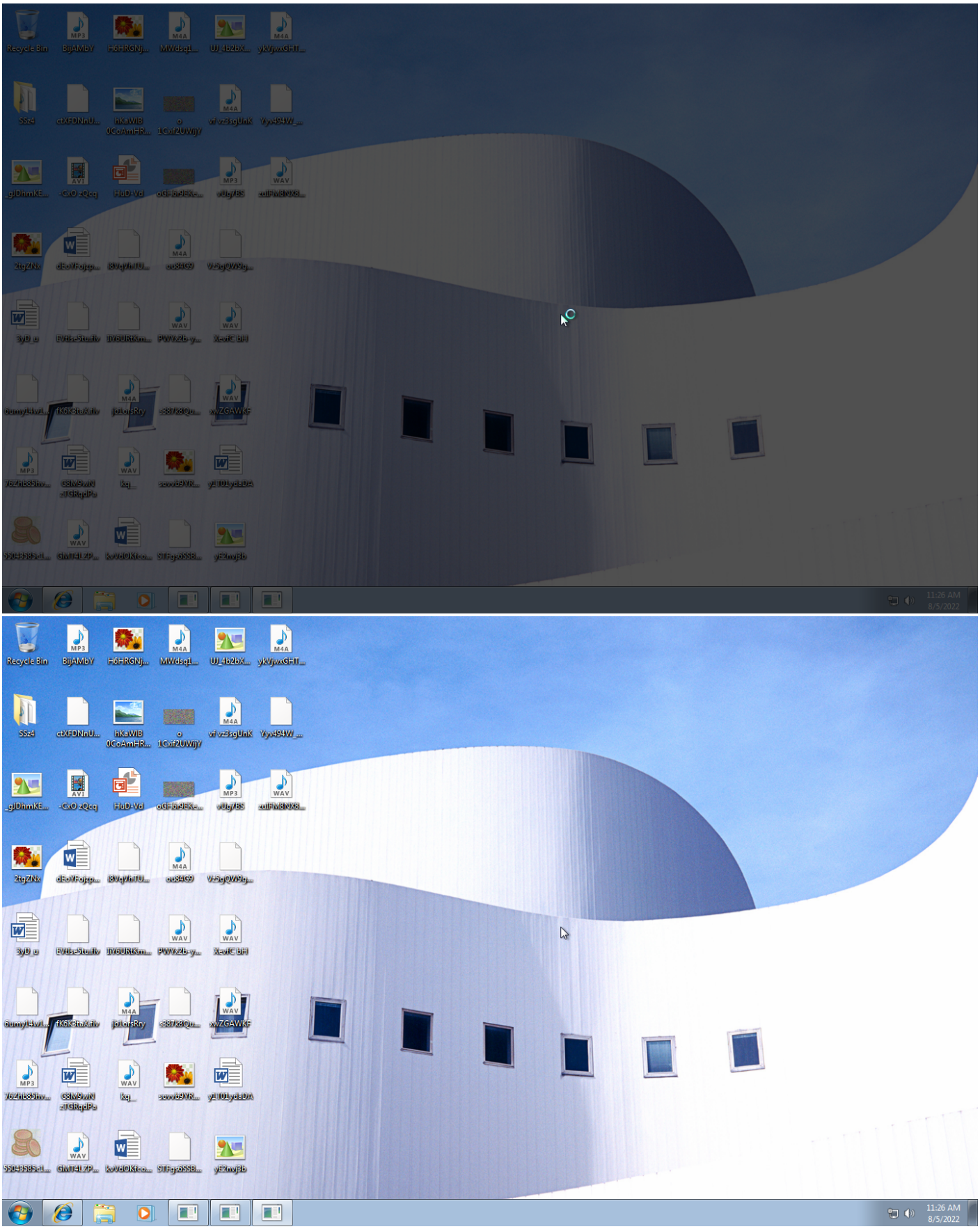
ID	#5067212
MD5	7d3324aba9cb81871405761ea678c751
SHA1	07d238ddaabe2010d5113354b5dac651c1dcf8c0
SHA256	55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c
SSDeep	12288:SfscGOYW1JxHUov45u3pRXPNuNbXZXFBoyU5r29dNBoE15NK:SQBSUp5uHUNbX1NU5Sh915l
ImpHash	52981a63110ae9001dc5c79717e57d47
File Name	55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe
File Size	730.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 13:25 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	9
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: 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

129.20 KB total sent

574.99 KB total received

4 ports 80, 443, 53, 445

6 contacted IP addresses

2 URLs extracted

4 files downloaded

0 malicious hosts detected

DNS

6 DNS requests for 5 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

4 URLs contacted, 3 servers

6 sessions, 6.23 KB sent, 476.65 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=9663E9B9567D9A7DCED1D0F506975904&first=true	-	-		0 bytes	NA
GET	http://acacaca.org/files/1/build3.exe	-	-		0 bytes	NA
GET	https://mas.to/@pavlenko349	-	-		0 bytes	NA
GET	https://t.me/pegasusfly1	-	-		0 bytes	NA
GET	https://api.2ip.ua/geo.json	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	api.2ip.ua	NO_ERROR	162.0.217.254		NA
A	t.me	NO_ERROR	149.154.167.99		NA
A	mas.to	NO_ERROR	88.99.75.82		NA
A	rgyui.top	NO_ERROR	110.14.121.123, 210.182.29.70, 196.200.111.5, 5.163.244.118, 211.119.84.112, 222.236.49.123, 211.53.230.67, 41.41.255.235, 195.158.3.162, 211.119.84.111		NA

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	acacaca.org	NO_ERROR	211.171.233.129, 196.200.111.5, 222.236.49.123, 187.170.251.250, 211.119.84.112, 211.40.39.251, 190.140.99.150, 211.53.230.67, 115.88.24.203, 116.121.62.237		NA

BEHAVIOR

Process Graph

Process #1: 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 47611, Reason: Analysis Target
Unmonitor End Time	End Time: 61835, Reason: Terminated
Monitor duration	14.22s
Return Code	0
PID	3932
Parent PID	1916
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	730.00 KB	55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c	✖

Host Behavior

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

Process #2: 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 59893, Reason: Child Process
Unmonitor End Time	End Time: 86694, Reason: Terminated
Monitor duration	26.80s
Return Code	0
PID	3940
Parent PID	3932
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\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xf60	0x400000(4194304)	0x400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xf60	0x401000(4198400)	0xca600	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xf60	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xf60	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xf60	0x52b000(5419008)	0x200	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xf60	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xf60	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xf60 / 0xf68	0x76f101c4(1995506116)	-	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	730.00 KB	55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c	✖

Host Behavior

Type	Count
System	4
Module	47
File	6
Environment	1
Process	98
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\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b" /deny *S-1-1-0:(OI)(CI)(DE,DC)
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81951, Reason: Child Process
Unmonitor End Time	End Time: 84233, Reason: Terminated
Monitor duration	2.28s
Return Code	0
PID	3980
Parent PID	3940
Bitness	32 Bit

Process #5: 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 84379, Reason: Child Process
Unmonitor End Time	End Time: 88574, Reason: Terminated
Monitor duration	4.20s
Return Code	0
PID	3996
Parent PID	3940
Bitness	32 Bit

Host Behavior

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

Process #6: 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 86748, Reason: Child Process
Unmonitor End Time	End Time: 110967, Reason: Terminated
Monitor duration	24.22s
Return Code	0
PID	4008
Parent PID	3996
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\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xfa0	0x400000(4194304)	0x400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xfa0	0x401000(4198400)	0xca600	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xfa0	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xfa0	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xfa0	0x52b000(5419008)	0x200	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xfa0	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xfa0	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#5: c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0xfa0 / 0xfac	0x76f101c4(1995506116)	-	✔	1

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe	438.00 KB	12a51367c5c85ff3c1dc73743cface2e01accecf2879a36adbddf566d52987b3	✖
C:\SystemID\PersonalID.txt	42 bytes	133276d46de8f4c5849b7ee9536406e0edfc2608134b2b0e4467d9e51c209f03	✖

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\bowsakkdestx.txt	557 bytes	3697f5de19894fd52f417f95a1eadd819359edca9b1cc944b110374bbdc821d6	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	4
Module	47
File	61
Environment	1
Process	97
Registry	7
COM	1
-	2
Mutex	1
User	1
Window	1
-	3

Network Behavior

Type	Count
HTTP	3
HTTPS	1

Process #7: build2.exe

ID	7
File Name	c:\users\keecfmwgj\appdata\local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 98213, Reason: Child Process
Unmonitor End Time	End Time: 102139, Reason: Terminated
Monitor duration	3.93s
Return Code	0
PID	4060
Parent PID	4008
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	76
File	6
Environment	1
Window	1
Process	1
-	3
-	7

Process #8: build2.exe

ID	8
File Name	c:\users\keecfmwgj\appdata\local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 100807, Reason: Child Process
Unmonitor End Time	End Time: 108963, Reason: Terminated
Monitor duration	8.16s
Return Code	1073807364
PID	4068
Parent PID	4060
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#7: c:\users\keecfmwgj\appdata\local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe	0xfe0	0x400000(4194304)	0x400	✔	1
Modify Memory	#7: c:\users\keecfmwgj\appdata\local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe	0xfe0	0x401000(4198400)	0x34000	✔	1
Modify Memory	#7: c:\users\keecfmwgj\appdata\local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe	0xfe0	0x435000(4411392)	0xde00	✔	1
Modify Memory	#7: c:\users\keecfmwgj\appdata\local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe	0xfe0	0x443000(4468736)	0x1c00	✔	1
Modify Memory	#7: c:\users\keecfmwgj\appdata\local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe	0xfe0	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#7: c:\users\keecfmwgj\appdata\local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe	0xfe0 / 0xfe8	0x76f101c4(1995506116)	-	✔	1

Host Behavior

Type	Count
System	8
Module	115
File	3
Environment	1
Registry	2
-	1

Network Behavior

Type	Count
HTTPS	2
TCP	2

Process #12: 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe

ID	12
File Name	c:\users\keecfmwgj\appdata\local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe" --AutoStart
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 160949, Reason: Autostart
Unmonitor End Time	End Time: 165926, Reason: Terminated
Monitor duration	4.98s
Return Code	0
PID	1840
Parent PID	1712
Bitness	32 Bit

Host Behavior

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

Process #13: 55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe

ID	13
File Name	c:\users\keecfmwgj\appdata\local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe" --AutoStart
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 164987, Reason: Child Process
Unmonitor End Time	End Time: 198566, Reason: Terminated
Monitor duration	33.58s
Return Code	0
PID	1928
Parent PID	1840
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0x734	0x400000(4194304)	0x400	✔	1
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0x734	0x401000(4198400)	0xca600	✔	1
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0x734	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0x734	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0x734	0x52b000(5419008)	0x200	✔	1
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0x734	0x52c000(5423104)	0xa400	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0x734	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\appdata\local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	0x734 / 0x78c	0x771601c4(1997930948)	-	✔	1

