MALICIOUS

Classifications: Ransomware

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

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe**
ID	#5067676
MD5	24b6effdd763befb6ff4a657e15c77bc
SHA1	dd09691ceccd54d7e68a9c6553a6b94452dc7c85
SHA256	d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797
File Size	857.50 KB
Report Created	2022-08-05 14:59 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (24 rules, 148 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #11) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #11) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 200 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\videos\lyqkedl\bp_f\d6ztvjfwwa.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\IS2B.jpg.vvyu".
- Rule "Djvu" from ruleset "Ransomware" has matched on a memory dump for (process #6) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe.
- 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\u2xcl6fk4p\buwavzcuhtmrml.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\lyqkedl\bp_f\wuud9p77x.mkv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\EbPUXvbq aj ZxnAB.png.vvyu".
- Rule "Djvu" from ruleset "Ransomware" has matched on a memory dump for (process #2) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe.
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\qzaaruieowyp 0mvbzk.docx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\YG8k.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\lyqkedl\mrt4.mkv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\t1mqysmsezilmfb.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Spaces.url.vvyu".
- Rule "Djvu" from ruleset "Ransomware" has matched on a memory dump for (process #11) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe.
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\dtcpak5wO kdkqu Ph.mkv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\7bevwhnu_fkrc\jxd7petv2jcni.xls.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\cv8-veyoh.wav.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\Music\CrZ6i\jjLwLGu.m4a.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\hqdktuf4etm1.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\desktop\5-xamft.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\xquj.docx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\VDue0.odt.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\WzOtFShww.rtf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\otrrqivqej6bkbcciq.docx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\70uMB.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\lyqkedl\izhxbinth.mp4.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\h63-85V.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\videos\lyqkedl\bp_f\pc3yf9pj6umpbxequ7nk.swf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\qs-f1e.pptx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\naFofVP436Y9.odp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\1HQ_0Ry\AoEQk-B.ppt.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\c34Mo1t-KwX2Fe92.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\s6KVYjgw4EOpy.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\pSXJ.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\u X_9CrHqo8CggdcB4.jpg.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\lYQkedL\OREWDZex5CeUn06c UN.flv.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\002z8yb-4ii p.docx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\Kt1gN2Zu4cLe_ffn1E.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\1hq_0ry\jn5w8pue5cpjcmbtd8.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\qUrDOWbjU_xfUkCK.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\MmtudzmA8-1ZtsXh1iI.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\8fWkzgyyD0qQR-ID9Sm.pptx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\xS0O4.gif.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\gGYFMJx.swf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Desktop\zH9UWAN96jNNa9sjtX.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\pictures\nlxnihq5_.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\rk2x.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\1hq_0ry\rnf1.rtf.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\t12gfq_xaghox.ppt.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\k2soyi-o5lstsd_n6rv.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\l001k\7rzoymi.xlsx.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\U2xcL6FK4p\hFSYfNeYKfRIr3.mp3.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\7HsBaAEuFJOdKC\QjjqmBh2.wav.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\mqT6p7TH.png.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Pictures\HGiMBm 8T.bmp.vvyu".
- Rule "DjvuEncryptedFile" from ruleset "Ransomware" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\l001k\uVwtXkawlnc12.xlsx.vvyu".

Score	Category	Operation	Count	Classification
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
4/5	Reputation	Contacts known malicious URL	3	-
	• Reputation analysis labels the URL "http://acacaca.org/files/1/build3.exe" which was contacted by (process #6) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "http://acacaca.org/test2/get.php?pid=B781B23F267DEB99256EE88043E0BDBC&first=true" which was contacted by (process #6) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "http://rgyui.top/dl/build2.exe" which was contacted by (process #6) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe as Mal/HTMLGen-A.		
4/5	Reputation	Resolves known malicious domain	2	-
	• Reputation analysis labels the resolved domain "rgyui.top" as Mal/HTMLGen-A. • Reputation analysis labels the resolved domain "acacaca.org" as Mal/HTMLGen-A.			
3/5	YARA	Suspicious content matched by YARA rules	8	-
	• Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\2fyWk_nuEZSWQOD.pdf.vvyu". • Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\2fyWk_nuEZSWQOD.pdf.vvyu". • Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\1flc8eh2.pdf.vvyu". • Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\1flc8eh2.pdf.vvyu". • Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\oAPMaSkphuOK7d.pdf.vvyu". • Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\oAPMaSkphuOK7d.pdf.vvyu". • Rule "PDF_Missing_startxref" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\ktAJOVysWpTdu.pdf.vvyu". • Rule "PDF_Missing_EOF" from ruleset "Malicious-Documents" has matched on the dropped file "C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\ktAJOVysWpTdu.pdf.vvyu".		
2/5	Hide Tracks	Deletes file after execution	1	-
	• (Process #2) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe deletes executed executable "C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe".			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #6) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe has a thread which sleeps more than 5 minutes.			
2/5	_data_collection	Reads sensitive application data	1	-
	• (Process #11) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe tries to read sensitive data of application "git" by file.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	3	-
	• (Process #1) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe modifies memory of (process #2) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe. • (Process #5) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe modifies memory of (process #6) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe. • (Process #10) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe modifies memory of (process #11) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	3	-

Score	Category	Operation	Count	Classification
	• (Process #1) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe alters context of (process #2) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe. • (Process #5) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe alters context of (process #6) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe. • (Process #10) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe alters context of (process #11) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe.		
2/5	Task Scheduling	Schedules task	1	-
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe", to be triggered by TIME. Task has been rescheduled by the analyzer.		
1/5	Obfuscation	Reads from memory of another process	3	-
	• (Process #1) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe reads from (process #1) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe. • (Process #5) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe reads from (process #5) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe. • (Process #10) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe reads from (process #10) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	3	-
	• (Process #1) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #5) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #10) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.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) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe enumerates running processes. • (Process #6) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe enumerates running processes. • (Process #11) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe enumerates running processes.		
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #2) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe adds ""C:\Users\kEecfMwgj\AppData\Local\12868036... ...6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe" --AutoStart" to Windows startup via registry.		
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #2) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe starts (process #2) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe with a hidden window.		
1/5	Mutex	Creates mutex	2	-
	• (Process #6) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe creates mutex with name "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}". • (Process #11) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe creates mutex with name "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}".		
1/5	Discovery	Tries to get network statistics	1	-
	• (Process #11) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe gets network statistics via API.		
1/5	Network Connection	Downloads file	1	-
	• (Process #6) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe downloads file via http from http://acacaca.org/test2/get.php?pid=B781B23F267DEB99256EE88043E0BDBC&first=true.		
1/5	Obfuscation	Resolves API functions dynamically	6	-

Score	Category	Operation	Count	Classification
		• (Process #1) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe resolves 43 API functions by name.		
		• (Process #2) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe resolves 37 API functions by name.		
		• (Process #5) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe resolves 43 API functions by name.		
		• (Process #6) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe resolves 37 API functions by name.		
		• (Process #10) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe resolves 43 API functions by name.		
		• (Process #11) d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.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					

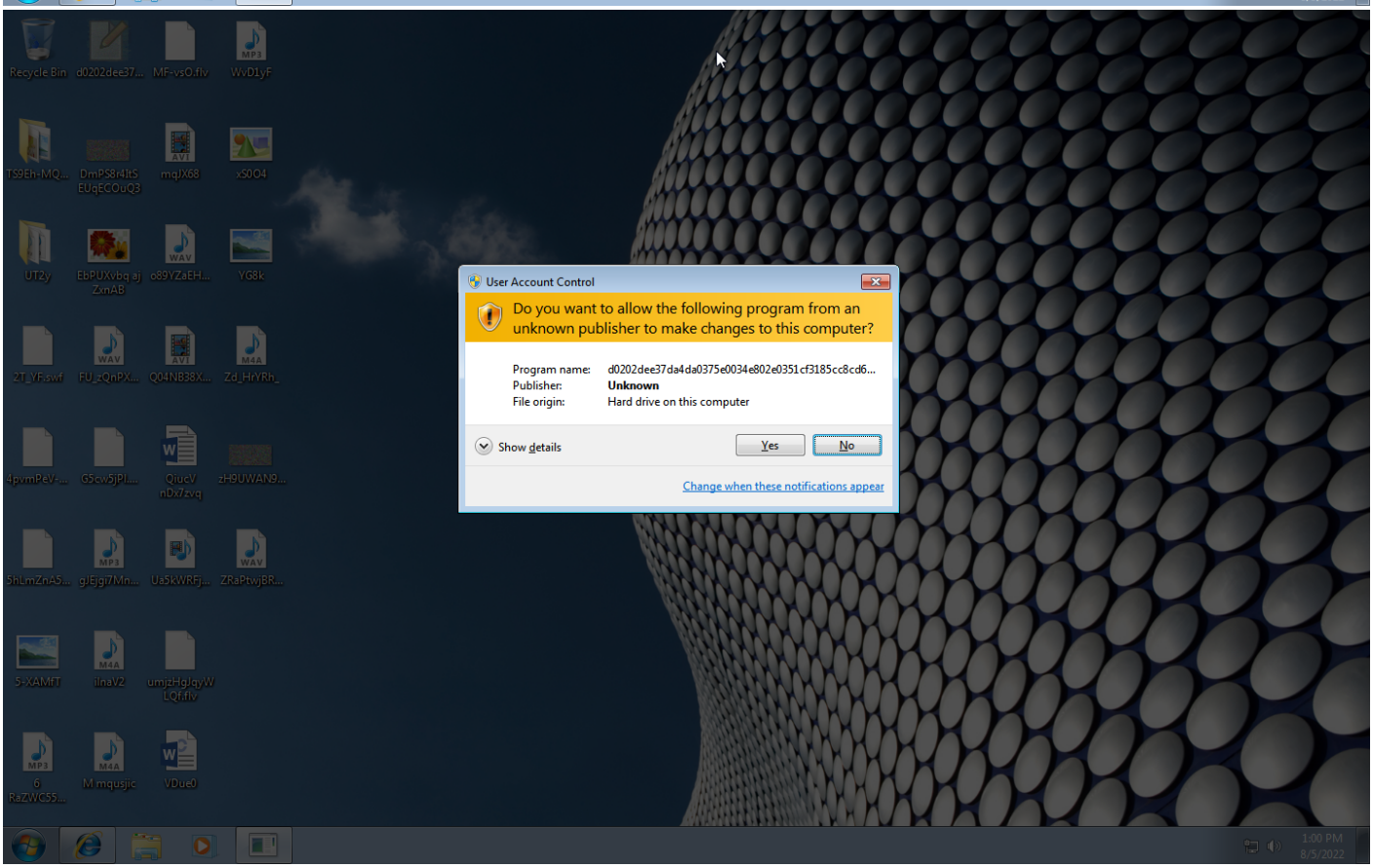
Sample Information

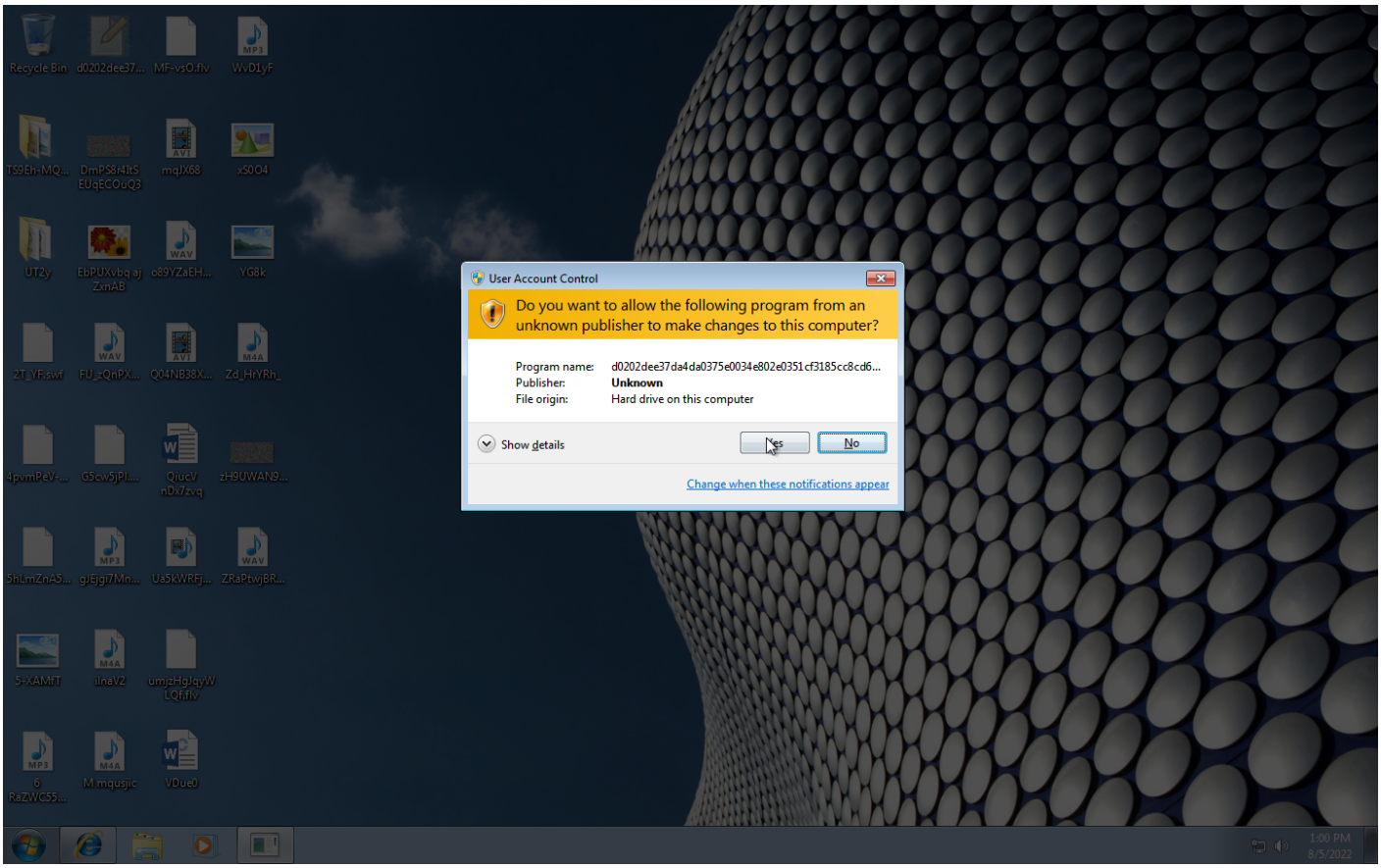
ID	#5067676
MD5	24b6effdd763befb6ff4a657e15c77bc
SHA1	dd09691ceccd54d7e68a9c6553a6b94452dc7c85
SHA256	d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797
SSDeep	24576:QnXVvjHfMfwQKIbr211TSgaUo6GF5iV8ig:QZUfwQvbr2p66GF4Vu
ImpHash	36d58c3755c94d900745b5260c0b6d11
File Name	d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe
File Size	857.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 14:59 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	10
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	286


