MALICIOUS

Classifications: Downloader | Ransomware

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

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe**
ID	#5068403
MD5	b7ea7d444d1ed5677537a96796a496dc
SHA1	738054720787a8f80e3a4f1bd92f08b3084190aa
SHA256	0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5
File Size	738.00 KB
Report Created	2022-08-05 17:58 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (25 rules, 153 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #12) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #12) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 196 files by appending the extension ".vvyu".			
5/5	YARA	Malicious content matched by YARA rules	100	Ransomware

- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\7p5jbw.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url.vvyu".
- Rule "Djvu" from ruleset "Ransomware" has matched on a memory dump for (process #6) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\j ucK2lALp_iPp\znTr-YRiXJ\0VhP5.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\z8twgmunehqoxqfe1k.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\j ucK2lALp_iPp\47m5sv0uqVNl\AZ2aRaMGzQB\5B4VEsMcGlm7c.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu".
- Rule "Djvu" from ruleset "Ransomware" has matched on a memory dump for (process #2) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\wICCgSS9cO9EJxpugq\wx0aR91G76sZ.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\n6jq6ucc95w9.docx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\j uck2lalp_ipp\47m5sv0uqvnl\ah3jwn0.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\ysw9udfa\bzhliohmivg2h0_pvvuu.pps.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\hA6nEQ04cdHym7b8.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\favorites\microsoft websites\microsoft at home.url.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\ippAwK.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\6_x m.odp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\djRHD.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\eSfxo-E.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\oq0h.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\q-8_5alv-aysztdlcx.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\hfgog8brvbw\0se02.odp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\j ucK2lALp_iPp\47m5sv0uqVNl\LPB-FW9jvpM0h.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\bxv5ql2id 9hkdxpv7.swf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\9hkv.mp4.vvyu".
- Rule "Djvu" from ruleset "Ransomware" has matched on a memory dump for (process #12) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\m0zrf.mkv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\877l5thXMZRFuEmTVa.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\acppdj.avi.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\jkgjiq3h.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\liaafon99lah9nu_j.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\-ctdcbmthlrz.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Contacts\Administrator.contact.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\j uck2lalp_ipp\dibgo7.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\mOm18edC.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\ynpbsi277\bp67ry2e oyq1fpgm.mp4.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\fpzctgqi5ys\m fzx23r02sywxh\l6ehb4ojilkrcleahkh.avi.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\xnjf1rqetdtxtc.mkv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\uCbdvMv01ecUQrS5kFhR.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\3Ad0c.mkv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\f6adjjdhq\cuol988xnblbr.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\rn1rbbo1eqymg_q.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\khh4ja_ffudblb.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\5U0VVnc3NrOc8n_Z\k8_cI3l6hV1-Y7\27Qc0VUi07zkn_VUAary.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\85NDX4GNPa9.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397_dSq\EotVe.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\9Qfl6h6W74ZaGdKZ7l.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\26hKDH\dhVO\fwWKBmZrXnqYjnf.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\ooz2bcvbppeb9wsu.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\f6adjjdhq\adia hvz87jstj8m.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\26hkdh\dhvo\waqploj2c0tw.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\3YV6ib1olpsefRwtFe.pdf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\3_n mmyv5xkxtc1mbc-u.pdf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\tqpcqxkko-qtvp1zn.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\j uck2lalp_ipp\47m5sv0uqvnl\dvuuti6.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\i_u5ln.wav.vvyu".

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

- The sample itself is a known malicious file.
- Reputation analysis labels embedded file "C:\Users\kEecfMwgj\AppData\Local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe" as Mal/Generic-S.

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

- Reputation analysis labels the URL "http://acacaca.org/files/1/build3.exe" which was contacted by (process #6) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "http://rgyui.top/dl/build2.exe" which was contacted by (process #6) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe as Mal/HTMLGen-A.
- Reputation analysis labels the URL "http://acacaca.org/test2/get.php?pid=BBBCA5C4A1C0DD06A87561C44E271CCC&first=true" which was contacted by (process #6) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe as Mal/HTMLGen-A.

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

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

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

- Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\3YV6ib1olpsefRwtFe.pdf.vvyu".
- Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\3YV6ib1olpsefRwtFe.pdf.vvyu".
- Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "c:\users\keecfmwgj\documents\3_n mmyv5xkxtc1mbc-u.pdf.vvyu".
- Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "c:\users\keecfmwgj\documents\3_n mmyv5xkxtc1mbc-u.pdf.vvyu".
- Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HlmfL\4E_Qp5b8\RAN3RZLWQzdFaTXUwx\AFrd4UxBD1.pdf.vvyu".
- Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HlmfL\4E_Qp5b8\RAN3RZLWQzdFaTXUwx\AFrd4UxBD1.pdf.vvyu".

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

- (Process #2) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe deletes executed executable "C:\Users\kEecfMwgj\AppData\Local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe".

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

- (Process #6) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe has a thread which sleeps more than 5 minutes.

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

- (Process #12) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe tries to read sensitive data of application "git" by file.

Score	Category	Operation	Count	Classification
2/5	Injection	Writes into the memory of a process started from a created or modified executable	4	-

- (Process #1) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe modifies memory of (process #2) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.
- (Process #5) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe modifies memory of (process #6) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.
- (Process #7) build2.exe modifies memory of (process #8) build2.exe.
- (Process #11) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe modifies memory of (process #12) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.

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

- (Process #1) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe alters context of (process #2) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.
- (Process #5) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe alters context of (process #6) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.
- (Process #7) build2.exe alters context of (process #8) build2.exe.
- (Process #11) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe alters context of (process #12) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.

Score	Category	Operation	Count	Classification
2/5	Task Scheduling	Schedules task	1	-
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe", to be triggered by TIME. Task has been rescheduled by the analyzer.		
1/5	Obfuscation	Reads from memory of another process	4	-
	• (Process #1) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe reads from (process #1) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe. • (Process #5) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe reads from (process #5) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe. • (Process #7) build2.exe reads from (process #7) build2.exe. • (Process #11) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe reads from (process #11) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	4	-
	• (Process #1) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #5) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #7) build2.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #11) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.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) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe enumerates running processes. • (Process #6) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe enumerates running processes. • (Process #12) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe enumerates running processes.		
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #2) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe adds ""C:\Users\kEecfMwgj\AppData\Local\fa1eafca... ... 9-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe" --AutoStart" to Windows startup via registry.		
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #2) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe starts (process #2) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe with a hidden window.		
1/5	Mutex	Creates mutex	2	-
	• (Process #6) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe creates mutex with name "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}". • (Process #12) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe creates mutex with name "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}".		
1/5	Discovery	Tries to get network statistics	1	-
	• (Process #12) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe gets network statistics via API.		
1/5	Network Connection	Downloads executable	1	Downloader
	• (Process #6) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe downloads Windows executable via http from http://rgyui.top/dl/build2.exe.		
1/5	Network Connection	Downloads file	1	-
	• (Process #6) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe downloads file via http from http://acacaca.org/test2/get.php?pid=BBBCA5C4A1C0DD06A87561C44E271CCC&first=true.		
1/5	Obfuscation	Resolves API functions dynamically	7	-

Score	Category	Operation	Count	Classification
		• (Process #1) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe resolves 39 API functions by name. • (Process #2) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe resolves 37 API functions by name. • (Process #5) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe resolves 39 API functions by name. • (Process #6) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe resolves 37 API functions by name. • (Process #7) build2.exe resolves 43 API functions by name. • (Process #11) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe resolves 39 API functions by name. • (Process #12) 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe resolves 58 API functions by name.		

Mitre ATT&CK Matrix

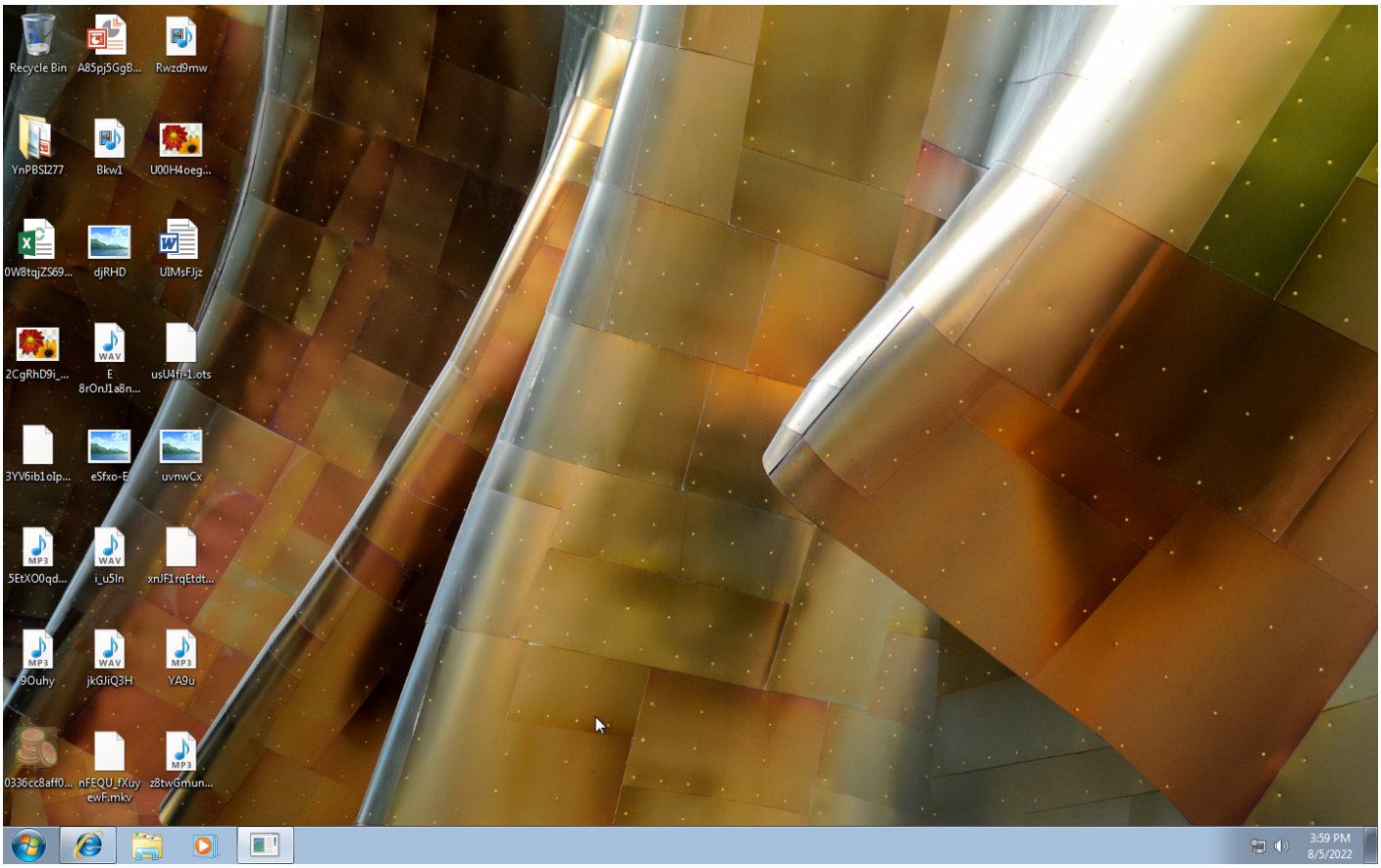
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1060 Registry Run Keys / Startup Folder	#T1053 Scheduled Task	#T1045 Software Packing	#T1081 Credentials in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