Dropped Files (222)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Music\zkBFKRCKZ7IX KV Wa4.m4a.vvyu	64.21 KB	4501aa1f9eb1bfc745fb4d49a53b241f0bac5b743929652b07a686e3bd528d3a	✔
c:\users\keecfmwgj\desktop\ou84g9.m4a.vvyu	58.36 KB	bfdf94d896203d19677e2f187d6881cb05896dbb0eb57d9efe4ebfd7cc42c4a0	✔
c:\users\keecfmwgj\desktop\bijamby.mp3.vvyu	35.74 KB	383d9de5fcd918c9b4fc270959eac59f69f1cbb6ef9d9a1e6522469a54e8da74	✔
c:\users\keecfmwgj\videos\zct8oosw8v0sthu.avi.vvyu	83.71 KB	b8f5faa8cfbdee189d99c52c4ad1564e4b3f02eb3e92e35f3bd8eefa7b0c45eb	✔
C:\Users\kEecfMwgj\Desktop\kq__.wav.vvyu	86.93 KB	dcce462c62d403f39d4b58437237be208854fb14ad40d3de6dfa225c9aa6d9ec	✔
C:\Users\kEecfMwgj\Music\VNMhw6NdT0N.m4a.vvyu	13.09 KB	48872a18363b9380f5b201f6c3ac7abde10852b3621186293a8e08a53566627a	✔
c:\users\keecfmwgj\videos\oa7uy-r84 e\v2hz1riby\-tfbdh.mkv.vvyu	63.68 KB	90f1edc42e4f19d19b9e37e6685b218ef9d2e9b125f105bd29949bffee1d545a	✔
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\xd4m_dlxrc.csv.vvyu	41.86 KB	7c7916211ebbcc93df0e07a21596373498fc6c10eb647cac6c5b7a8964da2994	✔
c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu	467 bytes	60e9876094016762501817a31749b04e9b41cea75cfe3f3533e7039078c8dd19	✔
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\yxnorx1icarsuvxvr.xls.vvyu	99.47 KB	2b933fa9ed3c3a1c0ee7e1e1e78e7e00e8bd8a9048165f7680f77b0316a30a07	✔
c:\users\keecfmwgj\pictures\ckh5enz\utklaz\fzsdv9ic_tv.bmp.vvyu	65.31 KB	e9a8206d4dcef12a5c4cfada5b351d2e039ab14d9e4bf9d9790afc31ab518c62	✔
C:\Users\kEecfMwgj\Documents\T4N8wuVG8qRit6NO.odp.vvyu	86.20 KB	3c43a3bab6899a4fa5e3ac0111faeedcd60bd3d0ff19d30cabee1bcc4ed85275	✔
c:\users\keecfmwgj\documents\wxhzvh5geamrbckdv0bk.pptx.vvyu	21.78 KB	5f2bce5a612406ccf5e0316fc1e55cad66df05793e59a9d99e59b5e4c1bf547d	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\ooeO67V 2A6dBdr.pps.vvyu	93.58 KB	f7414f64fc678792156c5ea00e784e003e1f7ddc53cbea752d035d8c319bb526	✔
C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\VNa8b_DcXSUWmzm.wav.vvyu	56.62 KB	2b5ee2904d6c476c40ca79e2ff976c34403c71d93a77ca7ed49299943e152ae9	✔
c:\users\keecfmwgj\desktop\i8vqvhtu5d8vngf1.flv.vvyu	32.43 KB	a251634399aeae24de83925af7dffbec5402a04d7c6a32d876d4293f98f06a50	✔
c:\users\keecfmwgj\documents\56a-hqjck-6jacz_y.docx.vvyu	46.97 KB	d4bdbece2fcda4586ae46d7e0233d0479d5c1bb7323ffda5ea77788290971c04	✔
c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu	467 bytes	149b40902583c08cea851ef887d8eb0cf34cc37bf8e860275f0c156004457279	✔
C:\Users\kEecfMwgj\Desktop\sovvb9YRGyMc-lzi435.png.vvyu	27.04 KB	008e5c903fd171779ab3f1b74b39a86e88daacdc1738a8d1bd91c4b25436940b	✔
c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\4x6n.gif.vvyu	54.15 KB	d71eb9ffcf328879882bbc58b289164ee204e1d5b37c4377183b7e6a467e6d55	✔
c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.vvyu	467 bytes	5faad79e2e4270409af99828a960e55b46a06c0a39210daa277ca68e700e20e3	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\rqq-bsnksl6mhoio1.png.vvyu	14.60 KB	fbaa1b4b4bd4b4b6c2bc3a99fa7233ac5eb15ba08eef33b1aac455e762269e73	✔
C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\v2hZ1rIby\LqnhMFL0C.mkv.vvyu	23.53 KB	063868000370b2298e03f8b70d9db9b1762a41460d784c67a3e1b74f186496e8	✔
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKIAZ\0Djnwc3CmEX6ks4d\rMc5RT6t.bmp.vvyu	74.55 KB	608aff464f808199d7a1f3d582c2003a49a91408c6eca71b2fe904b785030262	✔
c:\users\keecfmwgj\documents\cs0y__wvetbw2qsiy.docx.vvyu	14.40 KB	b2ebdda42062a722b4740796c0132584250d61f0b10f2c7a557285ec02083bfb	✔
C:\Users\kEecfMwgj\Music\s12J.m4a.vvyu	87.40 KB	3e459331f6a9f996471945a4dc294aded444052ee030faced71b42986bceb185	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\Plnb573cskZFLk.ots.vvyu	54.95 KB	4c1c3385cb9727e332b6eda90010971f6e75d2ee2594a65f5ebb042940e83a04	✔
c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\sy7kzm.wav.vvyu	25.63 KB	55cb375291c3109795542cf76e25ba73251df02d5b7595f3909313fddb3ced14	✔
c:\users\keecfmwgj\music\pd9daotni.m4a.vvyu	66.37 KB	eb01b06ec780f6ba037513b42ad5d0568379f5a4ba61e773bec23cc312fbdd4b	✔
C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\3OZhLDJPo6htg3.wav.vvyu	45.17 KB	4488b9389aa8050b61482a93ed3e608078833354c6f783f08ab942bd159ba5bb1	✔
c:\users\keecfmwgj\pictures\ckh5enz\mgf6_dztb1f94j.png.vvyu	50.93 KB	d26b37ec3159d17b4f67ae157a0869d281202c83f44298aee9dd1228d89bbae2	✔
C:\Users\kEecfMwgj\Music\q6aG5\M7TOG0.mp3.vvyu	20.08 KB	153c0d1ce952559684263a47f7a162b317726503b7edeb2e11aa7eb3c7110a31	✔
c:\users\keecfmwgj\desktop\gmt4lzpnvyjn.wav.vvyu	45.65 KB	7e7061e682dca5e16b8e2d25b9793fce2f85c308b1e36fcd383618c8fe497122	✔
c:\users\keecfmwgj\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe.vvyu	730.00 KB	55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c	✖
c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\jyj5.mp3.vvyu	31.87 KB	d90c9c8156ebcb68d2ef575fb0784c9d338f93a029392badbb8e7be9649f1da4	✔
C:\Users\kEecfMwgj\Documents\dHBKKyUiRLEo_ihqOR.xlsx.vvyu	26.50 KB	89e2d36a87aa253caa34164c90c879ff4446497f1eaca6d58889430d39dde5c6	✔
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\nj4aq\rfdw37vjsnr.ods.vvyu	71.39 KB	4ba35d50dbe7073e6662a71a916df5bb2202174c9c0f5494c79410f12f470590	✔
C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\puDbAQqOd3K9PVjvn1u.wav.vvyu	83.55 KB	1853ac4452599a52c695e357e895f29e09e9c943c72286cd1bef09be8923bc54	✔
c:\users\keecfmwgj\desktop\h6hrgnjnvqba.png.vvyu	69.06 KB	38b3be04010e6732c683951abdb9298eac94ed069e7c8cd4e089db1f04d59074	✔
C:\Users\kEecfMwgj\Desktop\-CxO zQcq.avi.vvyu	91.91 KB	abafd2c7ed45cb05134a08da7e202e5ad77caf998bc91758085c356cebf0188a	✔
c:\users\keecfmwgj\videos\jpdadhjnb.mkv.vvyu	6.96 KB	35475d8f7e0fcc2e29492a2ee875f10fb34693b0ee9cee5f0399cb13a04604fa	✔
c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\qexdtyv1z1q_cl0jaadt.m4a.vvyu	72.22 KB	03d2bba0297f716170ff3ce6af386b1b2395c0536adac9ab5af8026dd4eb1e3c	✔
C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\v2hZ1rIby\2u CRZIC7nvdh_M.mkv.vvyu	81.32 KB	907b71b06b08681080f5c28c8023f302c25302a641d8dd1fb4c6b512b559d998	✔
c:\users\keecfmwgj\videos\oa7uy-r84 e\mhdjwhf8pwlbd.flv.vvyu	15.38 KB	1f08ad52b977def28e847cad9bdaf97c576fcc30fd87115493fada9bbda04387	✔
c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\bojvfqm.wav.vvyu	6.86 KB	98552f464597ee19d51f79c21b18fe0d76a7238d3d09c9461628967da4563059	✔
C:\Users\kEecfMwgj\Videos\SFCuO8sWL2Jsj.flv.vvyu	43.83 KB	63f7c09054d84ceb45365eee7716fc3b348441bb3f9d92e192e73f278dda1822	✔
c:\users\keecfmwgj\favorites\links\web slice gallery.url.vvyu	560 bytes	6b15b2f6db55ac6ecc168a70ed8ee50db48233379ceb6ef46fdeeaa352c0189a	✔
c:\users\keecfmwgj\videos\fdd4gb84c4w3sg.mp4.vvyu	89.71 KB	3a7e6e862df82fae548e73a66e2503e51423c41af0271041dba024f506c50f64	✔

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\AKXppD7.m4a.vvyu	20.20 KB	c19b9de4cd2ebc4af7d6e469f5369b2bc733463911dc70390b66d90b66acd31b	✔
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\uomnanj\8ydbvfzvuknzyhmzsw2e.pptx.vvyu	76.45 KB	dc1a040695de8622736f2c61e5d178d1b7d297b2f642397dd3d5af992934944c	✔
c:\users\keecfmwgj\videos\q7szl.swf.vvyu	29.85 KB	887be69e9767a77f9bcf14e4f18d6912c54990095d9234ffbc9db66d27617736	✔
c:\users\keecfmwgj\videos\oa7uy-r84e\v2hz1riby\4zazfhouywh4e77ghf.swf.vvyu	24.81 KB	595559efd041f92bcf188421539c3693c59598c1875aa304c2d7c1ccc08b250c	✔
C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\GcroBq0Ap.flv.vvyu	98.01 KB	f40c3f38b45357570e96d956b12e5358caf3dd7eca29d0cde60a20ec5e7b84bb	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\gnn Elw-bv2A ZdUCx.csv.vvyu	51.06 KB	40268ffc8322fefdb27603a8a9fa041f115f308ca3742ceda2a8fa57ffffd943	✔
c:\users\keecfmwgj\pictures\ckh5enz\g9op7kzr.jpg.vvyu	53.05 KB	1f8175b8526c49072acc7b4ed86ade68a46613aaffe84cec8eb7c9c724d60744	✔
C:\Users\kEecfMwgj\Desktop\ctXFDNnUwfp1foZl.flv.vvyu	3.20 KB	d76d396590a6ec522da72da040e23526cd606acb6530b86a78c256cb01c25eab	✔
C:\Users\kEecfMwgj\Desktop\s387k8QuDVZj.flv.vvyu	32.55 KB	81708239cf69b4eea5a25983c956aac089d26e108d4d223218f9e25a333426ab	✔
c:\users\keecfmwgj\desktop\ssz4\us5ftz3jlmsu.mp4.vvyu	24.63 KB	2fba5a64c12883996ea6dd166dd7f364e10ec94d88b7c1101acda9379ace6f74	✔
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\-kPL6mXQjk.bmp.vvyu	7.54 KB	54b566a64e4e05544fb56b58246cc462fb492093c2093c1a1c1c8d136a7c1e23	✔
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\nj4aq\xq89ysrduds.pdf.vvyu	55.13 KB	90f8b03e08e28b84a9071240046c10a4546eb6d67dc56573dea77df3aa17adaf	✔
C:\Users\kEecfMwgj\Desktop_gJDhmKEYoYDlQq.gif.vvyu	13.04 KB	aed75eebad6b756af07cbddd7601506855d5e1e87a9e9111261bbdde9bb547d7	✔
C:\Users\kEecfMwgj\Desktop\SSz4\HT9Aw JQ.png.vvyu	69.06 KB	8b7464cf92fcf75ba7d6a9fe29e4274bff6f9eb856d551deb20250b59892de94	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\3X s\0R 3sVLz9jj8.rtf.vvyu	48.10 KB	9d70904c814896a852e358754328193d9018c4818d1109fb795d7e41686ccac7	✔
C:\Users\kEecfMwgj\Desktop\oGH6r9EKez2SrD.bmp.vvyu	100.26 KB	d247554d388711df1ce4777081d804741b4500889e5765ad9181e72334890c09	✔
c:\users\keecfmwgj\appdata\locallow\microsoft\internet explorer\services\search_{0633ee93-d776-472f-a0ff-e1416b8b2e3a}.ico.vvyu	4.51 KB	40920dd6a636cc8f69d8dad7cbb80b361a50f7ba9a2d2e3825fc87f00424bd88	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\6e2w9YoR-8.pdf.vvyu	94.46 KB	10d3e26496761e38324c462ec9ef7226fbaf9060581adf4e1997178d6f656152	✔
c:\users\keecfmwgj\music\q6ag5\pjtklq_dt3lt.wav.vvyu	61.53 KB	88da2f03b47dcd914afaec5ccffff4a98c30b9af7f66554b33fbc5b17cc6a181	✔
c:\users\keecfmwgj\pictures\9 qc8otgh1hix w8i.gif.vvyu	6.93 KB	814b60678495c39281479319bca0eb6873d2a8aae625a19d98c9bbe24771f3e5	✔
c:\users\keecfmwgj\desktop\ssz4\ol21.csv.vvyu	19.05 KB	3be6b2eada734b31552bd1389ddcd71b113afed25ad1151e9be13621821b1456	✔
c:\users\keecfmwgj\favorites\windows live\windows live mail.url.vvyu	467 bytes	a1db2318077f5bd0dcfadbf47589935d4a17e898e5e0d5ecbe1d844c1276ef1b	✔
c:\users\keecfmwgj\documents\egcel.ppt.vvyu	61.87 KB	71dd53571da2eb390b81b52076ab1b875f2c05a43b8ddc7af00c3d54121e0ed9	✔
c:\users\keecfmwgj\desktop\ssz4\7qttxszlkjh_fii.pdf.vvyu	71.79 KB	5e820f188ed3c203012c87f6c3387234dd3a2893136db68b6ddbac1663d8dde6	✔
c:\users\keecfmwgj\desktop\ssz4\wmqgvke.flv.vvyu	22.81 KB	e9fc8c229a1a18eaadfa6f9d22d1cecaa812a965d9e32a41fe1c9e24a3d4091e	✔
c:\users\keecfmwgj\desktop\jb1orsrry.m4a.vvyu	33.81 KB	5e3694b6ef8a20b17d447542c3639f35dda37c32a3fb9462984f078b8d2091e6	✔
C:\Users\kEecfMwgj\Pictures\CkH5eNz\UIPaZiiR-oQnLQB3Ey2.png.vvyu	79.66 KB	0beb15bcf563d5f95fe48da30a5bf4a14a4fc66a3ace9340e911d8237fae270c	✔
C:\Users\kEecfMwgj\Pictures\CkH5eNz\up4L8znJo05a3P.jpg.vvyu	31.65 KB	855d5ebe1e10a82bfd72b8bbaea07ae6063ae5c91a9b8e5fc560177c3b862d51	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\j2t8dyq7a9s.m4a.vvyu	27.44 KB	d522bc287c6d938ace7e1e23c70e80e2e42289fd66238df910432a95765d7bc8	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\ZFul69zRrETYF.docx.vvyu	60.06 KB	aabf05c61cb227bda1d5c403974d7c6e759a78c68f11cc8fe973206171b0ad61	✔
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\O2UTInld.gif.vvyu	14.31 KB	fb2e8e3a61edc8536b3a672fc0107d5263a79ff7aaa7bf0254eea3b0e5c5624b	✔
c:\users\keecfmwgj\videos\w9galst 6bnf-yf.mkv.vvyu	94.10 KB	e944bb460dc6647c718ed4b7eb7d4d3e4cb8c86a960baf0f15b9f93b328b252a	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\3QxjAR\T8wvyki0J9mO.ots.vvyu	40.19 KB	4d57a63dd3bbeacc7331ada2a3d51ac2148bc8de90915b969818bc032e7f63f9	✔
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\YNvx X.bmp.vvyu	58.19 KB	017fa3733fa5b759bd1336f0ea699c705ade6e5884684f1a483eee9655ba16f2	✔
c:\users\keecfmwgj\pictures\ckh5enz\0zp is.jpg.vvyu	95.71 KB	4ca9df76edbc2e10be02c481aa958318412af5c2ddc05822acd6e05fe0b770f1	✔
C:\Users\kEecfMwgj\Desktop\MWdsq1QYO68B.m4a.vvyu	45.89 KB	f7340b002ac0f953589ff172085f5024f6e8d8aa0ddb2aa2d951d0ef63ee3d21	✔
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\gx_wgirqaux_.pptx.vvyu	20.47 KB	c3a3ec5f89164367eac694c703f4015ffd823e336621ec64a5ed80f99a07838f	✔
c:\users\keecfmwgj\videos\oa7uy-r84 e\irrx7uvzuzqm6ox.avi.vvyu	38.65 KB	4fc6d20ede54857c1d310071235219fc95730efa229c0fc0b8bb8abe3a7c78f6	✔
c:\users\keecfmwgj\pictures\v-der pgnma_nx.png.vvyu	36.27 KB	ba3d838b6d06a693dd4e0e5177bac48130d80f76ef84dad2a2cea8b7903b5d8b	✔
c:\users\keecfmwgj\documents\5w2kb0xpz679okq9oh.doc.vvyu	24.55 KB	e5717d042b96213e7525d3601f1d6e2f96ebb8e78ff2c7c5e9545c8c11f770d6	✔
C:\Users\kEecfMwgj\Music\q6aG5\w5q7V-5Q7Epp.m4a.vvyu	80.01 KB	0a882c1660ad5f1bc70c5d206d16d435023f4d1e622f7ed901dccfb3613c2962	✔
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\JjOvnSZY.bmp.vvyu	94.32 KB	8e20e1d0e0b386168160bf77183678a3e384ad15a08fc5f0b3604137cf6ce4f1	✔
C:\Users\kEecfMwgj\Documents\Efz8vEEd1pSVsE6 PJdQ.xlsx.vvyu	100.28 KB	e2730913e97e55852274ac59fbedeea5f80606185cafdc83153b5363b9680d5d	✔
c:\users\keecfmwgj\documents\45jcquohqob2hs.xlsx.vvyu	9.42 KB	290c6310abfbae8fa7d98c8899cca8315b943ecfd42b510830bce1480f114a9c	✔
c:\users\keecfmwgj\music\q6ag5\6gb9swuoi.wav.vvyu	96.88 KB	87bbfcfdd1574b55313220affa686725ba9a8aa7433fdd00d677b9735c0b6a10	✔
C:\Users\kEecfMwgj\Videos\h8vWrl4X3qjJx.avi.vvyu	74.65 KB	149ad2cdf101b6f50f12c0c49ac7c442fca7467fdc0ffcd807daf5e300fe0ab1	✔
C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\v2hZ1rIby\6zZsCwOqJQhE.avi.vvyu	75.61 KB	dce6b8a41c2b1bf677b1ff4b8568083e3eb0dda96b2d2cffbf8dc28b4a70b46c	✔
c:\users\keecfmwgj\music\q6ag5\ylvock6jtrl_ur2.m4a.vvyu	3.64 KB	54d2884af398a63c9299290197b73d90dd363fbf9d27c31111adb0728c7069a6	✔
c:\users\keecfmwgj\desktop\6umy14w18jmqx-yvo.swf.vvyu	76.40 KB	85bdf54cf69443615c3c8cc6163ca75df7a1c79d29673608f46386e064f0f1cb	✔
C:\Users\kEecfMwgj\Music\ucR8jv0bs4.wav.vvyu	99.21 KB	632a21e6fc0b8c83fa64ab6b39de32418077112cdd27e4f3bf1a1076a2044992	✔
c:\users\keecfmwgj\desktop\g8m9wn ztgrqdpa.doc.vvyu	49.06 KB	9d9d58a552c25b03b61b27f83d0e642f90d6a75feaf89de2a5268a5d9c751334	✔
C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url.vvyu	467 bytes	65ce021b0b11d5490f43b0b0d39558a4129e114346d8964cb92b8ca83922f45d	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\NJ4Aq\JRCSXUX.rtf.vvyu	68.86 KB	f6814d7f1e64fc4f4e721cedf6d3552d9c57f33226893f739f4eb21234b1c8ef	✔
c:\users\keecfmwgj\pictures\0md97n-k.bmp.vvyu	2.97 KB	9ac425b276fcece7fff6236ec3b532432db7fcc227fa75c6f537c61a43d9afe0	✔
c:\users\keecfmwgj\documents_-fr_fxi6 yovrtv.pptx.vvyu	42.22 KB	72cf0e2d7e50e585963e2a4873e4724697ab6f1eb715829089f8379d9bdd2ae2	✔
c:\users\keecfmwgj\favorites\windows live\get windows live.url.vvyu	467 bytes	e4a2fa73a8f3554a9282a38ba85717c53b520275dfc7ff88b4ac3d8ce89d61eb	✔