Recycle Bin
d0202dee37...
MF-vsO.flv
WvD1yF
TS9Eh-MQ...
DmPS8r4ltS EUqECOuQ3
mqJX68
xS0O4
UT2y
EbPUXvbq aj ZxnAB
o89YZaEH...
YG8k
2T_YF.swf
FU_zQnPX...
Q04NB38X...
Zd_HrYRh_
4pvmPeV-...
G5cw5jPl....
QiucV nDx7zvq
zH9UWAN9...
5hLmZnA5...
gjEjgi7Mn...
Ua5kWRFj...
ZRaPtwjBR...
5-XAMfT
ilnaV2
umjzHgJqyW LQf.flv
6 RaZWC55...
M mqusjic
VDue0
1:00 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: d0202dee37da4da0375e0034e802e0351cf3185cc8cd6...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

124.57 KB total sent

118.98 KB total received

4 ports 80, 443, 53, 445

3 contacted IP addresses

1 URLs extracted

3 files downloaded

0 malicious hosts detected

DNS

4 DNS requests for 3 domains

1 nameservers contacted

1 total requests returned errors

HTTP/S

3 URLs contacted, 2 servers

5 sessions, 3.44 KB sent, 26.01 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://rgyui.top/dl/build2.exe	-	-		0 bytes	NA
GET	http://acacaca.org/test2/get.php?pid=B781B23F267DEB99256EE88043E0BDBC&first=true	-	-		0 bytes	NA
GET	http://acacaca.org/files/1/build3.exe	-	-		0 bytes	NA
GET	https://api.2ip.ua/geo.json	-	-		0 bytes	NA

DNS Requests

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

BEHAVIOR

Process Graph

Process #1: d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 45343, Reason: Analysis Target
Unmonitor End Time	End Time: 60976, Reason: Terminated
Monitor duration	15.63s
Return Code	0
PID	3860
Parent PID	1916
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	857.50 KB	d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797	✖

Host Behavior

Type	Count
System	252
Module	76
File	6
Environment	1
Window	1
Process	1
-	3
-	9

Process #2: d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 59175, Reason: Child Process
Unmonitor End Time	End Time: 85530, Reason: Terminated
Monitor duration	26.36s
Return Code	0
PID	3868
Parent PID	3860
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\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf18	0x400000(4194304)	0x400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf18	0x401000(4198400)	0xca600	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf18	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf18	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf18	0x52b000(5419008)	0x200	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf18	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf18	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf18 / 0xf20	0x76f101c4(1995506116)	-	✔	1

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	857.50 KB	d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797	✖

Host Behavior

Type	Count
System	4
Module	47
File	6
Environment	1
Process	97
Registry	4
COM	1

Network Behavior

Type	Count
HTTPS	1

Process #3: svchost.exe

ID	3
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 78396, Reason: RPC Server
Unmonitor End Time	End Time: 287369, Reason: Terminated by timeout
Monitor duration	208.97s
Return Code	Unknown
PID	872
Parent PID	3868
Bitness	64 Bit

Process #4: icacls.exe

ID	4
File Name	c:\windows\syswow64\icacls.exe
Command Line	icacls "C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12" /deny *S-1-1-0:(OI)(CI)(DE,DC)
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81121, Reason: Child Process
Unmonitor End Time	End Time: 83845, Reason: Terminated
Monitor duration	2.72s
Return Code	0
PID	3908
Parent PID	3868
Bitness	32 Bit

Process #5: d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82997, Reason: Child Process
Unmonitor End Time	End Time: 87948, Reason: Terminated
Monitor duration	4.95s
Return Code	0
PID	3924
Parent PID	3868
Bitness	32 Bit

Host Behavior

Type	Count
System	252
Module	76
File	6
Environment	1
Window	1
Process	1
-	3
-	9

Process #6: d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 86338, Reason: Child Process
Unmonitor End Time	End Time: 106024, Reason: Terminated
Monitor duration	19.69s
Return Code	0
PID	3936
Parent PID	3924
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\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf58	0x400000(4194304)	0x400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf58	0x401000(4198400)	0xca600	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf58	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf58	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf58	0x52b000(5419008)	0x200	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf58	0x52c000(5423104)	0xa400	✔	1
Modify Control Flow	#5: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf58 / 0xf64	0x76f101c4(1995506116)	-	✔	1
Modify Memory	#5: c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0xf58	0x7efde008(2130567176)	0x4	✔	1

Dropped Files (3)

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

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

Host Behavior

Type	Count
System	4
Module	47
File	16
Environment	1
Process	95
Registry	7
COM	1
-	2
Mutex	1
User	1
Window	1
-	3

Network Behavior

Type	Count
HTTP	3
HTTPS	1
TCP	1

Process #7: taskeng.exe

ID	7
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {58D0AF36-B196-4C0E-BD35-56E44726A7F4} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 99797, Reason: Child Process
Unmonitor End Time	End Time: 106357, Reason: Terminated
Monitor duration	6.56s
Return Code	1073807364
PID	3988
Parent PID	872
Bitness	64 Bit

Process #8: d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe

ID	8
File Name	c:\users\keecfmwgj\appdata\local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe
Command Line	C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe --Task
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 100955, Reason: Child Process
Unmonitor End Time	End Time: 104141, Reason: Terminated
Monitor duration	3.19s
Return Code	1073807364
PID	4020
Parent PID	3988
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	27
File	3
Environment	1

Process #10: d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe

ID	10
File Name	c:\users\keecfmwgj\appdata\local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe" --AutoStart
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 154471, Reason: Autostart
Unmonitor End Time	End Time: 159247, Reason: Terminated
Monitor duration	4.78s
Return Code	0
PID	1908
Parent PID	1720
Bitness	32 Bit

Host Behavior

Type	Count
System	252
Module	76
File	6
Environment	1
Window	1
Process	1
-	3
-	9

Process #11: d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe

ID	11
File Name	c:\users\keecfmwgj\appdata\local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe" --AutoStart
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 158751, Reason: Child Process
Unmonitor End Time	End Time: 190043, Reason: Terminated
Monitor duration	31.29s
Return Code	0
PID	1996
Parent PID	1908
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0x778	0x400000(4194304)	0x400	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0x778	0x401000(4198400)	0xca600	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0x778	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0x778	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0x778	0x52b000(5419008)	0x200	✔	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0x778	0x52c000(5423104)	0xa400	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#10: c:\users\keecfmwgj\appdata\local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0x778	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#10: c:\users\keecfmwgj\appdata\local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	0x778 / 0x7d0	0x77de01c4(2011038148)	-	✔	1

Dropped Files (203)

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\videos\lyqkedl\bp_f\d6ztvjfwwa.flv.vvyu	40.42 KB	80f6e86d1ca2934b6a512ae8760b162d24f5dcfcbdee490a932962082ce03fcd	✔
C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\IS2B.jpg.vvyu	89.48 KB	43e6f84df18e0ecdef1e894dfe7560276ecb6129467da392f24177d56afbfd6c	✔
C:\Users\kEecfMwgj\Contacts\Administrator.contact.vvyu	67.11 KB	9f5fec9b0eaae4e0cbced0783399e16fc98c2aa689cf05d568a1ac26e0ee3c1a	✔
c:\users\keecfmwgj\music\u2xcl6fk4p\buwavzcuhtmrml.wav.vvyu	88.41 KB	3e1c9e83abf0a080232a867f889ace95eca79f14f8110117cb9dfa9aa6f21b0b	✔
c:\users\keecfmwgj\videos\lyqkedl\bp_f\wuud9p77x.mkv.vvyu	12.31 KB	cec8599bb3470fd3dfc69b4e7788fd0065cd74809ed0cf5c28633b9038b0153a	✔
C:\Users\kEecfMwgj\Desktop\EbPUXvbq aj ZxnAB.png.vvyu	100.12 KB	923b159396d0b3de831f96c5ef3edf16e36b96c4e5d6ad2fa227b520df3f7668	✔
c:\users\keecfmwgj\documents\qzaaruieowyp 0mvbzk.docx.vvyu	34.86 KB	6bbce99cc1c931da081a05ec5cd68d9d5f5cedbaae4987e40a5e209ef9c602ab	✔
C:\Users\kEecfMwgj\Desktop\YG8k.jpg.vvyu	53.70 KB	48473a2c6fe8f1db5f1b7f17c2525ad0a2ed21cda728921ea5d004e4a9a18a60	✔
c:\users\keecfmwgj\videos\lyqkedl\mrt4.mkv.vvyu	3.25 KB	df1773702517ab25c9af0526d167112b73c9e4441e831ebb360b16c31d841e7c	✔
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\t1mqysmsezilmfb.m4a.vvyu	42.76 KB	1aefac166c4e5df5ec4aba5fcf262c928aa10ee5f9a35523ba534d8807d79dbc	✔
C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Spaces.url.vvyu	467 bytes	b63f6cd8684172a722603dc2bba4279ee6b14b442b90fe8ea3191a33754b6aae	✔
C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\dtcpak5wO kdkqu Ph.mkv.vvyu	89.11 KB	822141d70f49354ddef8f4cc778705f3732373e396ecd9a3c5a382e22e7fdd8a	✔
c:\users\keecfmwgj\documents\7bevwhnu_fkrc\jxd7petv2jcni.xls.vvyu	96.12 KB	3f1fe512a9524421cede2d93688ff7d5c5e973bac88607c6ff0967e1e6d37d25	✔
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\cv8-veyoh.wav.vvyu	13.97 KB	29af13d8fce607b0e048242f9746710bc9794d1efa02a79565e77290cd415235	✔
c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu	467 bytes	ff31f10671bf946d5c7311e865cdb4fc97bf826f9d91d7b96c0c7b36124c561f	✔
C:\Users\kEecfMwgj\Music\CrZ6i\jjLwLGu.m4a.vvyu	26.93 KB	940212712bada8893b8e9f842d35b90d67318a16bbb0bb187c8e65ea3bff3884	✔
c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe.vvyu	857.50 KB	d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797	✖
c:\users\keecfmwgj\pictures\hqdktuf4etm1.bmp.vvyu	57.67 KB	0ff70edc3ea76b4c09694d751d7dafbba70167807aa5bc34d7e700310433eb0c	✔
c:\users\keecfmwgj\desktop\5-xamft.jpg.vvyu	29.58 KB	b26e580c73f9b84a0555ebac4a2e230e63b6df3f32bfbf7b24d2be241356cb37	✔
c:\users\keecfmwgj\documents\xquj.docx.vvyu	79.17 KB	cbe07aa4abe72a1ee68bfef166f063062f00ac25fc7804e33ba4987cd2dba562	✔
C:\Users\kEecfMwgj\Desktop\VDue0.odt.vvyu	60.23 KB	ed8a80252cb0d0438c2e55e9c3db6120f59ec58272a3b91fabcd6f292343fa95	✔

