MALICIOUS

Classifications: Ransomware | Downloader | Injector

Threat Names: Djvu | Troj/Krypt-XU | Mal/Generic-S | STOP | SmokeLoader | Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe**
ID	#7980376
MD5	22acf65ad76e4322a020bc1afdc2c935
SHA1	808c2d353ded6249bdb2cc560047fb374e8bc5b2
SHA256	c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3
File Size	270.50 KB
Report Created	2023-06-07 02:15 (UTC)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (33 rules, 194 matches)

Score	Category	Operation	Count	Classification
5/5	User Data Modification	Modifies content of user files	1	Ransomware
	• (Process #21) 51f0.exe modifies the content of multiple user files.			
5/5	User Data Modification	Renames user files	1	Ransomware
	• (Process #21) 51f0.exe renames multiple user files.			
5/5	User Data Modification	Appends the same extension to many filenames	1	Ransomware
	• Renames 207 files by appending the extension ".neqp".			
5/5	Extracted Configuration	Smoke Loader configuration was extracted	1	Downloader
	• A configuration for Smoke Loader was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	100	Ransomware

- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Desktop\DsHy6owCtF.wav.neqp.
- YARA detected "Djvu" from ruleset "Ransomware" in memory dump data from (process #21) 51f0.exe.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\BqMJYpJI5- Av.csv.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Music\5_uaNmfND3.m4a.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Pictures\5tjEDT2i8f.png.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Music\UZ21XYbO5jhJZq.mp3.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\OvrR6bzipPtcj.docx.neqp.
- YARA detected "Djvu" from ruleset "Ransomware" in memory dump data from (process #13) 51f0.exe.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Music\u8_5OoZXD_BvAYx.wav.neqp.
- YARA detected "Djvu" from ruleset "Ransomware" in memory dump data from (process #4) 51f0.exe.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Contacts\Administrator.contact.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\ukOCS4.csv.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Pictures\XyS3y_CU 624bSCdh.bmp.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\ewxkZosyJKHNwpoz.docx.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\dohGx0T L.jpg.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Videos\bZ_MAu7.avi.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\G_bTFo.odp.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\uYkNWJF11O37vr\Xw0 5hxcA.pptx.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\sU3qV4 mwzLmj.pps.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Music\By0ls29bBPKLp631O9b.m4a.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\h9Ysje.pptx.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Music\XqlXfBNrZqo t.mp3.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Desktop\UpkLen56967zJ.flv.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\OeH1e-xhIt5Ie6VWmu4M.xlsx.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\1CIt3S.jpg.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\GhhediFJZwrU5kMr.xlsx.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Pictures\dCjDLPjgt.png.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Desktop\ET8KrYKeuj73U.swf.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Videos\ups I7.mkv.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Music\n-diJdt93vqLXJ.wav.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\3traX2.xlsx.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Desktop\aM0hOBR8.wav.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\Ydwe3q9JyYweb_55_.ots.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\uYkNWJF11O37vr\RRM0O7_xClNdkabdTozN.xlsx.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Videos\80uy.mkv.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\k7QtcBphpiUfUf6h4.rtf.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Pictures\c8-qdtkNHu0bJGmu.jpg.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Music\DcXaZQH.m4a.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\zT3A4flgAWjYzt7r4Xm.png.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Videos\kCiA6GopKG9.avi.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Videos\ueJknWfWvw.mkv.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\2VNUKKMN.xlsx.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\kduc8M4q0iGO.xlsx.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Videos__N93Zziz9RNY.mp4.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\rUec4u8CN1U.jpg.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Entertainment.url.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\DjfPSJtvQ\gXUwPJ.csv.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\OY4eRUo53OZ.rtf.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Videos\bGt49HOvptpF2AsDKl.mkv.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIRIeTh vq1qbRJ-L\aZ2HX2t0pm3.ots.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\OepL7uNfz0.jpg.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\G8oUQ7rKtGSWcT.ots.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIRIeTh vq1qbRJ-L\oV6zFBL.rtf.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Desktop\tkAxoIHRl8qEDbn.gif.neqp.
- YARA detected "Djvu" from ruleset "Ransomware" in memory dump data from (process #31) 3024.exe.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Videos\qG8i9G0tlhejna tR3l.flv.neqp.
- YARA detected "DjvuEncryptedFile" from ruleset "Ransomware" in the dropped file C:\Users\kEecfMwgj\Videos\FMXhA_W4EkE5pF8l.mp4.neqp.

Score	Category	Operation	Count	Classification
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #2) explorer.exe tries to delete zone identifier of file "C:\Users\kEecfMwgj\AppData\Roaming\uaieedr".			
4/5	Privilege Escalation	Creates elevated child process	2	-
	• (Process #4) 51f0.exe creates (process #12) 51f0.exe with elevated privileges. • (Process #25) 3024.exe creates (process #30) 3024.exe with elevated privileges.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #18) uaieedr modifies memory of (process #23) explorer.exe.			
4/5	Injection	Modifies control flow of another process	1	Injector
	• (Process #18) uaieedr creates thread in (process #23) explorer.exe.			
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels the sample itself as Mal/Generic-S. • Reputation analysis labels embedded file "" as Mal/Generic-S.			
4/5	Reputation	Contacts known malicious URL	6	-
	• Reputation analysis labels the URL "hxxps://paraslegal[.]com/tmp/index.php" which was contacted by (process #2) explorer.exe as Troj/Krypt-XU. • Reputation analysis labels the URL "hxxp://zexeq[.]com/lancer/get.php?pid=3822B4A9E2D4C1F1D716E5E90C8DE07D" which was contacted by (process #21) 51f0.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://45[.]9[.]74[.]80/wall.exe" which was contacted by (process #2) explorer.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://zexeq[.]com/lancer/get.php?pid=3822B4A9E2D4C1F1D716E5E90C8DE07D&first=true" which was contacted by (process #13) 51f0.exe as Mal/HTMLGen-A. • (Process #2) explorer.exe contacted known malicious URL hxxp://potunulit[.]org. • Reputation analysis labels the URL "hxxp://colisumy[.]com/dl/build.exe" which was contacted by (process #2) explorer.exe as Mal/HTMLGen-A.			
4/5	Reputation	Resolves known malicious domain	4	-
	• Reputation analysis labels the resolved domain "colisumy.com" as Mal/HTMLGen-A. • Resolved domain "paraslegal.com" is a known malicious domain. • Resolved domain "potunulit.org" is a known malicious domain. • Reputation analysis labels the resolved domain "zexeq.com" as Mal/HTMLGen-A.			
3/5	YARA	Suspicious content matched by YARA rules	6	-
	• YARA detected "PDF_Missing_startxref" from ruleset "Malicious-Documents" in the dropped file C:\Users\kEecfMwgj\Documents\FU2 nzV-k.pdf.neqp. • YARA detected "PDF_Missing_EOF" from ruleset "Malicious-Documents" in the dropped file C:\Users\kEecfMwgj\Documents\FU2 nzV-k.pdf.neqp. • YARA detected "PDF_Missing_EOF" from ruleset "Malicious-Documents" in the dropped file C:\Users\kEecfMwgj\Documents\p5HGkq_lz1hzZZQ1QzX\7lvhY-.pdf.neqp. • YARA detected "PDF_Missing_startxref" from ruleset "Malicious-Documents" in the dropped file C:\Users\kEecfMwgj\Documents\p5HGkq_lz1hzZZQ1QzX\7lvhY-.pdf.neqp. • YARA detected "PDF_Missing_EOF" from ruleset "Malicious-Documents" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\S7LH3hXtiTTmcVgH\4kaBTKfDmjtKDpmZU4\uc2h_7ZMsMjV1wdpv4D.pdf.neqp. • YARA detected "PDF_Missing_startxref" from ruleset "Malicious-Documents" in the dropped file C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\S7LH3hXtiTTmcVgH\4kaBTKfDmjtKDpmZU4\uc2h_7ZMsMjV1wdpv4D.pdf.neqp.			
2/5	Anti Analysis	Tries to detect debugger	1	-
	• (Process #1) c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Hide Tracks	Deletes file after execution	3	-

Score	Category	Operation	Count	Classification
	• (Process #2) explorer.exe deletes executed executable "C:\Users\kEecfMwgj\AppData\Roaming\uaieedr". • (Process #2) explorer.exe deletes executed executable "C:\Users\kEecfMwgj\Desktop\c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe". • (Process #4) 51f0.exe deletes executed executable "C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51F0.exe".			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #13) 51f0.exe has a thread which sleeps more than 5 minutes.			
2/5	Anti Analysis	Makes direct system call to possibly evade hooking based sandboxes	4	-
	• (Process #9) uaieedr makes a direct system call to "NtQueryInformationProcess". • (Process #1) c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe makes a direct system call to "NtQueryInformationProcess". • (Process #1) c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe makes a direct system call to "NtQuerySystemInformation". • (Process #9) uaieedr makes a direct system call to "NtQuerySystemInformation".			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	5	-
	• (Process #3) 51f0.exe modifies memory of (process #4) 51f0.exe. • (Process #12) 51f0.exe modifies memory of (process #13) 51f0.exe. • (Process #20) 51f0.exe modifies memory of (process #21) 51f0.exe. • (Process #24) 3024.exe modifies memory of (process #25) 3024.exe. • (Process #30) 3024.exe modifies memory of (process #31) 3024.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	5	-
	• (Process #3) 51f0.exe alters context of (process #4) 51f0.exe. • (Process #12) 51f0.exe alters context of (process #13) 51f0.exe. • (Process #20) 51f0.exe alters context of (process #21) 51f0.exe. • (Process #24) 3024.exe alters context of (process #25) 3024.exe. • (Process #30) 3024.exe alters context of (process #31) 3024.exe.			
2/5	Task Scheduling	Schedules task	3	-
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\uaieedr", to be triggered by LOGON. • Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\uaieedr", to be triggered by TIME. Task has been rescheduled by the analyzer. • Schedules task for command "C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51F0.exe", to be triggered by TIME. Task has been rescheduled by the analyzer.			
1/5	Discovery	Enumerates running processes	7	-
	• (Process #2) explorer.exe enumerates running processes. • (Process #4) 51f0.exe enumerates running processes. • (Process #13) 51f0.exe enumerates running processes. • (Process #21) 51f0.exe enumerates running processes. • (Process #23) explorer.exe enumerates running processes. • (Process #25) 3024.exe enumerates running processes. • (Process #31) 3024.exe enumerates running processes.			
1/5	Mutex	Creates mutex	4	-
	• (Process #2) explorer.exe creates mutex with name "DCEBF3F5A707CB556B65BC9D3C6783D08443A5AF". • (Process #13) 51f0.exe creates mutex with name "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}". • (Process #21) 51f0.exe creates mutex with name "{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}". • (Process #23) explorer.exe creates mutex with name "DCEBF3F5A707CB556B65BC9D3C6783D08443A5AF".			
1/5	Hide Tracks	Creates process with hidden window	5	-