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\HuD-Vd.ppt.vvyu	39.87 KB	a4b9e0ae5661623d933891127510a0e09f5f2b95ea07503f31edf2b62d1c4d3a	✔
c:\users\keecfmwgj\favorites\msn websites\msn.url.vvyu	467 bytes	b6a33245545d6d8d813981c99b398da3111d73cf923c18056dff7029997cb169	✔
c:\users\keecfmwgj\music\bqn7jsn2k_hp.wav.vvyu	48.49 KB	a5cb50ea5d800c8c7bffadd13737ec136db6d94b790172e4dc3f8ded12ebf993	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\3QxjAR\0nTeT5RDjQL6aro.csv.vvyu	63.67 KB	6b1dd5e6161dbb38c7e512c2d6c44b95d957b5e117f9cfc574343a8035ac725e	✔
c:\users\keecfmwgj\pictures\scabdm3i.bmp.vvyu	57.28 KB	b50d3160ff818c4f7f9be06fe6abdd8de1032055f403f739ffcc038bf0794065	✔
C:\Users\kEecfMwgj\Pictures\fjFyJ2LwCFuD.bmp.vvyu	25.04 KB	1a5c4dd3e6543038afed4e34a5313f9a31272c9e177266d7213767ca7ab46a0f	✔
c:\users\keecfmwgj\music\7rucdwyus.wav.vvyu	46.07 KB	079c11c7d28221f3c8d2c50fb7809e90ce423543f1f59db6f59cc053de83c091	✔
c:\users\keecfmwgj\desktop\yyv494w_m8z.mkv.vvyu	60.80 KB	19064aeda4c5dedfb2a6c6cc95770b4a6749f44f7b7d8921d944dc0b06cb4918	✔
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dejp0tkawtpu.xlsx.vvyu	54.03 KB	3071ee0aabd425d53fd8e4dcd1eb246d091f8ecd747c9850ea71f07fb3a79c94	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\hWL0ZU2H-.doc.vvyu	17.63 KB	c3211fd3c9b5474da3cb165ffe9a5d4e55ee6c0193866e92b95a6d1cfb265094	✔
C:\Users\kEecfMwgj\Videos\oa7UY-r84e_9xS8m5SRrPmY7bhauad.flv.vvyu	36.72 KB	9f2a8510a52dc176e8deec99aca0f9a440b4f32c6c74310b8639e46113399df5	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMDg2s\Uomn Anj\3X s\E6LAV7pmdeNqQC2aZ.rtf.vvyu	12.80 KB	f505038305a66d16f5795f870fdf3835913d5a7c095c2b6c453eef34839f25a5	✔
C:\Users\kEecfMwgj\Desktop\vf vz3sgUnK.m4a.vvyu	81.91 KB	edac848d0b66b3053ba752e0825b69226656c0ea3864a17dea68c9b04b990e99	✔
c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\oyuf.gif.vvyu	9.47 KB	bc9bd8f6883f3fe970e58438847ce5fa738bfa89930f5ec9a141fed549a3c08f	✔
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\4mQ2gMUrsax_RZzVhH.png.vvyu	75.78 KB	73ee17295d98f7cd8a800481c0109fb2645cf71d12aa05e843f62a106da48934	✔
c:\users\keecfmwgj\desktop\pwyx2b-yoplcn5mp.wav.vvyu	7.19 KB	8eadd74f33fe06dadc443508dde51b7ba0cef05a4c02b974633a103bd9dc1b07	✔
c:\users\keecfmwgj\documents\wr0kwgonpwoxie1pnc.pptx.vvyu	44.91 KB	7c935110b9074fc8f2cd14c657f061c072ca49954dabc9505f68463c4c582976	✔
c:\users\keecfmwgj\desktop\vz5gqw9gjyrik.swf.vvyu	21.06 KB	341bf813f7cab1709b641d5b6a37836b0a6e63050f03c344e424dd4500c496ed	✔
C:\Users\kEecfMwgj\Desktop\SSz4\9yAZzTXyNBlNhh5kD.mp3.vvyu	40.69 KB	40139799669a1a752a7b5e0109007c463b06bc77b064b5ae1036524c62228e7e	✔
C:\Users\kEecfMwgj\Contacts\Administrator.contact.vvyu	67.11 KB	1f76f0af856367c1932faa8d151822d5c2f96d304951b8a37a4ef15c14015333	✔
C:\Users\kEecfMwgj\Desktop\kvVdOKfcoMs.docx.vvyu	74.95 KB	0cb62dba7b0c20949d92e2a0382fb9af6e48771e7f75114bdaa3cda2da8ff98f	✔
c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\vnnb6-.png.vvyu	65.98 KB	4952e06f4fb9c1b2fb917f3a003c2dbbc200d851a1604279436da48cb10c4277	✔
C:\Users\kEecfMwgj\Music\Pk0h2Rnp8cQPR.wav.vvyu	51.83 KB	2441fe55ef73a6723c7687531f2d0cf8db0b9bbb0387ec7ba4c20bffb6fd20f1	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15lr8w0sJrhR-b\8OhTRGE.ods.vvyu	60.69 KB	a709fdd42a3f15aa945116121480eec5569a7a0a1a2c4444b8920dfb96405494	✔
C:\Users\kEecfMwgj\Music\nA1Vyxh1cNbdS.mp3.vvyu	18.29 KB	25135b6a5cee92d2d7423daf80b89533b611bd03271d0af2a079cb6b8359fa7e	✔
C:\Users\kEecfMwgj\Music\q6aG5\7URv2AmQZDAOxub1g.mp3.vvyu	39.63 KB	a961ab4c96e8c785877067639b1c7b0ae695b6b38072d6363308b373dc5472ff	✔
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\lviuhooev0pnicn.docx.vvyu	80.87 KB	0a5fb393094de01c32a15cb7de9e1fc183e6d401dfbacebf25132af9810dcf1e	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\videos\oa7uy-r84 e\v2hz1riby\d4q2ikayi.swf.vvyu	17.99 KB	c527d45374e7a7e54b9ef909e15b5961c80e76c267b06b4cabff80ccba522494	✔
c:\users\keecfmwgj\pictures\ckh5enz\utklaz\jnrbiji7doab7.bmp.vvyu	94.59 KB	01092879025f551f3bffea116916637c9235c85ae55513efc3c3abd887f2be6b	✔
c:\users\keecfmwgj\videos\0kzy5iydb0_9j1mvgm.avi.vvyu	95.62 KB	1b8f7dbce30a828e26285ebd310cd987c4674e92dd53ee50c86c418793f73d23	✔
c:\users\keecfmwgj\desktop\ye2nvj3b.gif.vvyu	65.37 KB	6949f9851893f1ac27d2421545a34778b15a34eee7c6e2ad4a7b9af687b1d4fa	✔
C:\Users\kEecfMwgj\Desktop\o 1Cxif2UWijY.bmp.vvyu	94.16 KB	f1d379a1039155237c540cbfc9395529a8aa00526d05e28336a0d93e9f6c2ecc	✔
c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\xwnlbab.m4a.vvyu	89.89 KB	a35444c1b3f981ebd6488a7573417259ef14574686ad53aef244ecf9fa519b7e	✔
C:\Users\kEecfMwgj\Music\XP3a5K43wYYvtQY.wav.vvyu	28.62 KB	a516db7de0e90c6910ed9bb105bd3c7e4981fead9837607879a323380f7b44d8	✔
c:\users\keecfmwgj\desktop\3yd_u.doc.vvyu	4.00 KB	a96da9526b076218ae3858547669eecfa8d96a6571922bd32b1532fb88dcd2a1	✔
C:\Users\kEecfMwgj\Music\x5xovotqfAL_W9MsP.wav.vvyu	23.63 KB	2a402bed573d72e41d37984fdec37ff3ae8c9057f7d285783d7919b4bfd95b58	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\f1rc6EXPyfw.pdf.vvyu	53.16 KB	6ca3d3c832a3dbca50a6f35129b47ed4b77099a7a50b595b3be55447516ed6d6	✔
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\gwmlsc2zpd0nk-c.ods.vvyu	48.08 KB	c1afbc02698d2bfcbcc95fd488b38047f550413db767db1564809099780be100	✔
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\5GbLDOSSAl.ppt.vvyu	82.15 KB	68a0d29d2c1eb738d8ad6517317fe9bc538b996a2d9bb80cf6f9dfd2e2a925a3	✔
c:\users\keecfmwgj\music\j6ymsltmtmc.wav.vvyu	18.25 KB	b057604aa6f896e7973d21b44b05afea42296aad07c52cea4b6afe39f5a9595e	✔
c:\users\keecfmwgj\favorites\microsoft websites\microsoft at home.url.vvyu	467 bytes	5da37bc27d99eee516497214e93e7735831a5d7f53d2021c80e21f6069fcf5d8	✔
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\m6h6LTvd.bmp.vvyu	20.08 KB	547eeaf9b5df0d8dad4bd3ed5cd9444c781c3697b11b4ef475550891b794cc3b	✔
C:\Users\kEecfMwgj\Videos\EOKz9As_PQ-0e NIZu2.swf.vvyu	32.74 KB	ac75a48ec327870417a93a42b34f6499c9a070f1aa1f0327d8b10808da9086fd	✔
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\uomnanj\tpc-xlgkaoki.ots.vvyu	57.78 KB	497d2e459c547793023e18fba6f0ae836c68d0b0840a52c5cc4b9278e734c1bd	✔
c:\users\keecfmwgj\desktop\iiy6urtkmkg.swf.vvyu	24.88 KB	9e1414393acf4cdf4f69ca3603849839276bcbb4373c70710faff4682ad5fc4c	✔
C:\Users\kEecfMwgj\Documents\mQVKO4ih33AabgIOBNO.xlsx.vvyu	50.43 KB	fc28a66433a632f835e1037d1215ca5634c6bf8cbc77eea370fb1eedfa071e95	✔