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\WzOtFShww.rtf.vvyu	55.44 KB	1a1e5d46b92b044661e09ac2a6fa12c1f41ab369349516b0212169a1aaa78401	✔
c:\users\keecfmwgj\documents\otrrqivqej6bkbcciq.docx.vvyu	96.58 KB	41f4295b5a673f97e71da22437fd60b09cf62bc9b48dd220305baf69d2ea6fb4	✔
C:\Users\kEecfMwgj\Pictures\70uMB.gif.vvyu	64.57 KB	65e5572556e34a9e3f38fb1c81625e280b5f31004b54531d72e1d7cea4b7841f	✔
c:\users\keecfmwgj\videos\lyqkedl\izhxbinth.mp4.vvyu	76.63 KB	90c137f810534e7e869ff654413c23914734036b6d1f8f08069d96665d892e73	✔
C:\Users\kEecfMwgj\Documents\h63-85V.xlsx.vvyu	82.50 KB	f35335deffacec40ca5679f4966b36e1b11ddca88faacd44f5c446ff5dc7c596	✔
c:\users\keecfmwgj\videos\lyqkedl\bp_f\pc3yf9pj6umpbxequ7nk.swf.vvyu	55.83 KB	a5282142cd953ba0ebabec93602fded6a9498cc5fbc985fade835d9f2aa05111	✔
c:\users\keecfmwgj\documents\qs-f1e.pptx.vvyu	27.94 KB	00fce946bb55202cf2125074ef23e13dc3ee501813fcbe8323546dbcb0acad44	✔
C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\naFofVP436Y9.odp.vvyu	24.74 KB	c9ac969f8ef55ccba82fee2c97562f6ae36f683b8287bf662b406f79cb756df5	✔
C:\Users\kEecfMwgj\Documents\1HQ_0Ry\AoEQk-B.ppt.vvyu	34.69 KB	dc5327569cffa667542bd34a5c3c031a4a8c81e66cf3506b81251616a5a45967	✔
C:\Users\kEecfMwgj\Pictures\c34Mo1t-KwX2Fe92.png.vvyu	16.55 KB	9a5b53aa58ba33a3e0f1be80d0508a027e3d86e63d064effeac25a2f797cecce	✔
C:\Users\kEecfMwgj\Documents\s6KVYjgw4EOpy.xlsx.vvyu	98.84 KB	601f88645c83d66d9762058a24438b3565fda105dd7be552aad88a051d133eb6	✔
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\pSXJ.mp3.vvyu	21.78 KB	bf56f0783534085f91f824bdda715050774d2c25e2ddc337cd0369722c20ab81	✔
C:\Users\kEecfMwgj\Pictures\u X_9CrHqo8CggdcB4.jpg.vvyu	55.18 KB	b2c6c44ae7af20c7432eb6ee4c42b65517ddc70903ca30af7ba8d0c26e9928a4	✔
C:\Users\kEecfMwgj\Videos\lYQkedL\OREWDZex5CeUn06cUN.flv.vvyu	48.37 KB	43cfde9b466dc8601ff358294f54048e31b43241ed0f1e29251adc4c5e5bedca	✔
c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\002z8yb-4ii p.docx.vvyu	86.87 KB	12b4774a9c1dc9a946051ce7065ad1815faf2ba1e32dc11f1913ea93a22f4605	✔
C:\Users\kEecfMwgj\Pictures\Kt1gN2Zu4cLe_ffn1E.png.vvyu	54.48 KB	4ec6cdffc1c9950b7287b891576887bea02e6e11fecf8f9c85c3cdef8cd54fcc	✔
c:\users\keecfmwgj\documents\1hq_0ry\jn5w8pue5cpjcmbtd8.xlsx.vvyu	84.87 KB	ffd497fc2208b791d010cc993adad9e829b23004c55aef6353f7d57c762c78de	✔
C:\Users\kEecfMwgj\Pictures\qUrDOWbjU_xfUkCK.png.vvyu	99.98 KB	acf445c072e13233bf0abb64938e289d6dd0829fe140a0418a4fde98ccf909a6	✔
C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\MmtudzmA8-1ZtsXh1iI.gif.vvyu	61.93 KB	392c7a25b70dd2343cd3028afc311e75e8baa711ec2529bd720d64d055e35895	✔
C:\Users\kEecfMwgj\Documents\8fWkzgyyD0qQR-ID9Sm.pptx.vvyu	70.42 KB	be45bac46879081c7afb33f2f5c90770939957ba601af685bf663d850217ec07f	✔
C:\Users\kEecfMwgj\Desktop\xS0O4.gif.vvyu	83.40 KB	80c88bb2f5c3d49a4f754c2e2471451504868e5f23c60c8e782980a0306effd8	✔
C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\gGYFMJx.swf.vvyu	43.09 KB	315d46a8406df2b126d0a925730ccbda75fe313bf0f3291811f3decaee300256	✔
C:\Users\kEecfMwgj\Desktop\zH9UWAN96jNNa9sjtX.bmp.vvyu	39.25 KB	346b409747a3d82667183088c0a2f145b72c1d5cfaf2d72d9ac8dc794c7f7b81	✔
c:\users\keecfmwgj\pictures\nlxnihq5_.png.vvyu	18.53 KB	86568eb03625bf0236817fa33d7b03bbb2e8c44dbdc7dffe5560dcb0c0a5cb24	✔
C:\Users\kEecfMwgj\Documents\rk2x.xlsx.vvyu	43.23 KB	24c05619b630f28f12c87e4d9843aef657fd61b81f91758c6c1245dbbdbdbf1c	✔
c:\users\keecfmwgj\documents\1hq_0ry\rnf1.rtf.vvyu	81.25 KB	1c3c0c1b1667a2b00da09a64fcc59cf715b9c242a5ea561c0bcd629eed3f5597	✔
c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\t12gfq_xaghox.ppt.vvyu	82.35 KB	414ddcc7d1187fed4c15fa90426b8afd683010f13e2c938f2e0330695bc71d35	✔
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\k2soyi-o5lsts d_n6rv.mp3.vvyu	78.27 KB	f1c9ece86254680d6109efc6280c729211bbea238e984b9217e0e33090cb822c	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\l001k\7rzoymi.xlsx.vvyu	22.04 KB	c2d483a4b78084261b8742b36e7c1ea7a62143f3f2322cce0ca74d61fd624752	✔
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\hFSYfNeYKfRlr3.mp3.vvyu	5.58 KB	60b7eaad3623421350f1581886ce65d178e1b895738598f91457d1591e193e8b	✔
C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Money.url.vvyu	467 bytes	b9fbaa65c6a0d3994e90c940fe086481d7da8909fb6bbc6b1a58ae2e60a09a2c	✔
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\7HsBaAEuFJOdKC\QjjqmBh2.wav.vvyu	88.31 KB	87dfadbb0c2c409d1ef1cd489b227610b4ec91ff789a6154078edef78f273dd5	✔
C:\Users\kEecfMwgj\Pictures\mqT6p7TH.png.vvyu	87.85 KB	cf11404057c407c2c3b5179ed323a96548549e8143eb07df327f045d01fba008	✔
C:\Users\kEecfMwgj\Pictures\HGiMBm 8T.bmp.vvyu	69.71 KB	bab42298d101a7b91e951f7bb0f6e90309fe6a514bb77241a9f41dba61d837cb	✔
C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\l001k\uVwtXkawlnc12.xlsx.vvyu	72.26 KB	5a77b306c9f507e4e88a27619a545f75156c30062807701630e568bc097bcc0e	✔
c:\users\keecfmwgj\pictures\k5e8ye4arc.gif.vvyu	41.30 KB	9d66ce261d0c5c18b2320d0b906fa27256a354d635059d02c62ca6c2b8c41cbd	✔
c:\users\keecfmwgj\music\1nge1tjhlu2ewpqe6.mp3.vvyu	9.90 KB	7963341fdc0e3fcb3e6136b2998c8535df58d0f539c8ac4d090b336eb1cd2403	✔
c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\nsm8w\mlbm.mp3.vvyu	25.37 KB	9d48213eed380f1d8717d0c883c7bec8bcd29012e588915194eb7088c6ffe4b5	✔
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\fecjkv.wav.vvyu	27.57 KB	4d2704f66fc91419cd8fd6013f964a9a2cd97b4a2629509a387d3815813b50b4	✔
c:\users\keecfmwgj\documents\1hq_0ry\zcrjc.csv.vvyu	87.14 KB	b440e9d4cb0f1d0b8c10c6145e0cc83d4c6557afbee49b46d8619d36d812305c	✔
C:\Users\kEecfMwgj\Pictures\N4KCoH3c2EBd4qZz.png.vvyu	42.57 KB	05d7c12af5d750963a87932144b5c35fb003733df547bba9ad53e59ca7e16eea	✔
C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\2fyWk_nuEZSWQOD.pdf.vvyu	31.23 KB	9d67618a0fa1a9f76e979275f205e927a44d2be3d1b9fc667ffbb2df06ff4d3d	✔
c:\users\keecfmwgj\videos\lyqkedl\bp_f\b77bp16rhy\vjumbjdocin1vnfnita.flv.vvyu	22.21 KB	81cba6f19c9d1fae7d35c1f29e47a1d6e730730a851c88a673ab1c467d7365a1	✔
c:\users\keecfmwgj\videos\lyqkedl\bp_f\b77bp16rhy\ffjifehmkb7gr\dz-kv.mkv.vvyu	4.91 KB	a08376a2d4249e885ec5bcbb1869d96aa1dafaa808bf1938433e055bb8c153bc	✔
C:\Users\kEecfMwgj\Desktop\Ua5kWRFjT8eGw64gW.mp4.vvyu	64.09 KB	7bd7f001fdc77ab7c08c292648de3889b8a8e0ec5b77f7308a5dffcd93514675	✔
C:\Users\kEecfMwgj\Desktop\4pvmPeV-Pn.flv.vvyu	46.91 KB	15c39e5de6cabcb82afee8652518f76c0c3be1bbff33675ad2899adb287e42d0	✔
c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\l001k\tlk8.ots.vvyu	50.38 KB	8e3e0ca2ba907929ac6f3f13c66c5b2f4eedaa47a0d6b40117bdde74d8ebccf3	✔
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\zhLBFDnBxClJdg.wav.vvyu	22.02 KB	a4ea4dff400fcf548fb6f230e197b4a90d4d88cbb2b66f55da90815f2c2f780d	✔
c:\users\keecfmwgj\desktop\g5cw5jpl.mkv.vvyu	70.62 KB	56ef700f6a9c12ee8333e0d909c9a4ca28d36d998e59e09d89951f9473073c07	✔
c:\users\keecfmwgj\videos\zaoit.avi.vvyu	45.70 KB	66f2edde5e76caa15aeedb2dc5abd59b7bc92b9fde12c0f22f1be96974dd7fde	✔
C:\Users\kEecfMwgj\Pictures\tQMmYT.png.vvyu	64.40 KB	f31ec2e930b09ec07e1d52f5fad69dc8ca8c9b607c09d28c06cebc1bb5d17552	✔
c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.vvyu	467 bytes	a2b73ce4298424df9687d7e5bbacebfa9cb3469c20239dd1accaf71f8d7387b2	✔
c:\users\keecfmwgj\desktop\ts9eh-mq2s2jrpdask\w3-dnej.docx.vvyu	75.22 KB	3061b4f97f1f2d09927e052c6d0b75756aa1e3b297986bcdb2a94b88ad1cb299	✔
C:\Users\kEecfMwgj\Pictures\L0X5uBCGS.jpg.vvyu	3.25 KB	d7370b32160b859288b809afbf1ab6621877102d80cc3f756092a474643c7006	✔
C:\Users\kEecfMwgj\Documents\1HQ_0Ry\fyo9G2M-VX0uEz.pptx.vvyu	96.40 KB	4c77905de8245b554bfa5d61b1661f770ae93ce61c532d8a5abbed1d87eec443	✔
c:\users\keecfmwgj\pictures\rykwux.png.vvyu	42.93 KB	4495daa5dee475ea2fda4d09e38299eaa521851b31c9f1aa070c718b5419c20e	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\documents\lbnq9x4z nerecwqi5cw.xlsx.vvyu	38.84 KB	5ad007662000238885cf5fcfbd576317f182eebff8cea28db168f4e6efe5c2f6	✔
c:\users\keecfmwgj\videos\jihul99r3n0.mp4.vvyu	34.13 KB	a9aca81d1fc8b30d9e40bf02e345a89d61b54e1a7e9f20a8e9c8975ea0d75f04	✔
C:\Users\kEecfMwgj\Desktop\ZRaPtwjBRWX3Lza6exVY.wav.vvyu	92.63 KB	b29d19232a6ca9af42fe07ae1c5d141b729aac0dbc71f88f31a931d96fa38596	✔
c:\users\keecfmwgj\desktop\o89yzaehg03nthchcn.wav.vvyu	32.16 KB	4daeeab369b95241d47fd41c2a726e5f81e585d78a7c7405d6f12142d2334e4d	✔
c:\users\keecfmwgj\videos\lyqkedl\yhy pbk4xcgins.flv.vvyu	64.34 KB	89fce05f69f7d379dbf24a1fabd5502f9cfde7947275e9302c3eac1b5e993492	✔
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\F59wFk.mp3.vvyu	28.41 KB	93c43ef67d47a1618d1978c24d5b4520e6594d9500e267be3a7e3b70a915d802	✔
c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\aczwje9qryq8jx.rtf.vvyu	57.54 KB	781ebf1ae5f6caab52c6d309922d88c0441396aa7842e7c02f5983cd5b252582	✔
c:\users\keecfmwgj\desktop\ut2y\cyxqypaxj5.mp3.vvyu	50.82 KB	e9fc08399f3f40aae47390f13ac522dc476c7c6e2643ad16d37707eda0c353c0	✔
C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\V9OdwraOWmDvfZs\lFFeDb7YF-O_1-.xlsx.vvyu	95.05 KB	4d76c0e3b295e01ebc020c97689a9c21774e9b6415a4584f708df36f8cc388de	✔
