MALICIOUS

Classifications: Downloader | Ransomware

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

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe**
ID	#5067640
MD5	28fb096cbce32cf1f87719254452014f
SHA1	50ceaddc379e1376a579e4c9d4465fd3c734c277
SHA256	1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98
File Size	730.50 KB
Report Created	2022-08-05 14:52 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (26 rules, 145 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #11) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #11) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 204 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\Documents\KUOP p2txHoo7bw7O.doc.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Contacts\Administrator.contact.vvyu".
- Rule "Djvu" from ruleset "Ransomware" has matched on a memory dump for (process #2) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe.
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\favorites\msn websites\msn.url.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\hhuy\z99M8Y1GRoOyuotMz.csv.vvyu".
- Rule "Djvu" from ruleset "Ransomware" has matched on a memory dump for (process #6) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe.
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\z2e0zt\zpv7u7xpwr7qk\rfes3vfwf3fsy6sx.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\itjgP.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\6pw8rpgl-.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\GW5kXQqybZPUP2d4.mp4.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd- y4\t laiuy5vumxfxacjn.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents_3WI5D4o0g2MKtP.pptx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\bQ6SJi8RO0rg0dP\3YgFUJ.rtf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\ilfMhH\5DS0X1cGBS4n2igZsE.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\bQiz44uQ681_7Dctbgxp.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\nmf9emihkrId8q1qs.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\cPfFJ9.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\567c.pdf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\hhuy\bju5iwgzcivxdeaczva1.odt.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\hhuy\r fixnl1vu2.ots.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\tkvyxwxrq.ots.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\olz6-jxmw7o1_h pvu.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\yOmL -Z4 9fyb2lF7S9.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\hhuy\ni1u7vxc2c n4uuhwh.pps.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\ijdhlcko.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\uo7bfSHfyn-0X-MGd.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\bq6sji8ro0rg0dp\9ecwyh_e3fhju.avi.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\desktop\rwqicw2qitxlv4.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\favorites\msn websites\msn autos.url.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\ilfMhH\9VRBBaa2E6cjsKGlie.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\ksif.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\hhuy\U-GFPMIYoqWy2p9O.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\mxrqwfqcp\jze7xrus.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\ydph4cpxgp3qwyuc\aougfr90ajw.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\bjhxlx\cmbsppstlrb9u.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\s_e2a5ScpFSgR9-.mkv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\tHLd WYzw.ots.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkl\HbqLBzpGm.wav.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\Music\BJHxLX\KnG7feMIAKlEoa_UW1s2.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\6LeN1-BfLiBS.rtf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\wa_4pk0l7jwgqv.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\z1niztmoyavazpqq.rtf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\CzDS-.pptx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkl\6y-Gle7CJ.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\hhuy\Qs2 hK9Y_.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\pfzhnu297.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd- y4\-ahhgkvlxn_kxd.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\ydph4cpxgp3qwyuc\x5tjkqt17l1kq.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\hDvzuhrdv.mkv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\nQrFKLA.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\K3t8MIfEa.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\rQja5oZ7_uz\EhqiUu8LgIRI.mp4.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\z2e0zt\zpv7u7xpwr7qk\iwi4py9f_tbuupcdk.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\hhuy\naiaggm8s5tskx.docx.vvyu".

Score	Category	Operation	Count	Classification
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
4/5	Reputation	Contacts known malicious URL	3	-
	• Reputation analysis labels the URL "http://acacaca.org/test2/get.php?pid=DEC2E953FC80DE582D412ECFEAA51D7B&first=true" which was contacted by (process #6) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "http://acacaca.org/test2/get.php?pid=DEC2E953FC80DE582D412ECFEAA51D7B" which was contacted by (process #11) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "http://rgyui.top/dl/build2.exe" which was contacted by (process #6) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe as Mal/HTMLGen-A.		
4/5	Reputation	Resolves known malicious domain	2	-
	• Reputation analysis labels the resolved domain "acacaca.org" as Mal/HTMLGen-A. • Reputation analysis labels the resolved domain "rgyui.top" as Mal/HTMLGen-A.			
3/5	YARA	Suspicious content matched by YARA rules	2	-
	• Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\567c.pdf.vvyu". • Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\567c.pdf.vvyu".			
2/5	Hide Tracks	Deletes file after execution	1	-
	• (Process #2) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe deletes executed executable "C:\Users\kEecfMwgj\AppData\Local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe".			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #6) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe has a thread which sleeps more than 5 minutes.			
2/5	_data_collection	Reads sensitive application data	1	-
	• (Process #11) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe tries to read sensitive data of application "git" by file.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	3	-
	• (Process #1) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe modifies memory of (process #2) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe. • (Process #5) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe modifies memory of (process #6) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe. • (Process #10) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe modifies memory of (process #11) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	3	-
	• (Process #1) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe alters context of (process #2) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe. • (Process #5) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe alters context of (process #6) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe. • (Process #10) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe alters context of (process #11) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe.			
2/5	Task Scheduling	Schedules task	1	-
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe", to be triggered by TIME. Task has been rescheduled by the analyzer.			
1/5	Obfuscation	Reads from memory of another process	3	-

Score	Category	Operation	Count	Classification
		• (Process #1) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe reads from (process #1) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe. • (Process #5) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe reads from (process #5) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe. • (Process #10) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe reads from (process #10) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	3	-
		• (Process #1) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #5) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #10) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.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) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe enumerates running processes. • (Process #6) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe enumerates running processes. • (Process #11) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe enumerates running processes.		
1/5	Persistence	Installs system startup script or application	1	-
		• (Process #2) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe adds ""C:\Users\kEecfMwgj\AppData\Local\4d45d74b... ... 9-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe" --AutoStart" to Windows startup via registry.		
1/5	Hide Tracks	Creates process with hidden window	1	-
		• (Process #2) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe starts (process #2) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe with a hidden window.		
1/5	Mutex	Creates mutex	2	-
		• (Process #6) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe creates mutex with name "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}". • (Process #11) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe creates mutex with name "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}".		
1/5	Discovery	Tries to get network statistics	1	-
		• (Process #11) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe gets network statistics via API.		
1/5	Network Connection	Downloads executable	1	Downloader
		• (Process #6) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe downloads Windows executable via http from http://rgyui.top/dl/build2.exe.		
1/5	Network Connection	Downloads file	2	-
		• (Process #6) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe downloads file via http from http://acacaca.org/test2/get.php?pid=DEC2E953FC80DE582D412ECFEAA51D7B&first=true. • (Process #11) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe downloads file via http from http://acacaca.org/test2/get.php?pid=DEC2E953FC80DE582D412ECFEAA51D7B.		
1/5	Obfuscation	Resolves API functions dynamically	6	-
		• (Process #1) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe resolves 39 API functions by name. • (Process #2) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe resolves 37 API functions by name. • (Process #5) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe resolves 39 API functions by name. • (Process #6) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe resolves 37 API functions by name. • (Process #10) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe resolves 39 API functions by name. • (Process #11) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe resolves 58 API functions by name.		
1/5	Execution	Drops PE file	1	-

Score	Category	Operation	Count	Classification
		• (Process #6) 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe drops file "C:\Users\kEecfMwgj\AppData\Local\c01688bb-f556-4db2-ba2c-05b15fa562c3\build2.exe".		

Mitre ATT&CK Matrix

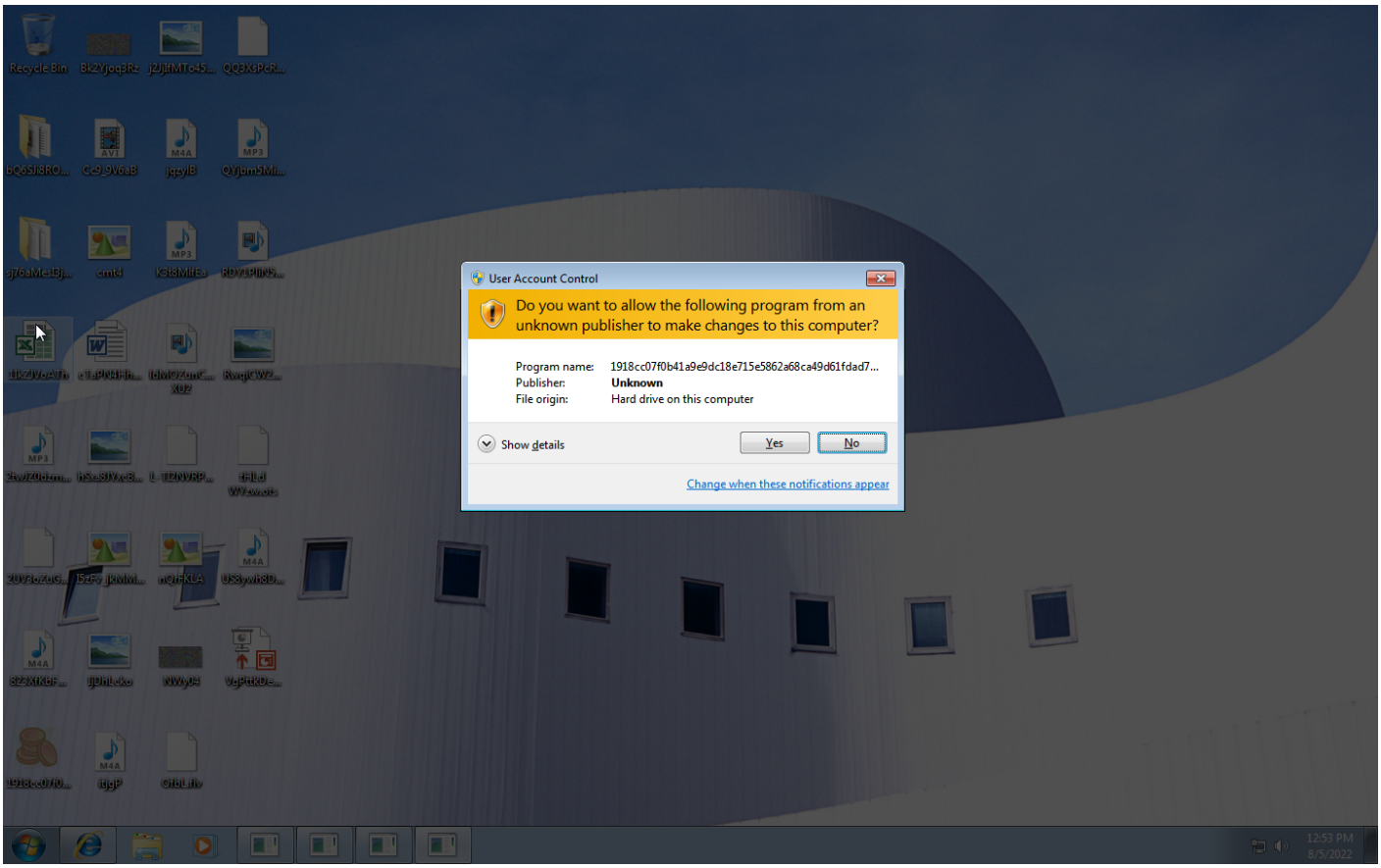
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1060 Registry Run Keys / Startup Folder	#T1053 Scheduled Task	#T1045 Software Packing	#T1081 Credentials in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