Reduced dataset

Host Behavior

Type	Count
System	282
Module	185
File	2631
Environment	1
Process	55
Registry	4
Mutex	1
User	1
Window	1
-	4

Network Behavior

Type	Count
HTTPS	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4501aa1f9eb1bfc745fb4d49a53b241f0bac5b743929652b07a686e3bd528d3a	C:\Users\kEecfMwgj\Music\zkBFKRCKZ7IX KV Wa4.m4a.vvyu, c:\users\keecfmwgj\music\zkbfkrckz7ixkv wa4.m4a.vvyu	Dropped File	64.21 KB	application/octet-stream	Access, Create, Write	MALICIOUS
bfdf94d896203d19677e2f187d6881cb05896dbb0eb57d9efe4ebfd7cc42c4a0	c:\users\keecfmwgj\desktop\ou84g9.m4a.vvyu, C:\Users\kEecfMwgj\Desktop\ou84G9.m4a.vvyu	Dropped File	58.36 KB	application/octet-stream	Access, Create, Write	MALICIOUS
383d9de5fcd918c9b4fc270959eac59f69f1cbb6ef9d9a1e6522469a54e8da74	c:\users\keecfmwgj\desktop\bijamby.mp3.vvyu, C:\Users\kEecfMwgj\Desktop\BijAMbY.mp3.vvyu	Dropped File	35.74 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b8f5faa8cfbdee189d99c52c4ad1564e4b3f02eb3e92e35f3bd8eefa7b0c45eb	c:\users\keecfmwgj\videos\zct8oosw8v0sthu.avi.vvyu, C:\Users\kEecfMwgj\Videos\zCT8OOsW8v0StHU.avi.vvyu	Dropped File	83.71 KB	application/octet-stream	Access, Create, Write	MALICIOUS
dcce462c62d403f39d4b58437237be208854fb14ad40d3de6dfa225c9aa6d9ec	C:\Users\kEecfMwgj\Desktop\kq__.wav.vvyu, c:\users\keecfmwgj\desktop\kq__.wav.vvyu	Dropped File	86.93 KB	application/octet-stream	Access, Create, Write	MALICIOUS
48872a18363b9380f5b201f6c3ac7abde10852b3621186293a8e08a53566627a	C:\Users\kEecfMwgj\Music\VNMhw6NdT0N.m4a.vvyu, c:\users\keecfmwgj\music\vnmhw6ndt0n.m4a.vvyu	Dropped File	13.09 KB	application/octet-stream	Access, Create, Write	MALICIOUS
90f1edc42e4f19d19b9e37e6685b218ef9d2e9b125f105bd29949bffee1d545a	c:\users\keecfmwgj\videos\oa7uy-r84e\v2hz1riby\-tfbdh.mkv.vvyu, C:\Users\kEecfMwgj\Videos\oa7UY-r84e\v2hZ1rIby\-TFbDH.mkv.vvyu	Dropped File	63.68 KB	application/octet-stream	Access, Create, Write	MALICIOUS
7c7916211ebbcc93df0e07a21596373498fc6c10eb647cac6c5b7a8964da2994	c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\xd4m_dlxrc.csv.vvyu, C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\xd4m_DLxrC.csv.vvyu	Dropped File	41.86 KB	application/octet-stream	Access, Create, Write	MALICIOUS
60e98760940167625018 17a31749b04e9b41cea75cfe3f3533e7039078c8dd19	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	MALICIOUS
2b933fa9ed3c3a1c0ee7e1e1e78e7e00e8bd8a9048165f7680f77b0316a30a07	c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\yxnorx1icarsuvxvr.xls.vvyu, C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\yxNORX1ICaRSUVxVR.xls.vvyu	Dropped File	99.47 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e9a8206d4dcef12a5c4cfada5b351d2e039ab14d9e4bf9d9790afc31ab518c62	c:\users\keecfmwgj\pictures\ckh5enz\utklaz\fzsdv9ic_tv.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\FZSdv9Ic_tv.bmp.vvyu	Dropped File	65.31 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3c43a3bab6899a4fa5e3ac0111faeedcd60bd3d0ff19d30cabee1bcc4ed85275	C:\Users\kEecfMwgj\Documents\T4N8wuVG8qRit6NO.odp.vvyu, c:\users\keecfmwgj\documents\t4n8wuvg8qrit6no.odp.vvyu	Dropped File	86.20 KB	application/zip	Access, Create, Write	MALICIOUS
5f2bce5a612406ccf5e0316fc1e55cad66df05793e59a9d99e59b5e4c1bf547d	c:\users\keecfmwgj\documents\wxhzvh5geamrbckdv0bk.pptx.vvyu, C:\Users\kEecfMwgj\Documents\wXHzVH5GEAmrbCkDV0bK.pptx.vvyu	Dropped File	21.78 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f7414f64fc678792156c5ea00e784e003e1f7ddc53cbea752d035d8c319bb526	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\ooeO67V 2A6dBdr.pps.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\ooeo67v 2a6dbdr.pps.vvyu	Dropped File	93.58 KB	application/octet-stream	Access, Create, Write	MALICIOUS
2b5ee2904d6c476c40ca79e2ff976c34403c71d93a77ca7ed49299943e152ae9	C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\VNa8b_DcXSUW mzm.wav.vvyu, c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\vna8b_dcxsuw mzm.wav.vvyu	Dropped File	56.62 KB	application/octet-stream	Access, Create, Write	MALICIOUS
a251634399aeae24de83925af7dffbec5402a04d7c6a32d876d4293f98f06a50	c:\users\keecfmwgj\desktop\i8vqvhtu5d8vngf1.flv.vvyu, C:\Users\kEecfMwgj\Desktop\i8VqVhTU5D8vngF1.flv.vvyu	Dropped File	32.43 KB	video/x-flv	Access, Create, Write	MALICIOUS
d4bdbece2fcda4586ae46d7e0233d0479d5c1bb7323ffda5ea7788290971c04	c:\users\keecfmwgj\documents\56a-hqjck-6jacz_y.docx.vvyu, C:\Users\kEecfMwgj\Documents\56A-hqjCk-6JaCz_Y.docx.vvyu	Dropped File	46.97 KB	application/zip	Access, Create, Write	MALICIOUS
149b40902583c08cea851ef887d8eb0cf34cc37bf8e860275f0c156004457279	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	MALICIOUS
008e5c903fd171779ab3f1b74b39a86e88daacdc1738a8d1bd91c4b25436940b	C:\Users\kEecfMwgj\Desktop\sovvb9YRGyMc-lzi435.png.vvyu, c:\users\keecfmwgj\desktop\sovvb9yrgymc-lzi435.png.vvyu	Dropped File	27.04 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d71eb9ffcf328879882bbc58b289164ee204e1d5b37c4377183b7e6a467e6d55	c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\4x6n.gif.vvyu, C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\4X6N.gif.vvyu	Dropped File	54.15 KB	image/gif	Access, Create, Write	MALICIOUS
5faad79e2e4270409af99828a960e55b46a06c0a39210daa277ca68e700e20e3	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	MALICIOUS
fbaa1b4b4bd4b4b6c2bc3a99fa7233ac5eb15ba08eef33b1aac455e762269e73	c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\rqq-bsnksl6mhoio1.png.vvyu, C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\RQQ-BsNkSL6MhOio1.png.vvyu	Dropped File	14.60 KB	application/octet-stream	Access, Create, Write	MALICIOUS
063868000370b2298e03f8b70d9db9b1762a41460d784c67a3e1b74f186496e8	C:\Users\kEecfMwgj\Videos\oa7UY-r84e\v2hZ1rIby\LqnhMFL0C.mkv.vvyu, c:\users\keecfmwgj\videos\oa7uy-r84e\v2hz1riby\lqnhmfl0c.mkv.vvyu	Dropped File	23.53 KB	application/octet-stream	Access, Create, Write	MALICIOUS
608aff464f808199d7a1f3d582c2003a49a91408c6eca71b2fe904b785030262	C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\rMc5RT6t.bmp.vvyu, c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\rmc5rt6t.bmp.vvyu	Dropped File	74.55 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b2ebdda42062a722b4740796c0132584250d61f0b10f2c7a557285ec02083bfb	c:\users\keecfmwgj\documents\cs0y__wvetbw2qsiy.docx.vvyu, C:\Users\kEecfMwgj\Documents\CS0y__wVETbw2QSiY.docx.vvyu	Dropped File	14.40 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3e459331f6a9f996471945a4dc294aded444052ee030faced71b42986bceb185	C:\Users\kEecfMwgj\Music\s12J.m4a.vvyu, c:\users\keecfmwgj\music\s12j.m4a.vvyu	Dropped File	87.40 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4c1c3385cb9727e332b6eda90010971f6e75d2ee2594a65f5ebb042940e83a04	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\PInb573cskZFLk.ots.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\pInb573cskzflk.ots.vvyu	Dropped File	54.95 KB	application/zip	Access, Create, Write	MALICIOUS
55cb375291c3109795542cf76e25ba73251df02d5b7595f3909313fddb3ced14	c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\sy7kzm.wav.vvyu, C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\sy7KZM.wav.vvyu	Dropped File	25.63 KB	application/octet-stream	Access, Create, Write	MALICIOUS
eb01b06ec780f6ba037513b42ad5d0568379f5a4ba61e773bec23cc312fbdd4b	c:\users\keecfmwgj\music\pd9daotni.m4a.vvyu, C:\Users\kEecfMwgj\Music\pD9DaOTNi.m4a.vvyu	Dropped File	66.37 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4488b9389aa8050b61482a93ed3e60807883354c6f783f08ab942bd159ba5bb1	C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\3OZhLDJPo6htg3.wav.vvyu, c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\3ozhldjpo6htg3.wav.vvyu	Dropped File	45.17 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d26b37ec3159d17b4f67ae157a0869d281202c83f44298aee9dd1228d89bbae2	c:\users\keecfmwgj\pictures\ckh5enz\mgf6_dztb1f94j.png.vvyu, C:\Users\kEecfMwgj\Pictures\CkH5eNz\MGf6_DZTb1f94j.png.vvyu	Dropped File	50.93 KB	application/octet-stream	Access, Create, Write	MALICIOUS
153c0d1ce952559684263a47f7a162b317726503b7edeb2e11aa7eb3c7110a31	C:\Users\kEecfMwgj\Music\q6aG5\M7TOG0.mp3.vvyu, c:\users\keecfmwgj\music\q6ag5\m7tog0.mp3.vvyu	Dropped File	20.08 KB	application/octet-stream	Access, Create, Write	MALICIOUS
7e7061e682dca5e16b8e2d25b9793fce2f85c308b1e36fcd383618c8fe497122	c:\users\keecfmwgj\desktop\gmt4lzpnvyjn.wav.vvyu, C:\Users\kEecfMwgj\Desktop\GMT4LZPnVYjN.wav.vvyu	Dropped File	45.65 KB	application/octet-stream	Access, Create, Write	MALICIOUS
55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c	C:\Users\kEecfMwgj\Desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe, c:\users\keecfmwgj\desktop\550435... ...\kEecfMwgj\AppData\Local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	Sample File	730.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Read, Write	MALICIOUS
d90c9c8156ebcb68d2ef575fb0784c9d338f93a029392badbb8e7be9649f1da4	c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\jyj5.mp3.vvyu, C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\JYJ5.mp3.vvyu	Dropped File	31.87 KB	application/octet-stream	Access, Create, Write	MALICIOUS
89e2d36a87aa253caa34164c90c879ff4446497f1eaca6d58889430d39dde5c6	C:\Users\kEecfMwgj\Documents\dHBKKyUiRLEo_ihqOR.xlsx.vvyu, c:\users\keecfmwgj\documents\dhbkkyuirleo_ihqor.xlsx.vvyu	Dropped File	26.50 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4ba35d50dbe7073e6662a71a916df5bb2202174c9c0f5494c79410f12f470590	c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\nj4aq\rfdw37vjsnr.ods.vvyu, C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\NJ4Aq\RfDW37vJSNr.ods.vvyu	Dropped File	71.39 KB	application/zip	Access, Create, Write	MALICIOUS
1853ac4452599a52c695e357e895f29e09e9c943c72286cd1bef09be8923bc54	C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\puDbAQqOd3K9PVjvn1u.wav.vvyu, c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\pudbaqqod3k9pvjvn1u.wav.vvyu	Dropped File	83.55 KB	application/octet-stream	Access, Create, Write	MALICIOUS
38b3be04010e6732c683951abdb9298eac94ed069e7c8cd4e089db1f04d59074	c:\users\keecfmwgj\desktop\h6hrgnjnvqba.png.vvyu, C:\Users\kEecfMwgj\Desktop\H6HRGNjnVqBA.png.vvyu	Dropped File	69.06 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
abafd2c7ed45cb05134a08da7e202e5ad77caf998bc91758085c356cebf0188a	C:\Users\kEecfMwgj\Desktop\-CxOzQcq.avi.vvyu, c:\users\keecfmwgj\desktop\-cxozqcq.avi.vvyu	Dropped File	91.91 KB	application/octet-stream	Access, Create, Write	MALICIOUS
35475d8f7e0fcc2e29492a2ee875f10fb34693b0ee9cee5f0399cb13a04604fa	c:\users\keecfmwgj\videos\jpdadhjnb.mkv.vvyu, C:\Users\kEecfMwgj\Videos\JPDadhjNB.mkv.vvyu	Dropped File	6.96 KB	application/octet-stream	Access, Create, Write	MALICIOUS
03d2bba0297f716170ff3ce6af386b1b2395c0536adac9ab5af8026dd4eb1e3c	c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\qexdtyv1z1q_cl0jaadt.m4a.vvyu, C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\QEXDTyV1z1Q_CL0Jaadt.m4a.vvyu	Dropped File	72.22 KB	application/octet-stream	Access, Create, Write	MALICIOUS
907b71b06b08681080f5c28c8023f302c25302a641d8dd1fb4c6b512b559d998	C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\v2hZ1rIby\2uCRZlC7nvdh_M.mkv.vvyu, c:\users\keecfmwgj\videos\oa7uy-r84e\v2hz1riby\2ucrzlc7nvdh_m.mkv.vvyu	Dropped File	81.32 KB	application/octet-stream	Access, Create, Write	MALICIOUS
1f08ad52b977def28e847cad9bdaf97c576fcc30fd87115493fada9bbda04387	c:\users\keecfmwgj\videos\oa7uy-r84e\mhdjwhf8pwlbd.flv.vvyu, C:\Users\kEecfMwgj\Videos\oa7UY-r84e\mhDJwHf8pwlbd.flv.vvyu	Dropped File	15.38 KB	video/x-flv	Access, Create, Write	MALICIOUS
98552f464597ee19d51f79c21b18fe0d76a7238d3d09c9461628967da4563059	c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\bojvfqm.wav.vvyu, C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\BoJvFqM.wav.vvyu	Dropped File	6.86 KB	application/octet-stream	Access, Create, Write	MALICIOUS
63f7c09054d84ceb45365eee7716fc3b348441bb3f9d92e192e73f278dda1822	C:\Users\kEecfMwgj\Videos\SFCuO8sWL2Jsj.flv.vvyu, c:\users\keecfmwgj\videos\sfcuo8swl2jsj.flv.vvyu	Dropped File	43.83 KB	video/x-flv	Access, Create, Write	MALICIOUS
6b15b2f6db55ac6ecc168a70ed8ee50db48233379ceb6ef46fdeeaa352c0189a	c:\users\keecfmwgj\favorites\links\web slice gallery.url.vvyu, C:\Users\kEecfMwgj\Favorites\Links\Web Slice Gallery.url.vvyu	Dropped File	560 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
3a7e6e862df82fae548e73a66e2503e51423c41af0271041dba024f506c50f64	c:\users\keecfmwgj\videos\fdd4gb84c4w3sg.mp4.vvyu, C:\Users\kEecfMwgj\Videos\fdD4Gb84c4w3sG.mp4.vvyu	Dropped File	89.71 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c19b9de4cd2ebc4af7d6e469f5369b2bc733463911dc70390b66d90b66acd31b	C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\AKXppD7.m4a.vvyu, c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\akxppd7.m4a.vvyu	Dropped File	20.20 KB	application/octet-stream	Access, Create, Write	MALICIOUS
dc1a040695de8622736f2c61e5d178d1b7d297b2f642397dd3d5af992934944c	c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\uomnanj\8ydbvfzvuknzyhmzsw2e.pptx.vvyu, C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\UomnAnj\8YDbvFZVuKnZyHMZsW2e.pptx.vvyu	Dropped File	76.45 KB	application/zip	Access, Create, Write	MALICIOUS
887be69e9767a77f9bcf14e4f18d6912c54990095d9234ffbc9db66d27617736	c:\users\keecfmwgj\videos\q7szl.swf.vvyu, C:\Users\kEecfMwgj\Videos\Q7szL.swf.vvyu	Dropped File	29.85 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
595559efd041f92bcf188421539c3693c59598c1875aa304c2d7c1ccc08b250c	c:\users\keecfmwgj\videos\oa7uy-r84e\v2hz1riby\4zazfhouywh4e77ghf.swf.vvyu, C:\Users\kEecfMwgj\Videos\oa7UY-r84e\v2hZ1rIby\4ZaZfHOuywH4E77ghf.swf.vvyu	Dropped File	24.81 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
12a51367c5c85ff3c1dc73743cface2e01accecf2879a36adbddf566d52987b3	C:\Users\kEecfMwgj\AppData\Local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe	Downloaded File	438.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
f40c3f38b45357570e96d956b12e5358caf3dd7eca29d0cde60a20ec5e7b84bb	C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\GcroBq0Ap.flv.vvyu, c:\users\keecfmwgj\videos\oa7uy-r84e\gcrobq0ap.flv.vvyu	Dropped File	98.01 KB	video/x-flv	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
40268ffc8322fefdb27603a8a9fa041f115f308ca3742ceda2a8fa57ffffd943	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\gnn Elw-bv2A ZdUCx.csv.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\gnn eiw-bv2a zducx.csv.vvyu	Dropped File	51.06 KB	application/octet-stream	Access, Create, Write	MALICIOUS
1f8175b8526c49072acc7b4ed86ade68a46613aaffe84cec8eb7c9c724d60744	c:\users\keecfmwgj\pictures\ckh5enz\g9op7kzr.jpg.vvyu, C:\Users\kEecfMwgj\Pictures\CkH5eNz\g9Op7Kzr.jpg.vvyu	Dropped File	53.05 KB	image/jpeg	Access, Create, Write	MALICIOUS
d76d396590a6ec522da72da040e23526cd606acb6530b86a78c256cb01c25eab	C:\Users\kEecfMwgj\Desktop\ctXFDNnUwfp1foZl.flv.vvyu, c:\users\keecfmwgj\desktop\ctxfdnnuwfp1fozl.flv.vvyu	Dropped File	3.20 KB	video/x-flv	Access, Create, Write	MALICIOUS
81708239cf69b4eea5a25983c956aac089d26e108d4d223218f9e25a333426ab	C:\Users\kEecfMwgj\Desktop\s387k8QuDVZj.flv.vvyu, c:\users\keecfmwgj\desktop\s387k8qudvzj.flv.vvyu	Dropped File	32.55 KB	video/x-flv	Access, Create, Write	MALICIOUS
2fba5a64c12883996ea6dd166dd7f364e10ec94d88b7c1101acda9379ace6f74	c:\users\keecfmwgj\desktop\ssz4\us5ftz3jlmsu.mp4.vvyu, C:\Users\kEecfMwgj\Desktop\SSz4\uS5fTz3JlMsU.mp4.vvyu	Dropped File	24.63 KB	application/octet-stream	Access, Create, Write	MALICIOUS
54b566a64e4e05544fb56b58246cc462fb492093c2093c1a1c1c8d136a7c1e23	C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\-kPL6mXQjk.bmp.vvyu, c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\-kpl6mxqjk.bmp.vvyu	Dropped File	7.54 KB	application/octet-stream	Access, Create, Write	MALICIOUS
90f8b03e08e28b84a90712400460c10a4546eb6d67dc56573dea77df3aa17adaf	c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\nj4aq\xq89ysrduds.pdf.vvyu, C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\NJ4Aq\xq89ysrDUDS.pdf.vvyu	Dropped File	55.13 KB	application/pdf	Access, Create, Write	MALICIOUS
aed75eebad6b756af07cbddd7601506855d5e1e87a9e9111261bbdde9bb547d7	C:\Users\kEecfMwgj\Desktop_gJDhmKEYoYDIQq.gif.vvyu, c:\users\keecfmwgj\desktop_gjdhmkeyoydlqq.gif.vvyu	Dropped File	13.04 KB	image/gif	Access, Create, Write	MALICIOUS