C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\B77bP16RhY\7vLuv6V2.swf.vvyu	42.15 KB	4e82dda9b501791a3ee1d7591f70b095bb1ada68e66df105d99c9442771ea806	✔
c:\users\keecfmwgj\desktop\dmps8r4its euqecouq3.bmp.vvyu	97.71 KB	98ab8608e9e426749b5c335da698c643b72d273641ca18d22c14afa103c58576	✔
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\uCoTL4ch-wEWMbF.m4a.vvyu	21.72 KB	dc7630c5ed5802935fc130f532275f8fa062f3828ca7547660fff2bc098d66d9	✔
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\ejhdcdvz_t.m4a.vvyu	31.19 KB	e44e48440e4fe95c19cafec2b114512317a189b10a5237099d55c93566537b26	✔
c:\users\keecfmwgj\desktop\ut2y\r5wn3p5jpommfls2s.wav.vvyu	88.63 KB	42340c34362b6e00021b8733eae9c5b6a427aa578b11875b27a6c0573bd74452	✔
C:\Users\kEecfMwgj\Documents\IC2B3nJ.docx.vvyu	38.59 KB	eca795417f1605fe2e8bc33c6f794c6f38f9aaf6b2930b574d0834dd761bb288	✔
C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\wnJQgJSzxWQZQ3T9b.gif.vvyu	38.23 KB	9bc1b075f13a6eefbe2855bb56af4bf35a3485fd898e99172f397f5c38a0551c	✔
c:\users\keecfmwgj\pictures\xxrgef8g_2lumbpgs.gif.vvyu	35.75 KB	21ecf43ab9d8c032541e39cf8e6a5d34ce857d9a8f0e1c2bf3fd3880ed71d6cb	✔
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\drvaf2.mp3.vvyu	1.71 KB	23f1244a184674fc6ba577d4293df7cb05502779409204c156a2df6a38f4926e	✔
c:\users\keecfmwgj\music\crz6i\5cx9jpbe2.wav.vvyu	44.76 KB	1f000e88a632b9352859f4f34f8a1a2a49d2b14b0516f7d1fc970a6b57e8bbea	✔
c:\users\keecfmwgj\pictures\0y4sxbvo2pcys9vij e.bmp.vvyu	98.36 KB	d5d511e25191e69dd9c6eab94a4f2dcf9b4056a90aa5c98e77074184cc03c923	✔
C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\l001k\T8Z573.ods.vvyu	93.34 KB	fd5fd0e6fd63b6aa32b8dfb290e07c538c3e005c6e90a6bde649ccb832160f53	✔
c:\users\keecfmwgj\pictures\eofw5_iu17ime9.png.vvyu	6.58 KB	fe1a4a6e9502b4c5b017d3db2f3aa8a6513013ffe4a67effd64c2f1e940a2092	✔
C:\Users\kEecfMwgj\Desktop\6 RaZWC55WZRBx2uhb.mp3.vvyu	87.60 KB	78f2e26d9f59da162ffd6be46986854540f2a0a04604c6f957b0dc2f8de690c8	✔
C:\Users\kEecfMwgj\Desktop\5hLmZnA5PAqwTlGkZ.flv.vvyu	11.78 KB	d0ddc64e6ac4dc71d8ca3b89dba0cb5f42b74bcc9673edc3f1f06d050304c014	✔
c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\nsm8w\euc6yoilzsh1vn.m4a.vvyu	63.67 KB	2ec3aacb480a197b17eed73e58e409bef25316dad703ceda88b8188964a099ce	✔
c:\users\keecfmwgj\documents\w3wlo_n9evs7ldf.pptx.vvyu	70.12 KB	034902aa1a8c24dbf6e21594cc0fe266efe256c711fb9636a35051306532283e	✔
c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu	467 bytes	90534f04d692c6e29f8ab56223a6789551f227b0d7381e9a425e845360721ca9	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\desktop\2t_yf.swf.vvyu	85.72 KB	a95349496db8c5725752b75dad0902e583df02d903ceb765133cb2794980d2db	✔
c:\users\keecfmwgj\pictures\mu izhmdaedj6rosn.png.vvyu	97.18 KB	aa7a0930b04899f46fdfbe1b2d463e484d0dcaca1cb2bd40890b383ae2cac21b	✔
C:\Users\kEecfMwgj\Desktop\mqJX68.avi.vvyu	97.94 KB	e6084fc685902ce6cf4af09fded2e80e4f9fad1d6d11a599a191a55002911d60	✔
c:\users\keecfmwgj\documents\1hq_0ry\iz9jh_ltuq.csv.vvyu	55.50 KB	c2fbd6bd6b35e53e8d18214c63acf9c8c3d838a34d600402e8c8f0c10307a9de	✔
C:\Users\kEecfMwgj\Videos\NcfXF2sB4dY.avi.vvyu	24.76 KB	30ad342b0d3f58e95a4d3d409ddebe2dc06669e6742c41d9d790ef32a0735284	✔
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\7HsBaAEuFJOdKC\obudae3fGOyKU IH.wav.vvyu	36.07 KB	1e68745c76095a0fd861ff270d22995d9964c5e3cd0a1b7f18d80a79bc3ce788	✔
c:\users\keecfmwgj\favorites\msn websites\msn sports.url.vvyu	467 bytes	75a560117791b920bd584a2860237c4c71b59e588e552dffc9244594eb07abcc	✔
c:\users\keecfmwgj\music\kdubnqjx5rovkqg1.m4a.vvyu	18.04 KB	ebe3f82d70e845e358b28e1af53b4d9ae41bb1152ae11bdc1c83dfdb402de532	✔
C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Gallery.url.vvyu	467 bytes	d9053b9f534e595f39ff89c796be0eaa3fe3930c9cca6445ed9d322ef2526ddd	✔
c:\users\keecfmwgj\favorites\microsoft websites\microsoft at home.url.vvyu	467 bytes	8c35fcf877278ee9251189151ad6f9db320333df56e06316c3e59b73d7ab8908	✔
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\1cab2.wav.vvyu	2.78 KB	f9749d827540796505489df1fb81140ec4c700e7ef7c729691f7168be4aed486	✔
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\ey662pveezsfar.wav.vvyu	46.60 KB	d7b849a0fc00b4261e048266027b44910223697a0195b71efe4fc31d961d2015	✔
C:\Users\kEecfMwgj\Desktop\MF-vsO.flv.vvyu	49.55 KB	9fef8af4468bb66e5a824651afe895f76f8a47695798c037361aeefe287aa09b	✔
c:\users\keecfmwgj\documents\outlook files\franc@gdllo.de.pst.vvyu	265.33 KB	2d20245c580a4f4c5ec07426cf6e3aa7732f3fd34f79cfa2b8e65e58297724d4	✔
C:\Users\kEecfMwgj\Pictures\yD7UYZJhgi.gif.vvyu	7.78 KB	a8d9e6c15f3c5bb635c528bf95d42ccb4ee179a7cef6a394cc8c8893f1d47770	✔
C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\OtZx7BdbiT9_sR8ibK.avi.vvyu	83.80 KB	a199362bda115460d72530e50a50a320a197dd5ddddda1afd51ba2639b9b3a5ba	✔
c:\users\keecfmwgj\documents\4oox2qc.pptx.vvyu	30.51 KB	8393ff81181fb9d5f7fa1754ed57b28388b99ce2375e4632b9caf21d3118dca8	✔
C:\Users\kEecfMwgj\Pictures\-tYby54-.gif.vvyu	92.07 KB	c67c77c519c9a91c1e8c93eb7f896557ce7e6a9e6b219351f084299789b2603f	✔
c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\d-t7fxif.pps.vvyu	22.24 KB	1c65f024a7677e9d9da933733772dc03c676a48711f797c922f5822b2b215780	✔
c:\users\keecfmwgj\videos\lyqkedl\gei2kwsrqiau.flv.vvyu	80.40 KB	191e7ce5ce201dd4dfb8e03b9c2b63d099fd1f9eb3ab134e62e2ede2f5595bd7	✔
c:\users\keecfmwgj\desktop\ut2y\1vtklu46j9zljyf.png.vvyu	62.56 KB	281b0652d548bde02a86df12e55e058774844488f722cc273ae41ff1fe2888df	✔
C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE Add-on site.url.vvyu	467 bytes	cb7f769454a95fbaf0163b9919bd6e348cb7670d643f63e21cf3999ba135a987	✔
c:\users\keecfmwgj\favorites\msn websites\msn autos.url.vvyu	467 bytes	6daa653c405613fc514650dee4f060f982f4f0fc90615a168d2ca9c42e988b61	✔
C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\B77bP16RhY\FfJifEhMKb7gr\HrxywvF.avi.vvyu	76.10 KB	7c58b35a8b0180650ed29949f1e963a7a5bc4d9d506968ad46eb4f9b59802cdb	✔
C:\Users\kEecfMwgj\Videos\lYQkedL\Fz-XgP8.avi.vvyu	43.24 KB	0d47df071f0b044846c0f688f324f05f7dc963bcb5ff3f76698f6acfd123ce21	✔
c:\users\keecfmwgj\desktop\ts9eh-mq2s2jrpdask\cvizy.png.vvyu	82.61 KB	a7ab0369cac2b788cfb54811208bfdd026316e61bc121b2fe6c33512b03d9ab4	✔
c:\users\keecfmwgj\videos\lyqkedl\bp_f\brfr.flv.vvyu	34.68 KB	baf222d787a76b3be1bea1b26d45ff15068f51cadcce4d5b45d7f0824bb5b5f8	✔
c:\users\keecfmwgj\appdata\locallow\microsoft\internet explorer\services\search_{0633ee93-d776-472f-a0ff-e1416b8b2e3a}.ico.vvyu	4.51 KB	ddacddf1ba38f2f1dadbb1ab59c37beb05c7069986d65f88921abbf9d16e5d1a	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\qkkp5il.wav.vvyu	13.95 KB	e39e4127137cc23e79f8bdabd90cb8396706c4e5d752f1a8b4a10006a23be07e	✔
c:\users\keecfmwgj\favorites\msn websites\msn.url.vvyu	467 bytes	b68ef4e01a9f8d0fe911bae312f489601a6a8f428f466cd0897b57b13c6da961	✔
c:\users\keecfmwgj\videos\lyqkedl\bp_f\b77bp16rhy\runduyt-pl209.swf.vvyu	97.37 KB	5d63fe9eca6bef019167bfec990797b45343bd0cbcc8eed1ef65a953cd9ee758	✔
c:\users\keecfmwgj\desktop\zd_hryrh_.m4a.vvyu	87.22 KB	3ee142baa66842107042553de76b1273547928d1a2e78411e2f87b3523f2b50e	✔
C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\e07kj.mp4.vvyu	37.86 KB	f03d6a13ea8fb00a47d526914761e89e42adbbd7cf794f82d8abe2898eed4a10	✔
C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Work.url.vvyu	467 bytes	d3e080116744d8025ad5ccc157349d4a3bc6c1b324d5a8031a6d38af8da2d13f	✔
C:\Users\kEecfMwgj\Pictures\qJwilfjoa.gif.vvyu	58.23 KB	539ec9da48c419ed465b3530be6c2192332d9fdfd3b01fc38c312a1778546e69	✔
c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\lw0ngqzthjhumamurh.mp3.vvyu	59.28 KB	c3ae33be13409ef5b5ce67c9cbbf9de6f189d10b154a9de628f7e88e7419b2c7	✔
c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\nsm8w\19w3oa-fxhny9lnmwhz.wav.vvyu	30.75 KB	4d2d54f8fd42db62499a8b28816cf382e7bc4b3544899a772e15acf58f66636b	✔
c:\users\keecfmwgj\favorites\windows live\get windows live.url.vvyu	467 bytes	68fcf3c8d44a750d285802a7c1be7057475f0ef4b0c29126a0ef389b510c4cc8	✔
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\b30igw41l3y9sjklhkpi.m4a.vvyu	10.70 KB	4cebc6357d356c334529d0566800df068fc035cd0891d2a63eb933dea9e7a7c8	✔
c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\muombxez-zs.odp.vvyu	62.71 KB	57856fb634695dfec249d79ac355954b18374d3bcece90ac6f07cfb64dbdfdef	✔
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\aVzqZXq4M-FZ\JG5i8r.m4a.vvyu	23.52 KB	d6af322ac9a0e4b7d47c606daea9f9684db2fcc1f0ee211c78c7f9957cce8e35	✔
c:\users\keecfmwgj\pictures\a3tvenkrzs u0e2m24js.png.vvyu	30.97 KB	dbf4439be833e8f9574768dae64f2981f51b77937f58bd18c7632fb43d4673ba	✔
c:\users\keecfmwgj\favorites\windows live\windows live mail.url.vvyu	467 bytes	b0c7d628714cfa074d6c993cbfe5c58eae5ae5ae7719b6640ce4d9bd1645d210	✔
C:\Users\kEecfMwgj\Videos\A08G XtmrDvZD.avi.vvyu	58.68 KB	c9c55945af727ead543c3e9ee5767b4c2f37197e3ab105ee8a6c55da21d80f12	✔
C:\Users\kEecfMwgj\Pictures\Ql6f.bmp.vvyu	30.12 KB	63bd24e895ef1aaefd5214b38b6bbf36c482b7bc4e6ff7a3eb048610c297a4b5	✔
c:\users\keecfmwgj\desktop\ut2y\8ow5.avi.vvyu	8.80 KB	3440c6b66392957fc8ff5f10767cb59ad5767d7e53ffd4697f203e250a72137f	✔