Score	Category	Operation	Count	Classification
		• (Process #2) explorer.exe starts (process #3) 51f0.exe with a hidden window. • (Process #3) 51f0.exe starts (process #4) 51f0.exe with a hidden window. • (Process #4) 51f0.exe starts (process #6) icacls.exe with a hidden window. • (Process #23) explorer.exe starts (process #24) 3024.exe with a hidden window. • (Process #24) 3024.exe starts (process #25) 3024.exe with a hidden window.		
1/5	Obfuscation	Reads from memory of another process	5	-
		• (Process #3) 51f0.exe reads from (process #4) 51f0.exe. • (Process #12) 51f0.exe reads from (process #13) 51f0.exe. • (Process #20) 51f0.exe reads from (process #21) 51f0.exe. • (Process #24) 3024.exe reads from (process #25) 3024.exe. • (Process #30) 3024.exe reads from (process #31) 3024.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	5	-
		• (Process #3) 51f0.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #12) 51f0.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #20) 51f0.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #24) 3024.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code. • (Process #30) 3024.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.		
1/5	Persistence	Installs system startup script or application	1	-
		• (Process #4) 51f0.exe adds ""C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51F0.exe" --AutoStart" to Windows startup via registry.		
1/5	Discovery	Tries to get network statistics	1	-
		• (Process #21) 51f0.exe gets network statistics via API.		
1/5	Network Connection	Downloads executable	2	Downloader
		• (Process #2) explorer.exe downloads Windows executable via http from hxxp://45[.]9[.]74[.]80/wall.exe. • (Process #23) explorer.exe downloads Windows executable via http from hxxp://45[.]9[.]74[.]80/wall.exe.		
1/5	Network Connection	Downloads file	2	-
		• (Process #2) explorer.exe downloads file via http from hxxp://potunulit[.]org. • (Process #23) explorer.exe downloads file via http from hxxp://potunulit[.]org.		
1/5	Execution	Drops PE file	2	-
		• (Process #2) explorer.exe drops file "C:\Users\KEECFM~1\AppData\Local\Temp\51F0.exe". • (Process #23) explorer.exe drops file "C:\Users\KEECFM~1\AppData\Local\Temp\3024.exe".		
1/5	Execution	Executes dropped PE file	1	-
		• Executes dropped file "C:\Users\KEECFM~1\AppData\Local\Temp\51F0.exe".		
1/5	Obfuscation	Resolves API functions dynamically	10	-

Score	Category	Operation	Count	Classification
	• (Process #3) 51f0.exe resolves 39 API functions by name. • (Process #4) 51f0.exe resolves 37 API functions by name. • (Process #12) 51f0.exe resolves 39 API functions by name. • (Process #13) 51f0.exe resolves 37 API functions by name. • (Process #20) 51f0.exe resolves 39 API functions by name. • (Process #21) 51f0.exe resolves 58 API functions by name. • (Process #24) 3024.exe resolves 39 API functions by name. • (Process #25) 3024.exe resolves 36 API functions by name. • (Process #30) 3024.exe resolves 39 API functions by name. • (Process #31) 3024.exe resolves 37 API functions by name.			
-	Trusted	Known clean file	1	-
	• File "C:\SystemID\PersonalID.txt" is a known clean file.			

Malware Configuration: SmokeLoader

Metadata	Key	Extracted Value
Mission ID	Value	2022
Encryption Key	Key Tags Algorithm	PvBoKg== Network Communication Decryption Key RC4
	Key Tags Algorithm	1F9PzA== Network Communication Encryption Key RC4
URL	Url	http://potunulit.org/
	Url	http://hutnilior.net/
	Url	http://bulimu55t.net/
	Url	http://soryytlic4.net/
	Url	http://novanosa5org.org/
	Url	http://nuljjjnuli.org/
	Url	http://tolilolihul.net/
	Url	http://somatoka51hub.net/
	Url	http://hujukui3.net/
	Url	http://bukubuka1.net/
	Url	http://golilopaster.org/
	Url	http://newzelannd66.org/
	Url	http://otriluyttn.org/

Mitre ATT&CK Matrix

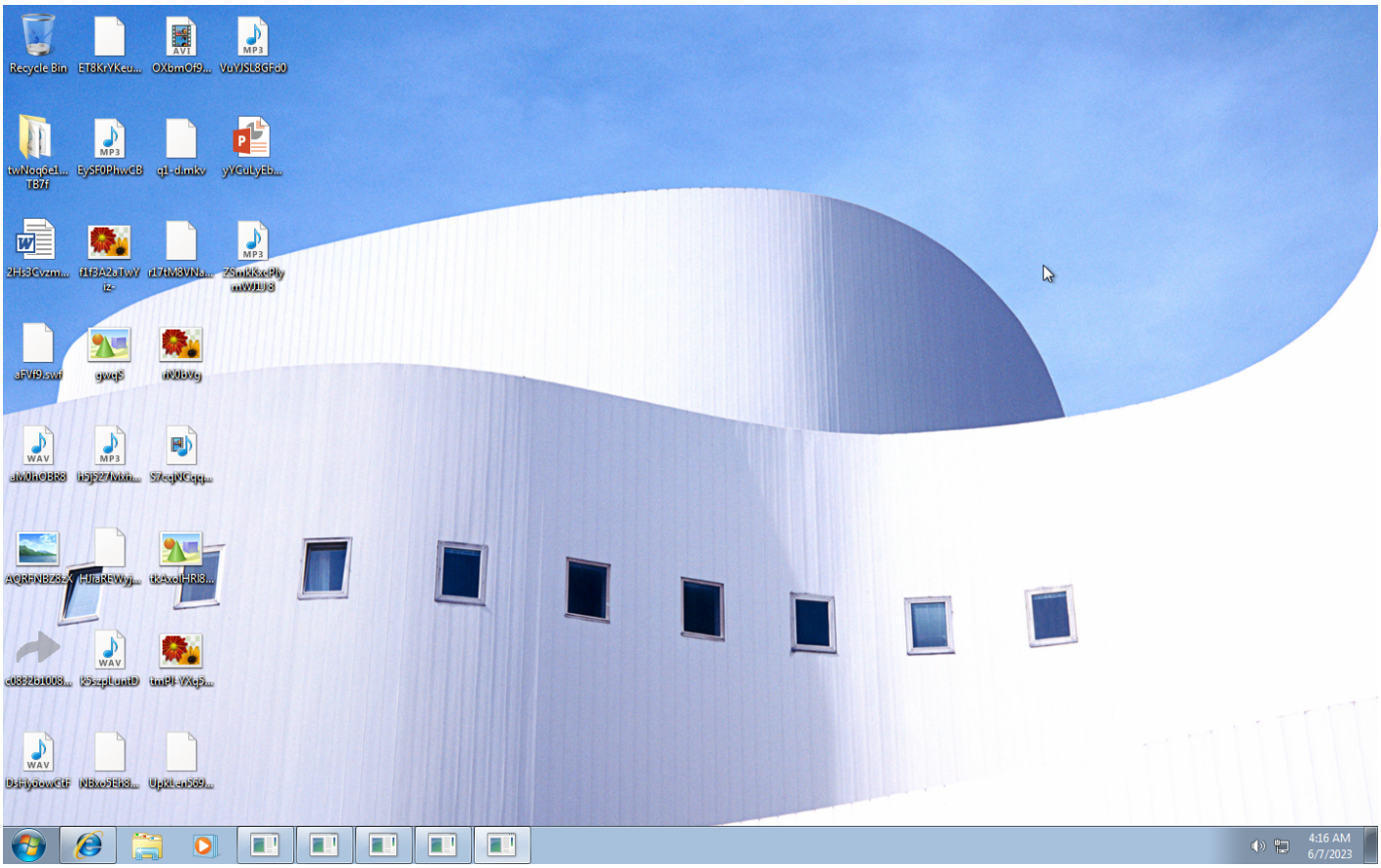
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1060 Registry Run Keys / Startup Folder	#T1053 Scheduled Task	#T1096 NTFS File Attributes		#T1057 Process Discovery	#T1105 Remote File Copy		#T1071 Standard Application Layer Protocol		#T1486 Data Encrypted for Impact
		#T1053 Scheduled Task		#T1143 Hidden Window		#T1016 System Network Configuration Discovery			#T1105 Remote File Copy		
				#T1045 Software Packing		#T1049 System Network Connections Discovery					
				#T1112 Modify Registry							