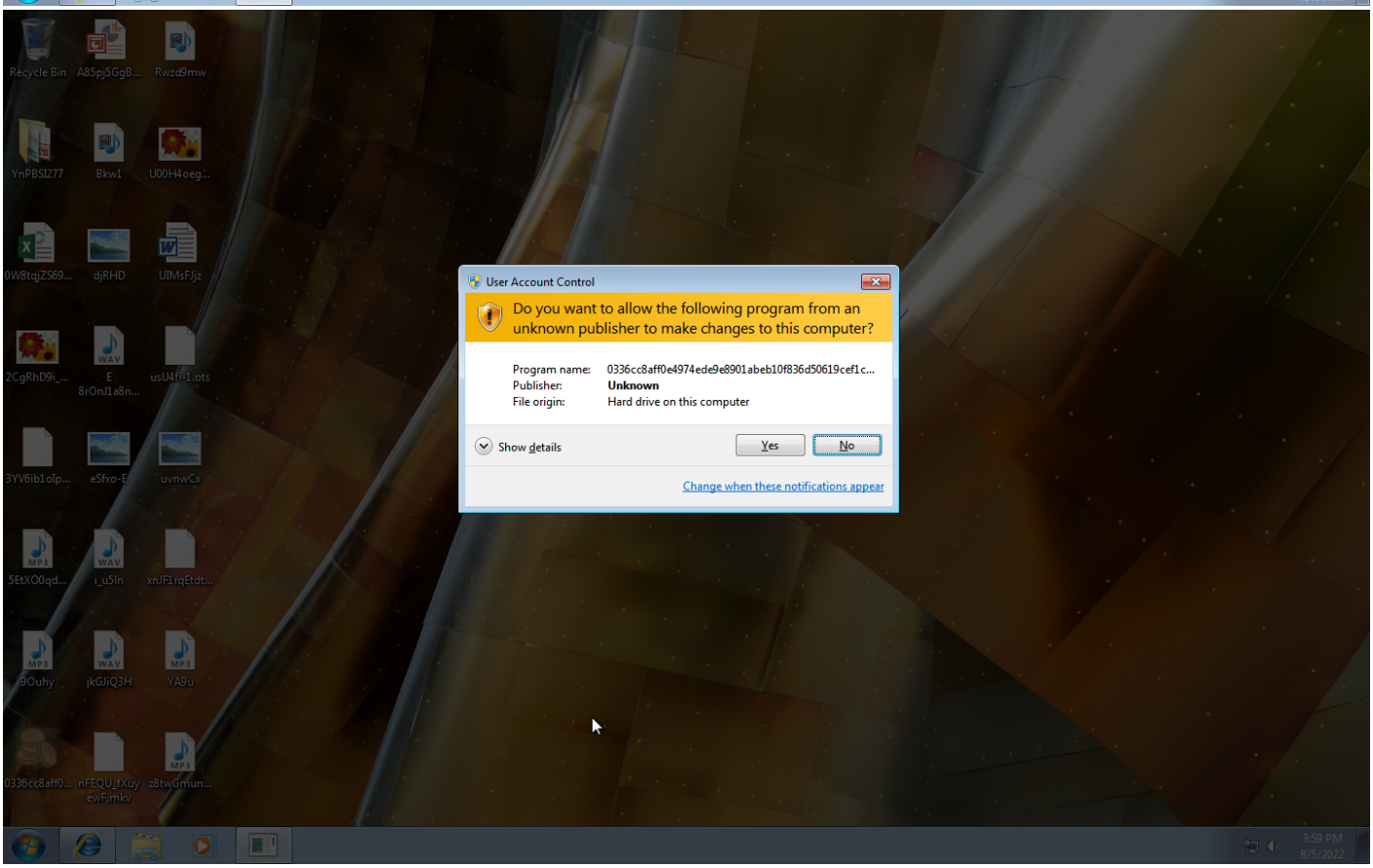
Sample Information

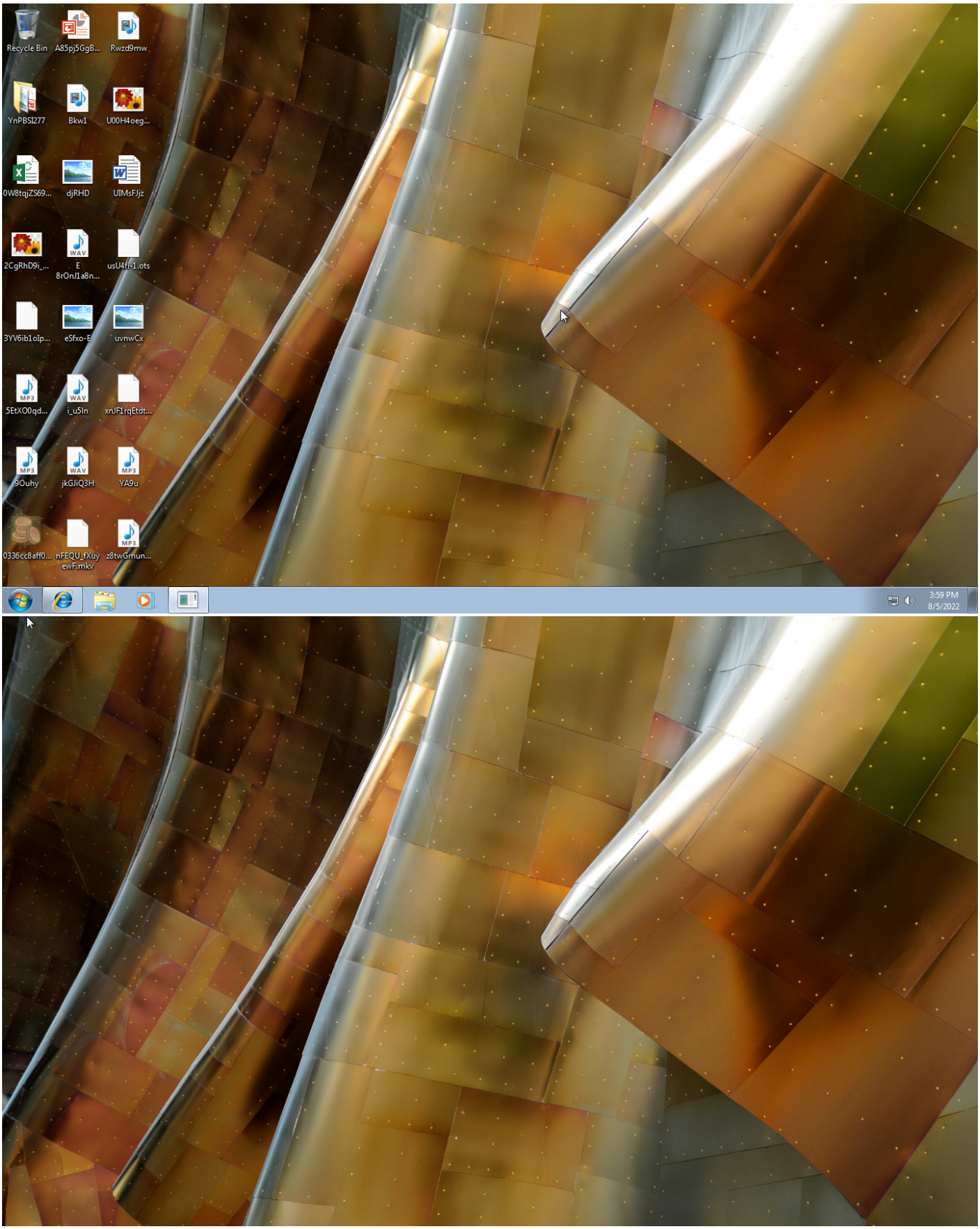
ID	#5068403
MD5	b7ea7d444d1ed5677537a96796a496dc
SHA1	738054720787a8f80e3a4f1bd92f08b3084190aa
SHA256	0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5
SSDeep	12288:P8i1GEboaDO//jjoN9oTUqJndee2eu2vIog/QMYPnGhGsDMaNidDXTVKEpK0lWgE:P8cGEbo9/bYendeNzog/QMXQQMaNkDDb
ImpHash	fcbdb87c73dba6603c8b6aba49ea683b
File Name	0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe
File Size	738.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 17:58 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	9
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	280


Recycle Bin
A85pj5GgB...
Rwzd9mw
YnPBSI277
Bkw1
U00H4oeg...
0W8tqjZS69...
djRHD
UIMsFJjz
2CgRhD9i_...
E 8rOnJ1a8n...
usU4fi-1.ots
3YV6ib1oIp...
eSfxo-E
uvnwCx
5EtXO0qd...
i_u5ln
xnJF1rqEtdt...
9Ouhy
jkGJiQ3H
YA9u
0336cc8aff0...
nFEQU_fXuy ewF.mkv
z8twGmun...
3:59 PM
8/5/2022


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1c...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

129.21 KB total sent

567.89 KB total received

4 ports 80, 443, 53, 445

4 contacted IP addresses

0 URLs extracted

4 files downloaded

0 malicious hosts detected

DNS

5 DNS requests for 3 domains

1 nameservers contacted

1 total requests returned errors

HTTP/S

4 URLs contacted, 3 servers

6 sessions, 8.06 KB sent, 475.27 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://acacaca.org/files/1/build3.exe	-	-		0 bytes	NA
GET	http://acacaca.org/test2/get.php?pid=BBBCA5C4A1C0DD06A87561C44E271CCC&first=true	-	-		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	189.164.252.207, 58.235.189.192, 211.59.14.90, 187.190.48.135, 210.182.29.70, 187.170.251.250, 31.166.90.88, 190.219.54.242, 211.119.84.112, 46.195.219.190		NA
A	rgyui.top	NO_ERROR	46.195.219.190, 187.156.10.94, 187.232.183.77, 138.36.3.134, 148.255.22.239, 124.109.61.160, 109.102.255.230, 211.40.39.251, 186.6.205.61, 187.170.251.250		NA

BEHAVIOR

Process Graph

Process #1: 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 59334, Reason: Analysis Target
Unmonitor End Time	End Time: 76533, Reason: Terminated
Monitor duration	17.20s
Return Code	0
PID	3728
Parent PID	1916
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	738.00 KB	0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5	✖

Host Behavior

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

Process #2: 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 71654, Reason: Child Process
Unmonitor End Time	End Time: 101407, Reason: Terminated
Monitor duration	29.75s
Return Code	0
PID	3744
Parent PID	3728
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\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xe94	0x400000(4194304)	0x400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xe94	0x401000(4198400)	0xca600	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xe94	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xe94	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xe94	0x52b000(5419008)	0x200	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xe94	0x52c000(5423104)	0xa400	✔	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xe94 / 0xea4	0x76f101c4(1995506116)	-	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xe94	0x7efde008(2130567176)	0x4	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	738.00 KB	0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5	✖

Host Behavior

Type	Count
System	4
Module	47
File	6
Environment	1
Process	94
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\fa1eafca-d2cd-4c04-a099-4159a69291ac" /deny *S-1-1-0:(OI)(CI)(DE,DC)
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 96350, Reason: Child Process
Unmonitor End Time	End Time: 97984, Reason: Terminated
Monitor duration	1.63s
Return Code	0
PID	3784
Parent PID	3744
Bitness	32 Bit

Process #5: 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 99044, Reason: Child Process
Unmonitor End Time	End Time: 103217, Reason: Terminated
Monitor duration	4.17s
Return Code	0
PID	3800
Parent PID	3744
Bitness	32 Bit

Host Behavior

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

Process #6: 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 101548, Reason: Child Process
Unmonitor End Time	End Time: 124078, Reason: Terminated
Monitor duration	22.53s
Return Code	0
PID	3812
Parent PID	3800
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\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xedc	0x400000(4194304)	0x400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xedc	0x401000(4198400)	0xca600	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xedc	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xedc	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xedc	0x52b000(5419008)	0x200	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xedc	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xedc	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#5: c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0xedc / 0xee8	0x76f101c4(1995506116)	-	✔	1

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe	438.00 KB	12a51367c5c85ff3c1dc73743cface2e01accecf2879a36adbddf566d52987b3	✖
C:\SystemID\PersonalID.txt	42 bytes	133276d46de8f4c5849b7ee9536406e0edfc2608134b2b0e4467d9e51c209f03	✖

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

Host Behavior

Type	Count
System	4
Module	47
File	61
Environment	1
Process	93
Registry	7
COM	1
-	2
Mutex	1
User	1
Window	1
-	3

Network Behavior

Type	Count
HTTP	3
HTTPS	1

Process #7: build2.exe

ID	7
File Name	c:\users\keecfmwgj\appdata\local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 110771, Reason: Child Process
Unmonitor End Time	End Time: 118239, Reason: Terminated
Monitor duration	7.47s
Return Code	0
PID	3856
Parent PID	3812
Bitness	32 Bit

Host Behavior

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

Process #8: build2.exe

ID	8
File Name	c:\users\keecfmwgj\appdata\local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 117011, Reason: Child Process
Unmonitor End Time	End Time: 122349, Reason: Terminated
Monitor duration	5.34s
Return Code	1073807364
PID	3872
Parent PID	3856
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#7: c:\users\keecfmwgj\appdata\local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe	0xf14	0x400000(4194304)	0x400	✔	1
Modify Memory	#7: c:\users\keecfmwgj\appdata\local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe	0xf14	0x401000(4198400)	0x34000	✔	1
Modify Memory	#7: c:\users\keecfmwgj\appdata\local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe	0xf14	0x435000(4411392)	0xde00	✔	1
Modify Memory	#7: c:\users\keecfmwgj\appdata\local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe	0xf14	0x443000(4468736)	0x1c00	✔	1
Modify Memory	#7: c:\users\keecfmwgj\appdata\local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe	0xf14	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#7: c:\users\keecfmwgj\appdata\local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe	0xf14 / 0xf24	0x76f101c4(1995506116)	-	✔	1

Host Behavior

Type	Count
System	6
Module	23
File	3
Environment	1

Process #11: 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe

ID	11
File Name	c:\users\keecfmwgj\appdata\local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe" --AutoStart
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 167383, Reason: Autostart
Unmonitor End Time	End Time: 171567, Reason: Terminated
Monitor duration	4.18s
Return Code	0
PID	1896
Parent PID	1784
Bitness	32 Bit

Host Behavior

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

Process #12: 0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe

ID	12
File Name	c:\users\keecfmwgj\appdata\local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe" --AutoStart
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 170580, Reason: Child Process
Unmonitor End Time	End Time: 202110, Reason: Terminated
Monitor duration	31.53s
Return Code	0
PID	2008
Parent PID	1896
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#11: c:\users\keecfmwgj\appdata\local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0x76c	0x400000(4194304)	0x400	✔	1
Modify Memory	#11: c:\users\keecfmwgj\appdata\local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0x76c	0x401000(4198400)	0xca600	✔	1
Modify Memory	#11: c:\users\keecfmwgj\appdata\local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0x76c	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#11: c:\users\keecfmwgj\appdata\local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0x76c	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#11: c:\users\keecfmwgj\appdata\local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0x76c	0x52b000(5419008)	0x200	✔	1
Modify Memory	#11: c:\users\keecfmwgj\appdata\local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0x76c	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#11: c:\users\keecfmwgj\appdata\local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0x76c	0x7efde008(2130567176)	0x4	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#11: c:\users\keecfmwgj\appdata\local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	0x76c / 0x7dc	0x76fb01c4(1996161476)	-	✔	1

Dropped Files (199)