Reduced dataset

Host Behavior

Type	Count
System	289
Module	185
File	2465
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
80f6e86d1ca2934b6a512ae8760b162d24f5dcfcbdee490a932962082ce03fcd	c:\users\keecfmwgj\videos\lyqkedl\bp_f\d6ztvjfwwa.flv.vvyu, C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\d6ztVjfWWA.flv.vvyu	Dropped File	40.42 KB	video/x-flv	Access, Create, Write	MALICIOUS
43e6f84df18e0ecdef1e894dfe7560276ecb6129467da392f24177d56afbfd6c	C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\lS2B.jpg.vvyu, c:\users\keecfmwgj\desktop\ts9eh-mq2s2jrpdask\is2b.jpg.vvyu	Dropped File	89.48 KB	image/jpeg	Access, Create, Write	MALICIOUS
9f5fec9b0eaae4e0cbced0783399e16fc98c2aa689cf05d568a1ac26e0ee3c1a	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
3e1c9e83abf0a080232a867f889ace95eca79f14f8110117cb9dfa9aa6f21b0b	c:\users\keecfmwgj\music\u2xcl6fk4p\buwavzcuhtmrml.wav.vvyu, C:\Users\kEecfMwgj\Music\U2xcL6FK4p\BUWavzCUHTMRML.wav.vvyu	Dropped File	88.41 KB	application/octet-stream	Access, Create, Write	MALICIOUS
cec8599bb3470fd3dfc69b4e7788fd0065cd74809ed0cf5c28633b9038b0153a	c:\users\keecfmwgj\videos\lyqkedl\bp_f\wuud9p77x.mkv.vvyu, C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\wuUd9p77x.mkv.vvyu	Dropped File	12.31 KB	application/octet-stream	Access, Create, Write	MALICIOUS
923b159396d0b3de831f96c5ef3edf16e36b96c4e5d6ad2fa227b520df3f7668	C:\Users\kEecfMwgj\Desktop\EbPUXvbqaj ZxnAB.png.vvyu, c:\users\keecfmwgj\desktop\ebpuxvbq aj zxnab.png.vvyu	Dropped File	100.12 KB	application/octet-stream	Access, Create, Write	MALICIOUS
6bbce99cc1c931da081a05ec5cd68d9d5f5cedbaae4987e40a5e209ef9c602ab	c:\users\keecfmwgj\documents\qzaaruieowyp 0mvbzk.docx.vvyu, C:\Users\kEecfMwgj\Documents\qZaArUiEowYp 0mvbzK.docx.vvyu	Dropped File	34.86 KB	application/zip	Access, Create, Write	MALICIOUS
48473a2c6fe8f1db5f1b7f17c2525ad0a2ed21cda728921ea5d004e4a9a18a60	C:\Users\kEecfMwgj\Desktop\YG8k.jpg.vvyu, c:\users\keecfmwgj\desktop\yg8k.jpg.vvyu	Dropped File	53.70 KB	image/jpeg	Access, Create, Write	MALICIOUS
df1773702517ab25c9af0526d167112b73c9e4441e831ebb360b16c31d841e7c	c:\users\keecfmwgj\videos\lyqkedl\mrt4.mkv.vvyu, C:\Users\kEecfMwgj\Videos\lYQkedL\mRT4.mkv.vvyu	Dropped File	3.25 KB	application/octet-stream	Access, Create, Write	MALICIOUS
1aefac166c4e5df5ec4aba5fcf262c928aa10ee5f9a35523ba534d8807d79dbc	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\t1mqysmsezilmfb.m4a.vvyu, C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\7HsBaAEuFJOdKC\t1mqYSMSeZiLMfb.m4a.vvyu	Dropped File	42.76 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b63f6cd8684172a722603dc2bba4279ee6b14b442b90fe8ea3191a33754b6aae	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
822141d70f49354ddef8f4cc778705f3732373e396ecd9a3c5a382e22e7fdd8a	C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\dtcpak5wO kdkqu Ph.mkv.vvyu, c:\users\keecfmwgj\videos\lyqkedl\bp_f\dtcpak5wo kdkqu ph.mkv.vvyu	Dropped File	89.11 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3f1fe512a9524421cede2d93688ff7d5c5e973bac88607c6ff0967e1e6d37d25	c:\users\keecfmwgj\documents\7bevwhnu_fkrc\jxd7petv2jcni.xls.vvyu, C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\jXD7PETV2JcNi.xls.vvyu	Dropped File	96.12 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
29af13d8fce607b0e048242f9746710bc9794d1efa02a79565e77290cd415235	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\cv8-veyoh.wav.vvyu, C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\Cv8-VEYOH.wav.vvyu	Dropped File	13.97 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ff31f10671bf946d5c7311e865cdb4fc97bf826f9d91d7b96c0c7b36124c561f	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
940212712bada8893b8e9f842d35b90d67318a16bbb0bb187c8e65ea3bff3884	C:\Users\kEecfMwgj\Music\CrZ6i\jjLwLGu.m4a.vvyu, c:\users\keecfmwgj\music\crz6i\jjlwlgu.m4a.vvyu	Dropped File	26.93 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797	C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d9...ad041ffca4c89d97797.exe.vvyu, C:\Users\kEecfMwgj\Desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe.vvyu	Sample File	857.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Read, Write	MALICIOUS
0ff70edc3ea76b4c09694d751d7dafbba70167807aa5bc34d7e700310433eb0c	c:\users\keecfmwgj\pictures\hqdktuf4etm1.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\HqDKtUf4Etm1.bmp.vvyu	Dropped File	57.67 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b26e580c73f9b84a0555ebac4a2e230e63b6df3f32bfbf7b24d2be241356cb37	c:\users\keecfmwgj\desktop\5-xamft.jpg.vvyu, C:\Users\kEecfMwgj\Desktop\5-XAMfT.jpg.vvyu	Dropped File	29.58 KB	image/jpeg	Access, Create, Write	MALICIOUS
cbe07aa4abe72a1ee68bfef166f063062f00ac25fc7804e33ba4987cd2dba562	c:\users\keecfmwgj\documents\xquj.docx.vvyu, C:\Users\kEecfMwgj\Documents\Xquj.docx.vvyu	Dropped File	79.17 KB	application/zip	Access, Create, Write	MALICIOUS
ed8a80252cb0d0438c2e55e9c3db6120f59ec58272a3b91fabcd6f292343fa95	C:\Users\kEecfMwgj\Desktop\VDue0.odt.vvyu, c:\users\keecfmwgj\desktop\vdue0.odt.vvyu	Dropped File	60.23 KB	application/zip	Access, Create, Write	MALICIOUS
1a1e5d46b92b044661e09ac2a6fa12c1f41ab369349516b0212169a1aaa78401	C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\WzOtFShww.rtf.vvyu, c:\users\keecfmwgj\documents\5v0uyr-um9wck\wzotfshww.rtf.vvyu	Dropped File	55.44 KB	text/rtf	Access, Create, Write	MALICIOUS
41f4295b5a673f97e71da22437fd60b09cf62bc9b48dd220305baf69d2ea6fb4	c:\users\keecfmwgj\documents\otrrqivqej6bkbcciq.docx.vvyu, C:\Users\kEecfMwgj\Documents\OtRRqiVqej6bkbcciq.docx.vvyu	Dropped File	96.58 KB	application/zip	Access, Create, Write	MALICIOUS
65e5572556e34a9e3f38fb1c81625e280b5f31004b54531d72e1d7cea4b7841f	C:\Users\kEecfMwgj\Pictures\70uMB.gif.vvyu, c:\users\keecfmwgj\pictures\70umb.gif.vvyu	Dropped File	64.57 KB	image/gif	Access, Create, Write	MALICIOUS
90c137f810534e7e869ff654413c239147340 36b6d1f8f08069d96665d892e73	c:\users\keecfmwgj\videos\lyqkedl\izhxbinth.mp4.vvyu, C:\Users\kEecfMwgj\Videos\lYQkedL\izhxBinth.mp4.vvyu	Dropped File	76.63 KB	application/octet-stream	Access, Create, Write	MALICIOUS
f35335deffacec40ca5679f4966b36e1b11ddca88faacd44f5c446ff5dc7c596	C:\Users\kEecfMwgj\Documents\h63-85V.xlsx.vvyu, c:\users\keecfmwgj\documents\h63-85v.xlsx.vvyu	Dropped File	82.50 KB	application/zip	Access, Create, Write	MALICIOUS
a5282142cd953ba0ebabec93602fded6a9498cc5fbc985fade835d9f2aa05111	c:\users\keecfmwgj\videos\lyqkedl\bp_f\pc3yf9pj6umpbxequ7nk.swf.vvyu, C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\Pc3Yf9pJ6uMPbXeQu7NK.swf.vvyu	Dropped File	55.83 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
00fce946bb55202cf2125074ef23e13dc3ee501813fcbe8323546dbcb0acad44	c:\users\keecfmwgj\documents\qs-f1e.pptx.vvyu, C:\Users\kEecfMwgj\Documents\QS-F1E.pptx.vvyu	Dropped File	27.94 KB	application/zip	Access, Create, Write	MALICIOUS
c9ac969f8ef55ccba82fee2c97562f6ae36f683b8287bf662b406f79cb756df5	C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\naFofVP436Y9.odp.vvyu, c:\users\keecfmwgj\documents\7bevwhnu_fkrc\nafofvp436y9.odp.vvyu	Dropped File	24.74 KB	application/zip	Access, Create, Write	MALICIOUS
dc5327569cffa667542bd34a5c3c031a4a8c81e66cf3506b81251616a5a45967	C:\Users\kEecfMwgj\Documents\1HQ_0Ry\AoEQk-B.ppt.vvyu, c:\users\keecfmwgj\documents\1hq_0ry\aoeqk-b.ppt.vvyu	Dropped File	34.69 KB	application/octet-stream	Access, Create, Write	MALICIOUS
9a5b53aa58ba33a3e0f1be80d0508a027e3d86e63d064effeac25a2f797cecce	C:\Users\kEecfMwgj\Pictures\c34Mo1t-KwX2Fe92.png.vvyu, c:\users\keecfmwgj\pictures\c34mo1t-kwx2fe92.png.vvyu	Dropped File	16.55 KB	application/octet-stream	Access, Create, Write	MALICIOUS
601f88645c83d66d9762058a24438b3565fda105dd7be552aad88a051d133eb6	C:\Users\kEecfMwgj\Documents\s6KVYjgw4EOpy.xlsx.vvyu, c:\users\keecfmwgj\documents\s6kvyjgw4eopy.xlsx.vvyu	Dropped File	98.84 KB	application/zip	Access, Create, Write	MALICIOUS
bf56f0783534085f91f824bdda715050774d2c25e2ddc337cd0369722c20ab81	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\pSXJ.mp3.vvyu, c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\psxj.mp3.vvyu	Dropped File	21.78 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b2c6c44ae7af20c7432eb6ee4c42b65517ddc70903ca30af7ba8d0c26e9928a4	C:\Users\kEecfMwgj\Pictures\uX_9CrHqo8CggdcB4.jpg.vvyu, c:\users\keecfmwgj\pictures\ux_9crhqo8cggdcb4.jpg.vvyu	Dropped File	55.18 KB	image/jpeg	Access, Create, Write	MALICIOUS
43cfde9b466dc8601ff358294f54048e31b43241ed0f1e29251adc4c5e5bedca	C:\Users\kEecfMwgj\Videos\IYQkedL\OREWDZex5CeUn06c UN.flv.vvyu, c:\users\keecfmwgj\videos\iyqkedl\orewdzex5ceun06c un.flv.vvyu	Dropped File	48.37 KB	video/x-flv	Access, Create, Write	MALICIOUS
12b4774a9c1dc9a946051ce7065ad1815faf2ba1e32dc11f1913ea93a22f4605	c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\002z8yb-4iip.docx.vvyu, C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\VA7_pJeF68Oc_g\002Z8Yb-4li p.docx.vvyu	Dropped File	86.87 KB	application/zip	Access, Create, Write	MALICIOUS
4ec6cdffc1c9950b7287b891576887bea02e6e11fecf8f9c85c3cdef8cd54fcc	C:\Users\kEecfMwgj\Pictures\Kt1gN2Zu4cLe_ffn1E.png.vvyu, c:\users\keecfmwgj\pictures\kt1gn2zu4cle_ffn1e.png.vvyu	Dropped File	54.48 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ffd497fc2208b791d010cc993adad9e829b23004c55aef6353f7d57c762c78de	c:\users\keecfmwgj\documents\1hq_0ry\jn5w8pue5cpjcmbtd8.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\1HQ_0Ry\jn5W8pUe5CpJcMBtD8.xlsx.vvyu	Dropped File	84.87 KB	application/zip	Access, Create, Write	MALICIOUS
acf445c072e13233bf0abb64938e289d6dd0829fe140a0418a4fde98ccf909a6	C:\Users\kEecfMwgj\Pictures\qUrDOWbjU_xfUkCK.png.vvyu, c:\users\keecfmwgj\pictures\qurdowbju_xfukck.png.vvyu	Dropped File	99.98 KB	application/octet-stream	Access, Create, Write	MALICIOUS
392c7a25b70dd2343cd3028afc311e75e8baa711ec2529bd720d64d055e35895	C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\MmtudzmA8-1ZtsXh1iI.gif.vvyu, c:\users\keecfmwgj\desktop\ts9eh-mq2s2jrpdask\mmtudzma8-1ztsxh1ii.gif.vvyu	Dropped File	61.93 KB	image/gif	Access, Create, Write	MALICIOUS
be45bac46879081c7afb33f2f5c9077093957ba601af685bf663d850217ec07f	C:\Users\kEecfMwgj\Documents\8fWkzgyyD0qQR-ID9Sm.pptx.vvyu, c:\users\keecfmwgj\documents\8fwkzgyyd0qqr-id9sm.pptx.vvyu	Dropped File	70.42 KB	application/zip	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
80c88bb2f5c3d49a4f754c2e2471451504868e5f23c60c8e782980a0306effd8	C:\Users\kEecfMwgj\Desktop\xS0O4.gif.vvyu, c:\users\keecfmwgj\desktop\xs0o4.gif.vvyu	Dropped File	83.40 KB	image/gif	Access, Create, Write	MALICIOUS
315d46a8406df2b126d0a925730ccbda75fe313bf0f3291811f3decaee300256	C:\Users\kEecfMwgj\Videos\lYQkedL\bp_fgGYFMJx.swf.vvyu, c:\users\keecfmwgj\videos\lyqkedl\bp_f\ggyfmjx.swf.vvyu	Dropped File	43.09 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
346b409747a3d82667183088c0a2f145b72c1d5cfaf2d72d9ac8dc794c7f7b81	C:\Users\kEecfMwgj\Desktop\zH9UWAN96jNNa9sjtX.bmp.vvyu, c:\users\keecfmwgj\desktop\zh9uwan96jnna9sjtx.bmp.vvyu	Dropped File	39.25 KB	application/octet-stream	Access, Create, Write	MALICIOUS
86568eb03625bf0236817fa33d7b03bbb2e8c44dbdc7dffe5560dcb0c0a5cb24	c:\users\keecfmwgj\pictures\nlxnihq5_.png.vvyu, C:\Users\kEecfMwgj\Pictures\nLXNihQ5_.png.vvyu	Dropped File	18.53 KB	application/octet-stream	Access, Create, Write	MALICIOUS
24c05619b630f28f12c87e4d9843aef657fd61b81f91758c6c1245dbbdbdbf1c	C:\Users\kEecfMwgj\Documents\rk2x.xlsx.vvyu, c:\users\keecfmwgj\documents\rk2x.xlsx.vvyu	Dropped File	43.23 KB	application/zip	Access, Create, Write	MALICIOUS
1c3c0c1b1667a2b00da09a64fcc59cf715b9c242a5ea561c0bcd629eed3f5597	c:\users\keecfmwgj\documents\1hq_0ry\rnf1.rtf.vvyu, C:\Users\kEecfMwgj\Documents\1HQ_0Ry\rnf1.rtf.vvyu	Dropped File	81.25 KB	text/rtf	Access, Create, Write	MALICIOUS
414ddcc7d1187fed4c15fa90426b8afd683010f13e2c938f2e0330695bc71d35	c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\t12gfq_xaghox.ppt.vvyu, C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\T12gFQ_XAGHOx.ppt.vvyu	Dropped File	82.35 KB	application/octet-stream	Access, Create, Write	MALICIOUS
f1c9ece86254680d6109efc6280c729211bbea238e984b9217e0e33090cb822c	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\k2soyi-o5lsts d_n6rv.mp3.vvyu, C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\aVzqZXq4M-FZ\k2SOyi-O5LsTs D_n6rv.mp3.vvyu	Dropped File	78.27 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c2d483a4b78084261b8742b36e7c1ea7a62143f3f2322cce0ca74d61fd624752	c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\l001k\7rzoymi.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\l001k\7rZoyMi.xlsx.vvyu	Dropped File	22.04 KB	application/octet-stream	Access, Create, Write	MALICIOUS