8b7464cf92fcf75ba7d6a9fe29e4274bff6f9eb856d551deb20250b59892de94	C:\Users\kEecfMwgj\Desktop\SSz4\HT9Aw JQ.png.vvyu, c:\users\keecfmwgj\desktop\ssz4\ht9awjq.png.vvyu	Dropped File	69.06 KB	application/octet-stream	Access, Create, Write	MALICIOUS
9d70904c814896a852e358754328193d9018c4818d1109fb795d7e41686ccac7	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\3Xs\0R 3sVLz9jj8.rtf.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\uomn anj\3x s\0r 3svlz9jj8.rtf.vvyu	Dropped File	48.10 KB	text/rtf	Access, Create, Write	MALICIOUS
d247554d388711df1ce4777081d804741b4500889e5765ad9181e72334890c09	C:\Users\kEecfMwgj\Desktop\oGH6r9EKez2SrD.bmp.vvyu, c:\users\keecfmwgj\desktop\ogh6r9ekez2srd.bmp.vvyu	Dropped File	100.26 KB	application/octet-stream	Access, Create, Write	MALICIOUS
40920dd6a636cc8f69d8dad7cbb80b361a50f7ba9a2d2e3825fc87f00424bd88	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
10d3e26496761e38324c462ec9ef7226fbaf9060581adf4e1997178d6f656152	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\6e2w9YoR-8.pdf.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\uomn anj\6e2w9yor-8.pdf.vvyu	Dropped File	94.46 KB	application/pdf	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
88da2f03b47dcd914afaec5ccffff4a98c30b9af7f66554b33fbc5b17cc6a181	c:\users\keecfmwgj\music\q6ag5\pjtklq_dt3lt.wav.vvyu, C:\Users\kEecfMwgj\Music\q6aG5\pJtkLq_dT3lT.wav.vvyu	Dropped File	61.53 KB	application/octet-stream	Access, Create, Write	MALICIOUS
814b60678495c39281479319bca0eb6873d2a8aae625a19d98c9bbe24771f3e5	c:\users\keecfmwgj\pictures\9qc8otgh1hix w8i.gif.vvyu, C:\Users\kEecfMwgj\Pictures\9qc8OtgH1HIX w8I.gif.vvyu	Dropped File	6.93 KB	image/gif	Access, Create, Write	MALICIOUS
3be6b2eada734b31552bd1389ddcd71b113afed25ad1151e9be13621821b1456	c:\users\keecfmwgj\desktop\ssz4\ol21.csv.vvyu, C:\Users\kEecfMwgj\Desktop\SSz4\Ol21.csv.vvyu	Dropped File	19.05 KB	application/octet-stream	Access, Create, Write	MALICIOUS
a1db2318077f5bd0dcfadbf47589935d4a17e898e5e0d5ecbe1d844c1276ef1b	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
71dd53571da2eb390b81b52076ab1b875f2c05a43b8ddc7af00c3d54121e0ed9	c:\users\keecfmwgj\documents\egcel.ppt.vvyu, C:\Users\kEecfMwgj\Documents\EgCel.ppt.vvyu	Dropped File	61.87 KB	application/octet-stream	Access, Create, Write	MALICIOUS
5e820f188ed3c203012c87f6c3387234dd3a2893136db68b6ddbac1663d8dde6	c:\users\keecfmwgj\desktop\ssz4\7qttxszlkjh_fii.pdf.vvyu, C:\Users\kEecfMwgj\Desktop\SSz4\7QttxsZlKJh_fli.pdf.vvyu	Dropped File	71.79 KB	application/pdf	Access, Create, Write	MALICIOUS
e9fc8c229a1a18eaadfa6f9d22d1cecaa812a965d9e32a41fe1c9e24a3d4091e	c:\users\keecfmwgj\desktop\ssz4\wmqgvke.flv.vvyu, C:\Users\kEecfMwgj\Desktop\SSz4\wmQgvKE.flv.vvyu	Dropped File	22.81 KB	video/x-flv	Access, Create, Write	MALICIOUS
5e3694b6ef8a20b17d447542c3639f35dda37c32a3fb9462984f078b8d2091e6	c:\users\keecfmwgj\desktop\jb1orsrry.m4a.vvyu, C:\Users\kEecfMwgj\Desktop\jb1orsRry.m4a.vvyu	Dropped File	33.81 KB	application/octet-stream	Access, Create, Write	MALICIOUS
0beb15bcf563d5f95fe48da30a5bf4a14a4fc66a3ace9340e911d8237fae270c	C:\Users\kEecfMwgj\Pictures\CkH5eNz\UIPaZiiR-oQnLQB3Ey2.png.vvyu, c:\users\keecfmwgj\pictures\ckh5enz\uipaziir-oqnlqb3ey2.png.vvyu	Dropped File	79.66 KB	application/octet-stream	Access, Create, Write	MALICIOUS
855d5ebe1e10a82bfd72b8bbaea07ae6063ae5c91a9b8e5fc560177c3b862d51	C:\Users\kEecfMwgj\Pictures\CkH5eNz\up4L8znJo05a3P.jpg.vvyu, c:\users\keecfmwgj\pictures\ckh5enz\up4l8znjo05a3p.jpg.vvyu	Dropped File	31.65 KB	image/jpeg	Access, Create, Write	MALICIOUS
d522bc287c6d938ace7e1e23c70e80e2e42289fd66238df910432a95765d7bc8	c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\j2t8dyq7a9 s.m4a.vvyu, C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\j2t8dyq7A9 S.m4a.vvyu	Dropped File	27.44 KB	application/octet-stream	Access, Create, Write	MALICIOUS
aabf05c61cb227bda1d5c403974d7c6e759a78c68f11cc8fe973206171b0ad61	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\ZFul69zRrETYF.docx.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\zful6 9zrretyf.docx.vvyu	Dropped File	60.06 KB	application/zip	Access, Create, Write	MALICIOUS
fb2e8e3a61edc8536b3a672fc0107d5263a79ff7aaa7bf0254eea3b0e5c5624b	C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\O2UTInId.gif.vvyu, c:\users\keecfmwgj\pictures\ckh5enz\utklaz\o2utinid.gif.vvyu	Dropped File	14.31 KB	image/gif	Access, Create, Write	MALICIOUS
e944bb460dc6647c718ed4b7eb7d4d3e4cb8c86a960baf0f15b9f93b328b252a	c:\users\keecfmwgj\videos\w9galst6bnf-yf.mkv.vvyu, C:\Users\kEecfMwgj\Videos\W9GALSt6BNf-yf.mkv.vvyu	Dropped File	94.10 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4d57a63dd3bbeacc7331ada2a3d51ac2148bc8de90915b969818bc032e7f63f9	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\3QxjAR\T8wvyki0J9mO.ots.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\3qxjar\t8wvyki0j9mo.ots.vvyu	Dropped File	40.19 KB	application/zip	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
017fa3733fa5b759bd1336f0ea699c705ade6e5884684f1a483eee9655ba16f2	C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\YNvx X.bmp.vvyu, c:\users\keecfmwgj\pictures\ckh5enz\utklaz\ynvx x.bmp.vvyu	Dropped File	58.19 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4ca9df76edbc2e10be02c481aa958318412af5c2ddc05822acd6e05fe0b770f1	c:\users\keecfmwgj\pictures\ckh5enz\0zp is.jpg.vvyu, C:\Users\kEecfMwgj\Pictures\CkH5eNz\0zP Is.jpg.vvyu	Dropped File	95.71 KB	image/jpeg	Access, Create, Write	MALICIOUS
f7340b002ac0f953589ff172085f5024f6e8d8aa0ddb2aa2d951d0ef63ee3d21	C:\Users\kEecfMwgj\Desktop\MWdsq1QYO68B.m4a.vvyu, c:\users\keecfmwgj\desktop\mwdsq1qyo68b.m4a.vvyu	Dropped File	45.89 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c3a3ec5f89164367eac694c703f4015ffd823e336621ec64a5ed80f99a07838f	c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\gx_wgirqaux_.pptx.vvyu, C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\GX_WgIRqauX_.pptx.vvyu	Dropped File	20.47 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4fc6d20ede54857c1d310071235219fc95730efa229c0fc0b8bb8abe3a7c78f6	c:\users\keecfmwgj\videos\oa7uy-r84e\irrx7uvzuzqm6ox.avi.vvyu, C:\Users\kEecfMwgj\Videos\oa7UY-r84e\Irrx7uVzUZQm6OX.avi.vvyu	Dropped File	38.65 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ba3d838b6d06a693dd4e0e5177bac48130d80f76ef84dad2a2cea8b7903b5d8b	c:\users\keecfmwgj\pictures\v-derpgnma_nx.png.vvyu, C:\Users\kEecfMwgj\Pictures\V-dERpgnmA_NX.png.vvyu	Dropped File	36.27 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e5717d042b96213e7525d3601f1d6e2f96ebb8e78ff2c7c5e9545c8c11f770d6	c:\users\keecfmwgj\documents\5w2kb0xpz679okq9oh.doc.vvyu, C:\Users\kEecfMwgj\Documents\5w2KB0xPz679OKQ9OH.doc.vvyu	Dropped File	24.55 KB	application/octet-stream	Access, Create, Write	MALICIOUS
0a882c1660ad5f1bc70c5d206d16d435023f4d1e622f7ed901dccfb3613c2962	C:\Users\kEecfMwgj\Music\q6aG5\w5q7V-5Q7Epp.m4a.vvyu, c:\users\keecfmwgj\music\q6ag5\w5q7v-5q7epp.m4a.vvyu	Dropped File	80.01 KB	application/octet-stream	Access, Create, Write	MALICIOUS
8e20e1d0e0b386168160bf77183678a3e384ad15a08fc5f0b3604137cf6ce4f1	C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4dJjOvnSZY.bmp.vvyu, c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\jjovnszy.bmp.vvyu	Dropped File	94.32 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e2730913e97e55852274ac59fbedeea5f80606185cafdc83153b5363b9680d5d	C:\Users\kEecfMwgj\Documents\Efz8vEEd1pSVsE6 PJdQ.xlsx.vvyu, c:\users\keecfmwgj\documents\efz8veed1psvse6 pjdq.xlsx.vvyu	Dropped File	100.28 KB	application/zip	Access, Create, Write	MALICIOUS
290c6310abfbae8fa7d98c8899cca8315b943ecfd42b510830bce1480f114a9c	c:\users\keecfmwgj\documents\45jcquohqob2hs.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\45jcQUohQOb2hs.xlsx.vvyu	Dropped File	9.42 KB	application/octet-stream	Access, Create, Write	MALICIOUS
87bbfcfdd1574b55313220affa686725ba9a8aa7433fdd00d677b9735c0b6a10	c:\users\keecfmwgj\music\q6ag5\6gb9swuoi.wav.vvyu, C:\Users\kEecfMwgj\Music\q6aG5\6gB9SwuOl.wav.vvyu	Dropped File	96.88 KB	application/octet-stream	Access, Create, Write	MALICIOUS
149ad2cdf101b6f50f12c0c49ac7c442fca7467fdc0ffcd807daf5e300fe0ab1	C:\Users\kEecfMwgj\Videos\h8vWrl4X3qjJx.avi.vvyu, c:\users\keecfmwgj\videos\h8vwrl4x3qjjx.avi.vvyu	Dropped File	74.65 KB	application/octet-stream	Access, Create, Write	MALICIOUS
dce6b8a41c2b1bf677b1ff4b8568083e3eb0dda96b2d2cffbf8dc28b4a70b46c	C:\Users\kEecfMwgj\Videos\oa7UY-r84e\v2hZ1rIby\6zZsCwOqJQhE.avi.vvyu, c:\users\keecfmwgj\videos\oa7uy-r84e\v2hz1riby\6zzscwoqjqhe.avi.vvyu	Dropped File	75.61 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6ca3d3c832a3dbca50a6f35129b47ed4b77099a7a50b595b3be55447516ed6d6	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\f1rc6EXPyfw.pdf.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\f1rc6expyfw.pdf.vvyu	Dropped File	53.16 KB	application/pdf	Access, Create, Write	SUSPICIOUS
5839f7e465deb2f8f56d9fda6d9ef37cfabc3f5ba0b3e38396f0fdcfbb5ef9fe	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\UomnAnj\5kZStye71WnSS.pdf.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\uomnanj\5kzstye71wnss.pdf.vvyu	Dropped File	60.53 KB	application/pdf	Access, Create, Write	SUSPICIOUS
a9342cb42c77afb4c88217d1fdfec39fcc12a92b194ed3d8aa94c6c4442317f5	-	Web Response	576 bytes	application/json	-	CLEAN
3c7d38aff2dd9e697cd3cc6c0a5d338ff2d0bdb948fb469cd21c76d8c36e53ee	-	Modified File	256.00 KB	application/octet-stream	-	CLEAN
54d2884af398a63c9299290197b73d90dd363fbf9d27c31111adb0728c7069a6	c:\users\keecfmwgj\music\q6ag5\yIvock6jtrl_ur2.m4a.vvyu, C:\Users\kEecfMwgj\Music\q6aG5\yIVOck6jtRL_uR2.m4a.vvyu	Dropped File	3.64 KB	application/octet-stream	Access, Create, Write	CLEAN
85bdf54cf69443615c3c8cc6163ca75df7a1c79d29673608f46386e064f0f1cb	c:\users\keecfmwgj\desktop\6umy14w18jmqx-yvo.swf.vvyu, C:\Users\kEecfMwgj\Desktop\6umy14w18jMqx-YvO.swf.vvyu	Dropped File	76.40 KB	application/x-shockwave-flash	Access, Create, Write	CLEAN
632a21e6fc0b8c83fa64ab6b39de32418077112cdd27e4f3bf1a1076a2044992	C:\Users\kEecfMwgj\Music\ucR8jv0bs4.wav.vvyu, c:\users\keecfmwgj\music\ucr8jv0bs4.wav.vvyu	Dropped File	99.21 KB	application/octet-stream	Access, Create, Write	CLEAN
9d9d58a552c25b03b61b27f83d0e642f90d6a75feaf89de2a5268a5d9c751334	c:\users\keecfmwgj\desktop\g8m9wnztgrqdpa.doc.vvyu, C:\Users\kEecfMwgj\Desktop\G8M9wNzTGRqdPa.doc.vvyu	Dropped File	49.06 KB	application/octet-stream	Access, Create, Write	CLEAN
65ce021b0b11d5490f43b0b0d39558a4129e114346d8964cb92b8ca83922f45d	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	CLEAN
f6814d7f1e64fc4f4e721cedf6d3552d9c57f33226893f739f4eb21234b1c8ef	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\NJ4Aq\JRCSXUX.rtf.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\nj4aq\jrcsxux.rtf.vvyu	Dropped File	68.86 KB	text/rtf	Access, Create, Write	CLEAN
9ac425b276fcece7fff6236ec3b532432db7fcc227fa75c6f537c61a43d9afe0	c:\users\keecfmwgj\pictures\0md97n-k.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\0mD97n-K.bmp.vvyu	Dropped File	2.97 KB	application/octet-stream	Access, Create, Write	CLEAN
72cf0e2d7e50e585963e2a4873e4724697ab6f1eb715829089f8379d9bdd2ae2	c:\users\keecfmwgj\documents_-fr_fxi6 yovrtv.pptx.vvyu, C:\Users\kEecfMwgj\Documents_-fR_fxi6 yoVrtv.pptx.vvyu	Dropped File	42.22 KB	application/zip	Access, Create, Write	CLEAN
e4a2fa73a8f3554a9282a38ba85717c53b520275dfc7ff88b4ac3d8ce89d61eb	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
a4b9e0ae5661623d933891127510a0e09f5f2b95ea07503f31edf2b62d1c4d3a	C:\Users\kEecfMwgj\Desktop\HuD-Vd.ppt.vvyu, c:\users\keecfmwgj\desktop\hud-vd.ppt.vvyu	Dropped File	39.87 KB	application/octet-stream	Access, Create, Write	CLEAN
b6a33245545d6d8d813981c99b398da3111d73cf923c18056dff7029997cb169	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
a5cb50ea5d800c8c7bffadd13737ec136db6d94b790172e4dc3f8ded12ebf993	c:\users\keecfmwgj\music\bqn7jsn2k_hp.wav.vvyu, C:\Users\kEecfMwgj\Music\BqN7jSN2K_hP.wav.vvyu	Dropped File	48.49 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6d214ad6b2cf334f0545be9f044bb26b2bd3d43dd77f5e124a5769b86c9ad995	-	Downloaded File	216 bytes	text/html	-	CLEAN
6b1dd5e6161dbb38c7e512c2d6c44b95d957b5e117f9cfc574343a8035ac725e	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\3QxjAR\0nTeT5RDjQL6aro.csv.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\3qxjar\0ntet5rdjql6aro.csv.vvyu	Dropped File	63.67 KB	application/octet-stream	Access, Create, Write	CLEAN
b50d3160ff818c4f7f9be06fe6abdd8de1032055f403f739ffcc038bf0794065	c:\users\keecfmwgj\pictures\scabdm3i.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\ScAbDm3l.bmp.vvyu	Dropped File	57.28 KB	application/octet-stream	Access, Create, Write	CLEAN
1a5c4dd3e6543038afed4e34a5313f9a31272c9e177266d7213767ca7ab46a0f	C:\Users\kEecfMwgj\Pictures\fjFyJ2LwCFuD.bmp.vvyu, c:\users\keecfmwgj\pictures\fjfyj2lwcfud.bmp.vvyu	Dropped File	25.04 KB	application/octet-stream	Access, Create, Write	CLEAN
079c11c7d28221f3c8d2c50fb7809e90ce423543f1f59db6f59cc053de83c091	c:\users\keecfmwgj\music\7rucdwyus.wav.vvyu, C:\Users\kEecfMwgj\Music\7RUcDwyUs.wav.vvyu	Dropped File	46.07 KB	application/octet-stream	Access, Create, Write	CLEAN
19064aeda4c5dedfb2a6c6cc95770b4a6749f44f7b7d8921d944dc0b06cb4918	c:\users\keecfmwgj\desktop\yyv494w_m8z.mkv.vvyu, C:\Users\kEecfMwgj\Desktop\Yyv494W_m8Z.mkv.vvyu	Dropped File	60.80 KB	application/octet-stream	Access, Create, Write	CLEAN
3071ee0aabd425d53fd8e4dcd1eb246d091f8ecd747c9850ea71f07fb3a79c94	c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dejp0tkawtpu.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\DeJP0TKaWtpU.xlsx.vvyu	Dropped File	54.03 KB	application/zip	Access, Create, Write	CLEAN
c3211fd3c9b5474da3cb165ffe9a5d4e55ee6c0193866e92b95a6d1cfb265094	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\hWL0ZU2H-.doc.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\hwl0zu2h-.doc.vvyu	Dropped File	17.63 KB	application/octet-stream	Access, Create, Write	CLEAN
9f2a8510a52dc176e8deec99aca0f9a440b4f32c6c74310b8639e46113399df5	C:\Users\kEecfMwgj\Videos\oa7UY-r84e_9xS8m5SRrPmY7bhauad.flv.vvyu, c:\users\keecfmwgj\videos\oa7uy-r84e_9xs8m5srrpmy7bhauad.flv.vvyu	Dropped File	36.72 KB	video/x-flv	Access, Create, Write	CLEAN
f505038305a66d16f5795f870fdf3835913d5a7c095c2b6c453eef34839f25a5	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\3Xs\E6LAV7pmdeNqQC2aZ.rtf.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\uomn anj\3xs\e6lav7pmdenqqc2az.rtf.vvyu	Dropped File	12.80 KB	text/rtf	Access, Create, Write	CLEAN
edac848d0b66b3053ba752e0825b69226656c0ea3864a17dea68c9b04b990e99	C:\Users\kEecfMwgj\Desktop\vfvz3sgUnK.m4a.vvyu, c:\users\keecfmwgj\desktop\vfvz3sgunk.m4a.vvyu	Dropped File	81.91 KB	application/octet-stream	Access, Create, Write	CLEAN
bc9bd8f6883f3fe970e58438847ce5fa738bfa89930f5ec9a141fed549a3c08f	c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\oyuf.gif.vvyu, C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\OYUf.gif.vvyu	Dropped File	9.47 KB	image/gif	Access, Create, Write	CLEAN
73ee17295d98f7cd8a800481c0109fb2645cf71d12aa05e843f62a106da48934	C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\4mQ2gMUrsax_RZzVhH.png.vvyu, c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\4mq2gmursax_rzzvhh.png.vvyu	Dropped File	75.78 KB	application/octet-stream	Access, Create, Write	CLEAN
8eadd74f33fe06dadc443508dde51b7ba0cef05a4c02b974633a103bd9dc1b07	c:\users\keecfmwgj\desktop\pwyx2b-yoplcn5mp.wav.vvyu, C:\Users\kEecfMwgj\Desktop\PWYx2b-yOplcn5mp.wav.vvyu	Dropped File	7.19 KB	application/octet-stream	Access, Create, Write	CLEAN
7c935110b9074fc8f2cd14c657f061c072ca49954dabc9505f68463c4c582976	c:\users\keecfmwgj\documents\wr0kwgonpwoxie1pnc.pptx.vvyu, C:\Users\kEecfMwgj\Documents\Wr0KwgONPWOXiE1pnc.pptx.vvyu	Dropped File	44.91 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
341bf813f7cab1709b641d5b6a37836b0a6e63050f03c344e424dd4500c496ed	c:\users\keecfmwgj\desktop\vz5gqw9gjyrik.swf.vvyu, C:\Users\kEecfMwgj\Desktop\Vz5gQW9gjYrik.swf.vvyu	Dropped File	21.06 KB	application/x-shockwave-flash	Access, Create, Write	CLEAN
40139799669a1a752a7b5e0109007c463b06bc77b064b5ae1036524c62228e7e	C:\Users\kEecfMwgj\Desktop\SSz4\9yAZzTXyNBlNhh5kD.mp3.vvyu, c:\users\keecfmwgj\desktop\ssz4\9yazztxynblnhh5kd.mp3.vvyu	Dropped File	40.69 KB	application/octet-stream	Access, Create, Write	CLEAN
1f76f0af856367c1932faa8d151822d5c2f96d304951b8a37a4ef15c14015333	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	CLEAN