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\pictures\7p5jbw.jpg.vvyu	91.94 KB	e0649b07f8980eb14453d11ed6c62dd68e825c5387bedaf90c53ae45f843e51c	✔
C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url.vvyu	467 bytes	6ed5bb4cb46be31f7f5b2268132d8f103c443cfa6a55032b087ebb6a8123c92d	✔
C:\Users\kEecfMwgj\Music\j ucK2lALp_iPp\znTr-YRiXJ\0VhP5.wav.vvyu	9.79 KB	137d38ac33c1b5827393d3d28176e18cd73a645bcbbdd6dbcf0765a546a49194	✔
c:\users\keecfmwgj\desktop\z8twgmunehqoxqfe1k.mp3.vvyu	88.39 KB	e20613dac0ca2d223af4707d51d1974b6a3285ad1fb762cc320ab5b6ab02bed5	✔
C:\Users\kEecfMwgj\Music\j ucK2lALp_iPp\47m5sv0uqVNl\AZ2aRaMGzQB\5B4VEsMcGlm7c.mp3.vvyu	38.94 KB	320eacd706d495117967f5b44d7df835cdc2bf13b7ed7a63b3a431841cc0825e	✔
c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu	467 bytes	2b0c2eba662593f4b003e70266fae0e4e181ed3aa4c49dc387dacd1b4ea76ef4	✔
C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\wICCgSS9cO9EJxpugq\wx0aR91G76sZ.flv.vvyu	92.28 KB	33b0820aa114f40bb3a4419eb95a0e5dc5a27281b042281d7f619166f933c6ab	✔
c:\users\keecfmwgj\documents\n6jq6ucc95w9.docx.vvyu	38.44 KB	bf00118fe5bed1175dd6af4c0b2ee63378eb4a85347d5b22e7d0694aca03f842	✔
c:\users\keecfmwgj\music\j uck2lalp_ipp\47m5sv0uqvnl\ah3jwn0.wav.vvyu	81.86 KB	cb9ca7d3e1e477c2cc69f58fd50615d64efa4f0f60fc868c9f405b0e933c1345	✔
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\ysw9udfa\bzhliohmivg2h0_pvvuu.pps.vvyu	12.51 KB	108448ce429c253e0fe11b281ce58ebde0dfe737413b8d8d369e45fea459e451	✔
C:\Users\kEecfMwgj\Videos\hA6nEQ04cdHym7b8.flv.vvyu	16.02 KB	477cfa8b80489db2df199d97ffac092f5fb72dda5360f24d129a05be5b2fe372	✔
c:\users\keecfmwgj\favorites\microsoft websites\microsoft at home.url.vvyu	467 bytes	0709b027e07743baa3b348053115229674d7c286c02f8bc4d5154e8719740936	✔
C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\ippAwK.flv.vvyu	46.00 KB	72d6a52150a653cc2f759f144e23f267836174ff56536f090772f6404a2e1c23	✔
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\6_x m.odp.vvyu	93.62 KB	a65e198609344df277b69c1d993e5168b471774536f8d15ee6ee01956e09f16c	✔
C:\Users\kEecfMwgj\Desktop\djRHD.jpg.vvyu	80.19 KB	e38000f5814848d4aae76c76fb9bb3fb8381df426cfb85b758c3b2d658e7f8b7	✔
C:\Users\kEecfMwgj\Desktop\eSfxo-E.jpg.vvyu	66.29 KB	22f798e9e6734a1c7af3aa84784ec36c5e71f31b2f43ca905d571b2ea846de58	✔
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\oq0h.flv.vvyu	67.87 KB	64279fa395a3d18745c4e3dac3cc7cf3a7b7c08e06b52cc564b702cfb6280bd4	✔
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\q-8_5alv-aysztdlcx.m4a.vvyu	38.38 KB	704fd863f914a31bb2d7caa2a2bf9e173d99eee8f226e70bf41783b695eba6b2	✔
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\hfgog8brvbw\0se02.odp.vvyu	21.63 KB	b1b6a2565aa33567cde2e05f259c57921d970af9c462c6874bbe93f603b6f616	✔
C:\Users\kEecfMwgj\Music\j ucK2lALp_iPp\47m5sv0uqVNl\LPB-FW9jvpM0h.wav.vvyu	28.07 KB	1dc7439c1f5f44c105f26282d016c75090293b523a75254afcb75a7408c0179b	✔
C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url.vvyu	468 bytes	f474f259c2309971964809e02e0cd1405203887427109cb523bee1cff9a7f2ff	✔
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\bxv5ql2id9hkdxpv7.swf.vvyu	36.30 KB	cdda1cd1b95414730f5fc7c3b43e3fd5c9947725c733689c19346ecc1f91d003	✔
c:\users\keecfmwgj\videos\9hkv.mp4.vvyu	87.31 KB	1cbf4c4ca05747ef89ce3fd9250bdc7944e4fc9468b1b40f343ee80c42b5ffa2	✔
c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.vvyu	738.33 KB	83aa737c7669451a99eeb4bd9fb0dade14873eafb501c892890964bdb9aed929	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\m0zrf.mkv.vvyu	92.26 KB	1bf152697eac08d5f62d44cc9905e149abe68d6bbdb21499602bfb0d77097d29	✔
C:\Users\kEecfMwgj\Pictures\877l5thXMZRFuEmTVa.png.vvyu	7.66 KB	815a7845da9b9335f529f808bd56f2f19ac83b1b3028bca5dc1791c209528179	✔
c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\acppdj.avi.vvyu	70.65 KB	c7b8ea486f52947445a6c21fddd4ce799b0387675b152181398f66e9da1fad0f	✔
c:\users\keecfmwgj\desktop\jkgjiq3h.wav.vvyu	32.54 KB	2a6e0d6157b8f7725f6860537e7122c55306a7cdb82f0f51e3444f363352bc05	✔
c:\users\keecfmwgj\documents\liaafon99lah9nu_j.xlsx.vvyu	92.22 KB	438c96c1ec8245d5a39986409478e2b28fc6216182be32656f9a2757c29fa915	✔
c:\users\keecfmwgj\pictures\-ctdcbmthlrz.jpg.vvyu	11.41 KB	d6198e57c7501b62635ea7f258215e9761db8c3c9372495e4d76f293bdf8670d	✔
C:\Users\kEecfMwgj\Contacts\Administrator.contact.vvyu	67.11 KB	1cc040019abce493d0e11defae2b0118304526b013941d015b56920e25066a50	✔
c:\users\keecfmwgj\music\j uck2lalp_ipp\dibgo7.wav.vvyu	48.61 KB	276d5057fd6ad3451b4e0fe8ad2a1d3587d69d236f0288b43c807913f2e4f1d1	✔
C:\Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\mOm18edC.mp3.vvyu	95.57 KB	3272fffda9e42b0bafdff0cc8905db24c10abc3370ea28aee55bf159131023b3	✔
c:\users\keecfmwgj\desktop\ynpbsi277\bp67ry2e oyq1fpgm.mp4.vvyu	63.37 KB	970bbaadcda492a43ccb533be7a12f7823b463a76e4c3be1f6d831c6c86527b1	✔
c:\users\keecfmwgj\videos\fpzctgqi5ys\mfzx23r02sywxh\l6ehb4ojilkrcleahkh.avi.vvyu	65.58 KB	d40e122dc6d86d508cc177ff545a0bb92a80b25642e6c8d4a47a82fb44005e66	✔
c:\users\keecfmwgj\desktop\xnjf1rqetdtxtc.mkv.vvyu	67.02 KB	8fe25390981b9d53f86acc8c31d1d1227a88fc3e13075d58819e40c39a477992	✔
C:\Users\kEecfMwgj\Pictures\uCbdvMv01ecUQrS5kFhR.gif.vvyu	98.09 KB	f5737997452e2611d4a891ab81fa875bdd904995904a70f13d279a820c0afc85	✔
C:\Users\kEecfMwgj\Videos\FPzctgql5yS\3Ad0c.mkv.vvyu	69.36 KB	11bc3b72c4e5558f5d97d0e19e5162693bd93d6fcf69ace580bf6c26b49871bf	✔
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\f6adjjdhq\cuol988xnblbr.m4a.vvyu	99.27 KB	306562f09762e1815c597567400e33072801810bffa398a82c7a509a4caa87a3	✔
c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu	467 bytes	8a15abf89f297426daa013cb2c918827c9a9dd603977930a4f3822c44d24f300	✔
c:\users\keecfmwgj\documents\rn1rbbo1eqymg_q.xlsx.vvyu	49.35 KB	0e002c115d35d2f84e18e9d47e6a54861ae4b39d186fcdf993f702d443c9d627	✔
c:\users\keecfmwgj\pictures\khh4ja_ffudblb.gif.vvyu	28.99 KB	2adef906c71dcea126662dad6b1f8a2b74f5703f4087fdfb63ced7d121ba6834	✔
C:\Users\kEecfMwgj\Music\5U0VVnc3NrOc8n_Z\k8_cI3l6hV1-Y7\27Qc0VUi07zkn_VUAary.wav.vvyu	69.90 KB	59c9c92684aae5e5832d34922f2a143b64b957d9f92dc5405cb69ca2620ed4a7	✔
C:\Users\kEecfMwgj\Music\85NDX4GNPa9.m4a.vvyu	32.30 KB	929283c4a3c541a98eb0ee2256e1664e01200899e6115821e5c57a466fea4e1b	✔
C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397_dSq\EotVe.bmp.vvyu	12.00 KB	67afdf10d7df308b3f9e1489c3dc0108698eb662e88586e3affe465fd74923c0	✔
C:\Users\kEecfMwgj\Music\9Qfl6h6W74ZaGdKZ7l.m4a.vvyu	60.85 KB	f23d8074f6577945e92a5bbf20022a6dbbf088f99fee0f477fc3467017716683	✔
C:\Users\kEecfMwgj\Music\26hKDH\dhVO\fwWKBmZrXnqYjnf.mp3.vvyu	43.82 KB	21423f3439da7e389a1f71f7621fa13075b53e9365b0e100c24c42f170cc3f71	✔
c:\users\keecfmwgj\pictures\ooz2bcvbppeb9wsu.png.vvyu	22.76 KB	523fbe08528681f2060ba07be4516c7cbf5a54156300890dca6d4fb411dd6b84	✔
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\f6adjjdhq\adiahvz87jstj8m.flv.vvyu	37.91 KB	ba8ee90fb4e6ec2eb044148b62c6b338d6318621b5b79fc9faf813a8f3af27b4	✔
c:\users\keecfmwgj\music\26hkdh\dhvo\waqploj2c0tw.wav.vvyu	74.06 KB	074fb4b529099065f17b55b89bf579b3c132ea349e7af2b9a7c9fd772ab05f40	✔
C:\Users\kEecfMwgj\Desktop\3YV6ib1olpsefRwtFe.pdf.vvyu	8.26 KB	6ab20d8ff33f670160c028f34545b13504be5cf1cad4c2e5d96b746b1ceab8ce	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\documents\3_n mmyv5xkxtc1mbc-u.pdf.vvyu	20.80 KB	6e6db717fb1c9f846f54d9c5d916517ea94aa26999f357553bbad3b4a1db73a2	✔
c:\users\keecfmwgj\pictures\tqpcqxkko-qtvp1zn.bmp.vvyu	6.29 KB	1ed025869f19808fec07e0ee81d5afffa5ddfa81d88798164e7c0133a32c995e	✔
c:\users\keecfmwgj\music\juck2lalp_ipp\47m5sv0uqvnl\dvuuti6.wav.vvyu	3.53 KB	ad6859a70222b9b61b4eeccceeed2413949b3ad03ba07089f2e2b6191ba13e3d1	✔
C:\Users\kEecfMwgj\Desktop\i_u5ln.wav.vvyu	12.34 KB	f7b16be008a4cbb8c8c7fbd5073b4d33e92804113a53d6bf6c9d331fa47ac063	✔
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\hfgog8brvbw\hsj_qr5bne5moizbn.csv.vvyu	24.55 KB	f77d7c8ac5555b713d4645ab46c39e2343079d2128f8fbba66910ab9a101ac77	✔
C:\Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\6X4EOyI76e.wav.vvyu	6.79 KB	369a6fcbfb7e593deab1c3078dd09854aa1be1f7a558f7e8cb6d7ce5151ace65	✔
c:\users\keecfmwgj\appdata\locallow\microsoft\internet explorer\services\search_{0633ee93-d776-472f-a0ff-e1416b8b2e3a}.ico.vvyu	4.51 KB	03ce2c42137a2ed7f7982a542f1a4de1bec7770a313a51cd03ba43335e9cc63b	✔
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\v_uid 9u5nghf.docx.vvyu	91.89 KB	585c8b95f26c7627bda14fb6b8d2aedeb0ae285e57d99be6d4339d4151cfa9af	✔
C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\NMttoz1zVMuEbci.swf.vvyu	37.85 KB	23c3f3d274223e835e7f4ca8dc560b9d0927f676aaa3e817708d3b8fd7224db9	✔
c:\users\keecfmwgj\pictures\3uvy.jpg.vvyu	39.85 KB	ee087460e166a03fcedaadd8d6493d71b26dcdc7e7c386d5c12e1e8a95370e54	✔
C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Work.url.vvyu	467 bytes	49c131171f65e3ee0626a16a5add15e92235d3fd925f3ff6f593b0de592b8b83	✔
C:\Users\kEecfMwgj\Documents\5usDb JNuS3uVdkW.xlsx.vvyu	32.64 KB	c59219b2f92fab1080562071eb98b2d530531ea9c5dacdc33d7b170a948a78ec	✔
C:\Users\kEecfMwgj\Pictures\hyglyDuy.bmp.vvyu	42.72 KB	00a58c5262f0a9db213000248c1970c3a95e8ad252e7c84ba3936104ec5787e3	✔
c:\users\keecfmwgj\videos\fpzctgqi5ys\0ipri83h.flv.vvyu	79.47 KB	d25a1e4c3f238cc735debf26cfd59b059a01279f76d68b3bb604c137ea20e6e5	✔
c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.vvyu	738.00 KB	0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5	✖
c:\users\keecfmwgj\pictures\qg2uxz3cw8a4fuol_l.gif.vvyu	36.67 KB	3735b45dfc823e67d5bcfc021c2b539b5f6ef3c45feec336e8890b9d1b067a99	✔
c:\users\keecfmwgj\desktop\ynpbsi277\ov6fzg.bmp.vvyu	3.59 KB	ae945708982b679620f07d3eafc8c45513a0c9f6829ecbb470ffa28d0151fd46	✔
C:\Users\kEecfMwgj\Desktop\U00H4oegdjWIv9LIU5.png.vvyu	77.70 KB	fdb790c9ed0e8af4b520553c51f0346c15a7bf2350a615d55ee46d1ce4a292d2	✔
c:\users\keecfmwgj\favorites\msn websites\msn sports.url.vvyu	467 bytes	c11a499cb36e5d4ae5fe4655315550832e50055bccf0ab54e1d6b91045d6b9e2	✔
c:\users\keecfmwgj\desktop\uimsfjjz.rtf.vvyu	56.92 KB	6fd80b37d46091ab42ea621f5cac138a5e0d99231e03b019880b9e44ba196420	✔
c:\users\keecfmwgj\favorites\links\web slice gallery.url.vvyu	560 bytes	8873062cd0684d82ed284dedb3fc98e31ff890b76a80f3cdcf4ac3e1fc6bda2b	✔
c:\users\keecfmwgj\pictures\rwx9qkj.png.vvyu	97.64 KB	a59aeb1cc8bc0c3714bcebc4bccaaf7384727622961a59cc5774619b1f1a4890	✔
C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Spaces.url.vvyu	467 bytes	abe0378f08fdfd7f0936a029d0e9a457965e7aafd9f254c22b730c5d0eed7a0a	✔
C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Gallery.url.vvyu	467 bytes	9e1c10571eeb00a8eae7a33a17d57886578c810034d26c04fa4369e4edf83786	✔
C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\hfGoG8BRVBw\DJyNf5d3ZVp0RV8Gb.docx.vvyu	70.19 KB	36259635cc41b60c80d665a39713d31446978f28156885be17fabacba0640e5e	✔
c:\users\keecfmwgj\desktop\ynpbsi277\hak2yhq7o.jpg.vvyu	91.08 KB	5ff72d7d56b6103e200e19cec2ade68ed269dc9efc400eed69968f6a3ce58b2e	✔
c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\cjrduvousoi.swf.vvyu	93.84 KB	1b6d871292c51b00684abe0d937fbb173ce36afbc43c12e03585f13f60d15f4d	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\pictures\vauzy4mlwuoc1eph.bmp.vvyu	19.34 KB	e664700d5a11d0c21232a95a42d663303c5a490e3f8ac1223cdb80a632df1347	✔
c:\users\keecfmwgj\music\j uck2lalp_ipp\zntr-yrixj\f8ilkitdoj8fsshi0.mp3.vvyu	87.89 KB	a6a271da428b15c51aa3b4f7e0329a82dcb4d82445576da2dab6641ede2103f4	✔
C:\Users\kEecfMwgj\Desktop\usU4fi-1.ots.vvyu	41.79 KB	68f540b64b8b7f61a5dcca2c3eb7781d6bf40d92c9e0e94bccaa8f920d9c0f5b	✔
c:\users\keecfmwgj\videos\fpzctgqi5ys\mfzx23r02sywxh\btrak.swf.vvyu	38.85 KB	aa09895ab60d8f81821665f8167ffe914deb6e85258bedf59c7c077cca028921	✔
C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HImfL\4E_Qp5b8\RAN3RZLWQzdFaTXUwx\AFrd4UxBD1.pdf.vvyu	18.94 KB	05a3902fa069f8ef4c4c96db4e4d8860d67fd4f46333babef27dfadbc2a2e694	✔
C:\Users\kEecfMwgj\Documents\RUCPVLyvfQF00lxB1.xlsx.vvyu	24.08 KB	179ba120095be1827615ef2ab64da8096df799f1a82c9383694fe0b77e9d2a79	✔
C:\Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\sTzvqONg_kzYdubo TTT.mp3.vvyu	27.34 KB	ab6942fb22806f4e815892b8b201da5fce970d5a04652b4b6ee37c17e62c3410	✔
c:\users\keecfmwgj\music\j uck2lalp_ipp\zntr-yrixj\mlh8upb9ymlbt.mp3.vvyu	45.42 KB	c95ec3557951604c5ace04735735a6e09cc8d53aca4f58fb4e3e1750a6d28f71	✔
C:\Users\kEecfMwgj\Pictures\DvPtakSDSqUBk1s-p5E_.jpg.vvyu	83.21 KB	3806b4441fd3ee3be7eae7460c6fbb849b86c0da97dc5b99df03a106832545f1	✔
C:\Users\kEecfMwgj\Documents\92-ieu- ecANbCAHxu3.pptx.vvyu	3.33 KB	a6104fb3fce294a226ef72c0a2977f24b83a474eafb88ebf4ffd9baa6195d17d	✔
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397_dsq\ywywxyty.mp3.vvyu	40.98 KB	4718f246c07568dda7c0deaf748b6d89660620cb91e76a43311f96224976d00e	✔
C:\Users\kEecfMwgj\Music\26hKDH\l5cha-37fB.mp3.vvyu	21.51 KB	503fb88d60626a697d9be83a34fdffee9c48dc5dab581c5f56f1523bc3f05b91	✔
c:\users\keecfmwgj\videos\z x z-1adfcazuf.mkv.vvyu	59.58 KB	bb600930855b5279efde2f28474664aadf14656b38ee6a37cf7ae261f9a1ce48	✔
c:\users\keecfmwgj\pictures\ujyi1dwdud6-j7pcelmb.png.vvyu	79.21 KB	babb7957ceb47a4e663a683308d60aa822bfba258cdc372ae18d9d8b149caa0d	✔
c:\users\keecfmwgj\desktop\9ouhy.mp3.vvyu	54.02 KB	e2eb787ed8fec96326356c6b859974ef29a4fcd99dc9e084507a65d94e3106ad	✔
c:\users\keecfmwgj\pictures\go3r.jpg.vvyu	54.58 KB	84c7f12e6ca2640bb76d80acebdfda731874b8ad266202bac029addc3c54227f	✔
C:\Users\kEecfMwgj\Music\26hKDH\dhVO\c-p32.m4a.vvyu	47.69 KB	e942870bcd555c84703d0bdd3e010492513d01850ac52f57c50b5227b4e55e90	✔
c:\users\keecfmwgj\pictures\vuc5gusp1h33w.png.vvyu	54.87 KB	68d5ab5e7cd0402af32d5629b4f6277da120661e72e4924d176a26e5132489dd	✔
c:\users\keecfmwgj\favorites\msn websites\msn autos.url.vvyu	467 bytes	1dbe197123855db6c0b652d49c034c991aba657954b47e48762480682d147c68	✔
c:\users\keecfmwgj\favorites\msn websites\msn.url.vvyu	467 bytes	b898e95d61d2fd7e8ca2ea851b881e17569b5139ed738bf696f44c4a9b8c2f33	✔
C:\Users\kEecfMwgj\Videos\07H2voZRMEM4mGd_N.swf.vvyu	88.10 KB	799bf5cde2cabce0073d8629d8159a9ec2eb1a0c818004d433d7fe20834cf897	✔
C:\Users\kEecfMwgj\Pictures\sfoK-fQjQEuAHhw.jpg.vvyu	45.92 KB	f6d62c54c0db829bcbdf0cd6386b5dd5f9780c1bfddadb920c97361af739805b	✔
c:\users\keecfmwgj\pictures\iv7y.bmp.vvyu	92.49 KB	0d695567a4ccd8343fdb9956f775984a3c3dc0ed646279c04b8c43b8c5a30be0	✔
C:\Users\kEecfMwgj\Videos\x7DOA nu7EAlTL.mkv.vvyu	3.56 KB	4a1e187cb85b2bf08b1c30b88aa514e97b80abc12d99f3c20fd14d9d21c0d703	✔
C:\Users\kEecfMwgj\Desktop\YnPBSl277\YZ4wuGCPKPt9a.pps.vvyu	63.44 KB	4feb9529a7f139f6e117a297299739dd39f81220d4541d6954388772a5c5dbd7	✔
c:\users\keecfmwgj\desktop\0w8tqjzs69qqxvzs-d8d.ods.vvyu	57.59 KB	b9365ceb3516d459562bd64c32c5bc15288ec05a0ac3c30e076803ebd366b6ea	✔
C:\Users\kEecfMwgj\Videos\FPzctgql5yS\MfZX23r02sYWxh\DyXmYMfEW2zZ74G.avi.vvyu	18.76 KB	1b91cea1f7fe4d9195c5eac0d587b466498f4800801565c928289a88c669303a	✔
C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\Y3zc_VVY6Kxz1vjr.mp3.vvyu	55.63 KB	d18be34b949327d4e690797a4349d76d03ed0e8e0ee4da9f698fc4b7988c9509	✔