60b7eaad3623421350f1581886ce65d178e1b8957385598f91457d1591e193e8b	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\hFSYfNeYKfRlr3.mp3.vvyu, c:\users\keecfmwgj\music\u2xcl6fk4p\hfsyfneykfrlr3.mp3.vvyu	Dropped File	5.58 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b9fbaa65c6a0d3994e90c940fe086481d7da8909fb6bbc6b1a58ae2e60a09a2c	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
87dfadbb0c2c409d1ef1cd489b227610b4ec91ff789a6154078edef78f273dd5	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\7HsBaAEuFJOdKC\QjjqmBh2.wav.vvyu, c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\qjjqmbh2.wav.vvyu	Dropped File	88.31 KB	application/octet-stream	Access, Create, Write	MALICIOUS
cf11404057c407c2c3b5179ed323a96548549e8143eb07df327f045d01fba008	C:\Users\kEecfMwgj\Pictures\mqT6p7TH.png.vvyu, c:\users\keecfmwgj\pictures\mqt6p7th.png.vvyu	Dropped File	87.85 KB	application/octet-stream	Access, Create, Write	MALICIOUS
bab42298d101a7b91e951f7bb0f6e90309fe6a514bb77241a9f41dba61d837cb	C:\Users\kEecfMwgj\Pictures\HGiMBm8T.bmp.vvyu, c:\users\keecfmwgj\pictures\hgimbm8t.bmp.vvyu	Dropped File	69.71 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5a77b306c9f507e4e88a27619a545f75156c30062807701630e568bc097bcc0e	C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\INuBJTWwJ5-Mjcy_1\l001k\uVwtXkawInc12.xlsx.vvyu, c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\l001k\uvwtxkawlnc12.xlsx.vvyu	Dropped File	72.26 KB	application/zip	Access, Create, Write	MALICIOUS
9d66ce261d0c5c18b2320d0b906fa27256a354d635059d02c62ca6c2b8c41cbd	c:\users\keecfmwgj\pictures\k5e8ye4arc.gif.vvyu, C:\Users\kEecfMwgj\Pictures\K5e8yE4arc.gif.vvyu	Dropped File	41.30 KB	image/gif	Access, Create, Write	MALICIOUS
7963341fdc0e3fcb3e6136b2998c8535df58d0f539c8ac4d090b336eb1cd2403	c:\users\keecfmwgj\music\1nge1tjhlu2ewpqe6.mp3.vvyu, C:\Users\kEecfMwgj\Music\1ngE1TJHLu2EwPqE6.mp3.vvyu	Dropped File	9.90 KB	application/octet-stream	Access, Create, Write	MALICIOUS
9d48213eed380f1d8717d0c883c7bec8bcd29012e588915194eb7088c6ffe4b5	c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\nsm8w\m lbm.mp3.vvyu, C:\Users\kEecfMwgj\Music\CrZ6i\hyD8dEUbAR8o\NSm8w\M lbm.mp3.vvyu	Dropped File	25.37 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4d2704f66fc91419cd8fd6013f964a9a2cd97b4a2629509a387d3815813b50b4	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\fecjkv.wav.vvyu, C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\7HsBaAEuFJOdKC\feCJKv.wav.vvyu	Dropped File	27.57 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b440e9d4cb0f1d0b8c10c6145e0cc83d4c6557afbee49b46d8619d36d812305c	c:\users\keecfmwgj\documents\1hq_0ry\zcrjc.csv.vvyu, C:\Users\kEecfMwgj\Documents\1HQ_0Ry\zcrJc.csv.vvyu	Dropped File	87.14 KB	application/octet-stream	Access, Create, Write	MALICIOUS
05d7c12af5d750963a87932144b5c35fb003733df547bba9ad53e59ca7e16eea	C:\Users\kEecfMwgj\Pictures\N4KCoH3c2EBd4qZz.png.vvyu, c:\users\keecfmwgj\pictures\n4kcoh3c2ebd4qzz.png.vvyu	Dropped File	42.57 KB	application/octet-stream	Access, Create, Write	MALICIOUS
9d67618a0fa1a9f76e979275f205e927a44d2be3d1b9fc667ffbb2df06ff4d3d	C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\2fyWk_nuEZSWQOD.pdf.vvyu, c:\users\keecfmwgj\documents\5v0uyr-um9wck\2fywk_nuezswqod.pdf.vvyu	Dropped File	31.23 KB	application/pdf	Access, Create, Write	MALICIOUS
81cba6f19c9d1fae7d35c1f29e47a1d6e730730a851c88a673ab1c467d7365a1	c:\users\keecfmwgj\videos\lyqkedl\bp_f\b77bp16rhy\vjumbjdocin1vnfnita.flv.vvyu, C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\B77bP16RhY\vjumBJdOCiN1VnFnita.flv.vvyu	Dropped File	22.21 KB	video/x-flv	Access, Create, Write	MALICIOUS
a08376a2d4249e885ec5bcbb1869d96aa1dafaa808bf1938433e055bb8c153bc	c:\users\keecfmwgj\videos\lyqkedl\bp_f\b77bp16rhy\ffjifehmkb7gr\dz-kv.mkv.vvyu, C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\B77bP16RhY\FfJifEhMKb7gr\dz-KV.mkv.vvyu	Dropped File	4.91 KB	application/octet-stream	Access, Create, Write	MALICIOUS
7bd7f001fdc77ab7c08c292648de3889b8a8e0ec5b77f7308a5dffcd93514675	C:\Users\kEecfMwgj\Desktop\Ua5kWRFjT8eGw64gW.mp4.vvyu, c:\users\keecfmwgj\desktop\ua5kwrfjt8egw64gw.mp4.vvyu	Dropped File	64.09 KB	application/octet-stream	Access, Create, Write	MALICIOUS
15c39e5de6cabcb82afee8652518f76c0c3be1bbff33675ad2899adb287e42d0	C:\Users\kEecfMwgj\Desktop\4pvmPeV-Pn.flv.vvyu, c:\users\keecfmwgj\desktop\4pvmpev-pn.flv.vvyu	Dropped File	46.91 KB	video/x-flv	Access, Create, Write	MALICIOUS
8e3e0ca2ba907929ac6f3f13c66c5b2f4eedaa47a0d6b40117bdde74d8ebccf3	c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\l001k\tlk8.ots.vvyu, C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\INuBJTWwJ5-Mjcy_1\l001k\TLk8.ots.vvyu	Dropped File	50.38 KB	application/zip	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a4ea4dff400fcf548fb6f230e197b4a90d4d88cbb2b66f55da90815f2c2f780d	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\zhLBFDnBxCIJdg.wav.vvyu, c:\users\keecfmwgj\music\u2xcl6fk4p\zhlbfdnbxcijdg.wav.vvyu	Dropped File	22.02 KB	application/octet-stream	Access, Create, Write	MALICIOUS
56ef700f6a9c12ee8333e0d909c9a4ca28d36d998e59e09d89951f9473073c07	c:\users\keecfmwgj\desktop\g5cw5jpl.mkv.vvyu, C:\Users\kEecfMwgj\Desktop\G5cw5jPl.mkv.vvyu	Dropped File	70.62 KB	application/octet-stream	Access, Create, Write	MALICIOUS
66f2edde5e76caa15aeedb2dc5abd59b7bc92b9fde12c0f22f1be96974dd7fde	c:\users\keecfmwgj\videos\zaoit.avi.vvyu, C:\Users\kEecfMwgj\Videos\zaoit.avi.vvyu	Dropped File	45.70 KB	application/octet-stream	Access, Create, Write	MALICIOUS
f31ec2e930b09ec07e1d52f5fad69dc8ca8c9b607c09d28c06cebc1bb5d17552	C:\Users\kEecfMwgj\Pictures\tQMmYT.png.vvyu, c:\users\keecfmwgj\pictures\tqmmyt.png.vvyu	Dropped File	64.40 KB	application/octet-stream	Access, Create, Write	MALICIOUS
a2b73ce4298424df9687d7e5bbacebfa9cb3469c20239dd1accaf71f8d7387b2	c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.vvyu, C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE site on Microsoft.com.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
3061b4f97f1f2d09927e052c6d0b75756aa1e3b297986bcdb2a94b88ad1cb299	c:\users\keecfmwgj\desktop\ts9eh-mq2s2jrpdask\w3-dnej.docx.vvyu, C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\W3-dnEj.docx.vvyu	Dropped File	75.22 KB	application/zip	Access, Create, Write	MALICIOUS
d7370b32160b859288b809afbf1ab6621877102d80cc3f756092a474643c7006	C:\Users\kEecfMwgj\Pictures\L0X5uBCGS.jpg.vvyu, c:\users\keecfmwgj\pictures\l0x5ubcgs.jpg.vvyu	Dropped File	3.25 KB	image/jpeg	Access, Create, Write	MALICIOUS
4c77905de8245b554bfa5d61b1661f770ae93ce61c532d8a5abbed1d87eec443	C:\Users\kEecfMwgj\Documents\1HQ_0Ry\fyo9G2M-VX0uEz.pptx.vvyu, c:\users\keecfmwgj\documents\1hq_0ry\fyo9g2m-vx0uez.pptx.vvyu	Dropped File	96.40 KB	application/zip	Access, Create, Write	MALICIOUS
4495daa5dee475ea2fda4d09e38299eaa521851b31c9f1aa070c718b5419c20e	c:\users\keecfmwgj\pictures\rykwux.png.vvyu, C:\Users\kEecfMwgj\Pictures\RYkWux.png.vvyu	Dropped File	42.93 KB	application/octet-stream	Access, Create, Write	MALICIOUS
5ad007662000238885cf5fcfbd576317f182eebff8cea28db168f4e6efe5c2f6	c:\users\keecfmwgj\documents\lbnq9x4znerecwqi5cw.xlsx.vvyu, C:\Users\kEecfMwgj\Documents\LBNq9X4Z NErEcWqI5CW.xlsx.vvyu	Dropped File	38.84 KB	application/octet-stream	Access, Create, Write	MALICIOUS
a9aca81d1fc8b30d9e40bf02e345a89d61b54e1a7e9f20a8e9c8975ea0d75f04	c:\users\keecfmwgj\videos\jihul99r3n0.mp4.vvyu, C:\Users\kEecfMwgj\Videos\JiHUl99r3n0.mp4.vvyu	Dropped File	34.13 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b29d19232a6ca9af42fe07ae1c5d141b729aac0dbc71f88f31a931d96fa38596	C:\Users\kEecfMwgj\Desktop\ZRaPtwjBRWX3Lza6exVY.wav.vvyu, c:\users\keecfmwgj\desktop\zraptwjbrwx3lza6exvy.wav.vvyu	Dropped File	92.63 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4daeeab369b95241d47fd41c2a726e5f81e585d78a7c7405d6f12142d2334e4d	c:\users\keecfmwgj\desktop\o89yzaehg03nthchcn.wav.vvyu, C:\Users\kEecfMwgj\Desktop\o89YZaEHg03ntHchcn.wav.vvyu	Dropped File	32.16 KB	application/octet-stream	Access, Create, Write	MALICIOUS
89fce05f69f7d379dbf24a1fabd5502f9cfde7947275e9302c3eac1b5e993492	c:\users\keecfmwgj\videos\lyqkedl\yhypbk4xcgins.flv.vvyu, C:\Users\kEecfMwgj\Videos\lYQkedL\Yhy PBk4xCGiNS.flv.vvyu	Dropped File	64.34 KB	video/x-flv	Access, Create, Write	MALICIOUS
93c43ef67d47a1618d1978c24d5b4520e6594d9500e267be3a7e3b70a915d802	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\F59wFk.mp3.vvyu, c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\f59wfk.mp3.vvyu	Dropped File	28.41 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
781ebf1ae5f6caab52c6d309922d88c0441396aa7842e7c02f5983cd5b252582	c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\aczwje9qryq8jx.rtf.vvyu, C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\VA7_pJeF68Oc_g\AcZwJe9QrYQ8jX.rtf.vvyu	Dropped File	57.54 KB	text/rtf	Access, Create, Write	MALICIOUS
e9fc08399f3f40aae47390f13ac522dc476c7c6e2643ad16d37707eda0c353c0	c:\users\keecfmwgj\desktop\ut2y\cyxqypaxj5.mp3.vvyu, C:\Users\kEecfMwgj\Desktop\UT2y\CyxQypaXj5.mp3.vvyu	Dropped File	50.82 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4d76c0e3b295e01ebc020c97689a9c21774e9b6415a4584f708df36f8cc388de	C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\V9OdwraOWmDvfZs\lFFeDb7YF-O_1-.xlsx.vvyu, c:\users\keecfmwgj\documents\7bevwhnu_fkrc\v9odwraowmdvfzs\lffedb7yf-o_1-.xlsx.vvyu	Dropped File	95.05 KB	application/zip	Access, Create, Write	MALICIOUS
4e82dda9b501791a3ee1d7591f70b095bb1ada68e66df105d99c9442771ea806	C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\B77bP16RhY\7vLuv6V2.swf.vvyu, c:\users\keecfmwgj\videos\lyqkedl\bp_f\b77bp16rhy\7vluv6v2.swf.vvyu	Dropped File	42.15 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
98ab8608e9e426749b5c335da698c643b72d273641ca18d22c14afa103c58576	c:\users\keecfmwgj\desktop\dmps8r4itseuqecouq3.bmp.vvyu, C:\Users\kEecfMwgj\Desktop\DmPS8r4ltS EUqECOuQ3.bmp.vvyu	Dropped File	97.71 KB	application/octet-stream	Access, Create, Write	MALICIOUS
dc7630c5ed5802935fc130f532275f8fa062f3828ca7547660fff2bc098d66d9	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\uCoTL4ch-wEWMbF.m4a.vvyu, c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\ucotl4ch-wewmbf.m4a.vvyu	Dropped File	21.72 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e44e48440e4fe95c19cafec2b114512317a189b10a5237099d55c93566537b26	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\ejhdcdvz_t.m4a.vvyu, C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\7HsBaAEuFJOdKC\EjhDCDvZ_T.m4a.vvyu	Dropped File	31.19 KB	application/octet-stream	Access, Create, Write	MALICIOUS
42340c34362b6e00021b8733eae9c5b6a427aa578b11875b27a6c0573bd74452	c:\users\keecfmwgj\desktop\ut2y\r5wn3p5jpommfls2s.wav.vvyu, C:\Users\kEecfMwgj\Desktop\UT2y\R5WN3p5JPommfLS2S.wav.vvyu	Dropped File	88.63 KB	application/octet-stream	Access, Create, Write	MALICIOUS
eca795417f1605fe2e8bc33c6f794c6f38f9aaf6b2930b574d0834dd761bb288	C:\Users\kEecfMwgj\Documents\lC2B3nJ.docx.vvyu, c:\users\keecfmwgj\documents\lc2b3nj.docx.vvyu	Dropped File	38.59 KB	application/octet-stream	Access, Create, Write	MALICIOUS
9bc1b075f13a6eefbe2855bb56af4bf35a3485fd898e99172f397f5c38a0551c	C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\wnJQgJSzxWQZQ3T9b.gif.vvyu, c:\users\keecfmwgj\desktop\ts9eh-mq2s2jrpdask\wnjqgjszxwqzq3t9b.gif.vvyu	Dropped File	38.23 KB	image/gif	Access, Create, Write	MALICIOUS
21ecf43ab9d8c032541e39cf8e6a5d34ce857d9a8f0e1c2bf3fd3880ed71d6cb	c:\users\keecfmwgj\pictures\xxrgef8g_2lumbpgs.gif.vvyu, C:\Users\kEecfMwgj\Pictures\xxRGEF8g_2lUmBpGS.gif.vvyu	Dropped File	35.75 KB	image/gif	Access, Create, Write	MALICIOUS
23f1244a184674fc6ba577d4293df7cb05502779409204c156a2df6a38f4926e	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\drvaf2.mp3.vvyu, C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\7HsBaAEuFJOdKC\dRvaf2.mp3.vvyu	Dropped File	1.71 KB	application/octet-stream	Access, Create, Write	MALICIOUS
1f000e88a632b9352859f4f34f8a1a2a49d2b14b0516f7d1fc970a6b57e8bbea	c:\users\keecfmwgj\music\crz6i\5cx9jpbe2.wav.vvyu, C:\Users\kEecfMwgj\Music\CrZ6i\5Cx9jpbE2.wav.vvyu	Dropped File	44.76 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d5d511e25191e69dd9c6eab94a4f2dcf9b4056a90aa5c98e77074184cc03c923	c:\users\keecfmwgj\pictures\0y4sxbvo2pcys9vij e.bmp.vvyu, C:\Users\kEecfMwgj\Pictures\0y4sxbVO2pcYS9Vij E.bmp.vvyu	Dropped File	98.36 KB	application/octet-stream	Access, Create, Write	MALICIOUS