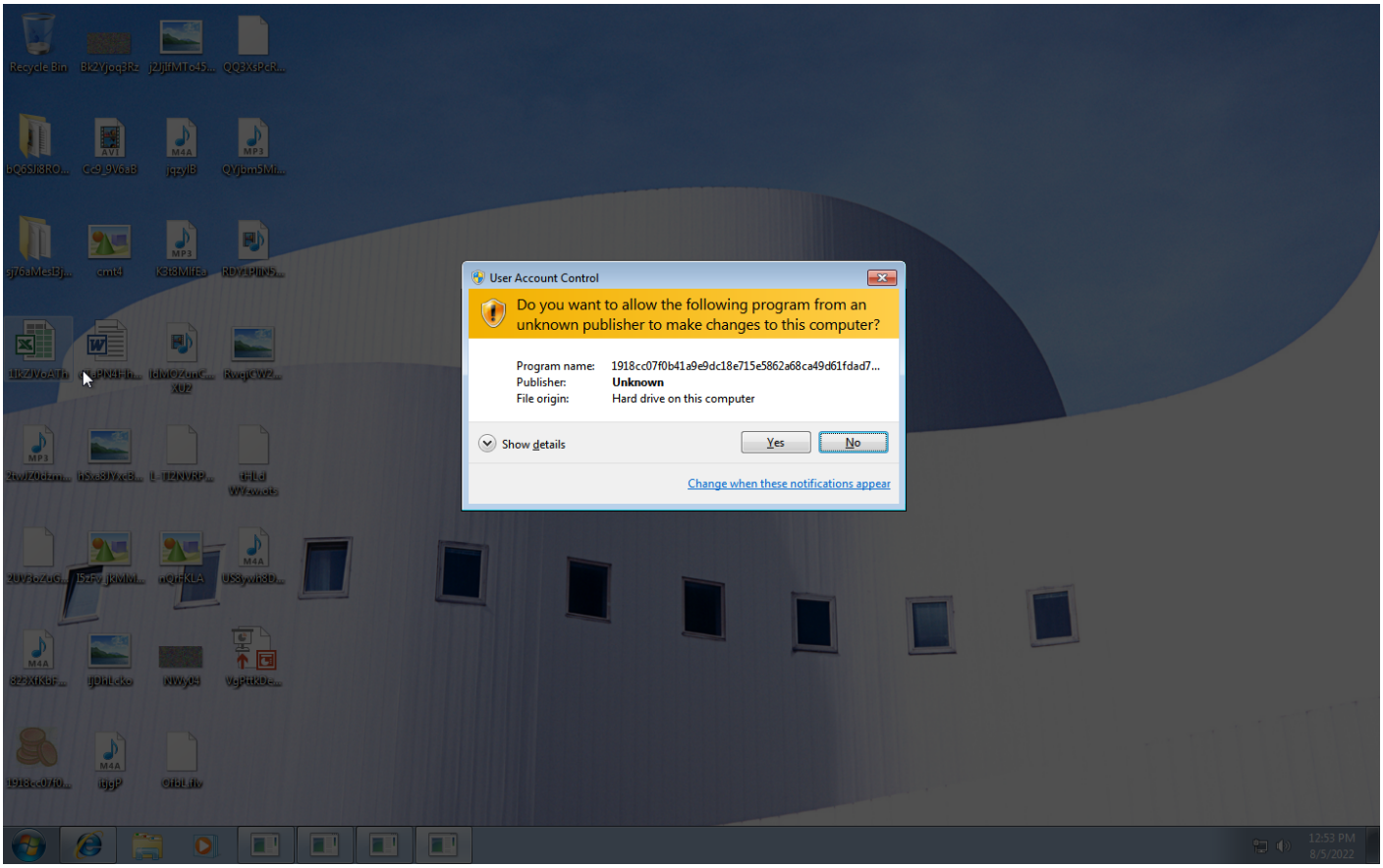
Sample Information

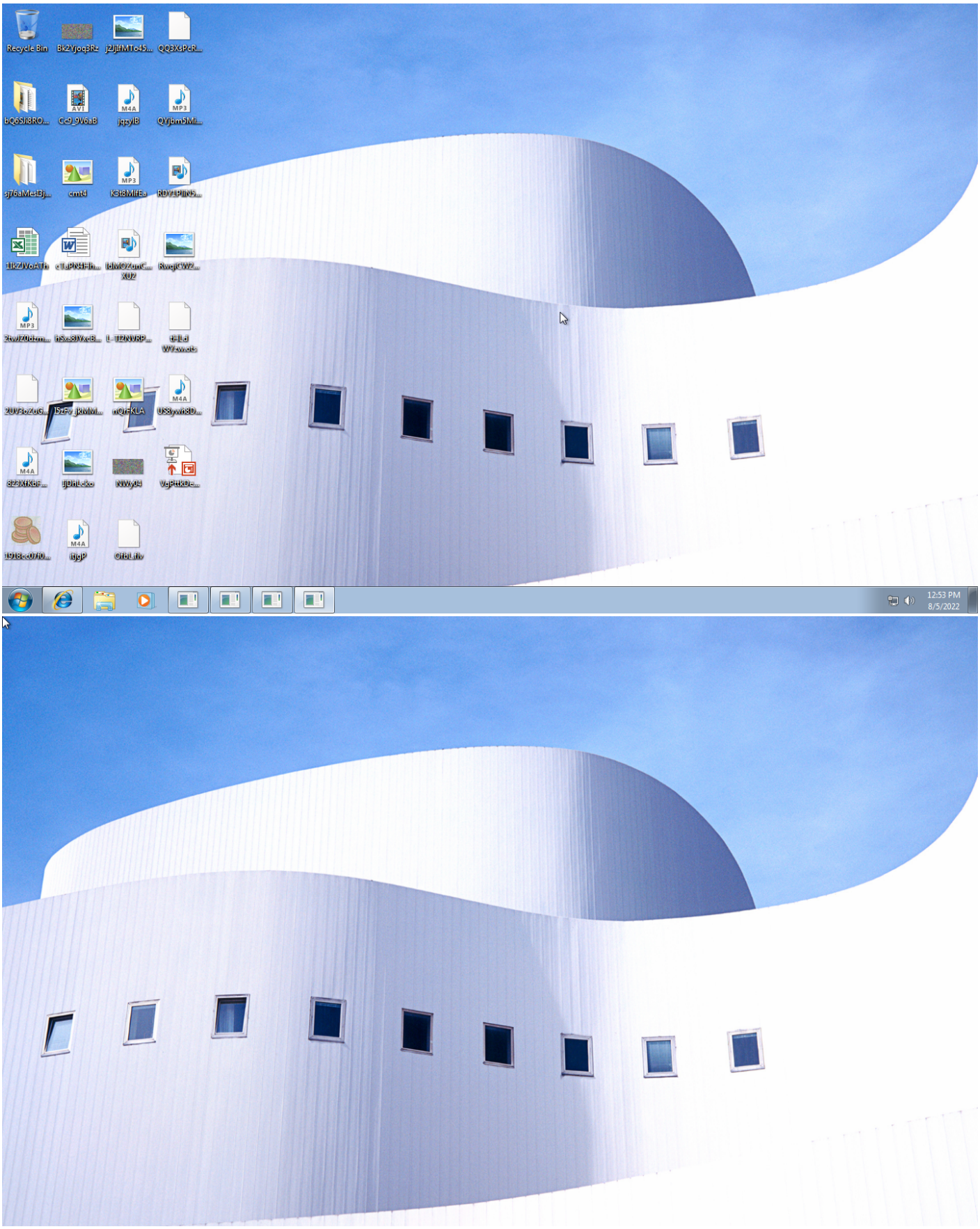
ID	#5067640
MD5	28fb096cbce32cf1f87719254452014f
SHA1	50ceaddc379e1376a579e4c9d4465fd3c734c277
SHA256	1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98
SSDeep	12288:+5v3qTuu7zbgLsSFKUilhkehB/MLfSTOIPAU+dmb:+5vo1SogidMLZHmb
ImpHash	52981a63110ae9001dc5c79717e57d47
File Name	1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe
File Size	730.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 14:52 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	7
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	282


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

128.71 KB total sent

573.91 KB total received

4 ports 80, 443, 53, 445

5 contacted IP addresses

0 URLs extracted

3 files downloaded

0 malicious hosts detected

DNS

5 DNS requests for 3 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

4 URLs contacted, 4 servers

6 sessions, 7.60 KB sent, 481.27 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://acacaca.org/test2/get.php?pid=DEC2E953FC80DE582D412ECFEAA51D7B&first=true	-	-		0 bytes	NA
GET	http://acacaca.org/test2/get.php?pid=DEC2E953FC80DE582D412ECFEAA51D7B	-	-		0 bytes	NA
GET	http://rgyui.top/dl/build2.exe	-	-		0 bytes	NA
GET	https://api.2ip.ua/geo.json	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	api.2ip.ua	NO_ERROR	162.0.217.254		NA
A	acacaca.org	NO_ERROR	190.219.54.242, 195.158.3.162, 41.41.255.235, 190.117.75.91, 109.102.255.230, 138.36.3.134, 58.235.189.192, 211.171.233.126, 109.98.58.98, 187.212.206.176		NA
A	rgyui.top	NO_ERROR	222.236.49.124, 190.117.75.91, 46.195.219.190, 211.119.84.111, 187.170.251.250, 151.251.24.5, 190.107.133.19, 109.98.58.98, 110.14.121.125, 115.88.24.203		NA

BEHAVIOR

Process Graph

Process #1: 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 57856, Reason: Analysis Target
Unmonitor End Time	End Time: 73545, Reason: Terminated
Monitor duration	15.69s
Return Code	0
PID	3808
Parent PID	1916
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	730.50 KB	1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98	✖

Host Behavior

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

Process #2: 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 69830, Reason: Child Process
Unmonitor End Time	End Time: 95938, Reason: Terminated
Monitor duration	26.11s
Return Code	0
PID	3816
Parent PID	3808
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\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xee4	0x400000(4194304)	0x400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xee4	0x401000(4198400)	0xca600	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xee4	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xee4	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xee4	0x52b000(5419008)	0x200	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xee4	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xee4	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xee4 / 0xeec	0x76f101c4(1995506116)	-	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	730.50 KB	1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98	✖

Host Behavior

Type	Count
System	4
Module	47
File	6
Environment	1
Process	101
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\4d45d74b-b67c-4b05-9c99-9061295dc2fa" /deny *S-1-1-0:(OI)(CI)(DE,DC)
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91518, Reason: Child Process
Unmonitor End Time	End Time: 94253, Reason: Terminated
Monitor duration	2.73s
Return Code	0
PID	3856
Parent PID	3816
Bitness	32 Bit

Process #5: 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 93550, Reason: Child Process
Unmonitor End Time	End Time: 97677, Reason: Terminated
Monitor duration	4.13s
Return Code	0
PID	3872
Parent PID	3816
Bitness	32 Bit

Host Behavior

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

Process #6: 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 96028, Reason: Child Process
Unmonitor End Time	End Time: 118062, Reason: Terminated
Monitor duration	22.03s
Return Code	0
PID	3884
Parent PID	3872
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\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xf24	0x400000(4194304)	0x400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xf24	0x401000(4198400)	0xca600	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xf24	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xf24	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xf24	0x52b000(5419008)	0x200	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xf24	0x52c000(5423104)	0xa400	✔	1
Modify Control Flow	#5: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xf24 / 0xf30	0x76f101c4(1995506116)	-	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0xf24	0x7efde008(2130567176)	0x4	✔	1

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
-	360.00 KB	97edd7cae37d3c44a353b6cad0258ad6c8d2fcace03cafe01556f57a3296fa57	✖
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	53
Environment	1
Process	99
Registry	7
COM	1
-	2
Mutex	1
User	1
Window	1
-	3

Network Behavior

Type	Count
HTTP	2
HTTPS	1

Process #10: 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe

ID	10
File Name	c:\users\keecfmwgj\appdata\local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe" --AutoStart
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 165274, Reason: Autostart
Unmonitor End Time	End Time: 170969, Reason: Terminated
Monitor duration	5.70s
Return Code	0
PID	1784
Parent PID	1604
Bitness	32 Bit

Host Behavior

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

Process #11: 1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe

ID	11
File Name	c:\users\keecfmwgj\appdata\local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe" --AutoStart
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 169772, Reason: Child Process
Unmonitor End Time	End Time: 205776, Reason: Terminated
Monitor duration	36.00s
Return Code	0
PID	2012
Parent PID	1784
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0x6fc	0x400000(4194304)	0x400	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0x6fc	0x401000(4198400)	0xca600	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0x6fc	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0x6fc	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0x6fc	0x52b000(5419008)	0x200	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0x6fc	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0x6fc	0x7efde008(2130567176)	0x4	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#10: c:\users\keecfmwgj\appdata\local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	0x6fc / 0x7e0	0x773101c4(1999700420)	-	✔	1

Dropped Files (207)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Documents\KUOP p2txHoo7bw7O.doc.vvyu	88.46 KB	dd16c6cf030e9120cc5f22c03fad7f4fc2aebe40b7afdef359c09898e8233b7c	✔
C:\Users\kEecfMwgj\Contacts\Administrator.contact.vvyu	67.11 KB	189ce1328b0e29a96efc189c17f247d714db449e274cc27996b06310feb5a733	✔
c:\users\keecfmwgj\favorites\msn websites\msn.url.vvyu	467 bytes	ada8bf2d4229e81809df4d559e8c18bab15cacd00fae3ea23f0d8d35a29bb4cc	✔
C:\Users\kEecfMwgj\Documents\hhuy\z99M8Y1GRoOyuotMz.csv.vvyu	59.06 KB	33a5d2d01e3e1967691b0ad91f3a61ee69d04651b32d352f3d27b6964182aa60	✔
c:\users\keecfmwgj\videos\z2e0zt\zpv7u7xpwr7qk\rfes3vfwf3fsy6sx.flv.vvyu	4.92 KB	3a96aeabbb0bcc7e73a5475c7dbffb6a6e57faf08dd398da1fc3124a1c8f6d38	✔
C:\Users\kEecfMwgj\Desktop\itjgP.m4a.vvyu	61.15 KB	4a0259c4686b41ea148ea36359d434885a71896d29dfbab0363e4183679371ad	✔
c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\6pw8rpgl-.flv.vvyu	38.90 KB	4a5d3bbc254ba37617c064f3848973257ffb69f97d6a7acfa39495a395116056	✔
C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\GW5kXQqybZPUP2d4.mp4.vvyu	69.76 KB	f4e2ca8796b7629bf2896c3a9ca12f37221ea6e3de37c093826740436d260cbf	✔
c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd- y4\tlaiuy5vumxfxacjn.wav.vvyu	10.79 KB	30350606cbacceac12eb6f37740f6a83bdf68b9c781b27a1af1d3dff5731d62c	✔
C:\Users\kEecfMwgj\Documents_3Wl5D4o0g2MKtP.pptx.vvyu	95.94 KB	894900d80f9b5abb5f40cb8d86378e79a8baca261d84080d33c1d3adec251725	✔
C:\Users\kEecfMwgj\Desktop\bQ6SJi8RO0rg0dP\3YgFUJ.rtf.vvyu	77.06 KB	f7253ca681f4ebde608a638e09e74549c7a6f17eee224e80c092dc5584eb3378	✔
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\ilfMhH\5DS0X1cGBS4n2igZsE.jpg.vvyu	70.97 KB	d9e8b6ff7ef08432ad9dea072b65adb94dfe85fa2bbf1ebd9db9dd23891a963d	✔
C:\Users\kEecfMwgj\Pictures\bQiz44uQ681_7Dctbgxp.jpg.vvyu	52.25 KB	473b7e1ba2117efc27a7ab5b524f2419ed8dd844ab566a5de159df24238b25ed	✔
c:\users\keecfmwgj\music\nmf9emihkrld8q1qs.mp3.vvyu	46.34 KB	4fc5c0fa864d6d3beece05a148cac43dde53f5fcf22b6a7e40b0dae4a44abcb1	✔
C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\cPfFJ9.flv.vvyu	39.58 KB	402cc932665b1145dcd00036df7ef0b335ba87097cb180387a4cec8290b6eba2	✔
C:\Users\kEecfMwgj\Documents\567c.pdf.vvyu	71.37 KB	b0472978a35878ca65dceb2aa8496916b7841b9f06d0a93b9b99dad64926a3af	✔
c:\users\keecfmwgj\documents\hhuy\bju5iwgzcivxdeaczva1.odt.vvyu	33.26 KB	272054bacb696311cfcaf3a321598a2d58bea81987481db3066179cbd5dad608	✔
c:\users\keecfmwgj\documents\hhuy\r fixnl1vu2.ots.vvyu	97.71 KB	734ef8197eae32ebbb05699038caf483c845cbc3ac184134aba9a2b0e7bf6a08	✔
c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\tkvyxwxrq.ots.vvyu	51.04 KB	5706a0a0883c3c6e646f5dfaf7ee9da761f6d6b657b80683bcabd47f393c1df6	✔
c:\users\keecfmwgj\music\olz6-jxmw7o1_h pvu.mp3.vvyu	7.53 KB	f9025e0e638cb18ca29f908b3d546390fcf8a11fab885c0d9f47b1b5b3e81d02	✔
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\yOmL -Z49fyb2lF7S9.png.vvyu	62.03 KB	398641fed9d5bc3dbe6b22bf875cb4c30ccc30d631ceaa4edbbc4acd86dfe9cd	✔
c:\users\keecfmwgj\documents\hhuy\ni1u7vxc2c n4uuhwh.pps.vvyu	22.70 KB	9d5fb3099874edd6728f924b78426d4e31624f43743605e20f012733e91b1ded	✔
c:\users\keecfmwgj\desktop\ijdhlcko.jpg.vvyu	66.40 KB	e72f727e0d057036134db697d330f38b8a4d9f5b6454f34ef3267450831f393e	✔
C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\uo7bfSHfyn-0X-MGd.bmp.vvyu	32.13 KB	031653457cec31d0795db170a5ae8756df32b9b422ed9091e222157b009d5a8a	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\desktop\bq6sji8ro0rg0dp\9ecwyh_e3fhju.avi.vvyu	55.57 KB	4e3e305fea79f1d263eea98d4c12a6f087e90331e47583fa2cb2dd693637c0a7	✔
c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu	467 bytes	5bc5ad5410f105ab9b5b25d0b3205680d06102698d2ec7ca554b6d66471a97a9	✔
c:\users\keecfmwgj\desktop\rwqicw2qitxlv4.jpg.vvyu	98.99 KB	19d28ff75492c000f8716c68e61927b887889033b1ce39304af98b47a6b740f4	✔
c:\users\keecfmwgj\favorites\msn websites\msn autos.url.vvyu	467 bytes	431a2acd28946a4b81df1a044fc57216ec54ee63a2a30acc09d1ab7f842ae0aa	✔
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\iIfMhH\9VRBBaa2E6cjsKGlie.gif.vvyu	57.00 KB	587e04449979b37f0d657abeedb66fbf094cf763e822d82851ce19de6a640db0	✔
c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\ksif.bmp.vvyu	95.24 KB	0e9e1ecb02e3e22046bca615aa88befa7dc39d8c7b18d2d0540ef51c83c55107	✔
C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe.vvyu	730.83 KB	43e2fa29b2173efa491920ab2126a6fe80628f224bb99f438bfc8d3eb4b48cf8	✔
C:\Users\kEecfMwgj\Documents\hhuy\U-GFPMIYoqWy2p9O.xlsx.vvyu	73.96 KB	9a396177cf04e8618d596aa98ed6d6ceec011568a1cda6bd98ecac5f2630f1f7	✔
c:\users\keecfmwgj\music\mxrqwfqcp\jze7xrus.m4a.vvyu	10.25 KB	d2a131213503fe81fcf49936d2feb8f36988a49a0327ab408c599ffb4d84871c	✔
c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\ydph4cpxgp3qwyuc\aougfr90ajw.jpg.vvyu	10.75 KB	1659c743af76e49d9fe13b2c559befbe3806dfd0defdab394c73ff944cd7ec3e	✔
c:\users\keecfmwgj\music\bjhxlx\cmbsppstlrb9u.m4a.vvyu	91.81 KB	47c07be7f50f3099f127c92737a9a8fa3e3595a060b5711b94e4132480370b5c	✔
C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\s_e2a5ScpFSgR9-.mkv.vvyu	74.79 KB	fe13edf5fc531caf016cd92328bbe438fd492d8276e1e5728c59d995f6fe6e04	✔
C:\Users\kEecfMwgj\Desktop\tHLd WYzw.ots.vvyu	24.69 KB	218daa75779284fe874259f4ec8d88a9b30ac8a2d5404216931b8964a4de2748	✔
C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkl\HbqLBzpGm.wav.vvyu	18.22 KB	b281c27a359981a22e3e5d044e1d51c0d355e2a2a51996c8545a6da246bbc3f7	✔
c:\users\keecfmwgj\favorites\links\web slice gallery.url.vvyu	560 bytes	df9020a2c2c61fd4b7da8475ac6321dba9338a0f060014f7c35b05daeabefcc1	✔
C:\Users\kEecfMwgj\Music\BJHxLX\KnG7feMIAKlEoa_UW1s2.wav.vvyu	81.21 KB	ff7ac932d26acfe13c4214d7fa81a0a2c48b05ddee9a009adfd28f5634ec9ce9	✔
C:\Users\kEecfMwgj\Documents\6LeN1-BfLiBS.rtf.vvyu	72.11 KB	7d4224f630e4938d9839ea653d0c408b0e876c7a6f7ca99ace46048af29bc1a1	✔
c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\wa_4pk0l7jwgqv.xlsx.vvyu	20.93 KB	4e1697043b6c8a655e7d03c9b93966105bcae8947f449e86ab3a6d085a236a5e	✔
c:\users\keecfmwgj\documents\z1niztmoyavazpqq.rtf.vvyu	21.56 KB	d5029c9c174733b887d9ebc9443dac72ac13269412780a53fc840d34ce0b4846	✔
C:\Users\kEecfMwgj\Documents\CzDS-.pptx.vvyu	20.72 KB	e0cdb066c7e3d5b202ed26ace83f3a939ccabbb07338b465ed01787a82284977	✔
C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkl\6y-Gle7CJ.m4a.vvyu	25.63 KB	551247baf79c97d9c25b46431f8df0905b95d21cd64d46c4735dc51d99be1fb0	✔
C:\Users\kEecfMwgj\Documents\hhuy\Qs2 hK9Y_.xlsx.vvyu	6.67 KB	caee0f4bb79e2b319c8593e45942d5ee8ec47500154e23519af9fee1f3a42977	✔
c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\pfzhnu297.png.vvyu	2.79 KB	3fa2646c6675f671dcf30d8b03ac854945fa419820a7408da09bd02540c9b30d	✔
c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd- y4\-ahhgkvlxn_kxd.m4a.vvyu	12.87 KB	7bc5f125a7a2970d7a7a6bac90320a6d81c29519280ed4bd54b591fdc066d9c1	✔
c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\ydph4cpxgp3qwyuc\x5tjkqt17l1kq.bmp.vvyu	24.73 KB	affbb7b542bcde7bb2fd1749df331ad470edfe50811147945c1794a9efa50e6c	✔
C:\Users\kEecfMwgj\Videos\hDvzuhrdv.mkv.vvyu	60.07 KB	6c5bc57525cd6e312a1f9a5b4c964407dc9b385163c7fef389aa2eedc7a315c9	✔
C:\Users\kEecfMwgj\Desktop\nQrFKLA.gif.vvyu	74.63 KB	2c9f90f7e9f2022f19782b0c45f62bdb61ce24d50cd9f5de2a8ffb1149491b33	✔