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\7lrwy.flv.vvyu	88.96 KB	729abc5616e8fccacdb0bcaec563b05d3517e042ec8f8588b6ab68fd0a9a107b	✔
C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\L59EH_1g_s_fJjq.mp4.vvyu	36.14 KB	8afb8f3689798274f15530735bdbd27a107bf85598c9fe4bdce26da8ec387c7d	✔
c:\users\keecfmwgj\pictures\lv2axv.jpg.vvyu	44.83 KB	7bd3d1d4c340529940bd24bb1e76873d818d824007b1ac79ac602a6fde7e39f9	✔
c:\users\keecfmwgj\videos\fpzctgqi5ys\mfzx23r02sywxh\0yoyfg2vyekk-r.swf.vvyu	29.08 KB	35fde246db17586abccd1a7d6ffbced608a21008091b94369365427e28effde6	✔
C:\Users\kEecfMwgj\Desktop\E 8rOnJ1a8nkX -7zzxk.wav.vvyu	6.86 KB	fa601ad4c51ca91df75647713f3599030ddaab354e222182e67898adcd4fc3d6	✔
c:\users\keecfmwgj\pictures\oq7rosq7byockq_wi3.gif.vvyu	84.80 KB	6735a1b15c6371fd621a54b655e4eeaae0277985fc4adcec0a05bdaea1befd0f	✔
C:\Users\kEecfMwgj\Desktop\2CgRhD9i_8EFMrM.png.vvyu	9.64 KB	3d82599e79492c4c462a272ec8b1f61353497d27ef1f1a9effc59a2182bd68e7	✔
C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397\adViIyse_4wpfxq.mp4.vvyu	19.86 KB	e80fc75c83175199767764ec62f171885eec57d502a8e77c22333447e505b279	✔
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\himfl\y3jgcuet.odt.vvyu	12.08 KB	55b3f53d7f6087eb91085b38b0075bf2b84fae64a1014e7d7bfaed8e8494b7c0	✔
c:\users\keecfmwgj\desktop\uvnwcx.jpg.vvyu	72.04 KB	02344681091a93e2474d0cc8822a863202c73d9d439faa9b8592c156b116a81e	✔
C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\CtfMZqR_ubHOI0.odt.vvyu	26.30 KB	106d9cff85d05ce30a8908dd0ddd990780d4e8f09e4a8e0510abee01bd9cedae	✔
C:\Users\kEecfMwgj\Videos\iqB1Fd.mkv.vvyu	68.13 KB	43d8d7a093e281a32e01a9f7891f22c25f084929b614e132cee19bf62624ad00	✔
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397_dsq\ouopevgnwd1-z0kjb.bmp.vvyu	19.62 KB	b11ad87bf6abc17bcf72fae4365aeb70de6b053c6b5cfae797e89dc9927b7df5	✔
c:\users\keecfmwgj\pictures\hppn3l0iwejl.gif.vvyu	39.84 KB	0ee8f50e1d9699aeab157745a49851dc851a1f8f2888bfe61bc9e032c02e58a7	✔
c:\users\keecfmwgj\documents\rinxjcpkfg.pptx.vvyu	51.29 KB	9a80f8e505ed21ff81c770bc07194f512b47e47e8c33c617cb1ae41da0009809	✔
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\himfl\4e_qp5b8\h0-ngmz.odt.vvyu	48.98 KB	1cf59c57ef7b3789ccfe9e94af1b864c136ccf102c34f429369948fb096434ed	✔
C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HImfL\22cygPlJe.ods.vvyu	36.96 KB	0cef471dca60ecc3c6d01d194ecb98d4bc9aca1b31a83cb15bb2ee8631ce6458	✔
C:\Users\kEecfMwgj\Pictures\f83rpj3sXX29oJ.jpg.vvyu	26.59 KB	30e77c7806e9308e89a8cd0abf07b8a149ac7c6bad7ddf6850b20c603d91ddbf	✔
C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\wICCgSS9cO9EJxpugq\P2QT4FKo.mp4.vvyu	28.25 KB	eda36dc0739d8049fc937ccbaa419336a3cecfb51aa3f409bec84894c7e86786	✔
C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397\WXRqwImP8omimb.bmp.vvyu	94.36 KB	138739bd275bf2627e4c0dfbfe239e9da8f0b8da9f155fbb16e64aff96f6328d	✔
c:\users\keecfmwgj\documents\qca-wrdfbpizyp.docx.vvyu	46.49 KB	be1ec249f95293c5fab9a8f8edad8d148ef50db9c505cf7fd886cc80b707821f	✔
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\ysw9udfa\io6kkqyuc.xlsx.vvyu	81.12 KB	1320837e0bb9e561d124a9a5638fc42c868cc0d5ff2fffc33fcee06b06b6e0c6	✔
c:\users\keecfmwgj\desktop\bkw1.mp4.vvyu	11.38 KB	1895f95febca6531bc20438a53f745c81f5ae7b9ac02d3a1a8ec9925d57b55d7	✔
C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\47m5sv0uqVNl\AZ2aRaMGzQB\xryUj16QF_9DxMTZ1QMq.m4a.vvyu	52.56 KB	a41ecdea59b8e39ec81d1ca67d4027621bfab9e936953ae72c4925bd10913a63	✔
c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.vvyu	467 bytes	a2839db93e844a1f1efe8a0a462cf7d4160362917c56b818715d27297d30aece	✔
C:\Users\kEecfMwgj\Pictures\cbyFXHxALB9ISR--lyv1.png.vvyu	48.40 KB	aa2caa916e9c94a5abc6dea70acc7656cf1c547949e88f87fb3685831e51677d	✔
c:\users\keecfmwgj\favorites\windows live\windows live mail.url.vvyu	467 bytes	d2b19b6572639abaea0d49592c0ca72d4b00b29e72515f25d18bbc3eaef22218	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\himfl\w9_k2r1yg22qfb5wtf98.ots.vvyu	41.94 KB	e363970dbaa463acbcb3af2a7ba08cc2d2f4028486bdb7801ba17c2a0d02a0ef	✔
c:\users\keecfmwgj\documents\a_eemub.docx.vvyu	50.19 KB	4f7f139823f9284a08bb09db90f260c79b5aaa68ecf39e90379bdbd6f7d5cafc	✔
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\s_caetbn.ots.vvyu	11.78 KB	72c13fff31e885e4bf33a2b552b45cd4fccd4f5a888ac55d924efd428c1ab5c1	✔
c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\kb5yp2q.avi.vvyu	36.95 KB	53e8db0007aa15007bc41321ac29e416bc6b81f7ca39d33aa063309006f45e7f	✔
C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\Ua71cE_srBW.docx.vvyu	81.42 KB	837ea95e174f181ba95ae55f8640eeeaf64feca13802904141dc77ad9f332156	✔
c:\users\keecfmwgj\favorites\windows live\get windows live.url.vvyu	467 bytes	db7ee8ddd4692605a5d688d72aeab66f36d8c0192df8c8653fb02039235ce096	✔
c:\users\keecfmwgj\music\5u0vvnc3nroc8n_z\udco8hlr7krd.m4a.vvyu	5.96 KB	fec8a5ab848f2b2a3da3f7f0903266aaa083d0303f6c35b638dba6bb4cb5032f	✔
C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\RpFnCBUaRW4M2CKB6Y8.avi.vvyu	76.98 KB	9f9febdd2161c940593a5e5c5bcc6e24b968a58d19d803fca63820bd49e8e1ec	✔
C:\Users\kEecfMwgj\Pictures\9IU4er.gif.vvyu	71.78 KB	9535babc99684847cf344a6ccb370f4ca8bf51fa7ab67250608fdd5942f304f2	✔
C:\Users\kEecfMwgj\Desktop\5EtXO0qde4mAaAj2.mp3.vvyu	99.36 KB	60bd079c58c6b350cd3a34558dbad00d602c60e6799029c73cc4dd6e27b87692	✔
c:\users\keecfmwgj\pictures\om3a-o87olj.gif.vvyu	10.34 KB	f8ab1961119edb4b8217954b1c523f96eed5e4a7bf9da4c12755acb387a1b446	✔
C:\Users\kEecfMwgj\Documents\MuVmmckS_6uXC.pptx.vvyu	80.35 KB	bd680d574610c90b0f2151d109fc47df0bbc4c4eec1daf61445491bb2c93ab70	✔
C:\Users\kEecfMwgj\Videos\onXJrQ0LQmJjW.avi.vvyu	24.22 KB	8772ed4605435520635aa0e470c5a8fe5b82baa676880f73176bde00e153959a	✔
c:\users\keecfmwgj\documents\outlook files\franc@gdllo.de.pst.vvyu	265.33 KB	abdd826de4f5edb194b54c1b427e7c4d054cc5b9ae6333ebf3104be404d9d3b9	✔
C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HImfL\4E_Qp5b8\OQIL9b4yk.odp.vvyu	41.06 KB	a5961df28e4b409d6934c6e08d08328605c5980912edf8aa4aeddee40bde1ab5	✔
c:\users\keecfmwgj\videos\cvfgvyfl7tfjuo7\p5dr5.mp4.vvyu	33.00 KB	1c23e573bc385eaa22f0d24340724093c81b2a52ebb9c085b932c08c9d2f8515	✔
C:\Users\kEecfMwgj\Documents\wXPNYv.xlsx.vvyu	87.95 KB	f8847fec9f7158881d1def466cdd574d6338d7a1223a67779586002dd3f2258d	✔

Reduced dataset

Host Behavior

Type	Count
System	269
Module	185
File	2434
Environment	1
Process	55
Registry	4
Mutex	1
User	1
Window	1
-	4