32c1d495707ffc4f883fbcc0df8dc33aebe870844766b6fc0402ada60b5f0ce9	c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\l1flc8eh2.pdf.vvyu, C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\VA7_pJeF68Oc_g\L1FLC8eh2.pdf.vvyu	Dropped File	99.27 KB	application/pdf	Access, Create, Write	SUSPICIOUS
633b7820a3ac11b46b9c858a7c760711458558899a1046544b18b5c67c020945	C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\oAPMaSkphuOK7d.pdf.vvyu, c:\users\keecfmwgj\documents\7bevwhnu_fkrc\oapmaskphuok7d.pdf.vvyu	Dropped File	87.07 KB	application/pdf	Access, Create, Write	SUSPICIOUS
eebca7272162ebbecea12410018a2e8db4d0742ad370291fddf9e40a5c1b8d11	C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\ktAJOVysWpTdu.pdf.vvyu, c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\ktajovyswptdu.pdf.vvyu	Dropped File	42.02 KB	application/pdf	Access, Create, Write	SUSPICIOUS
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
fdd0647b1117ee2aba7f5014e22642ba5b896ade4001d4f4651f6a4d9d25bc8c	-	Modified File	64.00 KB	application/octet-stream	-	CLEAN
fd5fd0e6fd63b6aa32b8dfb290e07c538c3e005c6e90a6bde649ccb832160f53	C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\l001k\T8Z573.ods.vvyu, c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\l001k\t8z573.ods.vvyu	Dropped File	93.34 KB	application/zip	Access, Create, Write	CLEAN
fe1a4a6e9502b4c5b017d3db2f3aa8a6513013ffe4a67effd64c2f1e940a2092	c:\users\keecfmwgj\pictures\eofw5_iu17ime9.png.vvyu, C:\Users\kEecfMwgj\Pictures\eofw5_iu17iME9.png.vvyu	Dropped File	6.58 KB	application/octet-stream	Access, Create, Write	CLEAN
78f2e26d9f59da162ffd6be46986854540f2a0a04604c6f957b0dc2f8de690c8	C:\Users\kEecfMwgj\Desktop\6RaZWC55WZRBx2uhb.mp3.vvyu, c:\users\keecfmwgj\desktop\6razwc55wzrbx2uhb.mp3.vvyu	Dropped File	87.60 KB	application/octet-stream	Access, Create, Write	CLEAN
d0ddc64e6ac4dc71d8ca3b89dba0cb5f42b74bcc9673edc3f1f06d050304c014	C:\Users\kEecfMwgj\Desktop\5hLmZnA5PAqwTlGkZ.flv.vvyu, c:\users\keecfmwgj\desktop\5hlmzna5paqwtlgkz.flv.vvyu	Dropped File	11.78 KB	video/x-flv	Access, Create, Write	CLEAN
2ec3aacb480a197b17eed73e58e409bef25316dad703ceda88b8188964a099ce	c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\nsm8w\euc6yoilzsh1vn.m4a.vvyu, C:\Users\kEecfMwgj\Music\CrZ6i\hyD8dEUbAR8o\NSm8w\EUC6yOIlZsH1VN.m4a.vvyu	Dropped File	63.67 KB	application/octet-stream	Access, Create, Write	CLEAN
034902aa1a8c24dbf6e21594cc0fe266efe256c711fb9636a35051306532283e	c:\users\keecfmwgj\documents\w3wlo_n9evs7ldf.pptx.vvyu, C:\Users\kEecfMwgj\Documents\w3wlO_N9Evs7ldf.pptx.vvyu	Dropped File	70.12 KB	application/zip	Access, Create, Write	CLEAN
90534f04d692c6e29f8ab56223a6789551f227b0d7381e9a425e845360721ca9	c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu, C:\Users\kEecfMwgj\Favorites\MSN Websites\MSNBC News.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a95349496db8c5725752b75dad0902e583df02d903ceb765133cb2794980d2db	c:\users\keecfmwgj\desktop\2t_yf.swf.vvyu, C:\Users\kEecfMwgj\Desktop\2T_YF.swf.vvyu	Dropped File	85.72 KB	application/x-shockwave-flash	Access, Create, Write	CLEAN
aa7a0930b04899f46fdfbe1b2d463e484d0dcaca1cb2bd40890b383ae2cac21b	c:\users\keecfmwgj\pictures\muizhmdaedj6rosn.png.vvyu, C:\Users\kEecfMwgj\Pictures\mUIZHMDaEDj6RoSN.png.vvyu	Dropped File	97.18 KB	application/octet-stream	Access, Create, Write	CLEAN
e6084fc685902ce6cf4af09fded2e80e4f9fad1d6d11a599a191a55002911d60	C:\Users\kEecfMwgj\Desktop\mqJX68.avi.vvyu, c:\users\keecfmwgj\desktop\mqjx68.avi.vvyu	Dropped File	97.94 KB	application/octet-stream	Access, Create, Write	CLEAN
c2fbd6bd6b35e53e8d18214c63acf9c8c3d838a34d600402e8c8f0c10307a9de	c:\users\keecfmwgj\documents\1hq_0ry\iz9jh_ltuq.csv.vvyu, C:\Users\kEecfMwgj\Documents\1HQ_0Ry\Iz9jH_LtuQ.csv.vvyu	Dropped File	55.50 KB	application/octet-stream	Access, Create, Write	CLEAN
30ad342b0d3f58e95a4d3d409ddebe2dc06669e6742c41d9d790ef32a0735284	C:\Users\kEecfMwgj\Videos\NcfXF2sB4dY.avi.vvyu, c:\users\keecfmwgj\videos\ncfxf2sb4dy.avi.vvyu	Dropped File	24.76 KB	application/octet-stream	Access, Create, Write	CLEAN
1e68745c76095a0fd861ff270d22995d9964c5e3cd0a1b7f18d80a79bc3ce788	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\7HsBaAEuFJODKC\obudae3fGOyKU IH.wav.vvyu, c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\obudae3fgoyku ih.wav.vvyu	Dropped File	36.07 KB	application/octet-stream	Access, Create, Write	CLEAN
75a560117791b920bd584a2860237c4c71b59e588e552dffc9244594eb07abcc	c:\users\keecfmwgj\favorites\msn websites\msn sports.url.vvyu, C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Sports.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
ebe3f82d70e845e358b28e1af53b4d9ae41bb1152ae11bdc1c83dfdb402de532	c:\users\keecfmwgj\music\kdubnqjx5rovkqg1.m4a.vvyu, C:\Users\kEecfMwgj\Music\kDubnqjX5ROvkqg1.m4a.vvyu	Dropped File	18.04 KB	application/octet-stream	Access, Create, Write	CLEAN
d9053b9f534e595f39ff89c796be0eaa3fe3930c9cca6445ed9d322ef2526ddd	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	CLEAN
8c35fcf877278ee9251189151ad6f9db320333df56e06316c3e59b73d7ab8908	c:\users\keecfmwgj\favorites\microsoft websites\microsoft at home.url.vvyu, C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Home.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
f9749d827540796505489df1fb81140ec4c700e7ef7c729691f7168be4aed486	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\1cab2.wav.vvyu, C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\aVzqZXq4M-FZ\1CaB2.wav.vvyu	Dropped File	2.78 KB	application/octet-stream	Access, Create, Write	CLEAN
d7b849a0fc00b4261e048266027b44910223697a0195b71efe4fc31d961d2015	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\ey662pveezsfar.wav.vvyu, C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\aVzqZXq4M-FZ\eY662pVeEZsFAR.wav.vvyu	Dropped File	46.60 KB	application/octet-stream	Access, Create, Write	CLEAN
9fef8af4468bb66e5a824651afe895f76f8a47695798c037361aeefe287aa09b	C:\Users\kEecfMwgj\Desktop\MF-vsO.flv.vvyu, c:\users\keecfmwgj\desktop\mf-vso.flv.vvyu	Dropped File	49.55 KB	video/x-flv	Access, Create, Write	CLEAN
2d20245c580a4f4c5ec07426cf6e3aa7732f3fd34f79cfa2b8e65e58297724d4	c:\users\keecfmwgj\documents\outlook files\franc@gdllo.de.pst.vvyu, C:\Users\kEecfMwgj\Documents\Outlook Files\franc@gdllo.de.pst.vvyu	Dropped File	265.33 KB	application/octet-stream	Access, Create, Write	CLEAN
a8d9e6c15f3c5bb635c528bf95d42ccb4ee179a7cef6a394cc8c8893f1d47770	C:\Users\kEecfMwgj\Pictures\yD7UYZJhgi.gif.vvyu, c:\users\keecfmwgj\pictures\yd7uyzjhgi.gif.vvyu	Dropped File	7.78 KB	image/gif	Access, Create, Write	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a199362bda115460d72530e50a50a320a197dd5dddda1afd51ba2639b9b3a5ba	C:\Users\kEecfMwgj\Videos\lYQkedL\bp_fOtZx7BdbiT9_sR8ibK.avi.vvyu, c:\users\keecfmwgj\videos\lyqkedl\bp_f\otzx7bdbit9_sr8ibk.avi.vvyu	Dropped File	83.80 KB	application/octet-stream	Access, Create, Write	CLEAN
0c5cceba5c416d5424387794429f89a2456b5326e2c7e5d8d2bd67f34bb616ec	-	Modified File	32.00 KB	application/octet-stream	-	CLEAN
8393ff81181fb9d5f7fa1754ed57b28388b99ce2375e4632b9caf21d3118dca8	c:\users\keecfmwgj\documents\4oox2qc.pptx.vvyu, C:\Users\kEecfMwgj\Documents\4OoX2QC.pptx.vvyu	Dropped File	30.51 KB	application/octet-stream	Access, Create, Write	CLEAN
c67c77c519c9a91c1e8c93eb7f896557ce7e6a9e6b219351f084299789b2603f	C:\Users\kEecfMwgj\Pictures\-tYby54-.gif.vvyu, c:\users\keecfmwgj\pictures\-tyby54-.gif.vvyu	Dropped File	92.07 KB	image/gif	Access, Create, Write	CLEAN
1c65f024a7677e9d9da933733772dc03c676a48711f797c922f5822b2b215780	c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\d-t7ftxif.pps.vvyu, C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\D-T7ftXIF.pps.vvyu	Dropped File	22.24 KB	application/octet-stream	Access, Create, Write	CLEAN
191e7ce5ce201dd4dfb8e03b9c2b63d099fd1f9eb3ab134e62e2ede2f5595bd7	c:\users\keecfmwgj\videos\lyqkedl\gei2kwsrqiau.flv.vvyu, C:\Users\kEecfMwgj\Videos\lYQkedL\gEI2KWSRQIaU.flv.vvyu	Dropped File	80.40 KB	video/x-flv	Access, Create, Write	CLEAN
281b0652d548bde02a86df12e55e058774844488f722cc273ae41ff1fe2888df	c:\users\keecfmwgj\desktop\ut2y\1vtklu46j9zljyf.png.vvyu, C:\Users\kEecfMwgj\Desktop\UT2y\1vtkLU46J9ZLjYf.png.vvyu	Dropped File	62.56 KB	application/octet-stream	Access, Create, Write	CLEAN
cb7f769454a95fbaf0163b9919bd6e348cb7670d643f63e21cf3999ba135a987	C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE Add-on site.url.vvyu, c:\users\keecfmwgj\favorites\microsoft websites\ie add-on site.url.vvyu	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
6daa653c405613fc514650dee4f060f982f4f0fc90615a168d2ca9c42e988b61	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
7c58b35a8b0180650ed29949f1e963a7a5bc4d9d506968ad46eb4f9b59802cdb	C:\Users\kEecfMwgj\Videos\lYQkedL\bp_fB77bP16RhY\FfJifEhMKb7gr\HrxywvF.avi.vvyu, c:\users\keecfmwgj\videos\lyqkedl\bp_f\b77bp16rhy\ffjifehmkb7gr\hrxywvf.avi.vvyu	Dropped File	76.10 KB	application/octet-stream	Access, Create, Write	CLEAN
0d47df071f0b044846c0f688f324f05f7dc963bcb5ff3f76698f6acfd123ce21	C:\Users\kEecfMwgj\Videos\lYQkedL\Fz-XgP8.avi.vvyu, c:\users\keecfmwgj\videos\lyqkedl\fz-xgp8.avi.vvyu	Dropped File	43.24 KB	application/octet-stream	Access, Create, Write	CLEAN
a7ab0369cac2b788cfb54811208bfdd026316e61bc121b2fe6c33512b03d9ab4	c:\users\keecfmwgj\desktop\ts9eh-mq2s2jrpdask\cvizy.png.vvyu, C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\cvIZY.png.vvyu	Dropped File	82.61 KB	application/octet-stream	Access, Create, Write	CLEAN
baf222d787a76b3be1bea1b26d45ff15068f51cadcce4d5b45d7f0824bb5b5f8	c:\users\keecfmwgj\videos\lyqkedl\bp_f\brfr.flv.vvyu, C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\Brfr.flv.vvyu	Dropped File	34.68 KB	video/x-flv	Access, Create, Write	CLEAN
ddacddf1ba38f2f1dadbb1ab59c37beb05c7069986d65f88921abbf9d16e5d1a	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	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e39e4127137cc23e79f8bdabd90cb8396706c4e5d752f1a8b4a10006a23be07e	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\qkkp5il.wav.vvyu, C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\7HsBaAEuFJOdKC\QkKp5IL.wav.vvyu	Dropped File	13.95 KB	application/octet-stream	Access, Create, Write	CLEAN
b68ef4e01a9f8d0fe911bae312f489601a6a8f428f466cd0897b57b13c6da961	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
5d63fe9eca6bef019167bfec990797b45343bd0cbcc8eed1ef65a953cd9ee758	c:\users\keecfmwgj\videos\lyqkedl\bp_f\b77bp16rhy\runduyt-pl209.swf.vvyu, C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\B77bP16RhY\RunDuyT-pl209.swf.vvyu	Dropped File	97.37 KB	application/x-shockwave-flash	Access, Create, Write	CLEAN
3ee142baa66842107042553de76b1273547928d1a2e78411e2f87b3523f2b50e	c:\users\keecfmwgj\desktop\zd_hryrh_.m4a.vvyu, C:\Users\kEecfMwgj\Desktop\Zd_HrYRh_.m4a.vvyu	Dropped File	87.22 KB	application/octet-stream	Access, Create, Write	CLEAN
f03d6a13ea8fb00a47d526914761e89e42adbbd7cf794f82d8abe2898eed4a10	C:\Users\kEecfMwgj\Videos\lYQkedL\bp_fe07kj.mp4.vvyu, c:\users\keecfmwgj\videos\lyqkedl\bp_f\e07kj.mp4.vvyu	Dropped File	37.86 KB	application/octet-stream	Access, Create, Write	CLEAN
d3e080116744d8025ad5ccc157349d4a3bc6c1b324d5a8031a6d38af8da2d13f	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	CLEAN
539ec9da48c419ed465b3530be6c2192332d9fdfd3b01fc38c312a1778546e69	C:\Users\kEecfMwgj\Pictures\qJwIfjoa.gif.vvyu, c:\users\keecfmwgj\pictures\qjwiifjoa.gif.vvyu	Dropped File	58.23 KB	image/gif	Access, Create, Write	CLEAN
c3ae33be13409ef5b5ce67c9cbbf9de6f189d10b154a9de628f7e88e7419b2c7	c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\lw0ngqzthjhumamurh.mp3.vvyu, C:\Users\kEecfMwgj\Music\CrZ6i\hyD8dEUbAR8o\Lw0NgQzthjhuMAMURh.mp3.vvyu	Dropped File	59.28 KB	application/octet-stream	Access, Create, Write	CLEAN
4d2d54f8fd42db62499a8b28816cf382e7bc4b3544899a772e15acf58f66636b	c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\nsm8w\19w3oa-fxhny9lnmwhz.wav.vvyu, C:\Users\kEecfMwgj\Music\CrZ6i\hyD8dEUbAR8o\NSm8w\19W3Oa-FxHnY9LNMWhz.wav.vvyu	Dropped File	30.75 KB	application/octet-stream	Access, Create, Write	CLEAN
68fcf3c8d44a750d285802a7c1be7057475f0ef4b0c29126a0ef389b510c4cc8	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