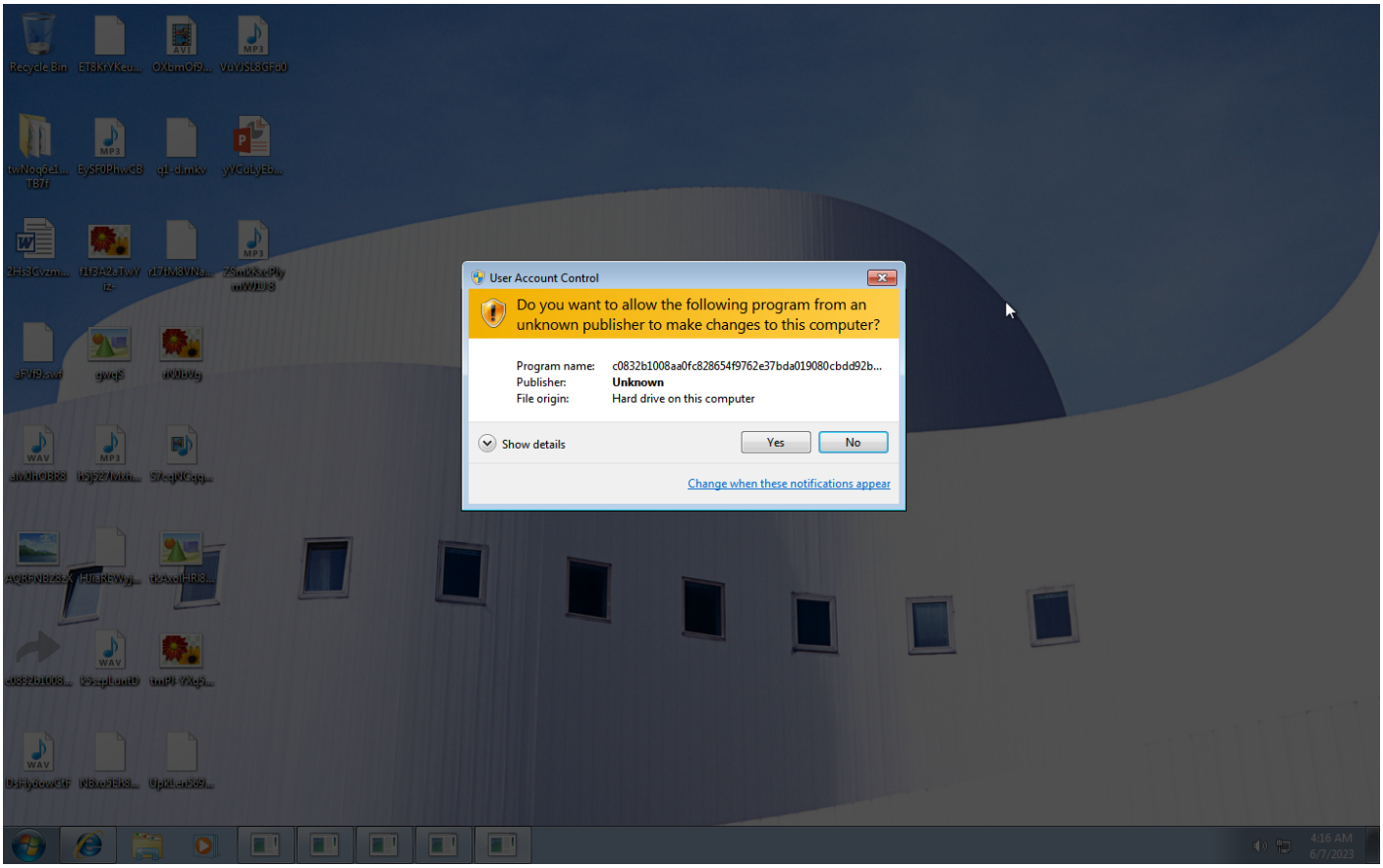
Sample Information

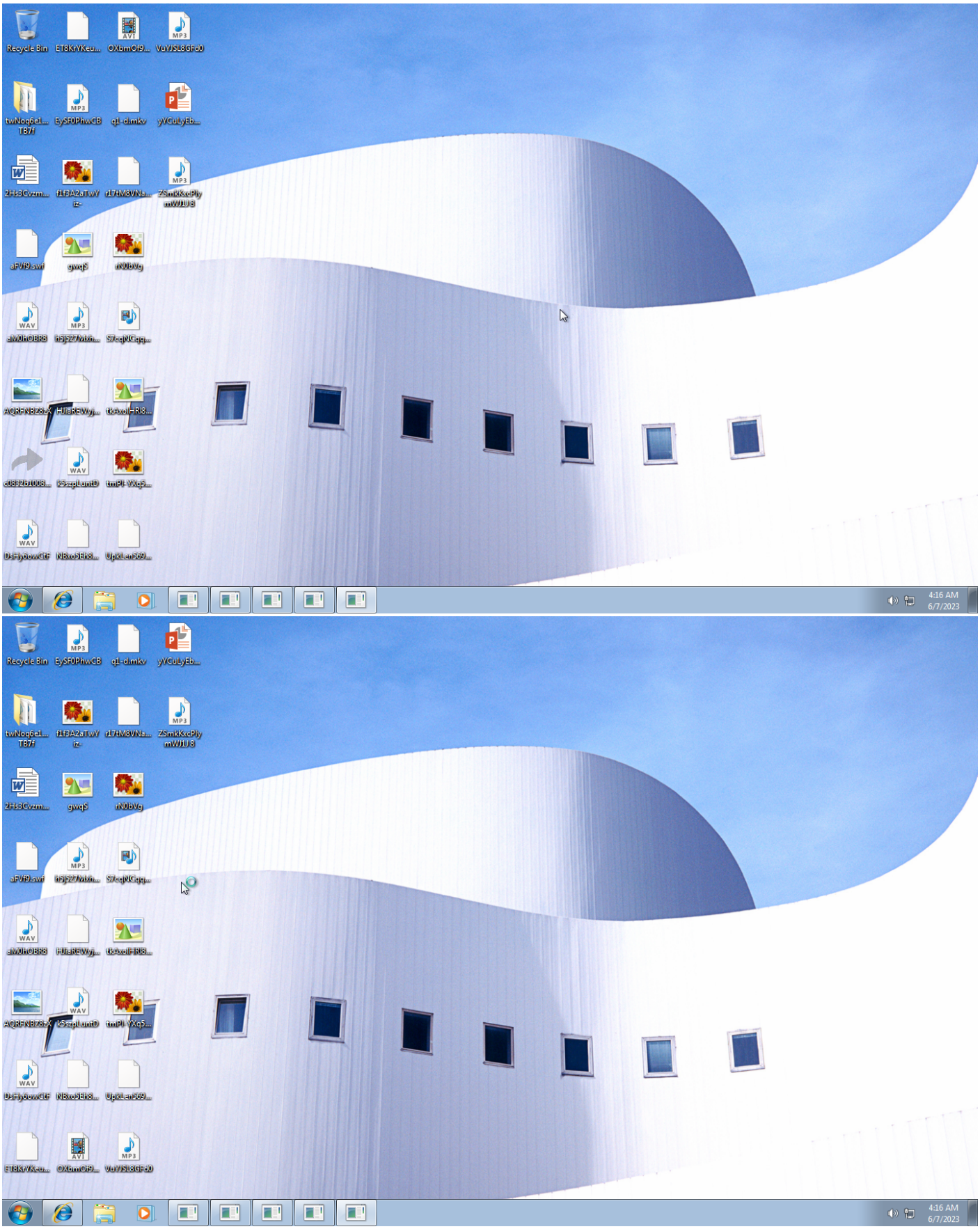
ID	#7980376
MD5	22acf65ad76e4322a020bc1afdc2c935
SHA1	808c2d353ded6249bdb2cc560047fb374e8bc5b2
SHA256	c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3
SSDeep	3072:cLeg2PMPu+JhaCkBmxvMcKedNTYko2WglgEYhQLRARwOblNwaUiraf2nXn:7g2P3ehaOxvDDrKUYhQOOwINwfirj
ImpHash	cffb13fd9da7f89cf243dfbae0e78962
File Name	c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe
File Size	270.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2023-06-07 02:15 (UTC)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	21
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	295




User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: c0832b1008aa0fc828654f9762e37bda019080cbdd92b...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

163.51 KB total sent

11537.77 KB total received

4 ports 80, 53, 443, 445

8 contacted IP addresses

13 URLs extracted

23 files downloaded

0 malicious hosts detected

DNS

12 DNS requests for 5 domains

1 nameservers contacted

3 total requests returned errors

HTTP/S

6 URLs contacted, 6 servers

12 sessions, 104.54 KB sent, 18421.62 KB received

HTTP Requests

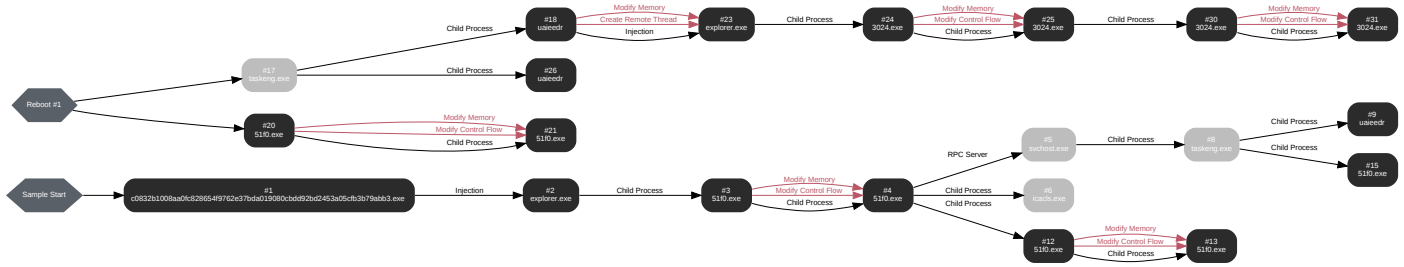
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	hxxp://potunulit[.]org	-	-	-	0 bytes	MALICIOUS
GET	hxxp://45[.]9[.]74[.]80/wall.exe	-	-	-	0 bytes	MALICIOUS
GET	hxxp://zexeq[.]com/lancer/get.php?pid=3822B4A9E2D4C1F1D716E5E90C8DE07D&first=true	-	-	-	0 bytes	MALICIOUS
GET	hxxp://colisumy[.]com/dl/build.exe	-	-	-	0 bytes	MALICIOUS
GET	hxxp://zexeq[.]com/lancer/get.php?pid=3822B4A9E2D4C1F1D716E5E90C8DE07D	-	-	-	0 bytes	MALICIOUS
GET	hxxps://paraslegal[.]com/tmp/index.php	-	-	-	0 bytes	MALICIOUS
GET	hxxps://api[.]2ip[.]ua/geo.json	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	colisumy[.]com	-	-	-	MALICIOUS
A	paraslegal[.]com	-	-	-	MALICIOUS
A	potunulit[.]org	NO_ERROR	104.21.18.99, 172.67.181.144	-	MALICIOUS
A	zexeq[.]com	NO_ERROR	37.34.248.24, 115.88.24.200, 201.110.217.38, 210.182.29.70, 58.235.189.192, 183.100.39.157, 109.98.58.98, 5.204.64.195, 195.158.3.162, 211.40.39.251	-	MALICIOUS
A	api[.]2ip[.]ua	NO_ERROR	162.0.217.254	-	CLEAN

BEHAVIOR

Process Graph



Process #1: c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 37943, Reason: Analysis Target
Unmonitor End Time	End Time: 49019, Reason: Terminated
Monitor duration	11.08s
Return Code	0
PID	3704
Parent PID	1908
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Desktop\c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe	270.50 KB	c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3	✖

Host Behavior

Type	Count
System	6
Module	40
File	4
Environment	1
Keyboard	2
-	1

Process #2: explorer.exe

ID	2
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 47947, Reason: Injection
Unmonitor End Time	End Time: 109649, Reason: Terminated
Monitor duration	61.70s
Return Code	1073807364
PID	1908
Parent PID	-
Bitness	64 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\51F0.exe	749.50 KB	5d1b0a63577d637eecfd075abf530d62b2c913c98b2bd38e116ffb8c21e5dd13	✖
C:\Users\kEecfMwgj\AppData\Roaming\uaieedr	270.50 KB	c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3	✖
C:\Users\KEECFM~1\AppData\Local\Temp\51F0.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	23
System	2526
Process	514
Mutex	1
Registry	3
File	14
User	1
COM	1

Network Behavior

Type	Count
HTTP	8
HTTPS	1
TCP	1

Process #3: 51f0.exe

ID	3
File Name	c:\users\keecfmwgj\appdata\local\temp\51f0.exe
Command Line	C:\Users\KEECFM~1\AppData\Local\Temp\51F0.exe
Initial Working Directory	C:\Users\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 70044, Reason: Child Process
Unmonitor End Time	End Time: 74116, Reason: Terminated
Monitor duration	4.07s
Return Code	0
PID	3768
Parent PID	1908
Bitness	32 Bit

Host Behavior

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

Process #4: 51f0.exe

ID	4
File Name	c:\users\keecfmwgj\appdata\local\temp\51f0.exe
Command Line	C:\Users\KEECFM~1\AppData\Local\Temp\51F0.exe
Initial Working Directory	C:\Users\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 72360, Reason: Child Process
Unmonitor End Time	End Time: 83093, Reason: Terminated
Monitor duration	10.73s
Return Code	0
PID	3776
Parent PID	3768
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#3: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xebc	0x400000(4194304)	0x400	✔	1
Modify Memory	#3: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xebc	0x401000(4198400)	0xca600	✔	1
Modify Memory	#3: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xebc	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#3: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xebc	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#3: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xebc	0x52b000(5419008)	0x200	✔	1
Modify Memory	#3: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xebc	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#3: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xebc	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#3: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xebc / 0xec4	0x77e201c4(2011300292)	-	✔	1

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51F0.exe	749.50 KB	5d1b0a63577d637eecfd075abf530d62b2c913c98b2bd38e116ffb8c21e5dd13	✖
-	489 bytes	fbe85e72ef956a08f392ecaccd7d16ddbf0f5e92c6c4c487bad722d6bcc25308	✖

Host Behavior

Type	Count
System	4
Module	47
File	6
Environment	1

Type	Count
Process	96
Registry	4
COM	1

Process #5: svchost.exe

ID	5
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: 75663, Reason: RPC Server
Unmonitor End Time	End Time: 279684, Reason: Terminated by timeout
Monitor duration	204.02s
Return Code	Unknown
PID	876
Parent PID	3776
Bitness	64 Bit

Process #6: icacls.exe

ID	6
File Name	c:\windows\syswow64\icacls.exe
Command Line	icacls "C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd" /deny *S-1-1-0:(OI)(CI)(DE,DC)
Initial Working Directory	C:\Users\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 76492, Reason: Child Process
Unmonitor End Time	End Time: 78175, Reason: Terminated
Monitor duration	1.68s
Return Code	0
PID	3808
Parent PID	3776
Bitness	32 Bit

Process #8: taskeng.exe

ID	8
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {D864A465-DF92-41F7-B6FE-4C380B7E9468} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 78943, Reason: Child Process
Unmonitor End Time	End Time: 102364, Reason: Terminated
Monitor duration	23.42s
Return Code	1073807364
PID	3872
Parent PID	876
Bitness	64 Bit

Process #9: uaieedr

ID	9
File Name	c:\users\keecfmwgj\appdata\roaming\uaieedr
Command Line	C:\Users\kEecfMwgj\AppData\Roaming\uaieedr
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 79465, Reason: Child Process
Unmonitor End Time	End Time: 94278, Reason: Terminated
Monitor duration	14.81s
Return Code	0
PID	3920
Parent PID	3872
Bitness	32 Bit

Host Behavior

Type	Count
System	6
Module	38
File	4
Environment	1
Keyboard	2
-	1

Process #12: 51f0.exe

ID	12
File Name	c:\users\keecfmwgj\appdata\local\temp\51f0.exe
Command Line	"C:\Users\KEECFM~1\AppData\Local\Temp\51F0.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 81694, Reason: Child Process
Unmonitor End Time	End Time: 85018, Reason: Terminated
Monitor duration	3.32s
Return Code	0
PID	4024
Parent PID	3776
Bitness	32 Bit

Host Behavior

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

Process #13: 51f0.exe

ID	13
File Name	c:\users\keecfmwgj\appdata\local\temp\51f0.exe
Command Line	"C:\Users\KEECFM~1\AppData\Local\Temp\51F0.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 83532, Reason: Child Process
Unmonitor End Time	End Time: 100988, Reason: Terminated
Monitor duration	17.46s
Return Code	0
PID	4036
Parent PID	4024
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xfbc	0x400000(4194304)	0x400	✔	1
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xfbc	0x401000(4198400)	0xca600	✔	1
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xfbc	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xfbc	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xfbc	0x52b000(5419008)	0x200	✔	1
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xfbc	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#12: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xfbc	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#12: c:\users\keecfmwgj\appdata\local\temp\51f0.exe	0xfbc / 0xfc8	0x77e201c4(2011300292)	-	✔	1