0cb62dba7b0c20949d92e2a0382fb9af6e48771e7f75114bdaa3cda2da8ff98f	C:\Users\kEecfMwgj\Desktop\kvVdOKfcoMs.docx.vvyu, c:\users\keecfmwgj\desktop\kvvdokfcoms.docx.vvyu	Dropped File	74.95 KB	application/zip	Access, Create, Write	CLEAN
4952e06f4fb9c1b2fb917f3a003c2dbbc200d851a1604279436da48cb10c4277	c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\vnnb6-.png.vvyu, C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\VnNB6-.png.vvyu	Dropped File	65.98 KB	application/octet-stream	Access, Create, Write	CLEAN
2441fe55ef73a6723c7687531f2d0cf8db0b9bbb0387ec7ba4c20bffb6fd20f1	C:\Users\kEecfMwgj\Music\Pk0h2Rnp8cQPR.wav.vvyu, c:\users\keecfmwgj\music\pk0h2rnp8cqpr.wav.vvyu	Dropped File	51.83 KB	application/octet-stream	Access, Create, Write	CLEAN
a709fdd42a3f15aa945116121480eec5569a7a0a1a2c4444b8920dfb96405494	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\8OhTRGE.ods.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\8ohtrge.ods.vvyu	Dropped File	60.69 KB	application/zip	Access, Create, Write	CLEAN
25135b6a5cee92d2d7423daf80b89533b611bd03271d0af2a079cb6b8359fa7e	C:\Users\kEecfMwgj\Music\nA1Vyxh1cNbdS.mp3.vvyu, c:\users\keecfmwgj\music\na1vyxh1cnbds.mp3.vvyu	Dropped File	18.29 KB	application/octet-stream	Access, Create, Write	CLEAN
a961ab4c96e8c785877067639b1c7b0ae695b6b38072d6363308b373dc5472ff	C:\Users\kEecfMwgj\Music\q6aG5\7URv2AmQZDAOxub1g.mp3.vvyu, c:\users\keecfmwgj\music\q6ag5\7urv2amqzdaoxub1g.mp3.vvyu	Dropped File	39.63 KB	application/octet-stream	Access, Create, Write	CLEAN
0a5fb393094de01c32a15cb7de9e1fc183e6d401dfbacebf25132af9810dcf1e	c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\lviuhooev0pnicn.docx.vvyu, C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\lvIUHooev0pnICn.docx.vvyu	Dropped File	80.87 KB	application/zip	Access, Create, Write	CLEAN
0c5cceba5c416d5424387794429f89a2456b5326e2c7e5d8d2bd67f34bb616ec	-	Modified File	32.00 KB	application/octet-stream	-	CLEAN
c527d45374e7a7e54b9ef909e15b5961c80e76c267b06b4cabff80ccba522494	c:\users\keecfmwgj\videos\oa7uy-r84e\v2hz1riby\d4q2ikayi.swf.vvyu, C:\Users\kEecfMwgj\Videos\oa7UY-r84e\v2hZ1rIby\D4q2IKayI.swf.vvyu	Dropped File	17.99 KB	application/x-shockwave-flash	Access, Create, Write	CLEAN
01092879025f551f3bffea116916637c9235c85ae55513efc3c3abd887f2be6b	c:\users\keecfmwgj\pictures\ckh5enz\utklaz\jnrbiji7doab7.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\JNRbIJi7dOAB7.bmp.vvyu	Dropped File	94.59 KB	application/octet-stream	Access, Create, Write	CLEAN
1b8f7dbce30a828e26285ebd310cd987c4674e92dd53ee50c86c418793f73d23	c:\users\keecfmwgj\videos\0kzy5iydb0_9j1mvgm.avi.vvyu, C:\Users\kEecfMwgj\Videos\0kZY5IYdB0_9j1MVgm.avi.vvyu	Dropped File	95.62 KB	application/octet-stream	Access, Create, Write	CLEAN
6949f9851893f1ac27d2421545a34778b15a34eee7c6e2ad4a7b9af687b1d4fa	c:\users\keecfmwgj\desktop\ye2nvj3b.gif.vvyu, C:\Users\kEecfMwgj\Desktop\yE2nvj3b.gif.vvyu	Dropped File	65.37 KB	image/gif	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f1d379a1039155237c540cbfc9395529a8aa00526d05e28336a0d93e9f6c2ecc	C:\Users\kEecfMwgj\Desktop\o1Cxif2UWijY.bmp.vvyu, c:\users\keecfmwgj\desktop\o1cxif2uwijy.bmp.vvyu	Dropped File	94.16 KB	application/octet-stream	Access, Create, Write	CLEAN
a35444c1b3f981ebd6488a7573417259ef14574686ad53aef244ecf9fa519b7e	c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\xwnlbab.m4a.vvyu, C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\XwNlBAb.m4a.vvyu	Dropped File	89.89 KB	application/octet-stream	Access, Create, Write	CLEAN
a516db7de0e90c6910ed9bb105bd3c7e4981fead9837607879a323380f7b44d8	C:\Users\kEecfMwgj\Music\XP3a5K43wYYvtQY.wav.vvyu, c:\users\keecfmwgj\music\xp3a5k43wyyvtqy.wav.vvyu	Dropped File	28.62 KB	application/octet-stream	Access, Create, Write	CLEAN
a96da9526b076218ae3858547669eecfa8d96a6571922bd32b1532fb88dcd2a1	c:\users\keecfmwgj\desktop\3yd_u.doc.vvyu, C:\Users\kEecfMwgj\Desktop\3yD_u.doc.vvyu	Dropped File	4.00 KB	application/octet-stream	Access, Create, Write	CLEAN
2a402bed573d72e41d37984fdec37ff3ae8c9057f7d285783d7919b4bfd95b58	C:\Users\kEecfMwgj\Music\x5xovotqfAL_W9MsP.wav.vvyu, c:\users\keecfmwgj\music\x5xovotqfal_w9msp.wav.vvyu	Dropped File	23.63 KB	application/octet-stream	Access, Create, Write	CLEAN
c1afbc02698d2bfcbcc95fd488b38047f550413db767db1564809099780be100	c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\gwmlsc2zpd0nk-c.ods.vvyu, C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\gwMlSC2zpd0NK-c.ods.vvyu	Dropped File	48.08 KB	application/octet-stream	Access, Create, Write	CLEAN
68a0d29d2c1eb738d8ad6517317fe9bc538b996a2d9bb80cf6f9dfd2e2a925a3	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMDg2s\5GbLDOSSAl.ppt.vvyu, c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\5gbldossal.ppt.vvyu	Dropped File	82.15 KB	application/octet-stream	Access, Create, Write	CLEAN
b057604aa6f896e7973d21b44b05afea42296aad07c52cea4b6afe39f5a9595e	c:\users\keecfmwgj\music\j6ymsltmtmc.wav.vvyu, C:\Users\kEecfMwgj\Music\j6yMSLtmTmC.wav.vvyu	Dropped File	18.25 KB	application/octet-stream	Access, Create, Write	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\videos\q7szl.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\j6ymsltmtmc.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\pd9daotni.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\lviuhooev0pnicn.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\h6hrgnjnvqba.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ckh5enz\utklaz\9avxor.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ckh5enz\utklaz\fzsdv9ic_tv.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\fjFyJ2LwCFuD.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\wr0kwgonpwoxie1pnc.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\XevfC bH.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\w9galst 6bnf-yf.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\uomnanj\tpc-xlgkaoki.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\cs0y__wvetbw2qsiy.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\uomn anj\3x s\ygjufjkixo9zime2--.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\dHBKKyUiRLEo_ihqOR.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\vf vz3sgUnK.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\SSz4\HT9Aw JQ.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\bd1jkl.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\EOKz9As_PQ-0e NIZu2.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\T4N8wuVG8qRit6NO.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\GcroBq0Ap.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ckh5enz\g9op7kzr.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\VNa8b_DcXSUWmzm.wav.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\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\3X s\0R 3sVLz9jj8.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\q6aG5\MxIGzOSUnBj1N-Hm_Cz.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ssz4\hhor6gwwzwspwwtizr7.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\qexdtyv1z1q_cl0jaadt.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\3X s\E6LAV7pmdeNqQC2aZ.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\t7c9fofd9kt\3qxjar_53mq3d4gztl-z.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop_gJDhmKEYoYDlQq.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\O2UTInld.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\dhm2oVTh3lhgkYuY-T.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\3OZhLDJPo6htg3.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\hKaWlB 0CoAmHRQqjswP.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\q6ag5\6gb9swuoi.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\NaSt.xls.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\oa7uy-r84 e\mhdjwhf8pwlbd.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\0md97n-k.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\y1T01ydaDA.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\nj4aq\xq89ysrduds.pdf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\rMc5RT6t.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\q6ag5\pjtklq_dt3lt.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\nA1Vyxh1cNbdS.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\desktop\3yd_u.doc.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\xwzgawkf.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\Plnb573cskZFLk.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\4mQ2gMUrsax_RZzVhH.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\v-der pgnma_nx.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ssz4\7qttxszlkjh_fii.pdf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\f1rc6EXPyfw.pdf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\pwyx2b-yoplcn5mp.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\ctXFDNnUwfp1foZl.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\0kzy5iydb0_9j1mvgm.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\jyj5.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\mQVKO4ih33AabglOBNO.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\oa7UY-r84e_9xS8m5SRrPmY7bhauad.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\CkH5eNz\vVOtpApjKaG.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\SSz4\wOWCVtjIK1-R.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\vomzdu.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\oa7uy-r84e\v2hz1riby\4zazfhouywh4e77ghf.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\jb1orsrry.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\pj33ix3vapezxx5ftd.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\bqn7jsn2k_hp.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\q6aG5\7URv2AmQZDAOxub1g.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\sovvb9YRGyMc-lzi435.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\nj4aq\rfdw37vjsnr.ods.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\JjOvnSZY.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\2tgZNx.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\ucR8jv0bs4.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	Sample File, Accessed File, VM File	Access, Delete, Read, 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\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\m6h6LTvd.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\oa7uy-r84 e\v2hz1riby\-tfbdh.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\gx_wgirqaux_.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\desktop\ykvjwxghtjh67j.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ou84g9.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\hWL0ZU2H-.doc.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\Videos\T_12gb.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\uomnanj\8ydbvfzvuknzyhmzsw2e.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ckh5enz\0zp is.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\q6ag5\ylvock6jtrl_ur2.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\zct8oosw8v0sthu.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\fk6k3tax.flv.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\desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\zkBFKRCKZ7lX KV Wa4.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\CkH5eNz\UIPaZiiR-oQnLQB3Ey2.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\vnnb6-.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\j2t8dyq7a9s.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\evtlse5tu.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\gnn Elw-bv2A ZdUCx.csv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\oa7uy-r84 e\v2hz1riby\p14cw.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\s387k8QuDVZj.flv.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\Videos\oa7UY-r84 e\v2hZ1rIby\2u CRZIC7nvdh_M.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\i8vqvhtu5d8vngf1.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\hfxb2ecm2er.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\kvVdOKfcoMs.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\q6aG5\M7TOG0.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\uvhJEjKV7-C WKqxn.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\Y3WLOzPu7e3b.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\xwnlbab.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\MWdsq1QYO68B.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\xd4m_dlxrc.csv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\iiy6urtkmkg.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dejp0tkawtpu.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\h8vWrl4X3qjJx.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\q6aG5\w5q7V-5Q7Epp.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\oa7uy-r84 e\v2hz1riby\d4q2ikayi.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\t7c9fofd9kt\arxo4ulawvhk8w8h1.ppt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\6e2w9YoR-8.pdf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\deoyfojzp0gudvzpna_.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\Pk0h2Rnp8cQPR.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\zuIFM8NX8rRSCWk.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\v2hZ1rIby\h5htKcYKQyPR4iO.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\v2hZ1rIby\LqnhMFL0C.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\-CuxYEa66mYn.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\oGH6r9EKez2SrD.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\VNMhw6NdT0N.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\ptejmkr0q.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ckh5enz\gmzn.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\kq__.wav.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\Music\x5xovotqfAL_W9MsP.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\fdd4gb84c4w3sg.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\9 qc8otgh1hix w8i.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\bp5Lq3Xfqz.pps.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\eipo1g9l1l6y bqxfc.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\56a-hqjck-6jacz_y.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\SSz4\9yAZzTXyNBlNhh5kD.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\Jz_yDfR.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\8OhTRGE.ods.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\oa7uy-r84 e\kivyeyyglbqsq0r.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ssz4\1kkv.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\bojvfqm.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\q4w1nrmqjy.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\1stwBGeldnm.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\o9negzjy_dtz.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\5GbLDOSSAI.ppt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ye2nvj3b.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\jnq_e2h.png.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\Pictures\CkH5eNz\utKlAZ\UHHhHG8Z.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\yxnorx1icarsuvxvr.xls.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\Efz8vEEd1pSVsE6 PJdQ.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\4STyoT-wdxQ0wVe.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ssz4\ol21.csv.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	-	211.40.39.251, 190.140.99.150, 222.236.49.123, 196.200.111.5, 115.88.24.203, 211.119.84.112, 211.171.233.129, 211.53.230.67, 116.121.62.237, 187.170.251.250	-	GET	MALICIOUS
http://rgyui.top/dl/build2.exe	-	222.236.49.123, 41.41.255.235, 210.182.29.70, 195.158.3.162, 196.200.111.5, 110.14.121.123, 211.119.84.112, 5.163.244.118, 211.53.230.67, 211.119.84.111	-	GET	MALICIOUS
http://acacaca.org/test2/get.php?pid=9663E9B9567D9A7DCED1D0F506975904&first=true	-	211.40.39.251, 190.140.99.150, 222.236.49.123, 196.200.111.5, 115.88.24.203, 211.119.84.112, 211.171.233.129, 211.53.230.67, 116.121.62.237, 187.170.251.250	-	GET	MALICIOUS
https://t.me/pegasusfly1	-	149.154.167.99	-	-	CLEAN
https://mas.to/@pavlenko349	-	88.99.75.82	-	-	CLEAN
https://api.2ip.ua/geo.json	-	162.0.217.254	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
acacaca.org	211.40.39.251, 190.140.99.150, 222.236.49.123, 196.200.111.5, 115.88.24.203, 211.119.84.112, 211.171.233.129, 211.53.230.67, 116.121.62.237, 187.170.251.250	-	TCP, HTTP, DNS	MALICIOUS