Network Behavior

Type	Count
HTTPS	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e0649b07f8980eb14453d11ed6c62dd68e825c5387bedaf90c53ae45f843e51c	c:\users\keecfmwgj\pictures\7p5jbw.jpg.vvyu, C:\Users\kEecfMwgj\Pictures\7p5JBw.jpg.vvyu	Dropped File	91.94 KB	image/jpeg	Access, Create, Write	MALICIOUS
6ed5bb4cb46be31f7f5b2268132d8f103c443cfa6a55032b087ebb6a8123c92d	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
137d38ac33c1b5827393d3d28176e18cd73a645bcbbdd6dbcf0765a546a49194	C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\znTr-YRiXJ\0VhP5.wav.vvyu, c:\users\keecfmwgj\music\juck2lalp_ipp\zntr-yrixj\0vhp5.wav.vvyu	Dropped File	9.79 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e20613dac0ca2d223af4707d51d1974b6a3285ad1fb762cc320ab5b6ab02bed5	c:\users\keecfmwgj\desktop\z8twgmunehqoxqfe1k.mp3.vvyu, C:\Users\kEecfMwgj\Desktop\z8twGmunEhQoxqFe1k.mp3.vvyu	Dropped File	88.39 KB	application/octet-stream	Access, Create, Write	MALICIOUS
320eacd706d495117967f5b44d7df835cdc2bf13b7ed7a63b3a431841cc0825e	C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\47m5sv0uqVNl\AZ2aRaMGzQB\5B4VEsMcGlm7c.mp3.vvyu, c:\users\keecfmwgj\music\juck2lalp_ipp\47m5sv0uqvnl\az2aramgzqb\5b4vesmcglm7c.mp3.vvyu	Dropped File	38.94 KB	application/octet-stream	Access, Create, Write	MALICIOUS
2b0c2eba662593f4b003e70266fae0e4e181ed3aa4c49dc387dacd1b4ea76ef4	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
33b0820aa114f40bb3a4419eb95a0e5dc5a27281b042281d7f619166f933c6ab	C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\wICCgSS9cO9EJxpugq\wx0aR91G76sZ.flv.vvyu, c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\wx0ar91g76sz.flv.vvyu	Dropped File	92.28 KB	video/x-flv	Access, Create, Write	MALICIOUS
bf00118fe5bed1175dd6af4c0b2ee63378eb4a85347d5b22e7d0694aca03f842	c:\users\keecfmwgj\documents\n6jq6ucc95w9.docx.vvyu, C:\Users\kEecfMwgj\Documents\N6jq6Ucc95w9.docx.vvyu	Dropped File	38.44 KB	application/zip	Access, Create, Write	MALICIOUS
cb9ca7d3e1e477c2cc69f58fd50615d64efa4f0f60fc868c9f405b0e933c1345	c:\users\keecfmwgj\music\juck2lalp_ipp\47m5sv0uqvnl\ah3jwn0.wav.vvyu, C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\47m5sv0uqVNl\ah3jWN0.wav.vvyu	Dropped File	81.86 KB	application/octet-stream	Access, Create, Write	MALICIOUS
108448ce429c253e0fe11b281ce58ebde0dfe737413b8d8d369e45fea459e451	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\ysw9udfa\bzhliohmivg2h0_pvvuu.pps.vvyu, C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\ySw9UDFA\BZhLiohmIvg2H0_PVVuu.pps.vvyu	Dropped File	12.51 KB	application/octet-stream	Access, Create, Write	MALICIOUS
477cfa8b80489db2df199d97ffac092f5fb72dda5360f24d129a05be5b2fe372	C:\Users\kEecfMwgj\Videos\hA6nEQ04cdHym7b8.flv.vvyu, c:\users\keecfmwgj\videos\ha6neq04cdhym7b8.flv.vvyu	Dropped File	16.02 KB	video/x-flv	Access, Create, Write	MALICIOUS
0709b027e07743baa3b348053115229674d7c286c02f8bc4d5154e8719740936	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	MALICIOUS
72d6a52150a653cc2f759f144e23f267836174ff56536f090772f6404a2e1c23	C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\ippAwK.flv.vvyu, c:\users\keecfmwgj\videos\cvfgvyfl7tfjuo7\ippawk.flv.vvyu	Dropped File	46.00 KB	video/x-flv	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a65e198609344df277b69c1d993e5168b471774536f8d15ee6ee01956e09f16c	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\6_x m.odp.vvyu, C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\6_x m.odp.vvyu	Dropped File	93.62 KB	application/zip	Access, Create, Write	MALICIOUS
e38000f5814848d4aae76c76fb9bb3fb8381df426cfb85b758c3b2d658e7f8b7	C:\Users\kEecfMwgj\Desktop\djRHD.jpg.vvyu, c:\users\keecfmwgj\desktop\djrhd.jpg.vvyu	Dropped File	80.19 KB	image/jpeg	Access, Create, Write	MALICIOUS
22f798e9e6734a1c7af3aa84784ec36c5e71f31b2f43ca905d571b2ea846de58	C:\Users\kEecfMwgj\Desktop\eSfxo-E.jpg.vvyu, c:\users\keecfmwgj\desktop\esfxo-e.jpg.vvyu	Dropped File	66.29 KB	image/jpeg	Access, Create, Write	MALICIOUS
64279fa395a3d18745c4e3dac3cc7cf3a7b7c08e06b52cc564b702cfb6280bd4	c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\oq0h.flv.vvyu, C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397\oq0H.flv.vvyu	Dropped File	67.87 KB	video/x-flv	Access, Create, Write	MALICIOUS
704fd863f914a31bb2d7caa2a2bf9e173d99eee8f226e70bf41783b695eba6b2	c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\q-8_5alv-aysztdlcx.m4a.vvyu, C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397\q-8_5Alv-AYsZTdLcX.m4a.vvyu	Dropped File	38.38 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b1b6a2565aa33567cde2e05f259c57921d970af9c462c6874bbe93f603b6f616	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\hfgog8brvbw\0se02.odp.vvyu, C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\hfGoG8BRVBw\0sE02.odp.vvyu	Dropped File	21.63 KB	application/zip	Access, Create, Write	MALICIOUS
1dc7439c1f5f44c105f26282d016c75090293b523a75254afcb75a7408c0179b	C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\47m5sv0uqVNl\LPB-FW9jvpM0h.wav.vvyu, c:\users\keecfmwgj\music\juck2lalp_ipp\47m5sv0uqvnl\lpb-fw9jvpm0h.wav.vvyu	Dropped File	28.07 KB	application/octet-stream	Access, Create, Write	MALICIOUS
f474f259c2309971964809e02e0cd1405203887427109cb523bee1cff9a7f2ff	C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft Store.url.vvyu, c:\users\keecfmwgj\favorites\microsoft websites\microsoft store.url.vvyu	Dropped File	468 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
cdda1cd1b95414730f5fc7c3b43e3fd5c9947725c733689c19346ecc1f91d003	c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\bxv5ql2id9hkdxpv7.swf.vvyu, C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397\BXV5Ql2Id9hKdXPV7.swf.vvyu	Dropped File	36.30 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
1cbf4c4ca05747ef89ce3fd9250bdc7944e4fc9468b1b40f343ee80c42b5ffa2	c:\users\keecfmwgj\videos\9hkv.mp4.vvyu, C:\Users\kEecfMwgj\Videos\9hkv.mp4.vvyu	Dropped File	87.31 KB	application/octet-stream	Access, Create, Write	MALICIOUS
83aa737c7669451a99eeb4bd9fb0dade14873eafb501c892890964bdb9aed929	c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.vvyu, C:\Users\kEecfMwgj\Desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.vvyu	Dropped File	738.33 KB	application/x-dosexec	Access, Create, Write	MALICIOUS
1bf152697eac08d5f62d44cc9905e149abe68d6bbdb21499602bfb0d77097d29	c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\m0zrf.mkv.vvyu, C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\wICCgSS9cO9EJxpugq\m0ZRF.mkv.vvyu	Dropped File	92.26 KB	application/octet-stream	Access, Create, Write	MALICIOUS
815a7845da9b9335f529f808bd56f2f19ac83b1b3028bca5dc1791c209528179	C:\Users\kEecfMwgj\Pictures\877l5thXMZRFuEmTVa.png.vvyu, c:\users\keecfmwgj\pictures\877l5thxmzrfuemtva.png.vvyu	Dropped File	7.66 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c7b8ea486f52947445a6c21fddd4ce799b0387675b152181398f66e9da1fad0f	c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\acppdj.avi.vvyu, C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\wICCgSS9cO9EJxpugq\AcPpdJ.avi.vvyu	Dropped File	70.65 KB	application/octet-stream	Access, Create, Write	MALICIOUS
2a6e0d6157b8f7725f6860537e7122c55306a7cdb82f0f51e3444f363352bc05	c:\users\keecfmwgj\desktop\jkgjiq3h.wav.vvyu, C:\Users\kEecfMwgj\Desktop\jkGJiQ3H.wav.vvyu	Dropped File	32.54 KB	application/octet-stream	Access, Create, Write	MALICIOUS
438c96c1ec8245d5a39986409478e2b28fc6216182be32656f9a2757c29fa915	c:\users\keecfmwgj\documents\liaafon99lah9nu_j.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\LIaaFON99laH9NU_j.xlsx.vvyu	Dropped File	92.22 KB	application/zip	Access, Create, Write	MALICIOUS
d6198e57c7501b62635ea7f258215e9761db8c3c9372495e4d76f293bdf8670d	c:\users\keecfmwgj\pictures\-ctdcbmthlrz.jpg.vvyu, C:\Users\kEecfMwgj\Pictures\-ctDCbmthLRz.jpg.vvyu	Dropped File	11.41 KB	image/jpeg	Access, Create, Write	MALICIOUS
1cc040019abce493d0e11defae2b0118304526b013941d015b56920e25066a50	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
276d5057fd6ad3451b4e0fe8ad2a1d3587d69d236f0288b43c807913f2e4f1d1	c:\users\keecfmwgj\music\juck2lalp_ipp\dibgo7.wav.vvyu, C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\dlbGo7.wav.vvyu	Dropped File	48.61 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3272fffda9e42b0bafdff0cc8905db24c10abc3370ea28aee55bf159131023b3	C:\Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\mOm18edC.mp3.vvyu, c:\users\keecfmwgj\music\eb_b9k_jdavxhxh0\mom18edc.mp3.vvyu	Dropped File	95.57 KB	application/octet-stream	Access, Create, Write	MALICIOUS
970bbaadcda492a43ccb533be7a12f7823b463a76e4c3be1f6d831c6c86527b1	c:\users\keecfmwgj\desktop\ynpbsi277\bp67ry2e oyq1fpgm.mp4.vvyu, C:\Users\kEecfMwgj\Desktop\YnPBSI277\bp67ry2E oYq1FPgm.mp4.vvyu	Dropped File	63.37 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d40e122dc6d86d508cc177ff545a0bb92a80b25642e6c8d4a47a82fb44005e66	c:\users\keecfmwgj\videos\fpzctgqi5ys\mfzx23r02sywxh\l6ehb4ojilkrcleahkh.avi.vvyu, C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\MfZX23r02sYWxh\L6EhB4OjIlkRcLeaHkH.avi.vvyu	Dropped File	65.58 KB	application/octet-stream	Access, Create, Write	MALICIOUS
8fe25390981b9d53f86acc8c31d1d1227a88fc3e13075d58819e40c39a477992	c:\users\keecfmwgj\desktop\xnjf1rqetdxtc.mkv.vvyu, C:\Users\kEecfMwgj\Desktop\xnJF1rqEtdtxtC.mkv.vvyu	Dropped File	67.02 KB	application/octet-stream	Access, Create, Write	MALICIOUS
f5737997452e2611d4a891ab81fa875bdd904995904a70f13d279a820c0afc85	C:\Users\kEecfMwgj\Pictures\uCbdvMv01ecUQrS5kFhR.gif.vvyu, c:\users\keecfmwgj\pictures\ucbdvmv01ecuqrs5kfhr.gif.vvyu	Dropped File	98.09 KB	image/gif	Access, Create, Write	MALICIOUS
12a51367c5c85ff3c1dc73743cface2e01accecf2879a36adbddf566d52987b3	C:\Users\kEecfMwgj\AppData\Local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe	Downloaded File	438.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
11bc3b72c4e5558f5d97d0e19e5162693bd93d6fcf69ace580bf6c26b49871bf	C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\3Ad0c.mkv.vvyu, c:\users\keecfmwgj\videos\fpzctgqi5ys\3ad0c.mkv.vvyu	Dropped File	69.36 KB	application/octet-stream	Access, Create, Write	MALICIOUS
306562f09762e1815c597567400e33072801810bffa398a82c7a509a4caa87a3	c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\f6adjjdhq\cuol988xnblbr.m4a.vvyu, C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397\f6AdJjDhQ\cuoL988XNBLbr.m4a.vvyu	Dropped File	99.27 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8a15abf89f297426daa013cb2c918827c9a9dd603977930a4f3822c44d24f300	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
0e002c115d35d2f84e18e9d47e6a54861ae4b39d186fcdf993f702d443c9d627	c:\users\keecfmwgj\documents\rn1rbbo1eqymg_q.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\RN1rbBo1eqYMG_Q.xlsx.vvyu	Dropped File	49.35 KB	application/zip	Access, Create, Write	MALICIOUS
2adef906c71dcea126662dad6b1f8a2b74f5703f4087fdfb63ced7d121ba6834	c:\users\keecfmwgj\pictures\khh4ja_ffudblb.gif.vvyu, C:\Users\kEecfMwgj\Pictures\khH4Ja_FfUDbLB.gif.vvyu	Dropped File	28.99 KB	image/gif	Access, Create, Write	MALICIOUS
59c9c92684aae5e5832d34922f2a143b64b957d9f92dc5405cb69ca2620ed4a7	C:\Users\kEecfMwgj\Music\5U0VVnc3NrOc8n_Z\k8_cI3l6hV1-Y7\27Qc0VUi07zkn_VUAary.wav.vvyu, c:\users\keecfmwgj\music\5u0vvnc3nroc8n_z\k8_ci3l6hv1-y7\27qc0vui07zkn_vuaary.wav.vvyu	Dropped File	69.90 KB	application/octet-stream	Access, Create, Write	MALICIOUS
929283c4a3c541a98eb0ee2256e1664e0120089 9e6115821e5c57a466fea4e1b	C:\Users\kEecfMwgj\Music\85NDX4GNPa9.m4a.vvyu, c:\users\keecfmwgj\music\85ndx4gnpa9.m4a.vvyu	Dropped File	32.30 KB	application/octet-stream	Access, Create, Write	MALICIOUS
67afdf10d7df308b3f9e1489c3dc0108698eb662e88586e3affe465fd74923c0	C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397_dSq\EotVe.bmp.vvyu, c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397_dsq\eotve.bmp.vvyu	Dropped File	12.00 KB	application/octet-stream	Access, Create, Write	MALICIOUS
f23d8074f6577945e92a5bbf20022a6dbbf088f99fee0f477fc3467017716683	C:\Users\kEecfMwgj\Music\9Qfl6h6W74ZaGdKZ7l.m4a.vvyu, c:\users\keecfmwgj\music\9qfi6h6w74zagdkz7l.m4a.vvyu	Dropped File	60.85 KB	application/octet-stream	Access, Create, Write	MALICIOUS
21423f3439da7e389a1f71f7621fa13075b53e9365b0e100c24c42f170cc3f71	C:\Users\kEecfMwgj\Music\26hKDH\dhVO\fwWKBmZrXnqYjnf.mp3.vvyu, c:\users\keecfmwgj\music\26hkdh\dhvo\fwwkbmzrxnqyjnf.mp3.vvyu	Dropped File	43.82 KB	application/octet-stream	Access, Create, Write	MALICIOUS
523fbe08528681f2060ba07be4516c7cbf5a54156300890dca6d4fb411dd6b84	c:\users\keecfmwgj\pictures\ooz2bcvbppeb9wsu.png.vvyu, C:\Users\kEecfMwgj\Pictures\Ooz2bCVbPPEb9WsU.png.vvyu	Dropped File	22.76 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ba8ee90fb4e6ec2eb044148b62c6b338d6318621b5b79fc9faf813a8f3af27b4	c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\f6adjjdhq\adiahvz87jstj8m.flv.vvyu, C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397\f6AdJjDhQ\AdlahVz87JStJ8m.flv.vvyu	Dropped File	37.91 KB	video/x-flv	Access, Create, Write	MALICIOUS
074fb4b529099065f17b55b89bf579b3c132ea349e7af2b9a7c9fd772ab05f40	c:\users\keecfmwgj\music\26hkdh\dhvo\waqploj2c0tw.wav.vvyu, C:\Users\kEecfMwgj\Music\26hKDH\dhVO\waqplOJ2C0tw.wav.vvyu	Dropped File	74.06 KB	application/octet-stream	Access, Create, Write	MALICIOUS
6ab20d8ff33f670160c028f34545b13504be5cf1cad4c2e5d96b746b1ceab8ce	C:\Users\kEecfMwgj\Desktop\3YV6ib1olpsefRwtFe.pdf.vvyu, c:\users\keecfmwgj\desktop\3yv6ib1oipsefrwtfe.pdf.vvyu	Dropped File	8.26 KB	application/pdf	Access, Create, Write	MALICIOUS
6e6db717fb1c9f846f54d9c5d916517ea94aa26999f357553bbad3b4a1db73a2	c:\users\keecfmwgj\documents\3_nmmyv5xkxtc1mbc-u.pdf.vvyu, C:\Users\kEecfMwgj\Documents\3_nMMYV5XKxtc1mbc-U.pdf.vvyu	Dropped File	20.80 KB	application/pdf	Access, Create, Write	MALICIOUS
1ed025869f19808fec07e0ee81d5afffa5ddfa81d88798164e7c0133a32c995e	c:\users\keecfmwgj\pictures\tqpcqxkko-qtvp1zn.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\tQPcQXKKo-QTVp1zN.bmp.vvyu	Dropped File	6.29 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ad6859a70222b9b61b4eecceeed2413949b3ad03ba07089f2e2b6191ba13e3d1	c:\users\keecfmwgj\music\juck2lalp_ipp\47m5sv0uqvnl\dvuuti6.wav.vvyu, C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\47m5sv0uqVNl\dVUUTI6.wav.vvyu	Dropped File	3.53 KB	application/octet-stream	Access, Create, Write	MALICIOUS
f7b16be008a4cbb8c8c7fbd5073b4d33e92804113a53d6bf6c9d331fa47ac063	C:\Users\kEecfMwgj\Desktop\i_u5ln.wav.vvyu, c:\users\keecfmwgj\desktop\i_u5ln.wav.vvyu	Dropped File	12.34 KB	application/octet-stream	Access, Create, Write	MALICIOUS
f77d7c8ac5555b713d4645ab46c39e2343079d2128f8fbba66910ab9a101ac77	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\hfgog8brvbw\hsj_qr5bne5moizbn.csv.vvyu, C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\hfGoG8BRVBw\hsj_qR5BNe5MoizBn.csv.vvyu	Dropped File	24.55 KB	application/octet-stream	Access, Create, Write	MALICIOUS
369a6fcbfb7e593deab1c3078dd09854aa1be1f7a558f7e8cb6d7ce5151ace65	C:\Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\6X4EOyI76e.wav.vvyu, c:\users\keecfmwgj\music\eb_b9k_jdavxhxh0\6x4eoyi76e.wav.vvyu	Dropped File	6.79 KB	application/octet-stream	Access, Create, Write	MALICIOUS
03ce2c42137a2ed7f7982a542f1a4de1bec7770a313a51cd03ba43335e9cc63b	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
585c8b95f26c7627bda14fb6b8d2aedeb0ae285e57d99be6d4339d4151cfa9af	c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\v_uid9u5nghf.docx.vvyu, C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397\v_uiD9U5nghF.docx.vvyu	Dropped File	91.89 KB	application/zip	Access, Create, Write	MALICIOUS
23c3f3d274223e835e7f4ca8dc560b9d0927f676aaa3e817708d3b8fd7224db9	C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\NMttoz1zVMuEbci.swf.vvyu, c:\users\keecfmwgj\videos\cvfgvyfl7tfjuo7\nmttoz1zvmuebci.swf.vvyu	Dropped File	37.85 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
ee087460e166a03fcedaadd8d6493d71b26dcdc7e7c386d5c12e1e8a95370e54	c:\users\keecfmwgj\pictures\3uvy.jpg.vvyu, C:\Users\kEecfMwgj\Pictures\3UVY.jpg.vvyu	Dropped File	39.85 KB	image/jpeg	Access, Create, Write	MALICIOUS
49c131171f65e3ee0626a16a5add15e92235d3fd925f3ff6f593b0de592b8b83	C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Work.url.vvyu, c:\users\keecfmwgj\favorites\microsoft websites\microsoft at work.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
c59219b2f92fab1080562071eb98b2d530531ea9c5dacdc33d7b170a948a78ec	C:\Users\kEecfMwgj\Documents\5usDbJNuS3uVdkW.xlsx.vvyu, c:\users\keecfmwgj\documents\5usdbjnus3uvdkw.xlsx.vvyu	Dropped File	32.64 KB	application/octet-stream	Access, Create, Write	MALICIOUS
00a58c5262f0a9db213000248c1970c3a95e8ad252e7c84ba3936104ec5787e3	C:\Users\kEecfMwgj\Pictures\hyglyDuy.bmp.vvyu, c:\users\keecfmwgj\pictures\hyglyduy.bmp.vvyu	Dropped File	42.72 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d25a1e4c3f238cc735debf26cfd59b059a01279f76d68b3bb604c137ea20e6e5	c:\users\keecfmwgj\videos\fpzctgqi5ys\0ipri83h.flv.vvyu, C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\0IPRI83H.flv.vvyu	Dropped File	79.47 KB	video/x-flv	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5	c:\users\keecfmwgj\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.vvyu, C:\Users\kEecfMwgj\Desktop\0... ...\kEecfMwgj\AppData\Local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	Sample File	738.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Read, Write	MALICIOUS