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\SystemID\PersonalID.txt	42 bytes	094c4931fdb2f2af417c9e0322a9716006e8211fe9017f671ac6e3251300acca	✖
C:\Users\kEecfMwgj\AppData\Local\bowsakkdestx.txt	562 bytes	a6ecf24713b62ba28ad4fdd406221134b49afb2b1d0092943dafbf8427b92cff	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	4
Module	47
File	16

Type	Count
Environment	1
Process	98
Registry	7
COM	1
-	2
Mutex	1
User	1
Window	1
-	3

Network Behavior

Type	Count
HTTP	1
HTTPS	1

Process #15: 51f0.exe

ID	15
File Name	c:\users\keecfmwgj\appdata\local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51f0.exe
Command Line	C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51F0.exe --Task
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 96115, Reason: Child Process
Unmonitor End Time	End Time: 105574, Reason: Terminated
Monitor duration	9.46s
Return Code	1073807364
PID	2808
Parent PID	3872
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	7
File	3
Environment	1

Process #17: taskeng.exe

ID	17
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {B59EC091-DBC7-4BE9-AC74-DC40D81A85AE} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 168463, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 279684, Reason: Terminated by timeout
Monitor duration	111.22s
Return Code	Unknown
PID	1288
Parent PID	4036
Bitness	64 Bit

Process #18: uaieedr

ID	18
File Name	c:\users\keecfmwgj\appdata\roaming\uaieedr
Command Line	C:\Users\kEecfMwgj\AppData\Roaming\uaieedr
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 169123, Reason: Child Process
Unmonitor End Time	End Time: 199021, Reason: Terminated
Monitor duration	29.90s
Return Code	0
PID	1336
Parent PID	1288
Bitness	32 Bit

Host Behavior

Type	Count
System	10
Module	46
File	4
Environment	1
Keyboard	2
-	1
Registry	20
Process	1

Process #20: 51f0.exe

ID	20
File Name	c:\users\keecfmwgj\appdata\local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51f0.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51F0.exe" --AutoStart
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 178763, Reason: Autostart
Unmonitor End Time	End Time: 186382, Reason: Terminated
Monitor duration	7.62s
Return Code	0
PID	1868
Parent PID	1632
Bitness	32 Bit

Host Behavior

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

Process #21: 51f0.exe

ID	21
File Name	c:\users\keecfmwgj\appdata\local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51f0.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51F0.exe" --AutoStart
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 185476, Reason: Child Process
Unmonitor End Time	End Time: 279684, Reason: Terminated by timeout
Monitor duration	94.21s
Return Code	Unknown
PID	2012
Parent PID	1868
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#20: c:\users\keecfmwgj\appdata\local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51f0.exe	0x750	0x400000(4194304)	0x400	✔	1
Modify Memory	#20: c:\users\keecfmwgj\appdata\local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51f0.exe	0x750	0x401000(4198400)	0xca600	✔	1
Modify Memory	#20: c:\users\keecfmwgj\appdata\local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51f0.exe	0x750	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#20: c:\users\keecfmwgj\appdata\local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51f0.exe	0x750	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#20: c:\users\keecfmwgj\appdata\local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51f0.exe	0x750	0x52b000(5419008)	0x200	✔	1
Modify Memory	#20: c:\users\keecfmwgj\appdata\local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51f0.exe	0x750	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#20: c:\users\keecfmwgj\appdata\local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51f0.exe	0x750	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#20: c:\users\keecfmwgj\appdata\local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51f0.exe	0x750 / 0x7e0	0x775901c4(2002321860)	-	✔	1

Dropped Files (209)

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\desktop\dshy6owctf.wav.neqp	10.27 KB	d0add83ec54489a6c58ba485bfa2c2f970b3305a35d7ea422b2f084ac1e95550	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\BqMJYpJI5- Av.csv.neqp	50.33 KB	3dac19d1db4685f8b801b3ac78121a3f049d72e1bb4de246b187abdacba16e94	✔
C:\Users\kEecfMwgj\Music\5_uaNmfND3.m4a.neqp	28.19 KB	48fd3ee4f0cf79b88d20dbc3c253e217f97d7a02e8b3b54386b014c99539d329	✔
C:\Users\kEecfMwgj\Pictures\5tjEDT2i8f.png.neqp	85.86 KB	2b548bd083d6d10a1c5b1632fc5b7663861d0a949d61f0c48aa2b6ee6f1eb5be	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\music\uz21xybo5jhjzq.mp3.neqp	59.37 KB	7ec1cafedf5ed9bd1a2ef28ed03b9ae8273edff5ee2df4c7cd9c869f7f0a9810	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\OvrR6bzipPtcj.docx.neqp	65.09 KB	176f6d8ebc37d77fa5a61394aa9809f7cad3948f0407807294db31fb5460e338	✔
C:\Users\kEecfMwgj\Music\u8_5OoZXD_BvAYx.wav.neqp	93.44 KB	b4872e0ab090d3a3dfb72bd37f27cd6a952b2dc3bbe587780ac101743300898b	✔
c:\users\keecfmwgj\contacts\administrator.contact.neqp	67.11 KB	0589c922ccaba6c7987ed88bb6d3d26fafd777352200a931bdf698d95543f2f9	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\ukOCS4.csv.neqp	56.24 KB	3fb9f1ff7a0b42b72ba37137d30803667156941c3ad37a547cfed897d379c835	✔
c:\users\keecfmwgj\pictures\xys3y_cu 624bscdh.bmp.neqp	60.09 KB	816d25ee80e83a6aa29d262a57fb592b5fc2246890786559046c357af9bf46d4	✔
c:\users\keecfmwgj\documents\ewxkzosyjkhnwpoz.docx.neqp	97.98 KB	7e8c4e7fa926ce5073608f7934366fdaeccaa39736f818c7b967554f1075d916	✔
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\dohgx0t l.jpg.neqp	37.67 KB	045d92a16de78b54cb5ab77996284cee6d69d455c9d1e8e8f02d841acdb497ea	✔
C:\Users\kEecfMwgj\Videos\bZ_MAu7.avi.neqp	29.32 KB	a69cdaf695dc8acfaba3db526547e4efaf737bdc6e4101de84516178f835bcf8	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\G_bTFo.odp.neqp	73.33 KB	c7fcffe6da5321f201b5cad712d4d104a1054d63236eed7d7a4b8848a09c2781	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\uYkNWJF11O37vr\Xw0 5hxcA.pptx.neqp	92.34 KB	817e9f64f100b4eb711f14cb603e566b8511a5d42915b8506f571c1ab07e9938	✔
C:\Users\kEecfMwgj\Documents\sU3qV4 mwzLmj.pps.neqp	22.43 KB	1ac82344c6443711e1ab35a893814bbd58bc41393b41dd460f5113fbd018bdb8	✔
c:\users\keecfmwgj\music\by0ls29bbpkIp631o9b.m4a.neqp	93.49 KB	1b4713efb38bba7ef00d4171db3222e2dbb4144c50aa65e18ac63cb11abcb71f	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\h9Ysje.pptx.neqp	48.19 KB	57017979cdf0ece4fb9973b6eff066db73a84bde37cf948fc6dce1e04624d767	✔
C:\Users\kEecfMwgj\Music\XqIXfBNrZqo t.mp3.neqp	48.39 KB	89a410c0f3aa7b9bcea17710cad7f6448ca5d65b97194639a2f868c2f7a39d38	✔
c:\users\keecfmwgj\desktop\upkIen56967zj.flv.neqp	41.72 KB	7ca9bc6375d215a2ecaead97a489ceb55fdf3caac83eabb60d847a97235522d8	✔
c:\users\keecfmwgj\documents\oeh1e-xhit5le6vwmu4m.xlsx.neqp	70.10 KB	2be60964729e3e7698d9148fe21d3766daf0c03caffac854b822bae7cb25f5b4	✔
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\1clt3s.jpg.neqp	60.07 KB	a8e765290ead6aea90a128c60ed158854d150bed8d3974d956cb99175c8f983c	✔
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\ghhedifjzwru5kmr.xlsx.neqp	72.65 KB	73fec684c1a6c0bc06ccac566c360b655d345e3a860acb11cfbcd9cfa67cd5d3	✔
C:\Users\kEecfMwgj\Pictures\dCjDLPjgt.png.neqp	20.07 KB	9205d3085b52dee0c9e3872097cc5b3d9d2ae45affe35ffcfa0a6d5dc7f84566	✔
c:\users\keecfmwgj\desktop\et8krykeuj73u.swf.neqp	24.49 KB	b077b4ed30cccee7435dedf2493ea9d39ce51c48f8e725539f82311b37f3073c	✔
C:\Users\kEecfMwgj\Videos\ups I7.mkv.neqp	50.34 KB	e73c01d3f4e170fb5dc671de42914c1973afcac3919bedef46518b3f10e0d14d	✔
C:\Users\kEecfMwgj\Music\n-diJdt93vqLXJ.wav.neqp	3.12 KB	c309bd448204da08748d872e7acf3fd0bfd686700eaafa043d704c9fa8bda356	✔
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\3trax2.xlsx.neqp	98.01 KB	69950c165ec0b9f5bdb3e79dd754d174afe788c5f2e4084294f5a13f55b967f8	✔
C:\Users\kEecfMwgj\Desktop\aM0hOBR8.wav.neqp	49.71 KB	3e5ba71b6cb632e12ae119980e72a86120476b8e11b096c07564367aa47d06d7	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\Ydwe3q9JyYweb_55_.ots.neqp	11.28 KB	71bca71399f874fa1d1b9a4954880af860bb4d9df7c1cb6549aff1774be22a82	✔