Domain	IP Address	Country	Protocols	Verdict
rgyui.top	222.236.49.123, 41.41.255.235, 210.182.29.70, 195.158.3.162, 196.200.111.5, 110.14.121.123, 211.119.84.112, 5.163.244.118, 211.53.230.67, 211.119.84.111	-	TCP, HTTP, DNS	MALICIOUS
t.me	149.154.167.99	-	TCP, DNS, TLS	CLEAN
api.2ip.ua	162.0.217.254	-	TCP, HTTPS, DNS	CLEAN
mas.to	88.99.75.82	-	TCP, DNS, TLS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
41.41.255.235	rgyui.top	Egypt	DNS	CLEAN
5.163.244.118	rgyui.top	Saudi Arabia	DNS	CLEAN
222.236.49.123	rgyui.top, acacaca.org	South Korea	DNS	CLEAN
162.0.217.254	api.2ip.ua	Netherlands	TCP, HTTPS, DNS	CLEAN
88.99.75.82	mas.to	Germany	TCP, DNS, TLS	CLEAN
211.119.84.111	rgyui.top	South Korea	DNS	CLEAN
196.200.111.5	rgyui.top, acacaca.org	Eritrea	DNS	CLEAN
149.154.167.99	t.me	United Kingdom	TCP, DNS, TLS	CLEAN
187.170.251.250	acacaca.org	Mexico	DNS	CLEAN
211.53.230.67	rgyui.top, acacaca.org	South Korea	DNS	CLEAN
211.171.233.129	acacaca.org	South Korea	TCP, HTTP, DNS	CLEAN
195.158.3.162	rgyui.top	Uzbekistan	DNS	CLEAN
211.40.39.251	acacaca.org	South Korea	DNS	CLEAN
211.119.84.112	rgyui.top, acacaca.org	South Korea	DNS	CLEAN
110.14.121.123	rgyui.top	South Korea	TCP, HTTP, DNS	CLEAN
190.140.99.150	acacaca.org	Panama	DNS	CLEAN
116.121.62.237	acacaca.org	South Korea	DNS	CLEAN
210.182.29.70	rgyui.top	South Korea	DNS	CLEAN
115.88.24.203	acacaca.org	South Korea	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}	access	55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion	access	55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\SysHelper	read, access, write	55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SysHelper	read, access, write	55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	build2.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	build2.exe	CLEAN