Reduced dataset

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\VDue0.odt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\lbnq9x4z nerecwqi5cw.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\lYQkedL\OREWDZex5CeUn06cUN.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\-tYby54-.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\u X_9CrHqo8CggdcB4.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\Ql6f.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\1nge1tjhlu2ewpqe6.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\l001k\uVwtXkawInc12.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\MzA_hckm7_swB.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\c34Mo1t-KwX2Fe92.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\hqdktuf4etm1.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\zaoit.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\wnJQgJSzxWQZQ3T9b.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\J4 DyZwJ9sl.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\V9OdwraOWmDvfZs\lFFeDb7YF-O_1-.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1HQ_0Ry\AoEQk-B.ppt.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\otrrqivqej6bkbcciq.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\A08G XtmrDvZD.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\lYQkedL\Fz-XgP8.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\tQMmYT.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\l001k\T8Z573.ods.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\mqJX68.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\M mqusjic.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\B77bP16RhY\lxVKv.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\7bevwhnu_fkrc\jxd7petv2jcni.xls.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\Desktop\Q04NB38XU1oN.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\fecjkv.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\r1qlmrxc3cdp2hj.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\xgSm1R9Zqu4JKgFkmXw.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\mu izhmdaedj6rosn.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\0y4sxbvo2pcys9vij e.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\EbPUXvbq aj ZxnAB.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\B77bP16RhY\FfJifEhMKb7gr\HrxywvF.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\uCoTL4ch-wEWMbF.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\p7fnrhbue2nij-3btzm.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\Y4t4pr6Mz4Wt_VJR.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\aVzqZXq4M-FZ\JG5i8r.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\cb4km4ywkhhpdlh.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\desktop\ut2y\r5wn3p5jpommfls2s.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\mqT6p7TH.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\ey662pveezsfar.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\lw0ngqzthjhumamurh.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\l001k\7rzoymi.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\rykwux.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ut2y\8ow5.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\lyqkedl\s_7dh5dokkvxw3gf2cnd.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\WvD1yF.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\1hq_0ry\aiiy-moqto8p.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\gjejgi7mnp2s-.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\kdubnqjx5rovkqg1.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1HQ_0Ry\DAEcp26Ep30AsNoAuHc.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\pSXJ.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\nsm8w\euc6yoilzsh1vn.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ut2y\1vtklu46j9zljyf.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\eofw5_iu17ime9.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\F59wFk.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\zhLBFDnBxCIJdg.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\ejhdcdvz_t.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\yD7UYZJhgi.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\nsm8w\19w3oa-fxhny9lnmwhz.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\lrxjj_ojmfg5h5f.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\CrZ6i\jjLwLGu.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\dtcpak5wO kdkquPh.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\l1flc8eh2.pdf.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\pictures\fexquahy4uxh2seih.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\lyqkedl\yhy pbk4xcgins.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	Sample File, Accessed File, VM File	Access, Delete, Read, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Documents\1HQ_0Ry\fyo9G2M-VX0uEz.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\OtZx7BdbiT9_sR8ibK.avi.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\P_MpI.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\xxrgef8g_2lumbpgs.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\aczwje9qryq8jx.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\ZRaPtwjBRWX3Lza6exVY.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\qs-f1e.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\CrZ6i\xJudM.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\MF-vsO.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\e07kj.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\CrZ6i\hyD8dEUbAR8o\NSm8w\0zrb.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\qzaaruieowyp 0mvbzk.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\QiucV nDx7zvq.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\L0X5uBCGS.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\appdata\locallow\microsoft\internet explorer\services\search_{0633ee93-d776-472f-a0ff-e1416b8b2e3a}.ico.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Spaces.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\hFSYfNeYKfRIr3.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\Ua5kWRFjT8eGw64gW.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\lyqkedl\bp_f\wuud9p77x.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\ilnaV2.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\k2soyi-o5lsts d_n6rv.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\jjbxw_fs-.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\muombxez-zs.odp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\7HsBaAEuFJOdKC\HbdZJwYobFQm.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\zH9UWAN96jNNa9sjtX.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\jihul99r3n0.mp4.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\5hLmZnA5PAqwTlGkZ.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\oAPMaSkphuOK7d.pdf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\qkkp5il.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\etu6.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\6F9xBIZhkcC1Zkgwd7k.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\7HsBaAEuFJOdKC\obudae3fGOyKU IH.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\6 RaZWC55WZRBx2uhb.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\QrK-kbLGW4AS.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\002z8yb-4ii p.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\7HsBaAEuFJOdKC\QjjqmBh2.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\u2xcl6fk4p\buwavzcuhtmrml.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\gGYFMJx.swf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\cv8-veyoh.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\h63-85V.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\1hq_0ry\rnf1.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\w3wlo_n9evs7ldf.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\N4KCoH3c2EBd4qZz.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\Vz9W.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\s6KVYjgw4EOpy.xlsx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\crz6i\5cx9jpbe2.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	Dropped File, Accessed File, VM File	Access, Create, Delete, Write	MALICIOUS
c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\1cab2.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\KVCbHcHNzJZLvA5z7u e.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\lyqkedl\bp_f\b77bp16rhy\vjumbjdocin1vnfnita.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\lyqkedl\mrt4.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\5-xamft.jpg.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\ut2y\cyxqypaxj5.mp3.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\un-n2otxgyzgta2hhk.xls.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\FjwYPRbpAtYuDK4_.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\MmtudzmA8-1ZtsXh1iI.gif.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\dmps8r4its euqecouq3.bmp.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\jcs1bzvbsa.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\WzOtFShww.rtf.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\videos\lyqkedl\gei2kwsrqiau.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\t12gfq_xaghox.ppt.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\IC2B3nJ.docx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\zd_hryrh_.m4a.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\1hq_0ry\zcrjc.csv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\FU_zQnPXBFcXiN5.wav.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\a3tvenkrzs u0e2m24js.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\lyqkedl\bp_f\b77bp16rhy\ffjifehmkb7gr\dz-kv.mkv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\l001k\tlk8.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\lyqkedl\bp_f\brfr.flv.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\lyqkedl\o 7trmbpu1b5dn.mp4.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\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\d-t7ftxif.pps.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\1hq_0ry\zgqoo-limasukc.ots.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\7bevwhnu_fkrc\v9odwraowmdvfzs\ok889i_j6dpzlzn5x.ots.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\nlxnihq5_.png.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\4oox2qc.pptx.vvyu	Dropped File, Accessed File	Access, Create, Write	MALICIOUS

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://acacaca.org/files/1/build3.exe	-	190.140.99.150, 189.164.252.207, 5.163.244.118, 110.14.121.125, 190.117.75.91, 190.219.54.242, 211.53.230.67, 116.121.62.237, 124.109.61.160, 187.170.251.250	-	GET	MALICIOUS
http://acacaca.org/test2/get.php?pid=B781B23F267DEB99256EE88043E0BDBC&first=true	-	190.140.99.150, 189.164.252.207, 5.163.244.118, 110.14.121.125, 190.117.75.91, 190.219.54.242, 211.53.230.67, 116.121.62.237, 124.109.61.160, 187.170.251.250	-	GET	MALICIOUS
http://rgyui.top/dl/build2.exe	-	-	-	-	MALICIOUS
https://api.2ip.ua/geo.json	-	162.0.217.254	-	GET	CLEAN

Domain

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

IP

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

Mutex

Name	Operations	Parent Process Name	Verdict
{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}	access	d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion	access	d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\SysHelper	read, access, write	d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SysHelper	read, access, write	d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	CLEAN

Process

Process Name	Commandline	Verdict
d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	"C:\Users\kEecfMwgj\Desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe"	MALICIOUS
d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	"C:\Users\kEecfMwgj\Desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe" --Admin IsNotAutoStart IsNotTask	MALICIOUS
d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe --Task	MALICIOUS

Process Name	Commandline	Verdict
d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	"C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe" --AutoStart	MALICIOUS
d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	"C:\Users\kEecfMwgj\Desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe"	SUSPICIOUS
d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	"C:\Users\kEecfMwgj\Desktop\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe" --Admin IsNotAutoStart IsNotTask	SUSPICIOUS
d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe	"C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12\d0202dee37da4da0375e0034e802e0351cf3185cc8cd6ad041ffca4c89d97797.exe" --AutoStart	SUSPICIOUS
icacls.exe	icacls "C:\Users\kEecfMwgj\AppData\Local\12868036-6d41-41a9-b0d6-efe01c2dda12" /deny *S-1-1-0:(OI)(CI)(DE,DC)	CLEAN
taskeng.exe	taskeng.exe {58D0AF36-B196-4C0E-BD35-56E44726A7F4} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (286)

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\lyqkedl\bp_f\d6ztvjfwwa.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\lS2B.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\Contacts\Administrator.contact.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\u2xcl6fk4p\buwavzcuhtmrml.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\lyqkedl\bp_f\wuud9p77x.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\EbPUXvbqaj ZxnAB.png.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\qzaaruieowyp 0mvbzk.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\YG8k.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\lyqkedl\mrt4.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\t1mqysmsezilmfb.m4a.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\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	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\dtcpak5wO kdkqu Ph.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\7bevwhnu_fkrc\jxd7petv2jcni.xls.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\cv8-veyoh.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\CrZ6i\jjLwLGu.m4a.vvyu	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\hqdktuf4etm1.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\5-xamft.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\xquj.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\VDue0.odt.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\WzOtFShww.rtf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\otrrqivqej6bkbcciq.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\70uMB.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\lyqkedl\izhxbinth.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\h63-85V.xlsx.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\lyqkedl\bp_f\pc3yf9pj6umpbxequ7nk.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\qs-f1e.pptx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\naFofVP436Y9.odp.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1HQ_0Ry\AoEQk-B.ppt.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\c34Mo1t-KwX2Fe92.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\s6KVYjgw4EOpy.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\pSXJ.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\uX_9CrHqo8CggdcB4.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\Videos\IYQkedL\OREWDZex5CeUn06c UN.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\002z8yb-4iip.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\Kt1gN2Zu4cLe_ffn1E.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\1hq_0ry\jn5w8pue5cpjcmbtd8.xlsx.vvyu	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\qUrDOWbjU_xfUkCK.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\TS9Eh-MQ2S2JrpdASk\MmtudzmA8-1ZtsXh1iI.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\8fWkzgyyD0qQR-ID9Sm.pptx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\xS0O4.gif.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\IYQkedL\bp_f\gGYFMJx.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\Desktop\zH9UWAN96jNNa9sjtX.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\nlxnihq5_.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\rk2x.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\1hq_0ry\rnf1.rtf.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\t12gfq_xaghox.ppt.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\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\k2soyi-o5lsts d_n6rv.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\l001k\7rzoymi.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\hFSYfNeYKfRIr3.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\Favorites\MSN Websites\MSN Money.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtIrpfg6Rc8C\7HsBaAEuFJOdKC\QjjqmBh2.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\Pictures\mqT6p7TH.png.vvyu	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\HGiMBm8T.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\l001k\uVwtXkawInc12.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\k5e8ye4arc.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\music\1nge1tjhlu2ewpqe6.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\nsm8w\m lbm.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\fecjkv.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\1hq_0ry\zcrjc.csv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\N4KCoH3c2EBd4qZz.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\2fyWk_nuEZSWQOD.pdf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\lyqkedl\bp_f\b77bp16rhy\vjumbjdocin1vnfnita.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\lyqkedl\bp_f\b77bp16rhy\ffjifehmkb7gr\dz-kv.mkv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\Ua5kWRFjT8eGw64gW.mp4.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\4pvmPeV-Pn.flv.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\5v0uyr-um9wck\lnubjtwwj5-mjcy_1\l001k\tlk8.ots.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\zhLBFDnBxCIJdg.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\g5cw5jpl.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\videos\zaoit.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\tQMmYT.png.vvyu	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ts9eh-mq2s2jrpdask\w3-dnej.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\L0X5uBCGS.jpg.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1HQ_0Ry\fyo9G2M-VX0uEz.pptx.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\rykwux.png.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\lbnq9x4znerecwqi5cw.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\jihul99r3n0.mp4.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\ZRaPtwjBRWX3Lza6exVY.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\o89yzaehg03nthchcn.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\lyqkedl\yhypbk4xcgins.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\F59wFk.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\5v0uyr-um9wck\va7_pjef68oc_g\aczwje9qryq8jx.rtf.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ut2y\cyxqypaxj5.mp3.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\7bEvWHNu_FkrC\V9OdwraOWmDvfZs\lFFeDb7YF-O_1-.xlsx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\lYQkedL\bp_f\B77bP16RhY\7vLuv6V2.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\desktop\dmps8r4iteuqecouq3.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\uCoTL4ch-wEWMbF.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\ejhdcdvz_t.m4a.vvyu	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\ut2y\r5wn3p5jpommfls2s.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\lC2B3nJ.docx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\TS9Eh-MQ2S2JrpdASk\wnJQgJSzxWQZQ3T9b.gif.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\xxrgef8g_2lumbpgs.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\music\u2xcl6fk4p\seofpmtirpfg6rc8c\7hsbaaeufjodkc\drvaf2.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\crz6i\5cx9jpbe2.wav.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\0y4sxbvo2pcys9vij e.bmp.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\5v0UyR-UM9wCK\lNuBJTWwJ5-Mjcy_1\l001k\T8Z573.ods.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\eofw5_iu17ime9.png.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\6RaZWC55WZRBx2uhb.mp3.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\5hLmZnA5PAqwTlGkZ.flv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\crz6i\hyd8deubar8o\nsm8w\euc6yoilzsh1vn.m4a.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\w3wlo_n9evs7ldf.pptx.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.vvyu	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\2t_yf.swf.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\muizhmdaedj6rosn.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\mqJX68.avi.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\1hq_0ry\iz9jh_ltuq.csv.vvyu	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\NcfXF2sB4dY.avi.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\Music\U2xcL6FK4p\sEOfpmtlrpfg6Rc8C\7HsBaAEuFJOdKC\obudae3fGOyKU lH.wav.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
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\kdubnqjx5rovkqg1.m4a.vvyu	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\favorites\microsoft websites\microsoft at home.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\u2xcl6fk4p\seofpmtirpfg6rc8c\avzqzxq4m-fz\1cab2.wav.vvyu	Ransomware	5/5

Reduced dataset

ENVIRONMENT

Virtual Machine Information

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

Platform Information

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

Software Information

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

System Information

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

System Root	C:\Windows