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\K3t8MIfEa.mp3.vvyu	12.73 KB	34d05b8778caf4770e09de8c2f66263f24b39b49e7bdfae7c4ace5a378dacc40	✔
C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\rQja5oZ7_uz\EhqiUu8LgIRl.mp4.vvyu	48.46 KB	dcc8ca54190953aaebc4920bd37bed47d28c783721a56af3a6c3e0be8fb008d8	✔
c:\users\keecfmwgj\videos\z2e0zt\zpv7u7xpwr7qk\iwi4py9f_tbuupcdk.flv.vvyu	24.45 KB	683d69769675a2aedc9c9ed5d3b236d63e388d6c32d6301fc9633e3c94b1ac0b	✔
c:\users\keecfmwgj\documents\hhuy\naiaggm8s5tskx.docx.vvyu	57.32 KB	0933f9d1a069169a47534b6338c052bc5f380172aa2171d446e0f359ba81ea3f	✔
C:\Users\kEecfMwgj\Desktop\cTaPN4HhRqe86tN.rtf.vvyu	3.34 KB	2222e65f4697f4a89deed2906b732f3fabb9d8887c6456e6f308e8cd7f84a3eb	✔
C:\Users\kEecfMwgj\Music\mXrqWFqcp\-xht.wav.vvyu	3.51 KB	c1aa0df3912ad585cdc48d7de4baaf09ff6597a32f052f5bcff2ae9490594569	✔
c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu	467 bytes	ae90c3e73ad1bf03b16c5c76379a2eac7cb37ecff753676a001c0dba8ebc934b	✔
C:\Users\kEecfMwgj\Documents\2oZu1wT.ppt.vvyu	8.98 KB	a07d0d82086b969b45bcad0383ed3899c4e9da6f8ff929634be61937acba8255	✔
C:\Users\kEecfMwgj\Documents\4l3gkybFjpw5wc.rtf.vvyu	6.57 KB	2b344bf7c2c0903367a4b6d92bb583f455b20c351e365bed92e2c4bb26550977	✔
C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\2j2l02AsmvpG-FW9.gif.vvyu	31.12 KB	06acc0feb751caf85f859845100bb0ed467d42a24136312ba453f058494b6ec5	✔
C:\Users\kEecfMwgj\Music\BJHxLX\dTVoZ bX824b.wav.vvyu	70.05 KB	ae5df317d6203597bb87fac899165235a5b9c060af95fb80da16b4501223dea9	✔
C:\Users\kEecfMwgj\Documents\4COwR1C7ya7.pptx.vvyu	52.76 KB	966f24e524cc4d24ef763e63db468aac00e7d7ee6cc7b399fa57ed5060ecf270	✔
C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\0jip-0WU2n5fd8 POL.bmp.vvyu	15.81 KB	f0a5f7e0d9d9659ddd6a04ee59fe3f336bae267a6366ed674b00d00566285ffa	✔
c:\users\keecfmwgj\videos\z2e0zt\zpv7u7xpwr7qk\1l1mbixtedk.mkv.vvyu	7.04 KB	24864d0dfa284d80d5013e818bccbfd5bafc17f110edfa2f73b00e121e44b4ee	✔
c:\users\keecfmwgj\desktop\ldmozuncs-h9r3 xu2.mp4.vvyu	96.31 KB	26bc3a8b110a24b3c1a4cec04f25c2c9ab887cbdd16ec226367fab86a952707b	✔
C:\Users\kEecfMwgj\Desktop\cmt4.gif.vvyu	85.31 KB	b3390fd47b8fdfb6dad0061e5eccab69d90d1677277f0924dbd4a0290d568011	✔
c:\users\keecfmwgj\appdata\locallow\microsoft\internet explorer\services\search_{0633ee93-d776-472f-a0ff-e1416b8b2e3a}.ico.vvyu	4.51 KB	4f8ed28f94accb436273bd2853d4b192bd631c2529ed2c970b8924f0dee8c74a	✔
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\v97V_KMwmgn4h6UDx.jpg.vvyu	40.53 KB	22cab0de91bf4e982352fef696c6393dad443f3f0d4d2b3019d736a2e4a453ec	✔
c:\users\keecfmwgj\documents\py_fftiab_q4nwhp.docx.vvyu	47.11 KB	83c5ded689b4ac46b6bf7f6c7555077c8ebd4f0902175f81a9987bb801e789d0	✔
c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\dtf66.png.vvyu	60.53 KB	69ff7fc1c062ba60f4d18039791853b3ef4da52e950d2d216758e7d5e89908d6	✔
C:\Users\kEecfMwgj\Pictures\O_9gyTeSlm.jpg.vvyu	77.50 KB	932115bf58ba9bcb34992a979c72196903b6f65911293583c7afa3be6ba241c0	✔
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\la08fq2wwngfs3w9kc.swf.vvyu	9.14 KB	8a0a52c012403823d23a515418dbaa5474e4d98539046c53de721526a25eb13b	✔
C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\MpjP3oSTE.mkv.vvyu	38.09 KB	c341873e0b4eb668af30cbb4b510722c6f1e9d1d0f27486f904c4fb5284b40ab	✔
c:\users\keecfmwgj\favorites\windows live\get windows live.url.vvyu	467 bytes	dfda77095c6a5eebb782e5445fde3e9dc05cf0df896c470503e135c6d3042676	✔
C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkl\a6C7l-Qq0p-ecvc_8DsT.wav.vvyu	74.36 KB	49f92e8c10a3de7e7f811559aeed142c4be052f7ca8c5bdc07d9d5445ab0736c	✔
c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd-y4\02rh90y7rebgxw.mp3.vvyu	37.27 KB	1e1b65b403d02636a3dd2bd42472d70bb97b087f6eb172e8eb0ec641cd53ed0a	✔
c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\5qvh55h.bmp.vvyu	59.72 KB	f1c47080665973de4ad0c37caf724f6deccd62df6cd08bf8a5115f24970c74b0	✔