3735b45dfc823e67d5bcfc021c2b539b5f6ef3c45feec336e8890b9d1b067a99	c:\users\keecfmwgj\pictures\qg2uxz3cw8a4fuol_l.gif.vvyu, C:\Users\kEecfMwgj\Pictures\QG2UxZ3cw8a4fuoL_L.gif.vvyu	Dropped File	36.67 KB	image/gif	Access, Create, Write	MALICIOUS
ae945708982b679620f07d3eafc8c45513a0c9f6829ecbb470ffa28d0151fd46	c:\users\keecfmwgj\desktop\ynpbsi277\ov6fzg.bmp.vvyu, C:\Users\kEecfMwgj\Desktop\YnPBSI277\ov6fZG.bmp.vvyu	Dropped File	3.59 KB	application/octet-stream	Access, Create, Write	MALICIOUS
fdb790c9ed0e8af4b520553c51f0346c15a7bf2350a615d55ee46d1ce4a292d2	C:\Users\kEecfMwgj\Desktop\U00H4oegdjWIv9LIU5.png.vvyu, c:\users\keecfmwgj\desktop\u00h4oegdjwiv9liu5.png.vvyu	Dropped File	77.70 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c11a499cb36e5d4ae5fe4655315550832e50055bccf0ab54e1d6b91045d6b9e2	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	MALICIOUS
6fd80b37d46091ab42ea621f5cac138a5e0d99231e03b019880b9e44ba196420	c:\users\keecfmwgj\desktop\uimsfjjz.rtf.vvyu, C:\Users\kEecfMwgj\Desktop\UIMsFJjz.rtf.vvyu	Dropped File	56.92 KB	text/rtf	Access, Create, Write	MALICIOUS
8873062cd0684d82ed284dedb3fc98e31ff890b76a80f3cdcf4ac3e1fc6bda2b	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
a59aeb1cc8bc0c3714bcebc4bccaaf7384727622961a59cc5774619b1f1a4890	c:\users\keecfmwgj\pictures\rwx9qkj.png.vvyu, C:\Users\kEecfMwgj\Pictures\rWx9qkj.png.vvyu	Dropped File	97.64 KB	application/octet-stream	Access, Create, Write	MALICIOUS
abe0378f08fdfd7f0936a029d0e9a457965e7aafd9f254c22b730c5d0eed7a0a	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	MALICIOUS
9e1c10571eeb00a8eae7a33a17d57886578c810034d26c04fa4369e4edf83786	C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Gallery.url.vvyu, c:\users\keecfmwgj\favorites\windows live\windows live gallery.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
36259635cc41b60c80d665a39713d31446978f28156885be17fabacba0640e5e	C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\hfGoG8BRVBw\DJyNf5d3ZVp0RV8Gb.docx.vvyu, c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\hfgog8brvbw\djynf5d3zvp0rv8gb.docx.vvyu	Dropped File	70.19 KB	application/zip	Access, Create, Write	MALICIOUS
5ff72d7d56b6103e200e19cec2ade68ed269dc9efc400eed69968f6a3ce58b2e	c:\users\keecfmwgj\desktop\ynpbsi277\hak2yhq7o.jpg.vvyu, C:\Users\kEecfMwgj\Desktop\YnPBSI277\hAK2yhq7O.jpg.vvyu	Dropped File	91.08 KB	image/jpeg	Access, Create, Write	MALICIOUS
1b6d871292c51b00684abe0d937fbb173ce36afbc43c12e03585f13f60d15f4d	c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\cjrduvousoi.swf.vvyu, C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\wICCgSS9cO9EJxpugq\CJrDuvoUsoi.swf.vvyu	Dropped File	93.84 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
e664700d5a11d0c21232a95a42d663303c5a490e3f8ac1223cdb80a632df1347	c:\users\keecfmwgj\pictures\vauzy4mlwuoc1eph.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\vaUZY4mlwUOC1Eph.bmp.vvyu	Dropped File	19.34 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a6a271da428b15c51aa3b4f7e0329a82dcb4d82445576da2dab6641ede2103f4	c:\users\keecfmwgj\music\juck2lalp_ipp\zntr-yrixj\f8ilkitdoj8fsshi0.mp3.vvyu, C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\znTr-YRiXJ\F8iLKItDoj8FssHi0.mp3.vvyu	Dropped File	87.89 KB	application/octet-stream	Access, Create, Write	MALICIOUS
68f540b64b8b7f61a5dcca2c3eb7781d6bf40d92c9e0e94bccaa8f920d9c0f5b	C:\Users\kEecfMwgj\Desktop\usU4fi-1.ots.vvyu, c:\users\keecfmwgj\desktop\usu4fi-1.ots.vvyu	Dropped File	41.79 KB	application/zip	Access, Create, Write	MALICIOUS
aa09895ab60d8f81821665f8167ffe914deb6e85258bedf59c7c077cca028921	c:\users\keecfmwgj\videos\fpzctgqi5ys\m fzx23r02sywxh\btrak.swf.vvyu, C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\M fZX23r02sYWxh\BTrak.swf.vvyu	Dropped File	38.85 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
05a3902fa069f8ef4c4c96db4e4d8860d67fd4f46333babef27dfadbc2a2e694	C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HImfL\4E_Qp5b8\RAN3RZLWQzdFaTXUwx\AFrd4UxBD1.pdf.vvyu, c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\himfl\4e_qp5b8\ran3rzlwqzdfatxuwx\afrd4uxbd1.pdf.vvyu	Dropped File	18.94 KB	application/pdf	Access, Create, Write	MALICIOUS
179ba120095be1827615ef2ab64da8096df799f1a82c9383694fe0b77e9d2a79	C:\Users\kEecfMwgj\Documents\RUCPVLyvfQF00lxB1.xlsx.vvyu, c:\users\keecfmwgj\documents\rucpvlyvfqf00ixb1.xlsx.vvyu	Dropped File	24.08 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ab6942fb22806f4e815892b8b201da5fce970d5a04652b4b6ee37c17e62c3410	C:\Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\sTzvqONg_kzYdub0TTT.mp3.vvyu, c:\users\keecfmwgj\music\eb_b9k_jdavxhxh0\stzvqong_kzydubottt.mp3.vvyu	Dropped File	27.34 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c95ec3557951604c5ace04735735a6e09cc8d53aca4f58fb4e3e1750a6d28f71	c:\users\keecfmwgj\music\juck2lalp_ipp\zntr-yrixj\mlh8upb9ymlbt.mp3.vvyu, C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\znTr-YRiXJ\mlh8UPb9YMIbt.mp3.vvyu	Dropped File	45.42 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3806b4441fd3ee3be7eae7460c6fbb849b86c0da97dc5b99df03a106832545f1	C:\Users\kEecfMwgj\Pictures\DvPtakSDSqUBk1s-p5E_.jpg.vvyu, c:\users\keecfmwgj\pictures\dvptaksdsqubk1s-p5e_.jpg.vvyu	Dropped File	83.21 KB	image/jpeg	Access, Create, Write	MALICIOUS
a6104fb3fce294a226ef72c0a2977f24b83a474eafb88ebf4ffd9baa6195d17d	C:\Users\kEecfMwgj\Documents\92-ieu- ecANbCAHxu3.pptx.vvyu, c:\users\keecfmwgj\documents\92-ieu-ecanbcahxu3.pptx.vvyu	Dropped File	3.33 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4718f246c07568dda7c0deaf748b6d89660620cb91e76a43311f96224976d00e	c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397_dsq\ywywxyty.mp3.vvyu, C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397_dSq\YWYWXYtY.mp3.vvyu	Dropped File	40.98 KB	application/octet-stream	Access, Create, Write	MALICIOUS
503fb88d60626a697d9be83a34fdffee9c48dc5dab581c5f56f1523bc3f05b91	C:\Users\kEecfMwgj\Music\26hKDH\l5cha-37fB.mp3.vvyu, c:\users\keecfmwgj\music\26hkdh\l5cha-37fb.mp3.vvyu	Dropped File	21.51 KB	application/octet-stream	Access, Create, Write	MALICIOUS
bb600930855b5279efde2f28474664aadf14656b38ee6a37cf7ae261f9a1ce48	c:\users\keecfmwgj\videos\z xz-1adfcazuf.mkv.vvyu, C:\Users\kEecfMwgj\Videos\z Xz-1ADfCAZUF.mkv.vvyu	Dropped File	59.58 KB	application/octet-stream	Access, Create, Write	MALICIOUS
babb7957ceb47a4e663a683308d60aa822bfba258cdc372ae18d9d8b149caa0d	c:\users\keecfmwgj\pictures\ujyi1dwdud6-j7pcelmb.png.vvyu, C:\Users\kEecfMwgj\Pictures\Ujyi1dWdud6-J7Pcelmb.png.vvyu	Dropped File	79.21 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e2eb787ed8fec96326356c6b859974ef29a4fcd99dc9e084507a65d94e3106ad	c:\users\keecfmwgj\desktop\9ouhy.mp3.vvyu, C:\Users\kEecfMwgj\Desktop\9Ouhy.mp3.vvyu	Dropped File	54.02 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
84c7f12e6ca2640bb76d80acebdfda731874b8ad266202bac029addc3c54227f	c:\users\keecfmwgj\pictures\go3r.jpg.vvyu, C:\Users\kEecfMwgj\Pictures\gO3R.jpg.vvyu	Dropped File	54.58 KB	image/jpeg	Access, Create, Write	MALICIOUS
e942870bcd555c84703d0bdd3e010492513d01850ac52f57c50b5227b4e55e90	C:\Users\kEecfMwgj\Music\26hKDH\dhVO\c-p32.m4a.vvyu, c:\users\keecfmwgj\music\26hkdh\dhvo\c-p32.m4a.vvyu	Dropped File	47.69 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4a1aaeed4747266983004f9fa25ff0ed024415f8232f30467b08441084b002e0	-	Web Response	554 bytes	text/html	-	CLEAN
3c7d38aff2dd9e697cd3cc6c0a5d338ff2d0bdb948fb469cd21c76d8c36e53ee	-	Modified File	256.00 KB	application/octet-stream	-	CLEAN
6d214ad6b2cf334f0545be9f044bb26b2bd3d43dd77f5e124a5769b86c9ad995	-	Downloaded File	216 bytes	text/html	-	CLEAN
247eb37b7ba897dc8020a06730fee38b939010c2a3f061580145ab6c7459ddd6	-	Modified File	64.00 KB	application/octet-stream	-	CLEAN
68d5ab5e7cd0402af32d5629b4f6277da120661e72e4924d176a26e5132489dd	c:\users\keecfmwgj\pictures\vuc5gusp1h33w.png.vvyu, C:\Users\kEecfMwgj\Pictures\Vuc5gUsp1H33w.png.vvyu	Dropped File	54.87 KB	application/octet-stream	Access, Create, Write	CLEAN
1dbe197123855db6c0b652d49c034c991aba657954b47e48762480682d147c68	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	CLEAN
b898e95d61d2fd7e8ca2ea851b881e17569b5139ed738bf696f44c4a9b8c2f33	c:\users\keecfmwgj\favorites\msn websites\msn.url.vvyu, C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
799bf5cde2cabce0073d8629d8159a9ec2eb1a0c818004d433d7fe20834cf897	C:\Users\kEecfMwgj\Videos\07H2voZRMEM4mGd_N.swf.vvyu, c:\users\keecfmwgj\videos\07h2vozrmem4mgd_n.swf.vvyu	Dropped File	88.10 KB	application/x-shockwave-flash	Access, Create, Write	CLEAN
f6d62c54c0db829bcbdf0cd6386b5dd5f9780c1bfddadb920c97361af739805b	C:\Users\kEecfMwgj\Pictures\sfoK-fQjQEuAHhw.jpg.vvyu, c:\users\keecfmwgj\pictures\sfok-fqjqeuahhw.jpg.vvyu	Dropped File	45.92 KB	image/jpeg	Access, Create, Write	CLEAN
0d695567a4ccd8343fdb9956f775984a3c3dc0ed646279c04b8c43b8c5a30be0	c:\users\keecfmwgj\pictures\iv7y.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\Iv7Y.bmp.vvyu	Dropped File	92.49 KB	application/octet-stream	Access, Create, Write	CLEAN
4a1e187cb85b2bf08b1c30b88aa514e97b80abc12d99f3c20fd14d9d21c0d703	C:\Users\kEecfMwgj\Videos\x7DOAnu7EAlTL.mkv.vvyu, c:\users\keecfmwgj\videos\x7doanu7ealtl.mkv.vvyu	Dropped File	3.56 KB	application/octet-stream	Access, Create, Write	CLEAN
4feb9529a7f139f6e117a297299739dd39f81220d4541d6954388772a5c5dbd7	C:\Users\kEecfMwgj\Desktop\YnPBSI277\YZ4wuGCPKPt9a.pps.vvyu, c:\users\keecfmwgj\desktop\ynpbsi277\yz4wugcpkpt9a.pps.vvyu	Dropped File	63.44 KB	application/octet-stream	Access, Create, Write	CLEAN
b9365ceb3516d459562bd64c32c5bc15288ec05a0ac3c30e076803ebd366b6ea	c:\users\keecfmwgj\desktop\0w8tqjzs69qqxvzs-d8d.ods.vvyu, C:\Users\kEecfMwgj\Desktop\0W8tqjZS69QqxVZS-D8D.ods.vvyu	Dropped File	57.59 KB	application/zip	Access, Create, Write	CLEAN
1b91cea1f7fe4d9195c5eac0d587b466498f4800801565c928289a88c669303a	C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\MfZX23r02sYWxh\DyXmYMfEW2zZ74G.avi.vvyu, c:\users\keecfmwgj\videos\fpzctgqi5ys\mfzx23r02sywxh\dyxmymfew2zz74g.avi.vvyu	Dropped File	18.76 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d18be34b949327d4e690797a4349d76d03ed0e8e0ee4da9f698fc4b7988c9509	C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\Y3zc_VVY6Kxz1vjr.mp3.vvyu, c:\users\keecfmwgj\music\juck2lalp_ipp\y3zc_vvy6kxz1vjr.mp3.vvyu	Dropped File	55.63 KB	application/octet-stream	Access, Create, Write	CLEAN
729abc5616e8fccacdb0bcaec563b05d3517e042ec8f8588b6ab68fd0a9a107b	C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\7lrwy.flv.vvyu, c:\users\keecfmwgj\videos\cvfgvyfl7tfjuo7\7lrwy.flv.vvyu	Dropped File	88.96 KB	video/x-flv	Access, Create, Write	CLEAN
8afb8f3689798274f15530735bdbd27a107bf85598c9fe4bdce26da8ec387c7d	C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\L59EH_1g_s_fJjq.mp4.vvyu, c:\users\keecfmwgj\videos\cvfgvyfl7tfjuo7\l59eh_1g_s_fjjq.mp4.vvyu	Dropped File	36.14 KB	application/octet-stream	Access, Create, Write	CLEAN
7bd3d1d4c340529940bd24bb1e76873d818d824007b1ac79ac602a6fde7e39f9	c:\users\keecfmwgj\pictures\lv2axv.jpg.vvyu, C:\Users\kEecfMwgj\Pictures\Lv2Axv.jpg.vvyu	Dropped File	44.83 KB	image/jpeg	Access, Create, Write	CLEAN
35fde246db17586abccd1a7d6ffbced608a21008091b94369365427e28effde6	c:\users\keecfmwgj\videos\fpzctgqi5ys\m fzx23r02sywxh\0yoyfg2vyekk-r.swf.vvyu, C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\M fZX23r02sYWxh\0yOYfg2VyeKk-r.swf.vvyu	Dropped File	29.08 KB	application/x-shockwave-flash	Access, Create, Write	CLEAN
fa601ad4c51ca91df75647713f3599030ddaab354e222182e67898adcd4fc3d6	C:\Users\kEecfMwgj\Desktop\E8rOnJ1a8nkX -7zzxk.wav.vvyu, c:\users\keecfmwgj\desktop\e8ronj1a8nkx -7zzxk.wav.vvyu	Dropped File	6.86 KB	application/octet-stream	Access, Create, Write	CLEAN
6735a1b15c6371fd621a54b655e4eeaae0277985fc4adcec0a05bdaea1befd0f	c:\users\keecfmwgj\pictures\oq7rosq7byockq_wi3.gif.vvyu, C:\Users\kEecfMwgj\Pictures\oQ7roSq7BYOcKq_wI3.gif.vvyu	Dropped File	84.80 KB	image/gif	Access, Create, Write	CLEAN
3d82599e79492c4c462a272ec8b1f61353497d27ef1f1a9effc59a2182bd68e7	C:\Users\kEecfMwgj\Desktop\2CgRhD9i_8EFMrM.png.vvyu, c:\users\keecfmwgj\desktop\2cgrhd9i_8efmrm.png.vvyu	Dropped File	9.64 KB	application/octet-stream	Access, Create, Write	CLEAN
e80fc75c83175199767764ec62f171885eec57d502a8e77c22333447e505b279	C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397\adViIyse_4wpfxq.mp4.vvyu, c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\adviiyse_4wpfxq.mp4.vvyu	Dropped File	19.86 KB	application/octet-stream	Access, Create, Write	CLEAN
55b3f53d7f6087eb91085b38b0075bf2b84fae64a1014e7d7bfaed8e8494b7c0	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\himfl\y3jgcuet.odt.vvyu, C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HImfL\y3jGcUeT.odt.vvyu	Dropped File	12.08 KB	application/zip	Access, Create, Write	CLEAN
0c5cceba5c416d5424387794429f89a2456b5326e2c7e5d8d2bd67f34bb616ec	-	Modified File	32.00 KB	application/octet-stream	-	CLEAN
02344681091a93e2474d0cc8822a863202c73d9d439faa9b8592c156b116a81e	c:\users\keecfmwgj\desktop\uvnwcx.jpg.vvyu, C:\Users\kEecfMwgj\Desktop\uvnwCx.jpg.vvyu	Dropped File	72.04 KB	image/jpeg	Access, Create, Write	CLEAN
106d9cff85d05ce30a8908dd0ddd990780d4e8f09e4a8e0510abee01bd9cedae	C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\CtfMZqR_ubHOI0.odt.vvyu, c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\ctfmzqr_ubhoi0.odt.vvyu	Dropped File	26.30 KB	application/zip	Access, Create, Write	CLEAN
43d8d7a093e281a32e01a9f7891f22c25f084929b614e132cee19bf62624ad00	C:\Users\kEecfMwgj\Videos\iqB1Fd.mkv.vvyu, c:\users\keecfmwgj\videos\iqb1fd.mkv.vvyu	Dropped File	68.13 KB	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b11ad87bf6abc17bcf72fae4365aeb70de6b053c6b5cfae797e89dc9927b7df5	c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397_dsq\ouopevgnwd1-z0kjb.bmp.vvyu, C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397_dSq\oUopEVgNwd1-z0KJB.bmp.vvyu	Dropped File	19.62 KB	application/octet-stream	Access, Create, Write	CLEAN
0ee8f50e1d9699aeab157745a49851dc851a1f8f2888bfe61bc9e032c02e58a7	c:\users\keecfmwgj\pictures\hppn3l0iwejl.gif.vvyu, C:\Users\kEecfMwgj\Pictures\HPPn3l0IweJl.gif.vvyu	Dropped File	39.84 KB	image/gif	Access, Create, Write	CLEAN
9a80f8e505ed21ff81c770bc07194f512b47e47e8c33c617cb1ae41da0009809	c:\users\keecfmwgj\documents\rinxjcpkfg.pptx.vvyu, C:\Users\kEecfMwgj\Documents\riNXJCPkFg.pptx.vvyu	Dropped File	51.29 KB	application/zip	Access, Create, Write	CLEAN
1cf59c57ef7b3789ccfe9e94af1b864c136ccf102c34f429369948fb096434ed	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\him fl\4e_qp5b8\h0-ngmz.odt.vvyu, C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HIm fL\4E_Qp5b8\h0-NgmZ.odt.vvyu	Dropped File	48.98 KB	application/zip	Access, Create, Write	CLEAN
0cef471dca60ecc3c6d01d194ecb98d4bc9aca1b31a83cb15bb2ee8631ce6458	C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HIm fL\22cygPlJe.ods.vvyu, c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\him fl\22cygpije.ods.vvyu	Dropped File	36.96 KB	application/octet-stream	Access, Create, Write	CLEAN
30e77c7806e9308e89a8cd0abf07b8a149ac7c6bad7ddf6850b20c603d91ddbf	C:\Users\kEecfMwgj\Pictures\f83rpj3sXX29oJ.jpg.vvyu, c:\users\keecfmwgj\pictures\f83rpj3sxx29oj.jpg.vvyu	Dropped File	26.59 KB	image/jpeg	Access, Create, Write	CLEAN
eda36dc0739d8049fc937ccbaa419336a3cecfb51aa3f409bec84894c7e86786	C:\Users\kEecfMwgj\Videos\FPzctgqI5ySwICCgSS9cO9EJxpugq\P2QT4FKo.mp4.vvyu, c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\p2qt4fko.mp4.vvyu	Dropped File	28.25 KB	application/octet-stream	Access, Create, Write	CLEAN
138739bd275bf2627e4c0dfbfe239e9da8f0b8da9f155fbb16e64aff96f6328d	C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397\WXRqwImP8omimb.bmp.vvyu, c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\wxrqwimp8omimb.bmp.vvyu	Dropped File	94.36 KB	application/octet-stream	Access, Create, Write	CLEAN
be1ec249f95293c5fab9a8f8edad8d148ef50db9c505cf7fd886cc80b707821f	c:\users\keecfmwgj\documents\qca-wrdfbpizyp.docx.vvyu, C:\Users\kEecfMwgj\Documents\qCa-wrdfbplzYp.docx.vvyu	Dropped File	46.49 KB	application/zip	Access, Create, Write	CLEAN
1320837e0bb9e561d124a9a5638fc42c868cc0d5ff2fffc33fcee06b06b6e0c6	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\ysw9udfa\io6kkqyuc.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\ySw9UDFA\io6KkQYuC.xlsx.vvyu	Dropped File	81.12 KB	application/zip	Access, Create, Write	CLEAN
1895f95febca6531bc20438a53f745c81f5ae7b9ac02d3a1a8ec9925d57b55d7	c:\users\keecfmwgj\desktop\bkw1.mp4.vvyu, C:\Users\kEecfMwgj\Desktop\Bkw1.mp4.vvyu	Dropped File	11.38 KB	application/octet-stream	Access, Create, Write	CLEAN
a41ecdea59b8e39ec81d1ca67d4027621bfab9e936953ae72c4925bd10913a63	C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\47m5sv0uqVNl\AZ2aRaMGzQB\xryUj16QF_9DxMTZ1QMq.m4a.vvyu, c:\users\keecfmwgj\music\juck2lalp_ipp\47m5sv0uqvnl\az2aramgzqb\xryuj16qf_9dxmtz1qmq.m4a.vvyu	Dropped File	52.56 KB	application/octet-stream	Access, Create, Write	CLEAN
a2839db93e844a1f1efe8a0a462cf7d4160362917c56b818715d27297d30aece	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