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\uYkNWJF11O37vr\RRM0O7_xCINdkabdTozN.xlsx.neqp	32.04 KB	9136f8bbb40b030da1a32e3856f1d41db3b131a598c39ee3b27134fda307d10a	✔
C:\Users\kEecfMwgj\Videos\80uy.mkv.neqp	22.95 KB	6cc5a4e8e249e3bfbaed056ddf1c1803464f7ff4004c5aae6eb08a2ba52ff06f	✔
C:\Users\kEecfMwgj\Documents\k7QtcBphpiUfUf6h4.rtf.neqp	80.09 KB	6ea3563e008269ecdd0f630cacea48c74bcf8970401dad252d281bd65e67e061	✔
c:\users\keecfmwgj\pictures\c8-qdtknhu0bjgmu.jpg.neqp	81.98 KB	a2ac9a1d0c1779549ac732ef64456735ebafa152d2d257a6160196a51fc4262c	✔
c:\users\keecfmwgj\music\dcxazqh.m4a.neqp	87.50 KB	40c616bbbb7a696fcbe40f83dd4cd8192abe8bc65f6c335b176d7b79c8b9e58c	✔
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\zt3a4flgawjyzt7r4xm.png.neqp	39.86 KB	3da8c5dfe9c18bf5830852a8c8b861e8a40bfe9b5de4aa6686cee6b7fe523bcb	✔
c:\users\keecfmwgj\videos\kcia6gopkg9.avi.neqp	24.69 KB	c7765038781cd3244fd96242b2971ac5fd05f0cba0e5cb93ad1158453732fe08	✔
C:\Users\kEecfMwgj\Videos\ueJknWfWvw.mkv.neqp	24.18 KB	da51d9fe5e748d055446e6e0db0db683d3fc369449c53ed54d992b849dccc3bd	✔
c:\users\keecfmwgj\documents\2vnukkmn.xlsx.neqp	45.08 KB	2792c50009dc1d367956d8c08654e1f69ed8acde53130297e2ebfb2d6d498a15	✔
C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLjTB7f\kduc8M4q0iGO.xlsx.neqp	47.83 KB	5591760e26390270da6aa832ff595201308d820fe37a0944ba71628d6c6baad2	✔
c:\users\keecfmwgj\videos__n93zziz9rny.mp4.neqp	99.42 KB	21a7a27731f45ff005c0a2003463ba695a779f5dff6ffe7a5c645306d4cdc4f1	✔
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\ruec4u8cn1u.jpg.neqp	8.96 KB	73b5be1ea2ec586b130560f88ba4383dd27738e25fe528852fceafaef6585be3	✔
c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.neqp	467 bytes	64d20dc7145a6014bd955d9eadc02afd318577b329bbf0da6e786553a48aaa3c	✔
c:\users\keecfmwgj\desktop\twnoq6e1v6eeljtb7f\djfpsjtvq\gxuwpj.csv.neqp	15.36 KB	cc4ebed9b5ba507180e3d3cd89025f7ca141e35479cc40edff9ffeada92f5b1f	✔
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\oy4eruo53oz.rtf.neqp	47.26 KB	71f582b5d18272207699f1b1cb74cad4207a8d12a8a1c4ea9a956bcbad861e64	✔
C:\Users\kEecfMwgj\Videos\bGt49HOvptpF2AsDKl.mkv.neqp	9.61 KB	67706071ac7a92d98c7dfd1139f0d42e0e60ebf41e6c6cff335a84a42fb76cfc	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIRleTh vq1qbRJ-L\aZ2HX2t0pm3.ots.neqp	27.57 KB	26fb40f54a2f8364cefc330f291bcc0bcdccba819189fb77737ebba0b5d6dc31	✔
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\oepl7unfz0.jpg.neqp	38.08 KB	b9687ffc3fea913f4ca3680d3868788484cad0bdd3b68b29eb6b2124c57aab7a	✔
C:\Users\kEecfMwgj\Documents\G8oUQ7rKtGSWcT.ots.neqp	34.10 KB	e5de7541f322ea5b1d436fc00a4b1f7b5eda86c7752c1a3afa31b5b557edeee0	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIRleTh vq1qbRJ-L\oV6zFBL.rtf.neqp	17.15 KB	3d8fa947bdcd9f309e67ddc08a696ef5915ef40981a17406e783360ed9318ec3	✔
c:\users\keecfmwgj\desktop\tkaxolhrl8qedbn.gif.neqp	75.29 KB	ca76b849fe783671d86d396fedf8eb52aaa34c546204e7042a655e28e1de003d	✔
c:\users\keecfmwgj\videos\qg8i9g0tihejna tr3l.flv.neqp	91.53 KB	19f5f2dd29bbcfeade1d9b7c03d269aafacf42714f20ea705c2cec42f7b45070	✔
c:\users\keecfmwgj\videos\fmxha_w4eke5pf8l.mp4.neqp	84.52 KB	159d189b403545fc73c2eae42d91ba59fe66190918e6d1fe6c552f12cc3bd6ef	✔
c:\users\keecfmwgj\favorites\msn websites\msn sports.url.neqp	467 bytes	5fff09985946ab4c541e335925f853ca8fb5fd8c3b034af584c3e38fc8a0cab7	✔
c:\users\keecfmwgj\documents\koomr.pptx.neqp	65.97 KB	ba82cca3e24aea86e0af29a0a3b7d2ff300678bd6bea1faec72cf1a9104319d4	✔
c:\users\keecfmwgj\pictures\byf8cf9eozrq2jwpt66.gif.neqp	7.79 KB	a71b66c0c077595753fbbb61c893faf0b0a65bd98411af80d1ccac4ef4249360	✔
c:\users\keecfmwgj\favorites\msn websites\msn.url.neqp	467 bytes	b8ee614ea2d827c73ec11b98bf3bc274c5a8d0ed0635b045b0ee714389265bfc	✔

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\Videos\n 7DfguJMJ.mp4.neqp	32.55 KB	afb02b0290206b01ccee45d8f98f2e35ae219d5640070696d894004f615d21d7	✔
C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Home.url.neqp	467 bytes	44f4ea2126b623bdc8ba9736084c369a662330ca25805b04ee3fdb8ee2407463	✔
c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.neqp	467 bytes	48d258fec956c0dd3d0bf3b53751517b045f556999a012dceaf0f83b7fa25084	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\c0Y tBs zGXD9sK\qJTFnnuSQ.ppt.neqp	83.41 KB	fc41fa34a2680ceba80fcf0f1ea1baf337651b613f5f9a88d5b6b92555dba15e	✔
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\jtbbgg - ujwe3.bmp.neqp	45.80 KB	46ccfbb7da1962ccd7fb5c9ed1be4faaa832dda81d436206bd12402e711090d5	✔
C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\NECDkoymaUw.png.neqp	62.52 KB	ba1278861d1e551337fb56b14bfd9669307bb824b390a2e166fec8a6d243e56c	✔
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\6ayirleth vq1qbrj-l\gbpqlruev5tl.pptx.neqp	17.26 KB	56bf3749556649cb55983f5251f487924d12ef6bd1a4eed31c4dfb2e8d161c20	✔
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\vztrk63idaphpsstgre.pptx.neqp	89.56 KB	321f7cc6122278e81286764c399ae72ba41a03086f09bc87cb0b81cc9b1659d1	✔
c:\users\keecfmwgj\videos\gfravduy7lom.swf.neqp	34.41 KB	6c78d46432f8cd84b5e81d4bfc77da4ff826432890a219a51f0e76a3b91fd164	✔
C:\Users\kEecfMwgj\Music\qYyGPLt6OoKeyh2R.m4a.neqp	74.98 KB	74ae57d78ad228016874fc29ad90fb35a82b35579c3b71f36dc4c44ff70343d4	✔
C:\Users\kEecfMwgj\Desktop\VuYJSL8GFd0.mp3.neqp	27.13 KB	a8caa46758c82c1f3a67808e3d5559d0986c83e2129d318ca4df5b15d83df2ac	✔
C:\Users\kEecfMwgj\Music\HAyp2zHURXEkt5y6c.mp3.neqp	58.05 KB	24bcff8f996c37406034de292c0a2a755a43cd9c0bd8da0862a8921215e46322	✔
C:\Users\kEecfMwgj\Videos\OJNEj2xIV52LVtvj-s0.flv.neqp	72.87 KB	0bc3226ae404d35c1ff34b10c23d0e64c6c284f52da31cff5d7e17e9b402a27b	✔
C:\Users\kEecfMwgj\Desktop\aFVf9.swf.neqp	22.38 KB	3c6db4dbc82aa01319e8bbb9d757161c39b9b0091117e89a8fd54e3703f212dd	✔
C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\qf XQc2cUy7GFzzlXBjR.m4a.neqp	24.60 KB	e13cf3f73f060f9338b866fd39241c041aa3b5fc9ac8297e67dc710adac317ff	✔
c:\users\keecfmwgj\music\hvolbk.mp3.neqp	91.71 KB	0956fed7cbf1d6ec29a544962a39785c55d148970ada824be469061d984bbf91	✔
c:\users\keecfmwgj\desktop\eysf0phwcb.mp3.neqp	53.65 KB	55ef6f13bdf69ae788b2098e2069c3adcb83d85ad7b5f658dbaa579aed79e6fd	✔
C:\Users\kEecfMwgj\Desktop\NBxo5Eh8J.swf.neqp	17.97 KB	e360ad4c59d573dc334fe9d4b972302d4bf9c14b6be87d81a669eb72798717d0	✔
C:\Users\kEecfMwgj\Videos\N hQ2zMqJr.flv.neqp	58.28 KB	cd47f9c4b3b6c33f29b81c6921b25391f98a870cf9a153639d089a9c182aa4b6	✔
c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\djfpsjtvq\-6sm.bmp.neqp	65.52 KB	492ce60054c78e32c636cc34c1200333e8d3f98158adb5d65dcb29d19b450977	✔
C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Gallery.url.neqp	467 bytes	850027588e455fc72023a04b7b8118a072e7a7c23558d653ccdc537642de9bfb	✔
C:\Users\kEecfMwgj\Music\YiJlu.mp3.neqp	49.57 KB	db2786ef7701c64a6601da55979530c685b3db423fd1683f668c92a642ec9ec8	✔
C:\Users\kEecfMwgj\Documents\SZzcxiUb3S1y0E.pptx.neqp	55.67 KB	b59c174297e759d859a2d26e051614064025fc6555037d2ec62c9f38204426d3	✔
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\rx-ru.png.neqp	49.89 KB	cc36568442ee4e7a01af47d4d80bc015aa31cb91929ed64c8436dd784cd16e98	✔
c:\users\keecfmwgj\pictures\nqugwix.bmp.neqp	58.94 KB	ecbe7bdad612287562bbe873b9830e1bebf10fef9f568e15b682c69b2f0555f2	✔
C:\Users\kEecfMwgj\Pictures\dwHz _UcKn2C.bmp.neqp	68.60 KB	8eb549c551f1dac7873d96a352145b2374928f20aa047a5ee20f8784f97329bc	✔
c:\users\keecfmwgj\videos\jcuukzkpdwtrtf.flv.neqp	65.06 KB	e3fe6bcd13e044be02878ddf0e1ffc43a730bf30547b71b4e75c7d319f1d422b	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\videos\osw75x o0982bw.swf.neqp	17.20 KB	e5eb5b1a0bbd8b059b4e49a573766f807b01d3efb2adf49e130bfbc09b5f5ede	✔
c:\users\keecfmwgj\videos\ompo2s.flv.neqp	9.55 KB	363034c912bbaaba361e7d0f49bb7e7fd73c9e171a6821aaccfb549e78dd6a19	✔
c:\users\keecfmwgj\music\epp3ouzeazkkjj5hj.wav.neqp	82.14 KB	47126b13c5ab1b98c030985425b4b63927954ade768ddbb06fa10cab81942d68	✔
c:\users\keecfmwgj\favorites\microsoft websites\ie add-on site.url.neqp	467 bytes	9304907895a74fcec35934937a066d8792ca22dc0bd0733d6a4a4de8e48af55d	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\c0Y tBs zGXD9sK\Yz_Q1.doc.neqp	15.96 KB	a57a769c198326295c7733e10e8b78c2e9e91abffba02bbcfa182e137889838b	✔
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\s7lh3hxtittmcvgh\r6fjlezzg_wtj.ots.neqp	68.20 KB	293b437fdbeb5f42575519f649927086e0c6cf3389a5f81d05de2a6ea6ff63c0	✔
c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\iyl6m - whjjeo.wav.neqp	41.00 KB	5ec80fca38a6bb8a331218c2cf0a0831b8b02354d7c1ca79d862470daac9c6ff	✔
C:\Users\kEecfMwgj\Documents\FU2 nzV-k.pdf.neqp	33.53 KB	f79da05e1456bc0c17153e35454bac68b5d89e1f77a139d70058d8cfa69325e7	✔
C:\Users\kEecfMwgj\Desktop\gwqS.gif.neqp	23.29 KB	b9593847de0c67f0f23ec0556fc86327530f78034d9aa3ed88e71a9542578ed4	✔
c:\users\keecfmwgj\music\d7illvxbgi6q.wav.neqp	28.39 KB	e5fd3efa78dd1245625130a2c4e50ddb04f259cefb82c10d1d91fc231af1f5cb	✔
c:\users\keecfmwgj\favorites\links\web slice gallery.url.neqp	560 bytes	1890500ca302d79185164dc7bb18c58ea70feb885d28929d8aeab831ba3cfe72	✔
c:\users\keecfmwgj\pictures\ote5jpyt.jpg.neqp	74.38 KB	8aa22e70515ff35e039bf99cbcc644f7e9f36390b1e4f5c3d1f356e18ef1927b	✔
C:\Users\kEecfMwgj\Desktop\AQRFNBZ8zX.jpg.neqp	13.37 KB	2b4e417e5594a5e9aec3322803aed47fbfb41b7f11033ea38ccd938c91d6394a	✔
c:\users\keecfmwgj\music\uftb9wa27mlfv.mp3.neqp	7.51 KB	8fc1ae1a523131741fc18ef2fcffcc5dd174a60516253c38dfff5be2e648f06b	✔
C:\Users\kEecfMwgj\Desktop\h5j527Mxht9SX2raeS80.mp3.neqp	95.32 KB	e8e572570459fbdb3170b2ce002c7b45c40de0b3fbff5d4f88913857f0cb0887	✔
c:\users\keecfmwgj\music\rrbusch3n2s3k7tf26.wav.neqp	61.13 KB	8df32ebbf3ecfca140e3d62b435e229cdfa858736aeae633ef5a9670f573672c	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\S7LH3hXtiTTmcVgH\VDXnqC 6DK_84Fuegb.xlsx.neqp	3.14 KB	0876ae69b6af6791dbb1cbbb657eaa814d410767e44037931f859eeb8b46fada	✔
C:\Users\kEecfMwgj\Documents\r5XNSimbuw.xlsx.neqp	4.85 KB	c82112f4307f5b2604c9c84dbd70b15271aba5fb58e8a2114651a511e597b442	✔
C:\Users\kEecfMwgj\Music\BBqFu3hstVTMPJkSfOH.mp3.neqp	21.01 KB	c8849d3c3d667761e66594bda703eb352ac1d6864a18a6e014d62257a085b618	✔
c:\users\keecfmwgj\videos\8nyqrh805h9- og.avi.neqp	56.58 KB	3b1568f911b06cc6280dba3a7d8e960051d1787c96ebfa771db9493543814d46	✔
c:\users\keecfmwgj\favorites\windows live\get windows live.url.neqp	467 bytes	ab00ee5292b3701499d7ade179fc704fc77fa4952b624733099d17ca41977d8f	✔
C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Autos.url.neqp	467 bytes	4a1c4e2fb3046808fb3142a9c3bed1a4ede0167c422e708cb11eba27e4996182	✔
C:\Users\kEecfMwgj\Documents\3r0MOWhcIDm.pptx.neqp	14.35 KB	c33053fa94a314a88b45f93965896e21e6b44b425d570aa0f7360a9b50204bac	✔
c:\users\keecfmwgj\music\xvszdq6io_y8wjxlgib.wav.neqp	13.62 KB	e779e406f7fea68e80a0a124b01e527bbc9fdd427e3cbbc6c1c0a2c291038621	✔
C:\Users\kEecfMwgj\Documents\A8Ch.xlsx.neqp	59.82 KB	6f22e0c30545bcd7e6612186a068b8fd5fa1966b11105e20af5dde0cb76998af	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\3BEbvfVE1d-gqz.doc.neqp	23.06 KB	74b49a04f3a9b50228f8099dddcf56876425608d7ddb84431dc1f0f18997a25c	✔
C:\Users\kEecfMwgj\Music\mqLZS9o6DtidQLz.m4a.neqp	22.91 KB	6211a386dfd7c018509aeb638c471d55dfc7fcc628c81b63d88fd2ae9ef02db9	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\fcf5zjaps1nelg.csv.neqp	84.38 KB	2761b6f1806fe4086dca316c39d88dc686f38e34bee58792a8be9b6206265104	✔
c:\users\keecfmwgj\favorites\windows live\windows live spaces.url.neqp	467 bytes	ccf6412efb5a4c33bf466106b5b121ffac32bf8c826361ca26a96ccb514482da	✔
C:\Users\kEecfMwgj\Desktop\tmPl-YXq5d584Uoy2.png.neqp	13.37 KB	bd323b859fb2b00b57d54e833d77b7342eae3900ea14271754a55268b1cff16d	✔
C:\Users\kEecfMwgj\Videos\hnzlwvtZPb.avi.neqp	3.77 KB	a4ab2d45e4723f33293ea7c5d2f0d5f7b31e05483b2a7b8c1032e524cd3e863f	✔
c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\djfpsjtvq\fojpf2zsdfusywc2q.m4a.neqp	63.31 KB	169be5f4c885cf368e95c0921c1b3c260edc6a53db7c2aa01219e87fb1a98a9a	✔
c:\users\keecfmwgj\music\ttf5tme9.mp3.neqp	98.36 KB	3554f260939e76db8cb830d0776ec42f842ad4ee04670c4eadb27b7932e8a691	✔
c:\users\keecfmwgj\videos\wb qjymk2xb5.avi.neqp	36.25 KB	8de68e17d891d138c353abe776aa366037563d271c1cbd2a6c830ab4e15bb6be	✔
C:\Users\kEecfMwgj\Desktop\2Hs3CvzmY0a1.doc.neqp	27.49 KB	3a225bbb9d296055883fcacdb26da4ad30084bc502af1b29a4300ceec2adf1a0	✔
c:\users\keecfmwgj\favorites\msn websites\msnbc news.url.neqp	467 bytes	6e2a2716c98bfa4d1d069eb4208453a1b8ad42ddec3a56d63e575534c7c184c3	✔
C:\Users\kEecfMwgj\Music\LE8AEqMT.wav.neqp	63.40 KB	96e173d264e5ba34dc80ff6b87000e8d10f8342c605457f5627fdf1b6487a32a	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIRIeTh vq1qbRJ-L\jSVU\rH2o4l1w9Tc5d.pptx.neqp	53.88 KB	c597cd6f1f9308bf48404592907044d34cf1e3e223eb16dd845f970e5de07530	✔
c:\users\keecfmwgj\desktop\rn0bvg.png.neqp	31.85 KB	be138077b206b61d13cce13cdba14ece17f953edb48aa644dd9e85a36231b997	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\uYkNWJF11O37vr\Wx5NaRQ.xlsx.neqp	50.81 KB	13332c8b72974d633550cc9aca5187d29015c1f6b4ee8864acb00bcdd2546959	✔
c:\users\keecfmwgj\desktop\zsmkkxcply mwj1j 8.mp3.neqp	33.58 KB	da2d6169c1b208052fc51b3a40aa6bebe3aec9885fb99a973a5494650df0f122	✔
C:\Users\kEecfMwgj\Music\UHzfZtepjKuO.wav.neqp	50.11 KB	a751c5c624690372298d230103dedfd50a4da8de2e23e7e9a198c145cbebdd39	✔
C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\fDxmHCHVp_.png.neqp	99.90 KB	bc916ad232998f1b70846dc06ca651d0fca5f44ed09e8d8a29c46b6ee2b04b16	✔
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\71py6.ots.neqp	83.52 KB	287779e5dfd1218691ba2781bf5fd28dd21b376eb021d0ec97614d7ab1f9a72c	✔
c:\users\keecfmwgj\documents\gcnsphuvaisovbzltws.xlsx.neqp	31.70 KB	847b16daf286d03d2b83c1e9acbd572e9b042eec75090dbd3f5e26ea491aa19a	✔
C:\Users\kEecfMwgj\Pictures\WzLSzXw7M.bmp.neqp	42.94 KB	6b9050c2b31a85b92b17fc6bd368e548d1cc8168d8d825c7f65c6a06b66def66	✔
C:\Users\kEecfMwgj\Pictures\U4sW0p.gif.neqp	10.32 KB	4a912259c7791ad1f1f882122a03873077afc425682e9ac77947abc4ca7a523d	✔
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\uyknwjf11o37vr\gr566la_hbzp.docx.neqp	42.84 KB	21c3e5b485b6f8208ad1e0de4d4d7b5345b837e02ba25384e48d3263ec437659	✔
c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\dxid.mp3.neqp	22.90 KB	a357b518b2deb0a119306d20845d6a40ba27588ed5d68627f3013896601f3d5f	✔
c:\users\keecfmwgj\favorites\microsoft websites\microsoft store.url.neqp	468 bytes	62478c1149ce37a1c7ff2175d845543c5120f9b782c7a576b534e58c11c574aa	✔
C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\szqw0q07Ao\gLy0rCq95A6.wav.neqp	33.43 KB	91167c51c66f9932413cae719b56ceff7b2149e6e969c3764d5accd706f40b01	✔
-	1.09 KB	726c52b586acd544bd1ae75afb1ed3609de03b2c50c687813c8d8d393ab85272	✖
c:\users\keecfmwgj\favorites\msn websites\msn money.url.neqp	467 bytes	b5e9794486c8db092ad52bea012ff32a296dfd18e51edef241ad3eea5c073eb1	✔
c:\users\keecfmwgj\desktop\f1f3a2atwy iz-.png.neqp	88.68 KB	9f0dad6e27902e2b184404e1f9fe314f9dba1694133b6f12b0dc437d5f677e5f	✔