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Pictures\n-nH-E2t.jpg.vvyu	63.23 KB	20eeb5c1f2b0a1dee443455087c3eae5fb5d3146968438700d13573056b6fe06	✔
c:\users\keecfmwgj\documents\hhuy\ynkbyrnkc6j3avv0zier.odt.vvyu	77.12 KB	ae7cd6922e5ae781bc6e12153af1c7ce9fd171a8b2880e6d57639d0afaefe76c	✔
c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\lxhmd.gif.vvyu	48.09 KB	953147e287a78bfecb52fe75299e5476e444b4e2efe37e6dc8f819a80252fe2b	✔
c:\users\keecfmwgj\desktop\i5zfv_jkmmjeubuqus.gif.vvyu	73.80 KB	74ad2158105670d3d103792254e93140ae903c1e0114240622972be2c21ef46f	✔
C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkI\GWrBK8mbOy.wav.vvyu	96.55 KB	dd04e553681e1090342e583ea5b3d6cac4bb8080c9b945e5af237d3d2651215e	✔
C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url.vvyu	467 bytes	5151cdaed76855740daf7e161bf28e5e1ff6ed9a3663a8778e62bdf0359c6135	✔
c:\users\keecfmwgj\documents\qtnn2gz.xlsx.vvyu	6.25 KB	f0e4d02e00c369d7ac1140c0cb106da5965ed3ed638fd117d27fb7ac4d8bcbd0	✔
c:\users\keecfmwgj\documents\hhuy\ytkydbos.xlsx.vvyu	29.81 KB	44eb9a0cb89c4b01a074b442f898c773ec537f517680c9a80036079bea4151c6	✔
c:\users\keecfmwgj\documents\outlook files\franc@gdllo.de.pst.vvyu	265.33 KB	4e457d70005729d8a9ae7d73ee3ab80c0b90f866c736819b7949d0b1d8ec4657	✔
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\b8gbt7knns9kt-gvh.swf.vvyu	42.99 KB	bc826210d063edff1db9570c195b4de4b7311d6317514ec63305d354caced0ef	✔
c:\users\keecfmwgj\desktop\hsxa8jyxcbsx17ja94r_.jpg.vvyu	3.73 KB	29cde7f05caa158e25cef5b613ab7b46b85ed1639f5b849a0864beb02fee6d9d	✔
c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\xudjwurucylo9.bmp.vvyu	75.70 KB	6cbc00787537559f670d109ddbaf36dba25ab0ac36a6665d8ddf262ec0da4e73	✔
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\a9pzarvgiar.avi.vvyu	54.89 KB	94cc6553591ef38ea49a01a39b8f4aaf2ce6c476f6ad674f0140117168662cc3	✔
C:\Users\kEecfMwgj\Documents\D1q0P.docx.vvyu	95.20 KB	1ab9b3b0544f96605222a450f98775bdc9b110e24e670a57c9f5a6afee3424b7	✔
c:\users\keecfmwgj\desktop\us8ywh8d_vcxiyfIf5e.m4a.vvyu	83.19 KB	c2732e2c403c3584d9828b8e7eed28051b09dac3e39a17b619030c6dc1cd4435	✔
C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\Asv9iqUaFA9rCWFze77.avi.vvyu	34.75 KB	c10930d37153c376e658f390097b51273e00f861524d454c21fe7727db4b3ae6	✔
c:\users\keecfmwgj\desktop\nwy04.bmp.vvyu	48.71 KB	cbbd6523c8d8173884e5778785b089ba0462f1562efd4670af7cf7efd46fcf86	✔
c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\ghprnga3a e4cboqmI8u.bmp.vvyu	54.01 KB	26f062dffa9b5852550bb31e36b1450e5a66f1250a9e669a9ba00fa97dfe9485	✔
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\kvyeo7pecdl1br27xvac.mkv.vvyu	26.65 KB	5e677e2368f0dc4d5a9e4e52aa37c5d51d40f5171eb97ee1a2904492f74ffeec	✔
C:\Users\kEecfMwgj\Desktop\Cc9_9V6aB.avi.vvyu	15.56 KB	83e1eaf04ef012175c3b4d16caa1ba50f00e814c7613c2a369cb050e35fab522	✔
C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Spaces.url.vvyu	467 bytes	c6fc229e5cfa5de6c5a49a6b993c64cad23277e507522ee7e05794ef4e5bea79	✔
C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url.vvyu	468 bytes	93d6488fcd9eb9f990339766fa9af4859d540503defbe61901a08f5279973414	✔
c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\ydxrjd.png.vvyu	10.72 KB	a7799c84303d1eb3a00371b037fa9a21406abcb760390390665d8e8922072e71	✔
c:\users\keecfmwgj\music\mxrqwfqcp\xxli1eqxvup5i 0hs6g.mp3.vvyu	91.12 KB	e6779d99f703a7c0b189700d09d968bc211838bbf884bc397a5a9760b1ada314	✔
C:\Users\kEecfMwgj\Documents\tPG-9VHK-uIBZI_Q.docx.vvyu	36.86 KB	2bd4c98884d4f3f10e932e7f7419880103a5cc594c9b2babf4b89f18e3353e85	✔
c:\users\keecfmwgj\documents\kw5j7a5.doc.vvyu	14.59 KB	2cf37d0ea9153599981d4767fddf3c7d3562debf4c192356937f9b5492d0a918	✔
c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\rqja5oz7_uz\kyIqcyn6yv.pps.vvyu	24.06 KB	98bc19031aba4f2a2e5e7866d548e2c1a0405187d451d734b3fcb7763197b03a	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\music\bjhxlx\rp0gg8vjq4u.wav.vvyu	12.34 KB	3203988b9bb84611e18fef6dda137b9aa1fc2407b90282bc464a751d18745a7c	✔
C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE Add-on site.url.vvyu	467 bytes	29827d39c616954d9ca8880f87298a2992d95088094fb85ad5565d44fa581899	✔
c:\users\keecfmwgj\desktop\2uv3ozugwqu6cyc7-l.swf.vvyu	42.88 KB	84d109fcb39e5c9e2eee3f272afe11bbc73536b99852eb3843b59ad813bb10c8	✔
c:\users\keecfmwgj\documents\jw5nfujdo04vpw2wo.xlsx.vvyu	54.02 KB	b9577300fafe21383c57d0a403db16b42c6c55397a6b628ff440aa833c226813	✔
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\mmfu p.mp4.vvyu	69.69 KB	4938142520f2d0df614ea3a0fe14d92ce75f5d3dcaef23e24f2669fa2cc4ac16	✔
C:\Users\kEecfMwgj\Desktop\1lkZJVoATh.xls.vvyu	12.96 KB	22e0a45a8d96ba56e8215c4eff6b0bb9ab61b65076db92fb455362aee5d13234	✔
C:\Users\kEecfMwgj\Documents\HeOaqMZgOojF528t.odt.vvyu	20.29 KB	c6063f8ff1234e5ff2ff84d7a8a935f9385576f1bfe8f919115f036c3c3aa51b	✔
C:\Users\kEecfMwgj\Documents\hhuy\jkSu2OlxWSDLnSWvMq.ods.vvyu	20.87 KB	117e8aa24da97662e538061d49200906d219627f014f7f96e52463afcd317a85	✔
c:\users\keecfmwgj\documents\dnsctzwstnyxbfiqs.docx.vvyu	94.21 KB	5cf384e0c5df07debe12dd305331620f942286060f018eb48ae5b1f126a6e48e	✔
c:\users\keecfmwgj\documents\t_ciyr3b-hwvi5yqwu4.ods.vvyu	19.30 KB	9cb7ca045088f7172bc860b812e6d02c2aba7ee1832a06790c021f67d072565b	✔
C:\Users\kEecfMwgj\Music\mXrqWFqcp_fBV4xgh8cLcTD-y4\hyXqTEnB.mp3.vvyu	92.68 KB	cf306f60e0a6604664afbce852bb202423267d27793a22f6ce0431dd1331a13d	✔
C:\Users\kEecfMwgj\Documents\hhuy\igCF Ho.ppt.vvyu	2.84 KB	5c62fab79ef97e057b0efdf47489e69f77005ac18bb76693e11a376e3c0d3393	✔
c:\users\keecfmwgj\favorites\windows live\windows live mail.url.vvyu	467 bytes	7db1cc7be21c6fd3d8be577e018d48732f2f9688ac5cfdbeef5cdd2fae54ec79	✔
c:\users\keecfmwgj\music\p5fl21.m4a.vvyu	19.65 KB	9d830dbe0d6bea424858222e52412ea02be27188d9c0be176c7b316823f722eb	✔
C:\Users\kEecfMwgj\Music\esAg2qtf u0s5C0MdPd.mp3.vvyu	27.15 KB	0ae13493b821c8e167d4848f2fbc58597b9d0d2448d34621439c68d0adad5389	✔
C:\Users\kEecfMwgj\Videos\SipikwOFNhn.swf.vvyu	77.00 KB	da8d2596f75483b55e9640f377db386b08c9c1d49dbb64c3fbc669f1040e5894	✔
c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\ae6i4hslrl.png.vvyu	26.18 KB	2950d9152b926628ef5aa29842eb390f55d201a7d74dc434ce2fe259001ca185	✔
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\yDPh4CpXgP3QwyUC\BY rE6U_U.png.vvyu	98.47 KB	3d0ed30d88e085ee7fd4ff018895822c8b64923b4cdd0be79fcb51203a1f2986	✔
C:\Users\kEecfMwgj\Documents\J0ThFcHeulkvK.odp.vvyu	53.63 KB	796990a3ef36e55c9e0aa25e8d865524ebc9d2ce8fd2fb0206fb3f00974ef95c	✔
C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\Tb8Pl4n8ykiF82PGQ8M.mkv.vvyu	93.10 KB	76fd10d1bea5437e13882d4150a3364c890e50a44ac9f60a78d435a1f1427f7b	✔
c:\users\keecfmwgj\documents\dijvxxa4.xlsx.vvyu	60.98 KB	afc00fecdb6a78c005c4b6ae77d042e9087f6b37ed369fc705eee83bc528c94c	✔
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\qq8tjsc3zm363.avi.vvyu	71.75 KB	939063d5a04e87026528b13059f37588d42f825ebbdfe29de88f9c8530b3dab6	✔
c:\users\keecfmwgj\documents_dmv92xp.pptx.vvyu	97.36 KB	0604e4874fcd90a1f4608dc3b74b28f66beb3f9104c5142a5419659dfcd8c0a7	✔
C:\Users\kEecfMwgj\Documents\hhuy\84p7mNA.doc.vvyu	32.60 KB	dec7037f2a106264a712825d6c6f23f88faec2a6d98d9fb0925e08bfba2fa156	✔
c:\users\keecfmwgj\favorites\microsoft websites\microsoft at home.url.vvyu	467 bytes	cf483a969ffc9707e39d04db5290a782ac96113eb679a04c0371ddb7fedf173f	✔
c:\users\keecfmwgj\documents\dygx.docx.vvyu	36.62 KB	b3283031ef4e07b92cd8d8cc6edd1f381cfd8df16a24dc1e0f1fe69ef6aff5c7	✔
C:\Users\kEecfMwgj\Desktop\QQ3XsPcRg.swf.vvyu	17.41 KB	3554860d3b4569052bb6593c6a9fedd8b40c47360641e884b62935ef1370c2b0	✔
C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\MHkDGPm.avi.vvyu	79.42 KB	2fd8f9383b9d83da87a53212e2a07534defaf86d51e6a13039bcfd14547de15f	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\pictures\77x _hi5d64n725my.bmp.vvyu	72.71 KB	5d98db98908ae2bbc97310bf25f5f4cef5fc7d2b25386cd1d511e9233cdd24f0	✔
c:\users\keecfmwgj\favorites\msn websites\msn sports.url.vvyu	467 bytes	1b7b9b22feb875d3cdda47672d7b4f783db75eb830f13a95fada199fc92487a8	✔
c:\users\keecfmwgj\documents\zliy3__ym6-.csv.vvyu	26.86 KB	cb626ae27f909a6c9cc93b949fde179166664a459b34afe6f8ba78c76eebfb4e	✔
c:\users\keecfmwgj\documents\hhuy\4q235s.pptx.vvyu	89.27 KB	e15ad4c8665f0b19cfa961fbcb9f9ccc40079f1f1f68f6be8428613576cd82be	✔
c:\users\keecfmwgj\documents\5h1grurzazne.docx.vvyu	61.67 KB	72f17a8ec6bc5334199fa842bd6d3c657b556df651a464dec70f86d29421a403	✔
C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK_qbp0nkGuotBuAqg\le5lbJNFps_4_oZKKr.mkv.vvyu	94.30 KB	25d3a545346e087cc462ac0c51a3b80a296ff40a9f3566265bee8ed94a950267	✔
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\8fbu8gjzxgn5dwk.avi.vvyu	67.59 KB	fbb291d250f035ce19eb70047d834c5eb9bdca314956acf364627d6c6d952aa8	✔
c:\users\keecfmwgj\desktop\l-ti2nvrpacp-tk9f.mkv.vvyu	23.31 KB	26d09de29cdfa13ba6d732474cdc30e57dad5c432c617695bcd0e7fb6a787df5	✔
C:\Users\kEecfMwgj\Videos\z2E0zT\g5znGT5HIbHq.mkv.vvyu	5.80 KB	1274234ccfb42ab981e5e904d22bea55053d9228c2ae30ea0a1336369ff28f49	✔
c:\users\keecfmwgj\music\bjhxlx\9ast-p\fgnl6u1fsaf.m4a.vvyu	75.18 KB	5b0f36a34235821a0b79750580442625522bb40a0d7a0047e2a8952a5ce3f1a5	✔
c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.vvyu	467 bytes	80c908b15e82bdd617fc2c181a5ba6c7ccd1ef128b7b67609611b02d7430e30c	✔
c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\rookllxyjwewp5im.wav.vvyu	51.11 KB	ff5ad71681777fea75e0a0c76694567e9fe80d1dad5c999ed7e7aefb7872b3b7	✔
c:\users\keecfmwgj\videos\k0zmij7sn.mp4.vvyu	69.21 KB	16b1bdacd8365ae8579d9bcf6ae7325fa7192be7b0a76d699aa6d79b9d7d21c1	✔
c:\users\keecfmwgj\music\bjhxlx\fwxn.wav.vvyu	55.56 KB	f3999a50dcdfa0954405763466b511bdd2e0b6ee87f7ebc5b623f7fa0fd113f9	✔
C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mzar\k_XON6PdpszzEOE.bmp.vvyu	74.87 KB	63b14b1553b3bd95b4105ac0d3ddd48dd3a423862cbb46bf869ecd6bd42dcaf6	✔
c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\ydph4cpxgp3qwyuc\irzpaayv6fb7p4.gif.vvyu	20.58 KB	c0ca45d13a7a69ca1d02a7d70ad2fcc382d1ffe75be2563bd979b0f05de38a6a	✔
C:\Users\kEecfMwgj\Documents\HbBtrfj.pptx.vvyu	87.23 KB	5094008edbb19192bc1cbaf1881b664ab386893854576de296a2d59bbe2a4769	✔

Reduced dataset

Host Behavior

Type	Count
System	287
Module	185
File	2510
Environment	1
Process	54
Registry	4
Mutex	1
User	1
Window	1
-	4