Process

Process Name	Commandline	Verdict
55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	"C:\Users\kEecfMwgj\Desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe"	MALICIOUS
55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	"C:\Users\kEecfMwgj\Desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe" --Admin IsNotAutoStart IsNotTask	MALICIOUS
build2.exe	"C:\Users\kEecfMwgj\AppData\Local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe"	MALICIOUS
55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	"C:\Users\kEecfMwgj\AppData\Local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe" --AutoStart	MALICIOUS
55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	"C:\Users\kEecfMwgj\Desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe"	SUSPICIOUS
55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	"C:\Users\kEecfMwgj\Desktop\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe" --Admin IsNotAutoStart IsNotTask	SUSPICIOUS
build2.exe	"C:\Users\kEecfMwgj\AppData\Local\22264cfd-727b-45d7-91c9-e74b24b1e0e5\build2.exe"	SUSPICIOUS
55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe	"C:\Users\kEecfMwgj\AppData\Local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b\55043585c15ff65ca4b8df91c0b0f1c883d4cfd40933c6d25c2d9159e2f0757c.exe" --AutoStart	SUSPICIOUS
icacls.exe	icacls "C:\Users\kEecfMwgj\AppData\Local\1b71cfc7-59d7-431f-bf72-fcbb51f37d3b" /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\Music\zkBFKRCKZ7IX KV Wa4.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ou84g9.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\bijamby.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\zct8oosw8v0sthu.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\kq__.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\VNMhw6NdT0N.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\videos\oa7uy-r84e\v2hz1riby\-tfbdh.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\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\xd4m_dlxrc.csv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\yxnorx1icarsuvxvr.xls.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ckh5enz\utklaz\fzsdv9ic_tv.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\T4N8wuVG8qRit6NO.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\documents\wxhzvh5geamrbckdv0bk.pptx.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\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\ooeO67V 2A6dBdr.pps.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\VNa8b_DcXSUWmzm.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\i8vqvhtu5d8vngf1.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\56a-hqjck-6jacz_y.docx.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\favorites\msn websites\msn entertainment.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\sovvb9YRGyMc-lzi435.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ckh5enz\utklaz\0djnwc3cmex6ks4d\4x6n.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\favorites\microsoft websites\ie site on microsoft.com.url.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\ckh5enz\utklaz\0djnwc3cmex6ks4d\rqq-bsnksl6mhoio1.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\v2hZ1rIby\LqnhMFL0C.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\rMc5RT6t.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\cs0y__wvetbw2qsiy.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\s12J.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\dLt-Gu15lr8w0sJrhR-b\Plnb573cskZFLk.ots.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\sy7kzm.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\music\pd9daotni.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\3OZhLDJPo6htg3.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ckh5enz\mgf6_dztb1f94j.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\q6aG5\M7TOG0.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\gmt4lzpnvyjn.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\music\15d3btm7ovs9nv4xvva\jyj5.mp3.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	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\Documents\dHBKKyUiRLEo_ihqOR.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\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\nj4aq\rfdw37vjsnr.ods.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\puDbAQqOd3K9PVjvn1u.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\h6hrgnjnvqba.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\-CxOzQcq.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\jpdadhjnb.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\15d3btm7ovs9nv4xvva\qexdtyv1z1q_cl0jaadt.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\Videos\oa7UY-r84 e\v2hZ1rIby\2uCRZIC7nvdh_M.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\oa7uy-r84e\mhdjwhf8pwlbd.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\15d3btm7ovs9nv4xvva\bojvfqm.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\Videos\SFCuO8sWL2Jsj.flv.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	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\fdd4gb84c4w3sg.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\15d3btm7OvS9NV4xvvA\AKXppD7.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\n4cmd g2s\uomnanj\8ydbvfzvuknzyhmzsw2e.pptx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\q7szl.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\oa7uy-r84e\v2hz1riby\4zazfhouywh4e77ghf.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\oa7UY-r84 e\GcroBq0Ap.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\gnn Elw-bv2A ZdUCx.csv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ckh5enz\g9op7kzr.jpg.vvyu	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\Desktop\ctXFDNnUwfp1foZl.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\s387k8QuDVZj.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ssz4\us5ftz3jlmsu.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\-kPL6mXQjk.bmp.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\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\nj4aq\xq89ysrduds.pdf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop_gJDhmKEYoYDlQq.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\SSz4\HT9Aw JQ.png.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\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\3Xs\0R 3sVLZ9jj8.rtf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\oGH6r9EKez2SrD.bmp.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\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\Documents\t7c9foFD9Kt\Du_\n4CMD g2s\Uomn Anj\6e2w9YoR-8.pdf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\q6ag5\pjtklq_dt3lt.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\9qc8otgh1hix w8i.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ssz4\ol21.csv.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\favorites\windows live\windows live mail.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\egcel.ppt.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\desktop\ssz4\7qttxszlkjh_fii.pdf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ssz4\wmqgvke.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\jb1orsrry.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\CkH5eNz\UIPaZiiR-oQnLQB3Ey2.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\CkH5eNz\up4L8znJo05a3P.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\music\15d3btm7ovs9nv4xvva\j2t8dyq7a9 s.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\ZFul69zRrETYF.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\CkH5eNz\utKlAZ\O2UTInId.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\w9galst6bnf-yf.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\3QxjAR\T8wvyki0J9mO.ots.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\Pictures\CkH5eNz\utKlAZ\YNvx X.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ckh5enz\0zp is.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\Desktop\MWdsq1QYO68B.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\documents\t7c9fofd9kt\du_\dlt-gu15ir8w0sjrhr-b\gx_wgirqaux_.pptx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\oa7uy-r84e\irrx7uvzuzqm6ox.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\v-derpgnma_nx.png.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\5w2kb0xpz679okq9oh.doc.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\q6aG5\w5q7V-5Q7Epp.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\CkH5eNz\utKlAZ\0Djnwc3CmEX6ks4d\JjOvnSZY.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\Efz8vEEd1pSVsE6 PJdQ.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\45jcquohqob2hs.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\q6ag5\6gb9swuoi.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\h8vWrI4X3qjJx.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\oa7UY-r84e\v2hZ1rIby\6zZsCwOqJQhE.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\q6ag5\ylvock6jtrl_ur2.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\6umy14w18jmqx-yvo.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\ucR8jv0bs4.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\desktop\g8m9wnztgrqdpa.doc.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\Documents\t7c9foFD9Kt\Du_\dLt-Gu15Ir8w0sJrhR-b\NJ4Aq\JRCSXUX.rtf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\0md97n-k.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents_-fr_fxi6 yovrtv.pptx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\windows live\get windows live.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\HuD-Vd.ppt.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\music\bqn7jsn2k_hp.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\3QxjAR\0nTeT5RDjQL6aro.csv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\scabdm3i.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\fjFyJ2LwCFuD.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\7rucdwyus.wav.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\yyv494w_m8z.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\t7c9fofd9kt\du_\dejp0tkawtpu.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\t7c9foFD9Kt\Du_\hWL0ZU2H-.doc.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\oa7UY-r84e_9xS8m5SRrPmY7bhauad.flv.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	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