File Name	File Size	SHA256	YARA Match
c:\users\keecfmwgj\music\dkfwau.mp3.neqp	72.19 KB	445de135beb94766fdd2af738bb2077505e7d0de7a87901643c632bdfaed5bcd	✔
C:\Users\kEecfMwgj\Documents\p5HGkq_lz1hzZZQ1QzX\7lvhY-.pdf.neqp	80.98 KB	f7d8dccfe4d3893389f55299ef95ded2a028256236dd216df0db3fc2c1ff4bea	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\uYkNWJF11O37vr\FvaFjmImszyo741.ots.neqp	56.33 KB	04a349da27f3c1539a75910966ef4ed9bb69339103583eb3d49f3d0527caf123	✔
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\v1fv6rf5h82idznir.png.neqp	64.45 KB	836d1278f41fb5bbc28f1498d29b3c531e4332be334da0ffc843a855a5c7d38a	✔
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\pkdosd r3vyy2rn3diw.png.neqp	80.64 KB	c38799068eb8e81038c9e1328dce78b9df70d3b1ebcbe16ac001292df440cbd4	✔
C:\Users\kEecfMwgj\Desktop\k5szpLuntD.wav.neqp	99.46 KB	34caa77a1be370f740391889ed59bd4c2e73b95658bd7e4b18e0a82a07057e21	✔
C:\Users\kEecfMwgj\Documents\FfstE6t9XHw9p.docx.neqp	74.18 KB	56c8bcb5bdded5f1c23de1ce4e1088e62023faeaa0b9cc41b1ff59dbf1681441	✔
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\gh3ediyqvyh.jpg.neqp	52.15 KB	ca9fb363d85bfcb3518f7127a8e60b7c2160a07597f58c2edd23a59b2174e7b0	✔
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\c0Y tBs zGXD9sK\pe4_1B.pptx.neqp	57.68 KB	df5f20fdb79d202433ff69627574ddb65bb942218a99ab6b7877915fe8d782e9	✔
C:\Users\kEecfMwgj\AppData\LocalLow\Sun\Java\Deployment\deployment.properties.neqp	1.04 KB	d3f588bedc7cef1a5219cfe51445c728046487b28a47f3c7cb1b534af3c95f9e	✔
c:\users\keecfmwgj\documents\outlook files\franc@gdllo.de.pst.neqp	265.33 KB	222035d3ac676ba3e1166a63185e36bfc46aa3595e5f709b3519f3fd736c502d	✔
C:\Users\kEecfMwgj\Videos\qo qbMr5VasZaX.flv.neqp	38.45 KB	1258565caf500684fcbe9109eaacc764bb163eb8458fae8285073cb107e98b55	✔

Reduced dataset

Host Behavior

Type	Count
System	290
Module	184
File	2206
Environment	1
Process	53
Registry	4
Mutex	1
User	1
Window	1
-	4

Network Behavior

Type	Count
HTTP	1
HTTPS	1

Process #23: explorer.exe

ID	23
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 198010, Reason: Injection
Unmonitor End Time	End Time: 279684, Reason: Terminated by timeout
Monitor duration	81.67s
Return Code	Unknown
PID	1632
Parent PID	1336
Bitness	64 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#18: c:\users\keecfmwgj\appdata\roaming\uaieedr	0x53c	0x2610000(39911424)	0x5000	✔	1
Modify Memory	#18: c:\users\keecfmwgj\appdata\roaming\uaieedr	0x53c	0x2760000(41287680)	0x16000	✔	1
Create Remote Thread	#18: c:\users\keecfmwgj\appdata\roaming\uaieedr	0x53c	0x2760000(41287680)	-	✔	1

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\3024.exe	749.50 KB	5d1b0a63577d637eecfd075abf530d62b2c913c98b2bd38e116ffb8c21e5dd13	✖
C:\Users\KEECFM~1\AppData\Local\Temp\3024.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	12
Process	17656
System	4712
Mutex	1
Registry	3
COM	2
User	1
File	6