Network Behavior

Type	Count
HTTP	1
HTTPS	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
dd16c6cf030e9120cc5f22c03fad7f4fc2aebe40b7afdef359c09898e8233b7c	C:\Users\kEecfMwgj\Documents\KUOPp2txHoo7bw7O.doc.vvyu, c:\users\keecfmwgj\documents\kuopp2txhoo7bw7o.doc.vvyu	Dropped File	88.46 KB	application/octet-stream	Access, Create, Write	MALICIOUS
189ce1328b0e29a96efc189c17f247d714db449e274cc27996b06310feb5a733	C:\Users\kEecfMwgj\Contacts\Administrator.contact.vvyu, c:\users\keecfmwgj\contacts\administrator.contact.vvyu	Dropped File	67.11 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ada8bf2d4229e81809df4d559e8c18bab15cacd00fae3ea23f0d8d35a29bb4cc	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	MALICIOUS
33a5d2d01e3e1967691b0ad91f3a61ee69d04651b32d352f3d27b6964182aa60	C:\Users\kEecfMwgj\Documents\hhuy\z99M8Y1GRoOyuotMz.csv.vvyu, c:\users\keecfmwgj\documents\hhuy\z99m8y1grooyuotmz.csv.vvyu	Dropped File	59.06 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3a96aeabbb0bcc7e73a5475c7dbffb6a6e57faf08dd398da1fc3124a1c8f6d38	c:\users\keecfmwgj\videos\z2e0zt\zpv7u7xpwr7qk\rfes3vfwf3fsy6sx.flv.vvyu, C:\Users\kEecfMwgj\Videos\z2E0zT\zpV7u7xPWr7qK\rfES3vfWf3fsY6Sx.flv.vvyu	Dropped File	4.92 KB	video/x-flv	Access, Create, Write	MALICIOUS
4a0259c4686b41ea148ea36359d434885a71896d29dfbab0363e4183679371ad	C:\Users\kEecfMwgj\Desktop\itjgP.m4a.vvyu, c:\users\keecfmwgj\desktop\itjgp.m4a.vvyu	Dropped File	61.15 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4a5d3bbc254ba37617c064f3848973257ffb69f97d6a7acfa39495a395116056	c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\6pw8rpgl-.flv.vvyu, C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\6pW8RpGL-.flv.vvyu	Dropped File	38.90 KB	video/x-flv	Access, Create, Write	MALICIOUS
f4e2ca8796b7629bf2896c3a9ca12f37221ea6e3de37c093826740436d260cbf	C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\GW5kXQqybZPUP2d4.mp4.vvyu, c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\gw5kxqqybzpup2d4.mp4.vvyu	Dropped File	69.76 KB	application/octet-stream	Access, Create, Write	MALICIOUS
30350606cbacceac12eb6f37740f6a83bdf68b9c781b27a1af1d3dff5731d62c	c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd- y4\tlaiuy5vumxfxacjn.wav.vvyu, C:\Users\kEecfMwgj\Music\mXrqWFqcp_fBV4xgh8cLcTD- y4\TlAiuy5VUmxfxAcJn.wav.vvyu	Dropped File	10.79 KB	application/octet-stream	Access, Create, Write	MALICIOUS
894900d80f9b5abb5f40cb8d86378e79a8baca261d84080d33c1d3adec251725	C:\Users\kEecfMwgj\Documents_3Wl5D4o0g2MKtP.pptx.vvyu, c:\users\keecfmwgj\documents_3wl5d4o0g2mktp.pptx.vvyu	Dropped File	95.94 KB	application/zip	Access, Create, Write	MALICIOUS
f7253ca681f4ebde608a638e09e74549c7a6f17eee224e80c092dc5584eb3378	C:\Users\kEecfMwgj\Desktop\bQ6SJi8RO0rg0dP\3YgFUJ.rtf.vvyu, c:\users\keecfmwgj\desktop\bq6sji8ro0rg0dp\3ygfuj.rtf.vvyu	Dropped File	77.06 KB	text/rtf	Access, Create, Write	MALICIOUS
d9e8b6ff7ef08432ad9dea072b65adb94dfe85fa2bbf1ebd9db9dd23891a963d	C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEhFXubwY\ifMhH\5DS0X1cGBS4n2igZsE.jpg.vvyu, c:\users\keecfmwgj\pictures\kir-tas9lgdehfxubwy\ifmhh\5ds0x1cgbs4n2igzse.jpg.vvyu	Dropped File	70.97 KB	image/jpeg	Access, Create, Write	MALICIOUS
473b7e1ba2117efc27a7ab5b524f2419ed8dd844ab566a5de159df24238b25ed	C:\Users\kEecfMwgj\Pictures\bQiz44uQ681_7Dctbgxp.jpg.vvyu, c:\users\keecfmwgj\pictures\bqiz44uq681_7dctbgxp.jpg.vvyu	Dropped File	52.25 KB	image/jpeg	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4fc5c0fa864d6d3beece05a148cac43dde53f5fcf22b6a7e40b0dae4a44abcb1	c:\users\keecfmwgj\music\nmf9emihkrld8q1qs.mp3.vvyu, C:\Users\kEecfMwgj\Music\nmf9EMIHkrld8q1qS.mp3.vvyu	Dropped File	46.34 KB	application/octet-stream	Access, Create, Write	MALICIOUS
402cc932665b1145dcd00036df7ef0b335ba87097cb180387a4cec8290b6eba2	C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\cPfFJ9.flv.vvyu, c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\cpffj9.flv.vvyu	Dropped File	39.58 KB	video/x-flv	Access, Create, Write	MALICIOUS
b0472978a35878ca65dceb2aa8496916b7841b9f06d0a93b9b99dad64926a3af	C:\Users\kEecfMwgj\Documents\567c.pdf.vvyu, c:\users\keecfmwgj\documents\567c.pdf.vvyu	Dropped File	71.37 KB	application/pdf	Access, Create, Write	MALICIOUS
272054bacb696311cfcaf3a321598a2d58bea81987481db3066179cbd5dad608	c:\users\keecfmwgj\documents\hhuy\bju5iwgzcivxdeaczva1.odt.vvyu, C:\Users\kEecfMwgj\Documents\hhuy\bJu5IwGZcIVxDeaCzVA1.odt.vvyu	Dropped File	33.26 KB	application/zip	Access, Create, Write	MALICIOUS
734ef8197eae32ebbb05699038caf483c845cbc3ac184134aba9a2b0e7bf6a08	c:\users\keecfmwgj\documents\hhuy\rfixnl1vu2.ots.vvyu, C:\Users\kEecfMwgj\Documents\hhuy\rFiXNL1vU2.ots.vvyu	Dropped File	97.71 KB	application/zip	Access, Create, Write	MALICIOUS
5706a0a0883c3c6e646f5dfaf7ee9da761f6d6b657b80683bcabd47f393c1df6	c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\tkvyxwxrq.ots.vvyu, C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\tkVyxwxrQ.ots.vvyu	Dropped File	51.04 KB	application/zip	Access, Create, Write	MALICIOUS
f9025e0e638cb18ca29f908b3d546390fcf8a11fab885c0d9f47b1b5b3e81d02	c:\users\keecfmwgj\music\olz6-jxmw7o1_h pvu.mp3.vvyu, C:\Users\kEecfMwgj\Music\OlZ6-jXMW7o1_h PvU.mp3.vvyu	Dropped File	7.53 KB	application/octet-stream	Access, Create, Write	MALICIOUS
398641fed9d5bc3dbe6b22bf875cb4c30ccc30d631ceaa4edbbc4acd86dfe9cd	C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\yOmL -Z4 9fyb2lF7S9.png.vvyu, c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\yoml -z4 9fyb2if7s9.png.vvyu	Dropped File	62.03 KB	application/octet-stream	Access, Create, Write	MALICIOUS
9d5fb3099874edd6728f924b78426d4e31624f43743605e20f012733e91b1ded	c:\users\keecfmwgj\documents\hhuy\ni1u7vxc2c n4uuhwh.pps.vvyu, C:\Users\kEecfMwgj\Documents\hhuy\Ni1u7VXc2C N4UUHwH.pps.vvyu	Dropped File	22.70 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e72f727e0d057036134db697d330f38b8a4d9f5b6454f34ef3267450831f393e	c:\users\keecfmwgj\desktop\ijdhlcko.jpg.vvyu, C:\Users\kEecfMwgj\Desktop\IjDhLcko.jpg.vvyu	Dropped File	66.40 KB	image/jpeg	Access, Create, Write	MALICIOUS
031653457cec31d0795db170a5ae8756df32b9b422ed9091e222157b009d5a8a	C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\uo7bfSHfyn-0X-MGd.bmp.vvyu, c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\uo7bfshfyn-0x-mgd.bmp.vvyu	Dropped File	32.13 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4e3e305fea79f1d263eea98d4c12a6f087e90331e47583fa2cb2dd693637c0a7	c:\users\keecfmwgj\desktop\bq6sji8ro0rg0dp\9ecwyh_e3fhju.avi.vvyu, C:\Users\kEecfMwgj\Desktop\bQ6SJi8RO0rg0dP\9eCWyh_E3fHJU.avi.vvyu	Dropped File	55.57 KB	application/octet-stream	Access, Create, Write	MALICIOUS
5bc5ad5410f105ab9b5b25d0b3205680d06102698d2ec7ca554b6d66471a97a9	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
19d28ff75492c000f8716c68e61927b887889033b1ce39304af98b47a6b740f4	c:\users\keecfmwgj\desktop\rwqicw2qitxlv4.jpg.vvyu, C:\Users\kEecfMwgj\Desktop\RwqiCW2QitXLv4.jpg.vvyu	Dropped File	98.99 KB	image/jpeg	Access, Create, Write	MALICIOUS
431a2acd28946a4b81df1a044fc57216ec54ee63a2a30acc09d1ab7f842ae0aa	c:\users\keecfmwgj\favorites\msn websites\msn autos.url.vvyu, C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Autos.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
587e04449979b37f0d657abeedb66fbf094cf763e822d82851ce19de6a640db0	C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\iIfMhH\9VRBBaa2E6cjsKGlie.gif.vvyu, c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\9vrbbaa2e6cjskglie.gif.vvyu	Dropped File	57.00 KB	image/gif	Access, Create, Write	MALICIOUS
0e9e1ecb02e3e22046bca615aa88befa7dc39d8c7b18d2d0540ef51c83c55107	c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\ksif.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\iIfMhH\ksIF.bmp.vvyu	Dropped File	95.24 KB	application/octet-stream	Access, Create, Write	MALICIOUS
43e2fa29b2173efa491920ab2126a6fe80628f224bb99f438bfc8d3eb4b48cf8	C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe.vvyu, c:\users\keecfmwgj\desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe.vvyu	Dropped File	730.83 KB	application/x-dosexec	Access, Create, Write	MALICIOUS
9a396177cf04e8618d596aa98ed6d6ceec011568a1cda6bd98ecac5f2630f1f7	C:\Users\kEecfMwgj\Documents\hhuy\U-GFPMIYoqWy2p9O.xlsx.vvyu, c:\users\keecfmwgj\documents\hhuy\u-gfpmiyoqwy2p9o.xlsx.vvyu	Dropped File	73.96 KB	application/zip	Access, Create, Write	MALICIOUS
d2a131213503fe81fcf49936d2feb8f36988a49a0327ab408c599ffb4d84871c	c:\users\keecfmwgj\music\mxrqwfqcp\jze7xrus.m4a.vvyu, C:\Users\kEecfMwgj\Music\mXrqWFqcp\jZE7XRus.m4a.vvyu	Dropped File	10.25 KB	application/octet-stream	Access, Create, Write	MALICIOUS
1659c743af76e49d9fe13b2c559befbe3806dfd0defdab394c73ff944cd7ec3e	c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\ydph4cpxgp3qwyuc\aougfr90ajw.jpg.vvyu, C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\yDPh4CpXgP3QwyUC\AoUGFR90ajW.jpg.vvyu	Dropped File	10.75 KB	image/jpeg	Access, Create, Write	MALICIOUS
47c07be7f50f3099f127c92737a9a8fa3e3595a060b5711b94e4132480370b5c	c:\users\keecfmwgj\music\bjhxlx\cmbspstlrb9u.m4a.vvyu, C:\Users\kEecfMwgj\Music\BJHxLX\cmBSppsTLRb9u.m4a.vvyu	Dropped File	91.81 KB	application/octet-stream	Access, Create, Write	MALICIOUS
fe13edf5fc531caf016cd92328bbe438fd492d8276e1e5728c59d995f6fe6e04	C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\s_e2a5ScpFSgR9-.mkv.vvyu, c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\s_e2a5scpfsgr9-.mkv.vvyu	Dropped File	74.79 KB	application/octet-stream	Access, Create, Write	MALICIOUS
218daa75779284fe874259f4ec8d88a9b30ac8a2d5404216931b8964a4de2748	C:\Users\kEecfMwgj\Desktop\tHLdWYzw.ots.vvyu, c:\users\keecfmwgj\desktop\thldwyzw.ots.vvyu	Dropped File	24.69 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b281c27a359981a22e3e5d044e1d51c0d355e2a2a51996c8545a6da246bbc3f7	C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkI\HbqLBzpGm.wav.vvyu, c:\users\keecfmwgj\music\bjhxlx\9ast-p\dktsn5wki\hbqlbzpgm.wav.vvyu	Dropped File	18.22 KB	application/octet-stream	Access, Create, Write	MALICIOUS
df9020a2c2c61fd4b7da8475ac6321dba9338a0f060014f7c35b05daeabefcc1	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
ff7ac932d26acfe13c4214d7fa81a0a2c48b05ddee9a009adfd28f5634ec9ce9	C:\Users\kEecfMwgj\Music\BJHxLX\KnG7feMIAKlEoa_UW1s2.wav.vvyu, c:\users\keecfmwgj\music\bjhxlx\kng7femiakleoa_uw1s2.wav.vvyu	Dropped File	81.21 KB	application/octet-stream	Access, Create, Write	MALICIOUS
7d4224f630e4938d9839ea653d0c408b0e876c7a6f7ca99ace46048af29bc1a1	C:\Users\kEecfMwgj\Documents\6LeN1-BfLiBS.rtf.vvyu, c:\users\keecfmwgj\documents\6len1-bflibs.rtf.vvyu	Dropped File	72.11 KB	text/rtf	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4e1697043b6c8a655e7d03c9b93966105bcae8947f449e86ab3a6d085a236a5e	c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\wa_4pk0l7jwgqv.xlsx.vvyu, C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\Wa_4PK0L7JwGQV.xlsx.vvyu	Dropped File	20.93 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d5029c9c174733b887d9ebc9443dac72ac13269412780a53fc840d34ce0b4846	c:\users\keecfmwgj\documents\z1niztmoyavazpqq.rtf.vvyu, C:\Users\kEecfMwgj\Documents\Z1NiZTMoyaVazPqQ.rtf.vvyu	Dropped File	21.56 KB	text/rtf	Access, Create, Write	MALICIOUS
e0cdb066c7e3d5b202ed26ace83f3a939ccabbb07338b465ed01787a82284977	C:\Users\kEecfMwgj\Documents\CzDS-.pptx.vvyu, c:\users\keecfmwgj\documents\czds-.pptx.vvyu	Dropped File	20.72 KB	application/octet-stream	Access, Create, Write	MALICIOUS
551247baf79c97d9c25b46431f8df0905b95d21cd64d46c4735dc51d99be1fb0	C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkl\6y-Gle7CJ.m4a.vvyu, c:\users\keecfmwgj\music\bjhxlx\9ast-p\dktsn5wki\6y-gle7cj.m4a.vvyu	Dropped File	25.63 KB	application/octet-stream	Access, Create, Write	MALICIOUS
caee0f4bb79e2b319c8593e45942d5ee8ec47500154e23519af9fee1f3a42977	C:\Users\kEecfMwgj\Documents\hhuy\Qs2 hK9Y_.xlsx.vvyu, c:\users\keecfmwgj\documents\hhuy\qs2 hk9y_.xlsx.vvyu	Dropped File	6.67 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3fa2646c6675f671dcf30d8b03ac854945fa419820a7408da09bd02540c9b30d	c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\pfzhnu297.png.vvyu, C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\iIfMhH\PFZhNu297.png.vvyu	Dropped File	2.79 KB	application/octet-stream	Access, Create, Write	MALICIOUS
7bc5f125a7a2970d7a7a6bac90320a6d81c29519280ed4bd54b591fdc066d9c1	c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd- y4\-ahhgkvlxn_kxd.m4a.vvyu, C:\Users\kEecfMwgj\Music\mXrqWFqcp_fBV4xgh8cLcTD- y4\-AHHgkVlxn_KxD.m4a.vvyu	Dropped File	12.87 KB	application/octet-stream	Access, Create, Write	MALICIOUS
affbb7b542bcde7bb2fd1749df331ad470edfe50811147945c1794a9efa50e6c	c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\ydph4cpxgp3qwyuc\x5tjkqt17l1kq.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\yDPh4CpXgP3QwyUC\X5TjkQT17l1kq.bmp.vvyu	Dropped File	24.73 KB	application/octet-stream	Access, Create, Write	MALICIOUS
6c5bc57525cd6e312a1f9a5b4c964407dc9b385163c7fef389aa2eedc7a315c9	C:\Users\kEecfMwgj\Videos\hDvzuhrdv.mkv.vvyu, c:\users\keecfmwgj\videos\hdvzuhrdv.mkv.vvyu	Dropped File	60.07 KB	application/octet-stream	Access, Create, Write	MALICIOUS
2c9f90f7e9f2022f19782b0c45f62bdb61ce24d50cd9f5de2a8ffb1149491b33	C:\Users\kEecfMwgj\Desktop\nQrFKLA.gif.vvyu, c:\users\keecfmwgj\desktop\nqrfkla.gif.vvyu	Dropped File	74.63 KB	image/gif	Access, Create, Write	MALICIOUS
34d05b8778caf4770e09de8c2f66263f24b39b49e7bdfae7c4ace5a378dacc40	C:\Users\kEecfMwgj\Desktop\K3t8MIfEa.mp3.vvyu, c:\users\keecfmwgj\desktop\k3t8mlfea.mp3.vvyu	Dropped File	12.73 KB	application/octet-stream	Access, Create, Write	MALICIOUS
dcc8ca54190953aaebc4920bd37bed47d28c783721a56af3a6c3e0be8fb008d8	C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\rQja5oZ7_uz\EhqiUu8LglRl.mp4.vvyu, c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\rqja5oz7_uz\ehqiuu8lglrl.mp4.vvyu	Dropped File	48.46 KB	application/octet-stream	Access, Create, Write	MALICIOUS
683d69769675a2aedc9c9ed5d3b236d63e388d6c32d6301fc9633e3c94b1ac0b	c:\users\keecfmwgj\videos\z2e0zt\zpv7u7xpwr7qk\iwi4py9f_tbuupcdk.flv.vvyu, C:\Users\kEecfMwgj\Videos\z2E0zT\zpV7u7xPWr7qK\Iwi4py9F_tBuUPcDK.flv.vvyu	Dropped File	24.45 KB	video/x-flv	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0933f9d1a069169a47534b6338c052bc5f380172aa2171d446e0f359ba81ea3f	c:\users\keecfmwgj\documents\hhuy\naiaggm8s5tskx.docx.vvyu, C:\Users\kEecfMwgj\Documents\hhuy\naiagGM8S5tSkx.docx.vvyu	Dropped File	57.32 KB	application/zip	Access, Create, Write	MALICIOUS
2222e65f4697f4a89deed2906b732f3fabb9d8887c6456e6f308e8cd7f84a3eb	C:\Users\kEecfMwgj\Desktop\cTaPN4HhRqe86tN.rtf.vvyu, c:\users\keecfmwgj\desktop\ctapn4hhrqe86tn.rtf.vvyu	Dropped File	3.34 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c1aa0df3912ad585cdc48d7de4baaf09ff6597a32f052f5bcff2ae9490594569	C:\Users\kEecfMwgj\Music\mXrqWFqcp\-xht.wav.vvyu, c:\users\keecfmwgj\music\mxrqwfqcp\-xht.wav.vvyu	Dropped File	3.51 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ae90c3e73ad1bf03b16c5c76379a2eac7cb37ecff753676a001c0dba8ebc934b	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
a07d0d82086b969b45bcad0383ed3899c4e9da6f8ff929634be61937acba8255	C:\Users\kEecfMwgj\Documents\2oZu1wT.ppt.vvyu, c:\users\keecfmwgj\documents\2ozu1wt.ppt.vvyu	Dropped File	8.98 KB	application/octet-stream	Access, Create, Write	MALICIOUS
2b344bf7c2c0903367a4b6d92bb583f455b20c351e365bed92e2c4bb26550977	C:\Users\kEecfMwgj\Documents\4l3gkybFjpw5wc.rtf.vvyu, c:\users\keecfmwgj\documents\4l3gkybfjpw5wc.rtf.vvyu	Dropped File	6.57 KB	text/rtf	Access, Create, Write	MALICIOUS
06acc0feb751caf85f859845100bb0ed467d42a24136312ba453f058494b6ec5	C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\2j2l02AsmvpG-FW9.gif.vvyu, c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\2j2l02asmvpg-fw9.gif.vvyu	Dropped File	31.12 KB	image/gif	Access, Create, Write	MALICIOUS
ae5df317d6203597bb87fac899165235a5b9c060af95fb80da16b4501223dea9	C:\Users\kEecfMwgj\Music\BJHxLX\dTVoZ bX824b.wav.vvyu, c:\users\keecfmwgj\music\bjhxlx\dtvozbx824b.wav.vvyu	Dropped File	70.05 KB	application/octet-stream	Access, Create, Write	MALICIOUS
966f24e524cc4d24ef763e63db468aac00e7d7ee6cc7b399fa57ed5060ecf270	C:\Users\kEecfMwgj\Documents\4COwR1C7ya7.pptx.vvyu, c:\users\keecfmwgj\documents\4cowr1c7ya7.pptx.vvyu	Dropped File	52.76 KB	application/zip	Access, Create, Write	MALICIOUS
f0a5f7e0d9d9659ddd6a04ee59fe3f336bae267a6366ed674b00d00566285ffa	C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\0jip-0WU2n5fd8 POL.bmp.vvyu, c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\0jip-0wu2n5fd8 pol.bmp.vvyu	Dropped File	15.81 KB	application/octet-stream	Access, Create, Write	MALICIOUS
24864d0dfa284d80d5013e818bccbfd5bafc17f110edfa2f73b00e121e44b4ee	c:\users\keecfmwgj\videos\z2e0zt\zpv7u7xpwr7qk\1l1mbixt edk.mkv.vvyu, C:\Users\kEecfMwgj\Videos\z2E0zT\zpV7u7xPWr7qK\1l1mBiXT EDK.mkv.vvyu	Dropped File	7.04 KB	application/octet-stream	Access, Create, Write	MALICIOUS
26bc3a8b110a24b3c1a4cec04f25c2c9ab887cbdd16ec226367fab86a952707b	c:\users\keecfmwgj\desktop\ldmozuncs-h9r3 xu2.mp4.vvyu, C:\Users\kEecfMwgj\Desktop\ldMOZuncCS-h9r3 XU2.mp4.vvyu	Dropped File	96.31 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b3390fd47b8fdfb6dad0061e5eccab69d90d1677277f0924dbd4a0290d568011	C:\Users\kEecfMwgj\Desktop\cmt4.gif.vvyu, c:\users\keecfmwgj\desktop\cmt4.gif.vvyu	Dropped File	85.31 KB	image/gif	Access, Create, Write	MALICIOUS