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
aa2caa916e9c94a5abc6dea70acc7656cf1c547949e88f87fb3685831e51677d	C:\Users\kEecfMwgj\Pictures\cbyFXHxALB9ISR--Iyv1.png.vvyu, c:\users\keecfmwgj\pictures\cbyfxhxalb9isr--iyv1.png.vvyu	Dropped File	48.40 KB	application/octet-stream	Access, Create, Write	CLEAN
d2b19b6572639abaea0d49592c0ca72d4b00b29e72515f25d18bbc3eaef22218	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
e363970dbaa463acbcb3af2a7ba08cc2d2f4028486bdb7801ba17c2a0d02a0ef	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\himfl\w9_k2r1yg22qfb5wtf98.ots.vvyu, C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HImfL\w9_K2R1YG22qFB5WTF98.ots.vvyu	Dropped File	41.94 KB	application/octet-stream	Access, Create, Write	CLEAN
4f7f139823f9284a08bb09db90f260c79b5aaa68ecf39e90379bdbd6f7d5cafc	c:\users\keecfmwgj\documents\a_eemub.docx.vvyu, C:\Users\kEecfMwgj\Documents\a_eeMub.docx.vvyu	Dropped File	50.19 KB	application/zip	Access, Create, Write	CLEAN
72c13fff31e885e4bf33a2b552b45cd4fccd4f5a888ac55d924efd428c1ab5c1	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\s_caetbn.ots.vvyu, C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\S_CAeTbN.ots.vvyu	Dropped File	11.78 KB	application/octet-stream	Access, Create, Write	CLEAN
53e8db0007aa15007bc41321ac29e416bc6b81f7ca39d33aa063309006f45e7f	c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\kb5yp2q.avi.vvyu, C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\wICCgSS9cO9EJxpugq\Kb5Yp2q.avi.vvyu	Dropped File	36.95 KB	application/octet-stream	Access, Create, Write	CLEAN
837ea95e174f181ba95ae55f8640eeeaf64feca13802904141dc77ad9f332156	C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\Ua71cE_srBW.docx.vvyu, c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\ua71ce_srbw.docx.vvyu	Dropped File	81.42 KB	application/zip	Access, Create, Write	CLEAN
db7ee8ddd4692605a5d688d72aeab66f36d8c0192df8c8653fb02039235ce096	c:\users\keecfmwgj\favorites\windows live\get windows live.url.vvyu, C:\Users\kEecfMwgj\Favorites\Windows Live\Get Windows Live.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
fec8a5ab848f2b2a3da3f7f0903266aaa083d0303f6c35b638dba6bb4cb5032f	c:\users\keecfmwgj\music\5u0vvnc3nroc8n_z\udco8hlr7krd.m4a.vvyu, C:\Users\kEecfMwgj\Music\5U0VVnc3NrOc8n_Z\uDCO8hlR7krD.m4a.vvyu	Dropped File	5.96 KB	application/octet-stream	Access, Create, Write	CLEAN
9f9febdd2161c940593a5e5c5bcc6e24b968a58d19d803fca63820bd49e8e1ec	C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\RpFnCBUaRW4M2CKB6Y8.avi.vvyu, c:\users\keecfmwgj\videos\cvfgvyfl7tfjuo7\rpfncbuarw4m2ckb6y8.avi.vvyu	Dropped File	76.98 KB	application/octet-stream	Access, Create, Write	CLEAN
9535babc99684847cf344a6ccb370f4ca8bf51fa7ab67250608fdd5942f304f2	C:\Users\kEecfMwgj\Pictures\9IU4er.gif.vvyu, c:\users\keecfmwgj\pictures\9iu4er.gif.vvyu	Dropped File	71.78 KB	image/gif	Access, Create, Write	CLEAN
60bd079c58c6b350cd3a34558dbad00d602c60e6799029c73cc4dd6e27b87692	C:\Users\kEecfMwgj\Desktop\5EtXO0qde4mAaAj2.mp3.vvyu, c:\users\keecfmwgj\desktop\5etxo0qde4maaaj2.mp3.vvyu	Dropped File	99.36 KB	application/octet-stream	Access, Create, Write	CLEAN
f8ab1961119edb4b8217954b1c523f96eed5e4a7bf9da4c12755acb387a1b446	c:\users\keecfmwgj\pictures\om3a-o87olj.gif.vvyu, C:\Users\kEecfMwgj\Pictures\OM3A-O87OLj.gif.vvyu	Dropped File	10.34 KB	image/gif	Access, Create, Write	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\music\j uck2lalp_ipp\47m5sv0uqvnl\f09xvkn7rnmgc_bzz.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\f6adjjdhq\cuol988xnblbr.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\tqpcqxkko-qtvp1zn.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\xr3nlex5czvfg.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\3uvy.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\wICCgSS9cO9EJxpugq\P2QT4FKo.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\cjrduvousoi.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\kLC6o4xsmRx_iA iEAy2.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\x7DOA nu7EAlTL.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\3YV6ib1olpsefRwtFe.pdf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\ippAwK.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\wICCgSS9cO9EJxpugq\wx0aR91G76sZ.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HImfL\4E_Qp5b8\RAN3RZLWQzdFaTXUwx\a_eNIZ ISa4B_.ppt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\m0zrf.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\oq7rosq7byockq_wi3.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\dr8uij1jmg.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\j uck2lalp_ipp\47m5sv0uqvnl\az2aramgzqb\i 1m.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\WOYOdoVl_y_ELRl.ppt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\3_n mmyv5xkxtc1mbc-u.pdf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\ah9z8QW.bmp.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\music\j uck2lalp_ipp\qiaob8kqt6gjfc.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HImfL\4E_Qp5b8\IcyHH4kvUj6MCZmB\NLDjOHMq5YqJ5Vaq-G-z.pps.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\onXJrQ0LQmJjW.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\rwx9qkj.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\xnjf1rqetdtxtc.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\uCbdvMv01ecUQrS5kFhR.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ynpbsi277\qia7.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ldaf6actl2hfcz.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\877l5thXMZRFuEmTVa.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\pictures\7p5jbw.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	Dropped File, Accessed File, VM File	Access, Create, Delete, Write	MALICIOUS
c:\users\keecfmwgj\pictures\99o q.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\fpzctgqi5ys\0ipri83h.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\92-ieu- ecANbCAHxu3.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\z x z-1adfcazuf.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\himfl\w9_k2r1yg22qfb5wtf98.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HImfL\4E_Qp5b8\RAN3RZLWQzdFaTXUwx\AFrd4UxBD1.pdf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\qg2uxz3cw8a4fuol_l.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\7lrwy.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\2CgRhD9i_8EFMrM.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\iv7y.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\5u0vvnc3nroc8n_z\udco8hlr7krd.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\f83rpj3sXX29oJ.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\tCNISe zbuiw.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\RUCPVLyvfQF00lxB1.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ujyi1dwdud6-j7pcelmb.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\vauzy4mlwuoc1eph.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\bdmsvg.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\fpzctgqi5ys\mfzx23r02sywxh\btrak.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\acppdj.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\j ucK2lALp_iPp\47m5sv0uqVNI\LPB-FW9jvpM0h.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\go3r.jpg.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\bkw1.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\9Qfl6h6W74ZaGdKZ7l.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397_dSq\EotVe.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\khh4ja_ffudblb.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\sfoK-fQjQEuAHhw.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\v_uid9u5nghf.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\j ucK2lALp_iPp\znTr-YRiXJ\0VhP5.wav.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