Network Behavior

Type	Count
HTTP	6
HTTPS	1
TCP	1

Process #24: 3024.exe

ID	24
File Name	c:\users\keecfmwgj\appdata\local\temp\3024.exe
Command Line	C:\Users\KEECFM~1\AppData\Local\Temp\3024.exe
Initial Working Directory	C:\Users\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 224789, Reason: Child Process
Unmonitor End Time	End Time: 228994, Reason: Terminated
Monitor duration	4.21s
Return Code	0
PID	1284
Parent PID	1632
Bitness	32 Bit

Host Behavior

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

Process #25: 3024.exe

ID	25
File Name	c:\users\keecfmwgj\appdata\local\temp\3024.exe
Command Line	C:\Users\KEECFM~1\AppData\Local\Temp\3024.exe
Initial Working Directory	C:\Users\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 226388, Reason: Child Process
Unmonitor End Time	End Time: 261146, Reason: Terminated
Monitor duration	34.76s
Return Code	0
PID	1380
Parent PID	1284
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#24: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x558	0x400000(4194304)	0x400	✔	1
Modify Memory	#24: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x558	0x401000(4198400)	0xca600	✔	1
Modify Memory	#24: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x558	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#24: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x558	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#24: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x558	0x52b000(5419008)	0x200	✔	1
Modify Memory	#24: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x558	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#24: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x558	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#24: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x558 / 0x55c	0x775901c4(2002321860)	-	✔	1

Host Behavior

Type	Count
System	4
Module	45
File	4
Environment	1
Process	26
Registry	2
COM	1

Network Behavior

Type	Count
HTTPS	1

Process #26: uaieedr

ID	26
File Name	c:\users\keecfmwgj\appdata\roaming\uaieedr
Command Line	C:\Users\kEecfMwgj\AppData\Roaming\uaieedr
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 234328, Reason: Child Process
Unmonitor End Time	End Time: 279684, Reason: Terminated by timeout
Monitor duration	45.36s
Return Code	Unknown
PID	1732
Parent PID	1288
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	7
File	3
Environment	1

Process #30: 3024.exe

ID	30
File Name	c:\users\keecfmwgj\appdata\local\temp\3024.exe
Command Line	"C:\Users\KEECFM~1\AppData\Local\Temp\3024.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 259500, Reason: Child Process
Unmonitor End Time	End Time: 268841, Reason: Terminated
Monitor duration	9.34s
Return Code	0
PID	1932
Parent PID	1380
Bitness	32 Bit

Host Behavior

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

Process #31: 3024.exe

ID	31
File Name	c:\users\keecfmwgj\appdata\local\temp\3024.exe
Command Line	"C:\Users\KEECFM~1\AppData\Local\Temp\3024.exe" --Admin IsNotAutoStart IsNotTask
Initial Working Directory	C:\Users\KEECFM~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 266118, Reason: Child Process
Unmonitor End Time	End Time: 279684, Reason: Terminated by timeout
Monitor duration	13.57s
Return Code	Unknown
PID	1260
Parent PID	1932
Bitness	32 Bit

Injection Information (8)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#30: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x7ac	0x400000(4194304)	0x400	✔	1
Modify Memory	#30: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x7ac	0x401000(4198400)	0xca600	✔	1
Modify Memory	#30: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x7ac	0x4cc000(5029888)	0x3dc00	✔	1
Modify Memory	#30: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x7ac	0x50a000(5283840)	0x6400	✔	1
Modify Memory	#30: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x7ac	0x52b000(5419008)	0x200	✔	1
Modify Memory	#30: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x7ac	0x52c000(5423104)	0xa400	✔	1
Modify Memory	#30: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x7ac	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#30: c:\users\keecfmwgj\appdata\local\temp\3024.exe	0x7ac / 0x534	0x775901c4(2002321860)	-	✔	1

Host Behavior

Type	Count
System	3
Module	46
File	5
Environment	1
Process	26
Registry	2
COM	1
-	2