4f8ed28f94accb436273bd2853d4b192bd631c2529ed2c970b8924f0dee8c74a	c:\users\keecfmwgj\appdata\locallow\microsoft\internet explorer\services\search_{0633ee93-d776-472f-a0ff-e1416b8b2e3a}.ico.vvyu, C:\Users\kEecfMwgj\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-472f-A0FF-E1416B8B2E3A}.ico.vvyu	Dropped File	4.51 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
22cab0de91bf4e982352fef696c6393dad443f3f0d4d2b3019d736a2e4a453ec	C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\v97V_KMwmgn4h6UDx.jpg.vvyu, c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\v97v_kmwmgn4h6udx.jpg.vvyu	Dropped File	40.53 KB	image/jpeg	Access, Create, Write	MALICIOUS
83c5ded689b4ac46b6bf7f6c7555077c8ebd4f0902175f81a9987bb801e789d0	c:\users\keecfmwgj\documents\py_fftiab_q4nwhp.docx.vvyu, C:\Users\kEecfMwgj\Documents\pY_fFtiab_Q4NWHp.docx.vvyu	Dropped File	47.11 KB	application/zip	Access, Create, Write	MALICIOUS
69ff7fc1c062ba60f4d18039791853b3ef4da52e950d2d216758e7d5e89908d6	c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\dtf66.png.vvyu, C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\dTf66.png.vvyu	Dropped File	60.53 KB	application/octet-stream	Access, Create, Write	MALICIOUS
932115bf58ba9bcb34992a979c72196903b6f65911293583c7afa3be6ba241c0	C:\Users\kEecfMwgj\Pictures\O_9gyTeSlm.jpg.vvyu, c:\users\keecfmwgj\pictures\o_9gytesl m.jpg.vvyu	Dropped File	77.50 KB	image/jpeg	Access, Create, Write	MALICIOUS
8a0a52c012403823d23a515418dbaa5474e4d98539046c53de721526a25eb13b	c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\la08fq2wwngfs3w9kc.swf.vvyu, C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK_qbp0nkGuotBuAqg\LA08Fq2WwngfS3W9kC.swf.vvyu	Dropped File	9.14 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
c341873e0b4eb668af30cbb4b510722c6f1e9d1d0f27486f904c4fb5284b40ab	C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\MpjP3oSTE.mkv.vvyu, c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\mpjp3oste.mkv.vvyu	Dropped File	38.09 KB	application/octet-stream	Access, Create, Write	MALICIOUS
dfda77095c6a5eebb782e5445fde3e9dc05cf0df896c470503e135c6d3042676	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	MALICIOUS
49f92e8c10a3de7e7f811559aeed142c4be052f7ca8c5bdc07d9d5445ab0736c	C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkl\a6C7l-Qq0p-ecvc_8DsT.wav.vvyu, c:\users\keecfmwgj\music\bjhxlx\9ast-p\dktsn5wki\a6c7l-qq0p-ecvc_8dst.wav.vvyu	Dropped File	74.36 KB	application/octet-stream	Access, Create, Write	MALICIOUS
1e1b65b403d02636a3dd2bd42472d70bb97b087f6eb172e8eb0ec641cd53ed0a	c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd-y4\02rh90y7rebgxw.mp3.vvyu, C:\Users\kEecfMwgj\Music\mXrqWFqcp_fBV4xgh8cLcTD-y4\02RH90y7ReBgxW.mp3.vvyu	Dropped File	37.27 KB	application/octet-stream	Access, Create, Write	MALICIOUS
f1c47080665973de4ad0c37caf724f6deccd62df6cd08bf8a5115f24970c74b0	c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\5qvh55h.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\5qVH55h.bmp.vvyu	Dropped File	59.72 KB	application/octet-stream	Access, Create, Write	MALICIOUS
20eeb5c1f2b0a1dee443455087c3eae5fb5d3146968438700d13573056b6fe06	C:\Users\kEecfMwgj\Pictures\n-nH-E2t.jpg.vvyu, c:\users\keecfmwgj\pictures\n-nh-e2t.jpg.vvyu	Dropped File	63.23 KB	image/jpeg	Access, Create, Write	MALICIOUS
ae7cd6922e5ae781bc6e12153af1c7ce9fd171a8b2880e6d57639d0afaefe76c	c:\users\keecfmwgj\documents\hhuy\ynkbyrnkc6j3avv0zier.odt.vvyu, C:\Users\kEecfMwgj\Documents\hhuy\YnkbYRnkC6J3AvV0Zier.odt.vvyu	Dropped File	77.12 KB	application/zip	Access, Create, Write	MALICIOUS
953147e287a78bfecb52fe75299e5476e444b4e2efe37e6dc8f819a80252fe2b	c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\lxhmd.gif.vvyu, C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\LXhmd.gif.vvyu	Dropped File	48.09 KB	image/gif	Access, Create, Write	MALICIOUS
74ad2158105670d3d1037922540622972be2c21ef46f	c:\users\keecfmwgj\desktop\i5zfv_jkmjeubuqus.gif.vvyu, C:\Users\kEecfMwgj\Desktop\I5zFv_jkMMjeubUquS.gif.vvyu	Dropped File	73.80 KB	image/gif	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
dd04e553681e1090342e583ea5b3d6cac4bb8080c9b945e5af237d3d2651215e	C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkl\GWrBK8mbOy.wav.vvyu, c:\users\keecfmwgj\music\bjhxlx\9ast-p\dktsn5wki\gwrbk8mboy.wav.vvyu	Dropped File	96.55 KB	application/octet-stream	Access, Create, Write	MALICIOUS
5151cdaed76855740daf7e161bf28e5e1ff6ed9a3663a8778e62bdf0359c6135	C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url.vvyu, c:\users\keecfmwgj\favorites\msn websites\msn money.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
f0e4d02e00c369d7ac1140c0cb106da5965ed3ed638fd117d27fb7ac4d8bcbd0	c:\users\keecfmwgj\documents\qtnn2gz.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\QtNn2GZ.xlsx.vvyu	Dropped File	6.25 KB	application/octet-stream	Access, Create, Write	MALICIOUS
44eb9a0cb89c4b01a074b442f898c773ec537f517680c9a80036079bea4151c6	c:\users\keecfmwgj\documents\hhuy\ytkydbos.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\hhuy\yTkydbos.xlsx.vvyu	Dropped File	29.81 KB	application/zip	Access, Create, Write	MALICIOUS
4e457d70005729d8a9ae7d73ee3ab80c0b90f866c736819b7949d0b1d8ec4657	c:\users\keecfmwgj\documents\outlook files\franc@gdllo.de.pst.vvyu, C:\Users\kEecfMwgj\Documents\Outlook Files\franc@gdllo.de.pst.vvyu	Dropped File	265.33 KB	application/octet-stream	Access, Create, Write	MALICIOUS
bc826210d063edff1db9570c195b4de4b7311d6317514ec63305d354caced0ef	c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\b8gbt7knns9kt-gvh.swf.vvyu, C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\B8Gbt7KNns9kT-gvh.swf.vvyu	Dropped File	42.99 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
29cde7f05caa158e25cef5b613ab7b46b85ed1639f5b849a0864beb02fee6d9d	c:\users\keecfmwgj\desktop\hsxa8jyxcbsx17ja94r_.jpg.vvyu, C:\Users\kEecfMwgj\Desktop\hSxa8JYxcBSx17jA94r_.jpg.vvyu	Dropped File	3.73 KB	image/jpeg	Access, Create, Write	MALICIOUS
6cbc00787537559f670d109ddbaf36dba25ab0ac36a6665d8ddf262ec0da4e73	c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\xudjwurucylo9.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\iIfMhH\XUdJWURucyLo9.bmp.vvyu	Dropped File	75.70 KB	application/octet-stream	Access, Create, Write	MALICIOUS
94cc6553591ef38ea49a01a39b8f4aaf2ce6c476f6ad674f0140117168662cc3	c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\a9pzarvgiar.avi.vvyu, C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK_qbp0nkGuotBuAqg\A9pzaRVglaR.avi.vvyu	Dropped File	54.89 KB	application/octet-stream	Access, Create, Write	MALICIOUS
1ab9b3b0544f96605222a450f98775bdc9b110e24e670a57c9f5a6afee3424b7	C:\Users\kEecfMwgj\Documents\D1q0P.docx.vvyu, c:\users\keecfmwgj\documents\d1q0p.docx.vvyu	Dropped File	95.20 KB	application/zip	Access, Create, Write	MALICIOUS
c2732e2c403c3584d9828b8e7eed28051b09dac3e39a17b619030c6dc1cd4435	c:\users\keecfmwgj\desktop\us8ywh8d_vcxiyflf5e.m4a.vvyu, C:\Users\kEecfMwgj\Desktop\US8ywh8D_vcXiYflf5e.m4a.vvyu	Dropped File	83.19 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c10930d37153c376e658f390097b51273e00f861524d454c21fe7727db4b3ae6	C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\Asv9iqUaFA9rCWFze77.avi.vvyu, c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\asv9iquafa9rcwfze77.avi.vvyu	Dropped File	34.75 KB	application/octet-stream	Access, Create, Write	MALICIOUS
cbbd6523c8d8173884e5778785b089ba0462f1562efd4670af7cf7efd46fcf86	c:\users\keecfmwgj\desktop\nwy04.bmp.vvyu, C:\Users\kEecfMwgj\Desktop\NWy04.bmp.vvyu	Dropped File	48.71 KB	application/octet-stream	Access, Create, Write	MALICIOUS
26f062dffa9b5852550bb31e36b1450e5a66f1250a9e669a9ba00fa97dfe9485	c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\ghprnga3a e4cboqml8u.bmp.vvyu, C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\GHPRnGA3a e4cbOQmL8U.bmp.vvyu	Dropped File	54.01 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98	C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe, C:\Users\kEecfMwgj\Desktop\1918cc... ... \kEecfMwgj\AppData\Local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	Sample File	730.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Read, Write	MALICIOUS
4a1aaeed4747266983004f9fa25ff0ed024415f8232f30467b08441084b002e0	-	Web Response	554 bytes	text/html	-	CLEAN
97edd7cae37d3c44a353b6cad0258ad6c8d2fcace03cafe01556f57a3296fa57	C:\Users\kEecfMwgj\AppData\Local\c01688bb-f556-4db2-ba2c-05b15fa562c3\build2.exe	Dropped File	360.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	CLEAN
3c7d38aff2dd9e697cd3cc6c0a5d338ff2d0bdb948fb469cd21c76d8c36e53ee	-	Modified File	256.00 KB	application/octet-stream	-	CLEAN
7d26da460ac85d8df173d3d63db203b40aad7c581ed8023cec40c91036090de5	-	Downloaded File	431.72 KB	application/vnd.microsoft.portable-executable	-	CLEAN
5e677e2368f0dc4d5a9e4e52aa37c5d51d40f5171eb97ee1a2904492f74ffeec	c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\kvyeo7pecdl1br27xvac.mkv.vvyu, C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\kvyEO7pECdl1BR27XVAc.mkv.vvyu	Dropped File	26.65 KB	application/octet-stream	Access, Create, Write	CLEAN
83e1eaf04ef012175c3b4d16caa1ba50f00e814c7613c2a369cb050e35fab522	C:\Users\kEecfMwgj\Desktop\Cc9_9V6aB.avi.vvyu, c:\users\keecfmwgj\desktop\cc9_9v6ab.avi.vvyu	Dropped File	15.56 KB	application/octet-stream	Access, Create, Write	CLEAN
c6fc229e5cfa5de6c5a49a6b993c64cad23277e507522ee7e05794ef4e5bea79	C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Spaces.url.vvyu, c:\users\keecfmwgj\favorites\windows live\windows live spaces.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
93d6488fcd9eb9f990339766fa9af4859d540503defbe61901a08f5279973414	C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url.vvyu, c:\users\keecfmwgj\favorites\microsoft websites\microsoft store.url.vvyu	Dropped File	468 bytes	application/octet-stream	Access, Create, Write	CLEAN
a7799c84303d1eb3a00371b037fa9a21406abcb760390390665d8e8922072e71	c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\ydxrjd.png.vvyu, C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\YdXrJd.png.vvyu	Dropped File	10.72 KB	application/octet-stream	Access, Create, Write	CLEAN
e6779d99f703a7c0b189700d09d968bc211838bbf884bc397a5a9760b1ada314	c:\users\keecfmwgj\music\mxrqwfqcp\xxli1eqxvup5i 0hs6g.mp3.vvyu, C:\Users\kEecfMwgj\Music\mXrqWFqcp\xXLI1eQxvUp5i 0hs6G.mp3.vvyu	Dropped File	91.12 KB	application/octet-stream	Access, Create, Write	CLEAN
2bd4c98884d4f3f10e932e7f7419880103a5cc594c9b2babf4b89f18e3353e85	C:\Users\kEecfMwgj\Documents\tPG-9VHK-ulBZl_Q.docx.vvyu, c:\users\keecfmwgj\documents\tpg-9vhk-ulbzl_q.docx.vvyu	Dropped File	36.86 KB	application/octet-stream	Access, Create, Write	CLEAN
2cf37d0ea9153599981d4767fddf3c7d3562debf4c192356937f9b5492d0a918	c:\users\keecfmwgj\documents\kw5j7a5.doc.vvyu, C:\Users\kEecfMwgj\Documents\KW5J7A5.doc.vvyu	Dropped File	14.59 KB	application/octet-stream	Access, Create, Write	CLEAN
98bc19031aba4f2a2e5e7866d548e2c1a0405187d451d734b3fcb7763197b03a	c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\rqja5oz7_uz\kylqcyn6yv.pps.vvyu, C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\rQja5oZ7_uz\kyLqCYn6yV.pps.vvyu	Dropped File	24.06 KB	application/octet-stream	Access, Create, Write	CLEAN
3203988b9bb84611e18fef6dda137b9aa1fc2407b90282bc464a751d18745a7c	c:\users\keecfmwgj\music\bjhxlx\rp0gg8vjq4u.wav.vvyu, C:\Users\kEecfMwgj\Music\BJHxLX\rp0gg8vJq4U.wav.vvyu	Dropped File	12.34 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
29827d39c616954d9ca8880f87298a2992d95088094fb85ad5565d44fa581899	C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE Add-on site.url.vvyu, c:\users\keecfmwgj\favorites\microsoft websites\ie add-on site.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
84d109fcb39e5c9e2eee3f272afe11bbc73536b99852eb3843b59ad813bb10c8	c:\users\keecfmwgj\desktop\2uv3ozugwqu6cyc7-l.swf.vvyu, C:\Users\kEecfMwgj\Desktop\2UV3oZuGwQu6CYc7-L.swf.vvyu	Dropped File	42.88 KB	application/x-shockwave-flash	Access, Create, Write	CLEAN
b9577300fafe21383c57d0a403db16b42c6c55397a6b628ff440aa833c226813	c:\users\keecfmwgj\documents\jw5nfujdo04vpw2wo.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\jw5nfUjDO04Vpw2Wo.xlsx.vvyu	Dropped File	54.02 KB	application/zip	Access, Create, Write	CLEAN
4938142520f2d0df614ea3a0fe14d92ce75f5d3dcaef23e24f2669fa2cc4ac16	c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\m mfup.mp4.vvyu, C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK_qbp0nkGuotBuAqg\M mFuP.mp4.vvyu	Dropped File	69.69 KB	application/octet-stream	Access, Create, Write	CLEAN
22e0a45a8d96ba56e8215c4eff6b0bb9ab61b65076db92fb455362aee5d13234	C:\Users\kEecfMwgj\Desktop\1IkZJVoATh.xls.vvyu, c:\users\keecfmwgj\desktop\1ikzjvoath.xls.vvyu	Dropped File	12.96 KB	application/octet-stream	Access, Create, Write	CLEAN
c6063f8ff1234e5ff2ff84d7a8a935f9385576f1bfe8f919115f036c3c3aa51b	C:\Users\kEecfMwgj\Documents\HeOaqMZgOojF528t.odt.vvyu, c:\users\keecfmwgj\documents\heoaqmzgoojf528t.odt.vvyu	Dropped File	20.29 KB	application/octet-stream	Access, Create, Write	CLEAN
117e8aa24da97662e538061d49200906d219627f014f7f96e52463afcd317a85	C:\Users\kEecfMwgj\Documents\hhuy\jkSu2OlxWSDLnSWvMq.ods.vvyu, c:\users\keecfmwgj\documents\hhuy\jksu2olxwsdlnswvmq.ods.vvyu	Dropped File	20.87 KB	application/zip	Access, Create, Write	CLEAN
5cf384e0c5df07debe12dd305331620f942286060f018eb48ae5b1f126a6e48e	c:\users\keecfmwgj\documents\dnsctzwstnyxbfiqs.docx.vvyu, C:\Users\kEecfMwgj\Documents\dnScTZWStNYxBfiQs.docx.vvyu	Dropped File	94.21 KB	application/zip	Access, Create, Write	CLEAN
9cb7ca045088f7172bc860b812e6d02c2aba7ee1832a06790c021f67d072565b	c:\users\keecfmwgj\documents\t_ciyr3b-hwvi5yqwu4.ods.vvyu, C:\Users\kEecfMwgj\Documents\T_CIyr3B-hwvI5YqWU4.ods.vvyu	Dropped File	19.30 KB	application/zip	Access, Create, Write	CLEAN
cf306f60e0a6604664afbce852bb202423267d27793a22f6ce0431dd1331a13d	C:\Users\kEecfMwgj\Music\mXrqWFqcp_fBV4xgh8cLcTD-y4\hyXqTEnB.mp3.vvyu, c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd- y4\hyxqtenb.mp3.vvyu	Dropped File	92.68 KB	application/octet-stream	Access, Create, Write	CLEAN
5c62fab79ef97e057b0efdf47489e69f77005ac18bb76693e11a376e3c0d3393	C:\Users\kEecfMwgj\Documents\hhuy\igCF Ho.ppt.vvyu, c:\users\keecfmwgj\documents\hhuy\igcfho.ppt.vvyu	Dropped File	2.84 KB	application/octet-stream	Access, Create, Write	CLEAN
7db1cc7be21c6fd3d8be577e018d48732f2f9688ac5cfdbeef5cdd2fae54ec79	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	CLEAN
9d830dbe0d6bea424858222e52412ea02be27188d9c0be176c7b316823f722eb	c:\users\keecfmwgj\music\p5fl21.m4a.vvyu, C:\Users\kEecfMwgj\Music\p5Fl21.m4a.vvyu	Dropped File	19.65 KB	application/octet-stream	Access, Create, Write	CLEAN
0ae13493b821c8e167d4848f2fbc58597b9d0d2448d34621439c68d0adad5389	C:\Users\kEecfMwgj\Music\esAg2qtfu0s5C0MdPd.mp3.vvyu, c:\users\keecfmwgj\music\esag2qtfu0s5c0mdpd.mp3.vvyu	Dropped File	27.15 KB	application/octet-stream	Access, Create, Write	CLEAN
da8d2596f75483b55e9640f377db386b08c9c1d49dbb64c3fbc669f1040e5894	C:\Users\kEecfMwgj\Videos\SipikwOFNhn.swf.vvyu, c:\users\keecfmwgj\videos\sipikwofnhn.swf.vvyu	Dropped File	77.00 KB	application/x-shockwave-flash	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2950d9152b926628ef5aa29842eb390f55d201a7d74dc434ce2fe259001ca185	c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\ae6i4hslrl.png.vvyu, C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\Ae6i4Hslrl.png.vvyu	Dropped File	26.18 KB	application/octet-stream	Access, Create, Write	CLEAN
0c5cceba5c416d5424387794429f89a2456b5326e2c7e5d8d2bd67f34bb616ec	-	Modified File	32.00 KB	application/octet-stream	-	CLEAN
3d0ed30d88e085ee7fd4ff018895822c8b64923b4cdd0be79fcb51203a1f2986	C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\yDPh4CpXgP3QwyUC\BY rE6U_U.png.vvyu, c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\ydph4cpxgp3qwyuc\by re6u_u.png.vvyu	Dropped File	98.47 KB	application/octet-stream	Access, Create, Write	CLEAN
796990a3ef36e55c9e0aa25e8d865524ebc9d2ce8fd2fb0206fb3f00974ef95c	C:\Users\kEecfMwgj\Documents\J0ThFcHeulkvK.odp.vvyu, c:\users\keecfmwgj\documents\j0thfcheulkvk.odp.vvyu	Dropped File	53.63 KB	application/zip	Access, Create, Write	CLEAN
76fd10d1bea5437e13882d4150a3364c890e50a44ac9f60a78d435a1f1427f7b	C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\Tb8Pl4n8ykiF82PGQ8M.mkv.vvyu, c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\tb8pi4n8ykif82pgq8m.mkv.vvyu	Dropped File	93.10 KB	application/octet-stream	Access, Create, Write	CLEAN
afc00fecdb6a78c005c4b6ae77d042e9087f6b37ed369fc705eee83bc528c94c	c:\users\keecfmwgj\documents\dijvxxa4.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\DIjVxXA4.xlsx.vvyu	Dropped File	60.98 KB	application/zip	Access, Create, Write	CLEAN
939063d5a04e87026528b13059f37588d42f825ebbdfe29de88f9c8530b3dab6	c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\qq8tjsc3zm363.avi.vvyu, C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK_qbp0nkGuotBuAqg\QQ8tJSc3zM363.avi.vvyu	Dropped File	71.75 KB	application/octet-stream	Access, Create, Write	CLEAN
0604e4874fcd90a1f4608dc3b74b28f66beb3f9104c5142a5419659dfcd8c0a7	c:\users\keecfmwgj\documents_dmv92xp.pptx.vvyu, C:\Users\kEecfMwgj\Documents_dmv92XP.pptx.vvyu	Dropped File	97.36 KB	application/zip	Access, Create, Write	CLEAN