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Spaces.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\MuVmmckS_6uXC.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\9IU4er.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\mOm18edC.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\cbyFXHxALB9ISR--Iyv1.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\OPCtfBG3jGTahU3.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\himfl\4e_qp5b8\h0-ngmz.odt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\rwzd9mw.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\uvnwcx.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\liaafon99lah9nu_j.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\26hKDH\dhVO\fwWKBmZrXnqYjnf.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\07H2voZRMEM4mGd_N.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\fpzctgqi5ys\mfzx23r02sywxh\0yoyfg2vyekk-r.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\47m5sv0uqVNl\AZ2aRaMGzQB\8b1WNKi0f8BaPAX.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\j uck2lalp_ipp\zntr-yrixj\zpa wj4.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\j uck2lalp_ipp\zntr-yrixj\mIh8upb9ymIbt.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\ysw9udfa\83p1pax.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\oq0h.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ooz2bcvbppeb9wsu.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\5_xd oyqt5ylzw2rnd.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\hfGoG8BRVBw\DJyNf5d3ZVp0RV8Gb.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\hfgog8brvbw\0se02.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397\adVilyse_4wpfxq.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\26hKDH\dhVO\c-p32.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\3Ad0c.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ynpbsi277\hak2yhq7o.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HImfL\4E_Qp5b8\OQIL9b4yk.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\cvfgvyfl7tfjuo7\hi5yoaj9.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	Sample File, Accessed File, VM File	Access, Delete, Read, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\26hKDH\l5cha-37fB.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\sTzvqONg_kzYdubo TTT.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\uimsfjjz.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\q-8_5alv-aysztdlcx.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\hfgog8brvbw\hsj_qr5bne5moizbn.csv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\E 8rOnJ1a8nkX -7zzxk.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\i_u5ln.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\wXPNYv.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\j uck2lalp_ipp\dibgo7.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\j uck2lalp_ipp\47m5sv0uqvnl\dvuuti6.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\9ouhy.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\jkgjiq3h.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\geIB4J_yYE XOIcR0.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397\WXRqwIm P8omimb.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HIm fL\4E_Qp5b8\RAN3RZLWQzdFaTXUwx\qSY7qB q Psxa19MFF.pps.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\f6adjjdhq\adia hvz87jstj8m.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\j ucK2lALp_iPp\47m5sv0uqVNl\AZ2aRaMGzQB\xryUj16QF_9DxMTZ 1QMq.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\fpzctgqi5ys\jf9t9.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\5u0vvnc3nroc8n_z\4g2bike6.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\windows live\windows live mail.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\s_caetbn.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\ysw9udfa\bzhliohmivg2h0_pvvuu.pps.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\fpzctgqi5ys\m fzx23r02sywxh\l6ehb4ojilkrcleahkh.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\L59EH_1g_s_fJjq.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397_dsq\ywywxyty.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\26hkdh\dhvo\waqploj2c0tw.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\5KliNx-drvR8.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\85NDX4GNPa9.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\rinxjcpkfg.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Videos\iqB1Fd.mkv.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\eSfxo-E.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\z8twgmunehqoxqfe1k.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\j ucK2lALp_iPp\Y3zc_VVY6Kxz1vjr.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\j ucK2lALp_iPp\47m5sv0uqVNl\AZ2aRaMGzQB\5B4VEsMcGlm7c.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C: \Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\RpFnCBUaRW4M2CKB6Y8.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\om3a-o87olj.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\FPzctgql5yS\MfZX23r02sYWxh\DyXmYMfEW2zZ74G.avi.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\pictures\br-ix6cu0omqu4 dzyj.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ya9u.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\j ucK2lALp_iPp\znTr-YRiXJ\d4OMzSyCrSqIiU9aYvRY.wav.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
c:\users\keecfmwgj\desktop\nfequ_fxuy ewf.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\usU4fi-1.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\ncui5d__zr45d.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\5usDb JNuS3uVdkW.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\DvPtakSDSqUBk1s-p5E_.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C: \Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\6X4EOyI76e.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ynpbsi277\bp67ry2e oyq1fpgm.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\djRHD.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\n6jq6ucc95w9.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\rn1rbbo1eqymg_q.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\YnPBSI277\YZ4wuGCPKPt9a.pps.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c: \users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397_dsq\ouopevgnwd1-z0kjb.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\cvfgvyfl7tfjuo7\p5dr5.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\liar.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://acacaca.org/files/1/build3.exe	-	46.195.219.190, 210.182.29.70, 211.59.14.90, 58.235.189.192, 189.164.252.207, 211.119.84.112, 187.190.48.135, 190.219.54.242, 187.170.251.250, 31.166.90.88	-	GET	MALICIOUS
http://rgyui.top/dl/build2.exe	-	211.40.39.251, 109.102.255.230, 46.195.219.190, 187.156.10.94, 148.255.22.239, 187.232.183.77, 124.109.61.160, 186.6.205.61, 138.36.3.134, 187.170.251.250	-	GET	MALICIOUS
http://acacaca.org/test2/get.php?pid=BBBCA5C4A1C0DD06A87561C44E271CCC&first=true	-	46.195.219.190, 210.182.29.70, 211.59.14.90, 58.235.189.192, 189.164.252.207, 211.119.84.112, 187.190.48.135, 190.219.54.242, 187.170.251.250, 31.166.90.88	-	GET	MALICIOUS
https://api.2ip.ua/geo.json	-	162.0.217.254	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
acacaca.org	46.195.219.190, 210.182.29.70, 211.59.14.90, 58.235.189.192, 189.164.252.207, 211.119.84.112, 187.190.48.135, 190.219.54.242, 187.170.251.250, 31.166.90.88	-	TCP, HTTP, DNS	MALICIOUS
rgyui.top	211.40.39.251, 109.102.255.230, 46.195.219.190, 187.156.10.94, 148.255.22.239, 187.232.183.77, 124.109.61.160, 186.6.205.61, 138.36.3.134, 187.170.251.250	-	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
109.102.255.230	rgyui.top	Romania	DNS	CLEAN
186.6.205.61	rgyui.top	Dominican Republic	DNS	CLEAN
190.219.54.242	acacaca.org	Panama	DNS	CLEAN
162.0.217.254	api.2ip.ua	Netherlands	TCP, HTTPS, DNS	CLEAN
189.164.252.207	acacaca.org	Mexico	TCP, HTTP, DNS	CLEAN
46.195.219.190	rgyui.top, acacaca.org	Sweden	TCP, HTTP, DNS	CLEAN
187.170.251.250	rgyui.top, acacaca.org	Mexico	DNS	CLEAN
187.156.10.94	rgyui.top	Mexico	DNS	CLEAN
31.166.90.88	acacaca.org	Saudi Arabia	DNS	CLEAN
187.190.48.135	acacaca.org	Mexico	DNS	CLEAN
138.36.3.134	rgyui.top	Brazil	DNS	CLEAN
211.40.39.251	rgyui.top	South Korea	DNS	CLEAN

IP Address	Domains	Country	Protocols	Verdict
211.119.84.112	acacaca.org	South Korea	DNS	CLEAN
124.109.61.160	rgyui.top	Pakistan	DNS	CLEAN
148.255.22.239	rgyui.top	Dominican Republic	DNS	CLEAN
210.182.29.70	acacaca.org	South Korea	DNS	CLEAN
187.232.183.77	rgyui.top	Mexico	DNS	CLEAN
211.59.14.90	acacaca.org	South Korea	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}	access	0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion	access	0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\SysHelper	read, access, write	0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SysHelper	read, access, write	0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	CLEAN

Process

Process Name	Commandline	Verdict
0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	"C:\Users\kEecfMwgj\Desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe"	MALICIOUS
0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	"C:\Users\kEecfMwgj\Desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe" --Admin IsNotAutoStart IsNotTask	MALICIOUS
build2.exe	"C:\Users\kEecfMwgj\AppData\Local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe"	MALICIOUS
0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	"C:\Users\kEecfMwgj\AppData\Local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe" --AutoStart	MALICIOUS
0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	"C:\Users\kEecfMwgj\Desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe"	SUSPICIOUS
0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	"C:\Users\kEecfMwgj\Desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe" --Admin IsNotAutoStart IsNotTask	SUSPICIOUS
build2.exe	"C:\Users\kEecfMwgj\AppData\Local\791a7d8c-ce1c-4b10-8bdd-9a6fed24ef19\build2.exe"	SUSPICIOUS
0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe	"C:\Users\kEecfMwgj\AppData\Local\fa1eafca-d2cd-4c04-a099-4159a69291ac\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe" --AutoStart	SUSPICIOUS
icacls.exe	icacls "C:\Users\kEecfMwgj\AppData\Local\fa1eafca-d2cd-4c04-a099-4159a69291ac" /deny *S-1-1-0:(OI)(CI)(DE,DC)	CLEAN

YARA / AV

YARA (280)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\7p5jbw.jpg.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	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\znTr-YRiXJ\0VhP5.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\z8twgmunehqoxqfe1k.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\47m5sv0uqVNl\AZ2aRaMGzQB\5B4VEsMcGlm7c.mp3.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	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\FPzctgqI5yS\wICCgSS9cO9EJxpugq\wx0aR91G76sZ.flv.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\n6jq6ucc95w9.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\juck2lalp_ipp\47m5sv0uqvnl\ah3jwn0.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\ysw9udfa\bzhliohmivg2h0_pvvuu.pps.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\hA6nEQ04cdHym7b8.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\microsoft websites\microsoft at home.url.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\ippAwK.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\6_x m.odp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\djRHD.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\eSfxo-E.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\desktop\ynpbsi277\5ctq03jfokji397\oq0h.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\q-8_5alv-aysztdlcx.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\hfgog8brvbw\0se02.odp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\47m5sv0uqVNI\LPB-FW9jvpM0h.wav.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\desktop\ynpbsi277\5ctq03jfokji397\bxv5ql2id9hkdxpv7.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\9hkv.mp4.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\desktop\0336cc8aff0e4974ede9e8901abeb10f836d50619cef1cb59aa41b447cea1ca5.exe.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\m0zrf.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\877l5thXMZRFuEmTVa.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\acppdj.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\jkgjiq3h.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\iaafon99lah9nu_j.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\pictures\-ctdcbmthlrz.jpg.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	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\juck2lalp_ipp\dibgo7.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\mOm18edC.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ynpbsi277\bp67ry2e oyq1fpgm.mp4.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\fpzctgqi5ys\mfzx23r02sywxh\l6ehb4ojilkrcleahkh.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\desktop\xnjf1rqetdtxtc.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\Pictures\uCbdvMv01ecUQrS5kFhR.gif.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\FPzctgql5yS\3Ad0c.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\f6adjjdhq\cuol988xnblbr.m4a.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	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\rn1rbbo1eqymg_q.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\khh4ja_ffudblb.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\5U0VVnc3NrOc8n_Z\k8_cI3l6hV1-Y7\27Qc0VUi07zkn_VUAary.wav.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\85NDX4GNPa9.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\YnPBSI277\5Ctq03jfOkJI397_dSq\EotVe.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\Music\9Qfl6h6W74ZaGdKZ7l.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\26hKDH\dhVO\fwWKBmZrXnqYjnf.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ooz2bcvbppeb9wsu.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397\f6adjjdhq\adiahvz87jstj8m.flv.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\26hkdh\dhvo\waqploj2c0tw.wav.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\3YV6ib1olpsefRwtFe.pdf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\3_nmmyv5xkxtc1mbc-u.pdf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\tqpcqxkko-qtvp1zn.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\juck2lalp_ipp\47m5sv0uqvnl\dvuuti6.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\i_u5ln.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\8nnli0koeom-mpum785\hfgog8brvbw\hsj_qr5bne5moizbn.csv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\6X4EOyl76e.wav.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\desktop\ynpbsi277\5ctq03jfokji397\v_uid 9u5nghf.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\NMttoz1zVMuEbci.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\3uvy.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\Favorites\Microsoft Websites\Microsoft At Work.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\5usDbJNuS3uVdkW.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\hyglyDuy.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\fpzctgqi5ys\0ipri83h.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\pictures\qg2uxz3cw8a4fuol_l.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ynpbsi277\ov6fzg.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\U00H4oegdjWIv9LIU5.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\msn websites\msn sports.url.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\uimsfjjz.rtf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\links\web slice gallery.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\rwx9qkj.png.vvyu	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	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Gallery.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\hfGoG8BRVBw\DJyNf5d3ZVp0RV8Gb.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ynpbsi277\hak2yhq7o.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\fpzctgqi5ys\wiccgss9co9ejxpugq\cjrduvousoi.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\pictures\vauzy4mlwuoc1eph.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\juck2lalp_ipp\zntr-yrixj\f8ilkitdoj8fsshi0.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\Desktop\usU4fi-1.ots.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\fpzctgqi5ys\m fzx23r02sywxh\btrak.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\8NNLi0kOEoM-mpUM785\HImfL\4E_Qp5b8\RAN3RZLWQzdFaTXUwx\AFrd4UxBD1.pdf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\RUCPVLyvfQF00lxB1.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\Eb_B9k_JDAVxhXh0\sTzvqONg_kzYduboTTT.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\juck2lalp_ipp\zntr-yrixj\mlh8upb9ymlbt.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\DvPtakSDSqUBk1s-p5E_.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\92-ieu- ecANbCAHxu3.pptx.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ynpbsi277\5ctq03jfokji397_dsq\ywywxyty.mp3.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\26hKDH\l5cha-37fB.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\z x z-1adfcazuf.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ujyi1dwdud6-j7pcelmb.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\desktop\9ouhy.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\go3r.jpg.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\26hKDH\dhVO\c-p32.m4a.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\vuc5gusp1h33w.png.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\favorites\msn websites\msn.url.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\Videos\07H2voZRMEM4mGd_N.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\sfoK-fQjQEuAHhw.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\iv7y.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\x7DOAnu7EAlTL.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\YnPBSI277\YZ4wuGCPKPt9a.pps.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\0w8tqjzs69qqxvzs-d8d.ods.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\FPzctgqI5yS\MfZX23r02sYWxh\DyXmYMfEW2zZ74G.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\jucK2lALp_iPp\Y3zc_VVY6Kxz1vjr.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\Videos\cvfGVyFL7tFjUO7\7lrwy.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\cvfGVyFL7tFjUO7\L59EH_1g_s_fJjq.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\lv2axv.jpg.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5

Reduced dataset

ENVIRONMENT

Virtual Machine Information

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

Platform Information

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

Software Information

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

System Information

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

System Root	C:\Windows