dec7037f2a106264a712825d6c6f23f88faec2a6d98d9fb0925e08bfba2fa156	C:\Users\kEecfMwgj\Documents\hhuy\84p7mNA.doc.vvyu, c:\users\keecfmwgj\documents\hhuy\84p7mna.doc.vvyu	Dropped File	32.60 KB	application/octet-stream	Access, Create, Write	CLEAN
cf483a969ffc9707e39d04db5290a782ac96113eb679a04c0371ddb7fedf173f	c:\users\keecfmwgj\favorites\microsoft websites\microsoft at home.url.vvyu, C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Home.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
b3283031ef4e07b92cd8d8cc6edd1f381cfd8df16a24dc1e0f1fe69ef6aff5c7	c:\users\keecfmwgj\documents\dygx.docx.vvyu, C:\Users\kEecfMwgj\Documents\DygX.docx.vvyu	Dropped File	36.62 KB	application/zip	Access, Create, Write	CLEAN
3554860d3b4569052bb6593c6a9fedd8b40c47360641e884b62935ef1370c2b0	C:\Users\kEecfMwgj\Desktop\QQ3XsPcRg.swf.vvyu, c:\users\keecfmwgj\desktop\qq3xspcrg.swf.vvyu	Dropped File	17.41 KB	application/x-shockwave-flash	Access, Create, Write	CLEAN
2fd8f9383b9d83da87a53212e2a07534defaf86d51e6a13039bcfd14547de15f	C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\MHkDGP m.avi.vvyu, c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\mhkdgp m.avi.vvyu	Dropped File	79.42 KB	application/octet-stream	Access, Create, Write	CLEAN
5d98db98908ae2bbc97310bf25f5f4cef5fc7d2b25386cd1d511e9233cdd24f0	c:\users\keecfmwgj\pictures\77x_hi5d64n725my.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\77x_hl5d64N725mY.bmp.vvyu	Dropped File	72.71 KB	application/octet-stream	Access, Create, Write	CLEAN
1b7b9b22feb875d3cdda47672d7b4f783db75eb830f13a95fada199fc92487a8	c:\users\keecfmwgj\favorites\msn websites\msn sports.url.vvyu, C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Sports.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
cb626ae27f909a6c9cc93b949fde179166664a459b34afe6f8ba78c76eebfb4e	c:\users\keecfmwgj\documents\zliy3__ym6-.csv.vvyu, C:\Users\kEecfMwgj\Documents\zlIY3__yM6-.csv.vvyu	Dropped File	26.86 KB	application/octet-stream	Access, Create, Write	CLEAN
e15ad4c8665f0b19cfa961fbcb9f9ccc40079f1f1f68f6be8428613576cd82be	c:\users\keecfmwgj\documents\hhuy\4q235s.pptx.vvyu, C:\Users\kEecfMwgj\Documents\hhuy\4Q235S.pptx.vvyu	Dropped File	89.27 KB	application/zip	Access, Create, Write	CLEAN
72f17a8ec6bc5334199fa842bd6d3c657b556df651a464dec70f86d29421a403	c:\users\keecfmwgj\documents\5h1grurzazne.docx.vvyu, C:\Users\kEecfMwgj\Documents\5h1GruRzAZNE.docx.vvyu	Dropped File	61.67 KB	application/zip	Access, Create, Write	CLEAN
25d3a545346e087cc462ac0c51a3b80a296ff40a9f3566265bee8ed94a950267	C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK_qbp0nkGuotBuAqg\le5lbJNFps_4_oZKKr.mkv.vvyu, c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\ie5lbjnfps_4_ozkkr.mkv.vvyu	Dropped File	94.30 KB	application/octet-stream	Access, Create, Write	CLEAN
fbb291d250f035ce19eb70047d834c5eb9bdca314956acf364627d6c6d952aa8	c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\8fbu8gjzxgn5dwk.avi.vvyu, C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\8fbu8GjzXGN5dWk.avi.vvyu	Dropped File	67.59 KB	application/octet-stream	Access, Create, Write	CLEAN
26d09de29cdfa13ba6d732474cdc30e57dad5c432c617695bcd0e7fb6a787df5	c:\users\keecfmwgj\desktop\l-ti2nvrpacp-tk9f.mkv.vvyu, C:\Users\kEecfMwgj\Desktop\L-TI2NVRPaCP-tk9F.mkv.vvyu	Dropped File	23.31 KB	application/octet-stream	Access, Create, Write	CLEAN
1274234ccfb42ab981e5e904d22bea55053d9228c2ae30ea0a1336369ff28f49	C:\Users\kEecfMwgj\Videos\z2E0zT\g5znGT5HlbHq.mkv.vvyu, c:\users\keecfmwgj\videos\z2e0zt\g5zngt5hlbhq.mkv.vvyu	Dropped File	5.80 KB	application/octet-stream	Access, Create, Write	CLEAN
5b0f36a34235821a0b79750580442625522bb40a0d7a0047e2a8952a5ce3f1a5	c:\users\keecfmwgj\music\bjhxlx\9ast-p\fgnl6u1fsaf.m4a.vvyu, C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\FGNL6u1fSAF.m4a.vvyu	Dropped File	75.18 KB	application/octet-stream	Access, Create, Write	CLEAN
80c908b15e82bdd617fc2c181a5ba6c7ccd1ef128b7b67609611b02d7430e30c	c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.vvyu, C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE site on Microsoft.com.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\ksif.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\i5zfv_jkmmjeubuqus.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\z2E0zT\ufb ajK.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\a9pzarvgiar.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\py_fftiab_q4nwhp.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\pfzhnu297.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\HZvZCiMH.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\bjhxlx\rbnh h.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\bQiz44uQ681_7Dctbgxp.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\dtf66.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\yOmL -Z4 9fyb2lF7S9.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\-F78Z7ifiP0.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\Cc9_9V6aB.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\ydxrjd.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\eotpxodhmybxn _gv_k_.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd- y4\t laiuy5vumxfxacjn.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\bjhxlx\rp0gg8vjq4u.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\tkvyxwxrq.ots.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\jw5nfujdo04vpw2wo.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\hhuy\r fixnl1vu2.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\hhuy\jkSu2OlxWSDLnSWvMq.ods.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\j2jjifmto45jzep.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\hhuy\fndguil2ubhxleqmkv.odt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\uo7bfSHfyn-0X-MGd.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd-y4\02rh90y7rebgxw.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\mXrqWFqcp_fBV4xgh8cLcTD-y4\hyXqTEnB.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\Tb8Pl4n8ykiF82PGQ8M.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkl\6y-Gle7CJ.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\hhuy\z99M8Y1GRoOyuotMz.csv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\us8ywh8d_vcxiyflf5e.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\2twJZ0dzmRfJrmP6B.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\tPG-9VHK-ulBZl_Q.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\3lz_j5_6ki.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	Sample File, Accessed File, VM File	Access, Delete, Read, Write	MALICIOUS
c:\users\keecfmwgj\documents\hhuy\bju5iwgzcivxdeaczva1.odt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\zliy3__ym6-.csv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\ae6i4hslrl.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\MpjP3oSTE.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\cqa0h3g9.ppt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\hhuy\gGXI3yELI78C2wDp.pps.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\desktop\bq6sji8ro0rg0dp\3ysvczxv.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkl\2wJfl-RZYJEjLJl_Hmt.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\z2e0zt\zpv7u7xpwr7qk\iwi4py9f_tbuupcdk.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\hhuy\6a8RDH85d8whH-HX.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkl\a6C7l-Qq0p-ecvc_8DsT.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\6pw8rpgl-.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\tHLd WYzw.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE Add-on site.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ijdhlcko.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\p5fl21.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\l-ti2nvrpacp-tk9f.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\hhuy\ynkbyrnkc6j3avv0zier.odt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\v97V_KMwmgn4h6UDx.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkl\HbqLBzpGm.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	Dropped File, Accessed File, VM File	Access, Create, Delete, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\hhuy\NxH6NL2Af5s5IGX.doc.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\YZcqJ4cWJ.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\esAg2qtf u0s5C0MdPd.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\bmpgaj9.xlsx.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\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\1OTdzHn.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\yDPh4CpXgP3QwyUC\faTUjwnla.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\mxrqwfqcp\jze7xrus.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\mxrqwfqcp\xxli1eqxvup5i 0hs6g.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\n-nH-E2t.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\z2E0zT\g5znGT5HIbHq.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\HbBtrfj.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\hhuy\4q235s.pptx.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\Videos\z2E0zT\vtiS4AAZ_oK\s_e2a5ScpFSgR9-.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\music\bjhxlx\9ast-p\fgnl6u1fsaf.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\lxhmd.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\O_9gyTeSlm.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\iIfMhH\VL493DrYWM.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\823XfKbFCBWP.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C: \Users\kEecfMwgj\Music\mXrqWFqcp\o2CgGnJETcQ5zceImOM_. m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\D1q0P.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\J0ThFcHeulkvK.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\6s3WjoHyRIY3EiBz5-U.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\nmf9emihkrld8q1qs.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\Bk2Yjoq3Rz.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C: \Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMs W0c\powW2.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\bjhxlx\cmbsppstlrb9u.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\j6jnv8gx8rxbh.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\itjgP.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c: \users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0 c\rqja5oz7_uz\kyIqcyn6yv.pps.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents_dmv92xp.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\K0IcD1nSajNFFT.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\z2E0zT\kYxGt6chL81vzY.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\nQrFKLA.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\wnp_miikwb9ajxhhez.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\k_XON6PdpszzEOE.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\hhuy\naiaggm8s5tskx.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\bQ6SJi8RO0rg0dP\3YgFUJ.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\yDPh4CpXgP3QwyUC\BY rE6U_U.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\567c.pdf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\iIfMhH\tOBMO.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\2j2l02AsmvpG-FW9.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c: \users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0 c\wa_4pk0l7jwgqv.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\dygx.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\xudjwurucylo9.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\RDY1PliN5xV7.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\4COwR1C7ya7.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\VgPttkDeNDF2VRfHy.pps.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\K3t8MIfEa.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\cPfFJ9.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\BJHxLX\KnG7feMIAKlEoa_UW1s2.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\bjhxlx\9ast-p\dktsn5wki\4gn5bamth.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\i8obtvhhmb.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\mmfu p.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\olz6-jxmw7o1_h pvu.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\z2e0zt\zpv7u7xpwr7qk\1l1mbixtedk.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\0jip-0WU2n5fd8 POL.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents_3Wl5D4o0g2MKtP.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\hsxa8jyxcbsx17ja94r_.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\hhuy\ytkydbos.xlsx.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\Videos\z2E0zT\vtiS4AAZ_oK_qbp0nkGuotBuAqg\le5lbJNFps_4_oZKKr.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\38n2o1isspyqrtic8.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\z1niztmoyavazpqq.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\hDvzuhrdv.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\dnsctzwstnyxbfiqs.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\bq6sji8ro0rg0dp\9ecwyh_e3fhju.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\QYjbm5MiXLG2.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\cTaPN4HhRqe86tN.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\mXrqWFqcp\-xht.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\ghprnga3a e4cboqml8u.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\qq8tjsc3zm363.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\5h1grurzazne.docx.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\desktop\ldmozuncs-h9r3 xu2.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\yDPh4CpXgP3QwyUC\tNBhPX6T.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\desktop\rwqicw2qitxlv4.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\k0zmij7sn.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\ydph4cpxgp3qwyuc\x5tjkqt17l1kq.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\cmt4.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\ydph4cpxgp3qwyuc\aougfr90ajw.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C: \Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\a8eg.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\windows live\get windows live.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c: \users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\rookllxyjwewp5im.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\ilfMhH\5DS0X1cGBS4n2igZsE.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\6LeN1-BfLiBS.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\hhuy\8tiqyxue.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c: \users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\9zmn.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ZzmcSYQ7d6yY4Z.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\outlook files\franc@gdllo.de.pst.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://acacaca.org/test2/get.php?pid=DEC2E953FC80DE582D412ECFEAA51D7B&first=true	-	109.102.255.230, 41.41.255.235, 187.212.206.176, 195.158.3.162, 58.235.189.192, 190.117.75.91, 190.219.54.242, 211.171.233.126, 138.36.3.134, 109.98.58.98	-	GET	MALICIOUS
http://acacaca.org/test2/get.php?pid=DEC2E953FC80DE582D412ECFEAA51D7B	-	109.102.255.230, 41.41.255.235, 187.212.206.176, 195.158.3.162, 58.235.189.192, 190.117.75.91, 190.219.54.242, 211.171.233.126, 138.36.3.134, 109.98.58.98	-	GET	MALICIOUS
http://rgyui.top/dl/build2.exe	-	151.251.24.5, 46.195.219.190, 115.88.24.203, 110.14.121.125, 190.117.75.91, 222.236.49.124, 109.98.58.98, 190.107.133.19, 187.170.251.250, 211.119.84.111	-	GET	MALICIOUS
https://api.2ip.ua/geo.json	-	162.0.217.254	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
acacaca.org	109.102.255.230, 41.41.255.235, 187.212.206.176, 195.158.3.162, 58.235.189.192, 190.117.75.91, 190.219.54.242, 211.171.233.126, 138.36.3.134, 109.98.58.98	-	TCP, HTTP, DNS	MALICIOUS
rgyui.top	151.251.24.5, 46.195.219.190, 115.88.24.203, 110.14.121.125, 190.117.75.91, 222.236.49.124, 109.98.58.98, 190.107.133.19, 187.170.251.250, 211.119.84.111	-	TCP, HTTP, DNS	MALICIOUS
api.2ip.ua	162.0.217.254	-	TCP, HTTPS, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
58.235.189.192	acacaca.org	South Korea	DNS	CLEAN
41.41.255.235	acacaca.org	Egypt	TCP, HTTP, DNS	CLEAN
211.171.233.126	acacaca.org	South Korea	DNS	CLEAN
109.102.255.230	acacaca.org	Romania	DNS	CLEAN
190.219.54.242	acacaca.org	Panama	TCP, HTTP, DNS	CLEAN
162.0.217.254	api.2ip.ua	Netherlands	TCP, HTTPS, DNS	CLEAN
211.119.84.111	rgyui.top	South Korea	DNS	CLEAN
46.195.219.190	rgyui.top	Sweden	DNS	CLEAN
187.170.251.250	rgyui.top	Mexico	DNS	CLEAN
222.236.49.124	rgyui.top	South Korea	TCP, HTTP, DNS	CLEAN
187.212.206.176	acacaca.org	Mexico	DNS	CLEAN
195.158.3.162	acacaca.org	Uzbekistan	DNS	CLEAN
110.14.121.125	rgyui.top	South Korea	DNS	CLEAN
138.36.3.134	acacaca.org	Brazil	DNS	CLEAN
190.117.75.91	rgyui.top, acacaca.org	Peru	DNS	CLEAN
109.98.58.98	rgyui.top, acacaca.org	Romania	DNS	CLEAN
190.107.133.19	rgyui.top	Honduras	DNS	CLEAN
115.88.24.203	rgyui.top	South Korea	DNS	CLEAN
151.251.24.5	rgyui.top	Bulgaria	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}	access	1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion	access	1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\SysHelper	read, access, write	1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SysHelper	read, access, write	1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	CLEAN

Process

Process Name	Commandline	Verdict
1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	"C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe"	MALICIOUS
1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	"C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe" --Admin IsNotAutoStart IsNotTask	MALICIOUS
1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	"C:\Users\kEecfMwgj\AppData\Local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe" --AutoStart	MALICIOUS
1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	"C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe"	SUSPICIOUS
1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	"C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe" --Admin IsNotAutoStart IsNotTask	SUSPICIOUS
1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe	"C:\Users\kEecfMwgj\AppData\Local\4d45d74b-b67c-4b05-9c99-9061295dc2fa\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe" --AutoStart	SUSPICIOUS
icacls.exe	icacls "C:\Users\kEecfMwgj\AppData\Local\4d45d74b-b67c-4b05-9c99-9061295dc2fa" /deny *S-1-1-0:(OI)(CI)(DE,DC)	CLEAN

YARA / AV

YARA (282)

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\KUOPp2txHoo7bw7O.doc.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Contacts\Administrator.contact.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\msn websites\msn.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\hhuy\z99M8Y1GRoOyuotMz.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\videos\z2e0zt\zpv7u7xpwr7qk\rfes3vfwf3fsy6sx.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\itjgP.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\desktop\sj76amesi3jmtoue2hz\6pw8rpgl-.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\GW5kXQqybZPUP2d4.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd- y4\tlaiuy5vumxfxacjn.wav.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents_3Wl5D4o0g2MKtP.pptx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\bQ6SJi8RO0rg0dP\3YgFUJ.rtf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEhFXubwY\ilfMhH\5DS0X1cGBS4n2igZsE.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\Pictures\bQiz44uQ681_7Dctbgxp.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\nmf9emihkrld8q1qs.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\cPfFJ9.flv.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\567c.pdf.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\documents\hhuy\bju5iwgzcivxdeaczva1.odt.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\hhuy\rfixnl1vu2.ots.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\tkvyxwxrq.ots.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\olz6-jxmw7o1_h pvu.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\yOmL -Z4 9fyb2lF7S9.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\hhuy\ni1u7vxc2c n4uuhwh.pps.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\ijdhlcko.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\kyMAgs7f-4q1mza r\uo7bfSHfyn-0X-MGd.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\bq6sji8ro0rg0dp\9ecwyh_e3fhju.avi.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	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\rwqicw2qitxlv4.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\msn websites\msn autos.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\iIfMhH\9VRBBaa2E6cjsKGlie.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\ksif.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98.exe.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\hhuy\U-GFPMIYoqWy2p9O.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\mxrqwfqcp\jze7xrus.m4a.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\pictures\kir-tas9lgdeh fxubwy\ydph4cpxgp3qwyuc\aougfr90ajw.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\bjhxlx\cmbsppstlrb9u.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\Videos\z2E0zT\vtiS4AAZ_oK\s_e2a5ScpFSgR9-.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\Desktop\tHLdWYzw.ots.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkI\HbqLBzpGm.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\favorites\links\web slice gallery.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\BJHxLX\KnG7feMIAKlEoa_UW1s2.wav.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\6LeN1-BfLiBS.rtf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\wa_4pk0l7jwgqv.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\z1niztmoyavazpqq.rtf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\CzDS-.pptx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\BJHxLX\9AsT-P\dKtSN5wkI\6y-GIe7CJ.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\Documents\hhuy\Qs2 hK9Y_.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\iifmhh\pfzhnu297.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd- y4\-ahhgkvlxn_kxd.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\ydph4cpxgp3qwyuc\x5tjkqt17l1kq.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\Videos\hDvzuhrdv.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\nQrFKLA.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\K3t8MIfEa.mp3.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\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\rQja5oZ7_uz\EhqiUu8LglRl.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\z2e0zt\zpv7u7xpwr7qk\iwi4py9f_tbuupcdk.flv.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\hhuy\naiaggm8s5tskx.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\cTaPN4HhRqe86tN.rtf.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\mXrqWFqcp\-xht.wav.vvyu	Ransomware	5/5
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\Documents\2oZu1wT.ppt.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\4l3gkybFjpw5wc.rtf.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\kyMAgs7f-4q1mza r\2j2l02AsmvpG-FW9.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\BJHxLX\dTVoZ bX824b.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\4COwR1C7ya7.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\Desktop\sj76aMesI3jmtOuE2hz\UovhOsbqK0eMsW0c\0jip-0WU2n5fd8 POL.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\z2e0zt\zpv7u7xpwr7qk\1l1mbixt edk.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ldmozuncs-h9r3 xu2.mp4.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\cmt4.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\appdata\locallow\microsoft\internet explorer\services\search_{0633ee93-d776-472f-a0ff-e1416b8b2e3a}.ico.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\KiR-tAs9lgdEh FXubwY\v97V_KMwmgn4h6UDx.jpg.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\documents\py_fftiab_q4nwhp.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\dtf66.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\O_9gyTeSlm.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\la08fq2wwngfs3w9kc.swf.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\z2E0zT\vtiS4AAZ_oK\MpjP3oSTE.mkv.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\Music\BJHxLX\9AsT-P\dKtSN5wkl\a6C7l-Qq0p-ecvc_8DsT.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\mxrqwfqcp_fbv4xgh8clctd-y4\02rh90y7rebgxw.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\kir-tas9lgdeh fxubwy\5qvh55h.bmp.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\n-nH-E2t.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\hhuy\ynkbyrnkc6j3avv0zier.odt.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\lxhmd.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\i5zfv_jkmmjeubuqus.gif.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\BJHxLX\9AsT-P\dKtSN5wkl\GWrBK8mbOy.wav.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\qtnn2gz.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\hhuy\ytkydbos.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\outlook files\franc@gdllo.de.pst.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\z2e0zt\vtis4aaz_ok\b8gbt7knns9kt-gvh.swf.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\hsxa8jyxcbsx17ja94r_.jpg.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\kir-tas9lgdeh fxubwy\iifmhh\xudjwurucylo9.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\a9pzarvgiar.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\D1q0P.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\us8ywh8d_vcxiyflf5e.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\z2E0zT\vtiS4AAZ_oK\Asv9iqUaFA9rCWFze77.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\nwy04.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\ghprnga3a e4cboqml8u.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok\kvyeo7pecdl1br27xvac.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\Cc9_9V6aB.avi.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\Windows Live\Windows Live Spaces.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\kymags7f-4q1mza r\ydxrjd.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\music\mxrqwfqcp\xxli1eqxvup5i 0hs6g.mp3.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\tPG-9VHK-ulBZI_Q.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\kw5j7a5.doc.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\sj76amesi3jmtoue2hz\uovhosbqk0emsw0c\rqja5oz7_uz\kylqcyn6yv.pps.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\bjhxlx\rp0gg8vjq4u.wav.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\Favorites\Microsoft Websites\IE Add-on site.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\2uv3ozugwqu6cyc7-l.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\jw5nfujdo04vpw2wo.xlsx.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\z2e0zt\vtis4aaz_ok_qbp0nkguotbuaqg\m mfup.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\1IkZJVoATh.xls.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\HeOaqMZgOojF528t.odt.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\hhuy\jkSu2OlxWSDLnSWvMq.ods.vvyu	Ransomware	5/5

Reduced dataset

ENVIRONMENT

Virtual Machine Information

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

Platform Information

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

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

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

System Root	C:\Windows