Network Behavior

Type	Count
HTTPS	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d0add83ec54489a6c58ba485bfa2c2f970b3305a35d7ea422b2f084ac1e95550	c:\users\keecfmwgj\desktop\dshy6owctf.wav.neqp, C:\Users\kEecfMwgj\Desktop\DsHy6owCtF.wav.neqp	Dropped File	10.27 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ef1682f582ae280b5ab2d4fc2c1d3fb28c312751c6697577f28f7663dcc8cd07	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
3dac19d1db4685f8b801b3ac78121a3f049d72e1bb4de246b187abdacba16e94	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\BqMJYpJI5- Av.csv.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\bqmjypji5-av.csv.neqp	Dropped File	50.33 KB	application/octet-stream	Access, Create, Write	MALICIOUS
48fd3ee4f0cf79b88d20dbc3c253e217f97d7a02e8b3b54386b014c99539d329	C:\Users\kEecfMwgj\Music\5_uaNmfND3.m4a.neqp, c:\users\keecfmwgj\music\5_uanmfnd3.m4a.neqp	Dropped File	28.19 KB	application/octet-stream	Access, Create, Write	MALICIOUS
2b548bd083d6d10a1c5b1632fc5b7663861d0a949d61f0c48aa2b6ee6f1eb5be	C:\Users\kEecfMwgj\Pictures\5tjEDT2i8f.png.neqp, c:\users\keecfmwgj\pictures\5tjedt2i8f.png.neqp	Dropped File	85.86 KB	application/octet-stream	Access, Create, Write	MALICIOUS
7ec1cafedf5ed9bd1a2ef28ed03b9ae8273edff5ee2df4c7cd9c869f7f0a9810	c:\users\keecfmwgj\music\uz21xybo5jhjzq.mp3.neqp, C:\Users\kEecfMwgj\Music\UZ21XYbO5jhJZq.mp3.neqp	Dropped File	59.37 KB	application/octet-stream	Access, Create, Write	MALICIOUS
176f6d8ebc37d77fa5a61394aa9809f7cad3948f0407807294db31fb5460e338	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\OvrR6bzipPtcj.docx.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\ovrr6bzipptcj.docx.neqp	Dropped File	65.09 KB	application/zip	Access, Create, Write	MALICIOUS
89e078fb68353108924d444daac30761e2f3a17b0ac7ded2c9f30334eaff9646	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
7fe6e06a41e7da91a8d71068fdbfa3d39310b0fe1d2ace3b6651b92c1bfd982c	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
b4872e0ab090d3a3dfb72bd37f27cd6a952b2dc3bbe587780ac101743300898b	C:\Users\kEecfMwgj\Music\u8_5OoZXD_BvAYx.wav.neqp, c:\users\keecfmwgj\music\u8_5oozxd_bvayx.wav.neqp	Dropped File	93.44 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3445e80809f2a260a7d9ad20ef528840976968ee43ba52a63abba0a56381aec0	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
0589c922ccaba6c7987ed88bb6d3d26fafd777352200a931bdf698d95543f2f9	c:\users\keecfmwgj\contacts\administrator.contact.neqp, C:\Users\kEecfMwgj\Contacts\Administrator.contact.neqp	Dropped File	67.11 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3fb9f1ff7a0b42b72ba37137d30803667156941c3ad37a547cfed897d379c835	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\ukOCS4.csv.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\ukocs4.csv.neqp	Dropped File	56.24 KB	application/octet-stream	Access, Create, Write	MALICIOUS
816d25ee80e83a6aa29d262a57fb592b5fc2246890786559046c357af9bf46d4	c:\users\keecfmwgj\pictures\xys3y_cu624bscdh.bmp.neqp, C:\Users\kEecfMwgj\Pictures\XyS3y_CU 624bSCdh.bmp.neqp	Dropped File	60.09 KB	application/octet-stream	Access, Create, Write	MALICIOUS
7e8c4e7fa926ce5073608f7934366fdaeccaa39736f818c7b967554f1075d916	c:\users\keecfmwgj\documents\ewxkzosyjkhnwpoz.docx.neqp, C:\Users\kEecfMwgj\Documents\ewxkZosyJKHNwpoz.docx.neqp	Dropped File	97.98 KB	application/zip	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
045d92a16de78b54cb5ab77996284cee6d69d455c9d1e8e8f02d841acdb497ea	c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\dohgx0t l.jpg.neqp, C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\dohGx0T L.jpg.neqp	Dropped File	37.67 KB	image/jpeg	Access, Create, Write	MALICIOUS
a69cdaf695dc8acfaba3db526547e4efaf737bdc6e4101de84516178f835bcf8	C:\Users\kEecfMwgj\Videos\bZ_MAu7.avi.neqp, c:\users\keecfmwgj\videos\bz_mau7.avi.neqp	Dropped File	29.32 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c7fcffe6da5321f201b5cad712d4d104a1054d63236eed7d7a4b8848a09c2781	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\G_bTFo.odp.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\g_btfo.odp.neqp	Dropped File	73.33 KB	application/zip	Access, Create, Write	MALICIOUS
817e9f64f100b4eb711f14cb603e566b8511a5d42915b8506f571c1ab07e9938	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\uYkNWJF11O37vr\Xw05hxcA.pptx.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\uyknwjf11o37vr\xw0 5hxca.pptx.neqp	Dropped File	92.34 KB	application/zip	Access, Create, Write	MALICIOUS
8ed6dfe9d6815dc22c326c308b7402ab97af5b76b37a4ce7f76a6793e8642615	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
1ac82344c6443711e1ab35a893814bbd58bc41393b41dd460f5113fbd018bdb8	C:\Users\kEecfMwgj\Documents\sU3qV4 mwzLmj.pps.neqp, c:\users\keecfmwgj\documents\su3qv4 mwzlmj.pps.neqp	Dropped File	22.43 KB	application/octet-stream	Access, Create, Write	MALICIOUS
1b4713efb38bba7ef00d4171db3222e2dbb4144c50aa65e18ac63cb11abcb71f	c:\users\keecfmwgj\music\by0ls29bbpklp631o9b.m4a.neqp, C:\Users\kEecfMwgj\Music\By0ls29bBPKLp631O9b.m4a.neqp	Dropped File	93.49 KB	application/octet-stream	Access, Create, Write	MALICIOUS
57017979cdf0ece4fb9973b6eff066db73a84bde37cf948fc6dce1e04624d767	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\h9Ysje.pptx.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\h9ysje.pptx.neqp	Dropped File	48.19 KB	application/octet-stream	Access, Create, Write	MALICIOUS
89a410c0f3aa7b9bcea17710cad7f6448ca5d65b97194639a2f868c2f7a39d38	C:\Users\kEecfMwgj\Music\XqIXfBNrZqo t.mp3.neqp, c:\users\keecfmwgj\music\xqixfbnrzqo t.mp3.neqp	Dropped File	48.39 KB	application/octet-stream	Access, Create, Write	MALICIOUS
7ca9bc6375d215a2ecaead97a489ceb55fdf3caac83eabb60d847a97235522d8	c:\users\keecfmwgj\desktop\upklen56967zj.flv.neqp, C:\Users\kEecfMwgj\Desktop\UpkLen56967zJ.flv.neqp	Dropped File	41.72 KB	video/x-flv	Access, Create, Write	MALICIOUS
420d80df5d3d75e956e079719b6c0ce0303406f1b513d136c1a5efd4686a5840	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
2be60964729e3e7698d9148fe21d3766daf0c03caffac854b822bae7cb25f5b4	c:\users\keecfmwgj\documents\oeh1e-xhit5le6vwmu4m.xlsx.neqp, C:\Users\kEecfMwgj\Documents\OeH1e-xhIt5le6VWmu4M.xlsx.neqp	Dropped File	70.10 KB	application/zip	Access, Create, Write	MALICIOUS
a8e765290ead6aea90a128c60ed158854d150bed8d3974d956cb99175c8f983c	c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\1clt3s.jpg.neqp, C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\1Clt3S.jpg.neqp	Dropped File	60.07 KB	image/jpeg	Access, Create, Write	MALICIOUS
73fec684c1a6c0bc06ccac566c360b655d345e3a860acb11cfbcd9cfa67cd5d3	c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\ghhedifjzwru5kmr.xlsx.neqp, C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\GhhediFJZwrU5kMr.xlsx.neqp	Dropped File	72.65 KB	application/zip	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9205d3085b52dee0c9e3872097cc5b3d9d2ae45affe35ffcfa0a6d5dc7f84566	C:\Users\kEecfMwgj\Pictures\dCjDLPjgt.png.neqp, c:\users\keecfmwgj\pictures\dcjdlpjgt.png.neqp	Dropped File	20.07 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b077b4ed30cccee7435dedf2493ea9d39ce51c48f8e725539f82311b37f3073c	c:\users\keecfmwgj\desktop\et8krykeuj73u.swf.neqp, C:\Users\kEecfMwgj\Desktop\ET8KrYKeuj73U.swf.neqp	Dropped File	24.49 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
e73c01d3f4e170fb5dc671de42914c1973afcac3919bedef46518b3f10e0d14d	C:\Users\kEecfMwgj\Videos\upsI7.mkv.neqp, c:\users\keecfmwgj\videos\upsi7.mkv.neqp	Dropped File	50.34 KB	application/octet-stream	Access, Create, Write	MALICIOUS
0c0b6a4685e84f89f8c444e84864bb70790dcc090ef99e83fc9dacf81f9605cc	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c309bd448204da08748d872e7acf3fd0bfd686700eaafa043d704c9fa8bda356	C:\Users\kEecfMwgj\Music\n-diJdt93vqLXJ.wav.neqp, c:\users\keecfmwgj\music\n-dijdt93vqlxj.wav.neqp	Dropped File	3.12 KB	application/octet-stream	Access, Create, Write	MALICIOUS
69950c165ec0b9f5bdb3e79dd754d174afe788c5f2e4084294f5a13f55b967f8	c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\3trax2.xlsx.neqp, C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\3traX2.xlsx.neqp	Dropped File	98.01 KB	application/zip	Access, Create, Write	MALICIOUS
f3f2ddd6a521ee76a224de1cac93b3d80ebffa75e65cdd984f8e0a136199c5a3	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
cbe28fa5e05b394252bda74839e4f7b04b62b382aaa0dcee5196919f1912410c	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
3e5ba71b6cb632e12ae119980e72a86120476b8e11b096c07564367aa47d06d7	C:\Users\kEecfMwgj\Desktop\aM0hOBR8.wav.neqp, c:\users\keecfmwgj\desktop\am0hobr8.wav.neqp	Dropped File	49.71 KB	application/octet-stream	Access, Create, Write	MALICIOUS
71bca71399f874fa1d1b9a4954880af860bb4d9df7c1cb6549aff1774be22a82	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\Ydwe3q9JyYweb_55_.ots.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\ydwe3q9jyyweb_55_.ots.neqp	Dropped File	11.28 KB	application/octet-stream	Access, Create, Write	MALICIOUS
9136f8bbb40b030da1a32e3856f1d41db3b131a598c39ee3b27134fda307d10a	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\uYkNWJF11O37vr\RRM0O7_xCINdkabdTozN.xlsx.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\uyknwjf11o37vr\rrm0o7_xclndkabdtozn.xlsx.neqp	Dropped File	32.04 KB	application/zip	Access, Create, Write	MALICIOUS
6cc5a4e8e249e3bfbaed056ddf1c1803464f7ff4004c5aae6eb08a2ba52ff06f	C:\Users\kEecfMwgj\Videos\80uy.mkv.neqp, c:\users\keecfmwgj\videos\80uy.mkv.neqp	Dropped File	22.95 KB	application/octet-stream	Access, Create, Write	MALICIOUS
6ea3563e008269ecdd0f630cacea48c74bcf8970401dad252d281bd65e67e061	C:\Users\kEecfMwgj\Documents\k7QtcBphpiUfUf6h4.rtf.neqp, c:\users\keecfmwgj\documents\k7qtcbphpiufuf6h4.rtf.neqp	Dropped File	80.09 KB	text/rtf	Access, Create, Write	MALICIOUS
a2ac9a1d0c1779549ac732ef64456735ebafa152d2d257a6160196a51fc4262c	c:\users\keecfmwgj\pictures\c8-qdtknhu0bjgmu.jpg.neqp, C:\Users\kEecfMwgj\Pictures\c8-qdtkNHu0bJGmu.jpg.neqp	Dropped File	81.98 KB	image/jpeg	Access, Create, Write	MALICIOUS
40c616bbbb7a696fcbe40f83dd4cd8192abe8bc65f6c335b176d7b79c8b9e58c	c:\users\keecfmwgj\music\dcxazqh.m4a.neqp, C:\Users\kEecfMwgj\Music\DcXaZQH.m4a.neqp	Dropped File	87.50 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3da8c5dfe9c18bf5830852a8c8b861e8a40bfe9b5de4aa6686cee6b7fe523bcb	c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\zt3a4flgawjyzt7r4xm.png.neqp, C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\zT3A4flgAWjYzt7r4Xm.png.neqp	Dropped File	39.86 KB	application/octet-stream	Access, Create, Write	MALICIOUS
3c5571a767be08f4e53c70695c84ef1fdf162432d9811d8c712a99fb110850bd	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c7765038781cd3244fd96242b2971ac5fd05f0cba0e5cb93ad1158453732fe08	c:\users\keecfmwgj\videos\kcia6gopkg9.avi.neqp, C:\Users\kEecfMwgj\Videos\kCiA6GopKG9.avi.neqp	Dropped File	24.69 KB	application/octet-stream	Access, Create, Write	MALICIOUS
da51d9fe5e748d055446e6e0db0db683d3fc369449c53ed54d992b849dccc3bd	C:\Users\kEecfMwgj\Videos\ueJknWfWvw.mkv.neqp, c:\users\keecfmwgj\videos\uejknwfwvw.mkv.neqp	Dropped File	24.18 KB	application/octet-stream	Access, Create, Write	MALICIOUS
2792c50009dc1d367956d8c08654e1f69ed8acde53130297e2ebfb2d6d498a15	c:\users\keecfmwgj\documents\2vnukkmn.xlsx.neqp, C:\Users\kEecfMwgj\Documents\2VNUKKMN.xlsx.neqp	Dropped File	45.08 KB	application/zip	Access, Create, Write	MALICIOUS
5591760e26390270da6aa832ff595201308d820fe37a0944ba71628d6c6baad2	C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\kduc8M4q0iGO.xlsx.neqp, c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\kduc8m4q0igo.xlsx.neqp	Dropped File	47.83 KB	application/zip	Access, Create, Write	MALICIOUS
21a7a27731f45ff005c0a2003463ba695a779f5dff6ffe7a5c645306d4cdc4f1	c:\users\keecfmwgj\videos__n93zziz9rny.mp4.neqp, C:\Users\kEecfMwgj\Videos__N93Zziz9RNY.mp4.neqp	Dropped File	99.42 KB	application/octet-stream	Access, Create, Write	MALICIOUS
73b5be1ea2ec586b130560f88ba4383dd27738e25fe528852fceafaef6585be3	c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\ruec4u8cn1u.jpg.neqp, C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\rUec4u8CN1U.jpg.neqp	Dropped File	8.96 KB	image/jpeg	Access, Create, Write	MALICIOUS
f43500d99e886576aa2f3367d538b8d6cad05c81c34a924b4f3a8eb84b243714	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
bc2549b38d66f9eeb9895647caf5dc4d866376de1396b5044f95e97ce19608a7	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
64d20dc7145a6014bd955d9eadc02afd318577b329bbf0da6e786553a48aaa3c	c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.neqp, C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Entertainment.url.neqp	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
cc4ebed9b5ba507180e3d3cd89025f7ca141e35479cc40edff9ffeada92f5b1f	c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\djfpsjtvq\gxuwpj.csv.neqp, C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\DjfPSJtvQ\gXUwPJ.csv.neqp	Dropped File	15.36 KB	application/octet-stream	Access, Create, Write	MALICIOUS
71f582b5d18272207699f1b1cb74cad4207a8d12a8a1c4ea9a956bcbad861e64	c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\oy4eruo53oz.rtf.neqp, C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\OY4eRUo53OZ.rtf.neqp	Dropped File	47.26 KB	text/rtf	Access, Create, Write	MALICIOUS
67706071ac7a92d98c7dfd1139f0d42e0e60ebf41e6c6cff335a84a42fb76cfc	C:\Users\kEecfMwgj\Videos\bGt49HOvptpF2AsDKl.mkv.neqp, c:\users\keecfmwgj\videos\bgt49hovptpf2asdkl.mkv.neqp	Dropped File	9.61 KB	application/octet-stream	Access, Create, Write	MALICIOUS
26fb40f54a2f8364cefc330f291bcc0bcdccba819189fb77737ebba0b5d6dc31	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIReTh vq1qbRJ-L\aZ2HX2t0pm3.ots.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\6ayirleth vq1qbrj-l\az2hx2t0pm3.ots.neqp	Dropped File	27.57 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3a1678ecda6f53b6eabdecbbb07d30bba268edbd28fe7ecf6eeee0838b62820f	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
b9687ffc3fea913f4ca3680d3868788484cad0bdd3b68b29eb6b2124c57aab7a	c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\oepl7unfz0.jpg.neqp, C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\OepL7uNfz0.jpg.neqp	Dropped File	38.08 KB	image/jpeg	Access, Create, Write	MALICIOUS
e5de7541f322ea5b1d436fc00a4b1f7b5eda86c7752c1a3afa31b5b557edeee0	C:\Users\kEecfMwgj\Documents\G8oUQ7rKtGSWcT.ots.neqp, c:\users\keecfmwgj\documents\g8ouq7rktgswct.ots.neqp	Dropped File	34.10 KB	application/zip	Access, Create, Write	MALICIOUS
3d8fa947bdcd9f309e67ddc08a696ef5915ef40981a17406e783360ed9318ec3	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIRleTh vq1qbRJ-L\oV6zFBL.rtf.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\6ayirleth vq1qbrj-l\ov6zfbl.rtf.neqp	Dropped File	17.15 KB	text/rtf	Access, Create, Write	MALICIOUS
ca76b849fe783671d86d396fedf8eb52aaa34c546204e7042a655e28e1de003d	c:\users\keecfmwgj\desktop\tkaxolhrl8qedbn.gif.neqp, C:\Users\kEecfMwgj\Desktop\tkAxolHRl8qEDbn.gif.neqp	Dropped File	75.29 KB	image/gif	Access, Create, Write	MALICIOUS
0d24aa85f5dde8bb3d59b783e23500c25bc0deaf80ef6d8e2b1578cadb4076ea	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
19f5f2dd29bbcfeade1d9b7c03d269aafacf42714f20ea705c2cec42f7b45070	c:\users\keecfmwgj\videos\qg8i9g0tihejna tr3l.flv.neqp, C:\Users\kEecfMwgj\Videos\qG8i9G0tlhejna tR3l.flv.neqp	Dropped File	91.53 KB	video/x-flv	Access, Create, Write	MALICIOUS
7d2a17a1969eb01411d56352a0f7008df8127d35bf9bbccef76590d2474ad2cc	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
159d189b403545fc73c2eae42d91ba59fe66190918e6d1fe6c552f12cc3bd6ef	c:\users\keecfmwgj\videos\fmxha_w4eke5pf8l.mp4.neqp, C:\Users\kEecfMwgj\Videos\FMXhA_W4EkE5pF8l.mp4.neqp	Dropped File	84.52 KB	application/octet-stream	Access, Create, Write	MALICIOUS
7d5a7c649121fe8ffdb3f33d7990e72f7f82d348393b691f9c7f3f545d72fb58	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
5fff09985946ab4c541e335925f853ca8fb5fd8c3b034af584c3e38fc8a0cab7	c:\users\keecfmwgj\favorites\msn websites\msn sports.url.neqp, C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Sports.url.neqp	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
8611096fe95209ae1dba414e2822e1846ef5d334a498f9259a425bcc4417a460	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
ba82cca3e24aea86e0af29a0a3b7d2ff300678bd6bea1faec72cf1a9104319d4	c:\users\keecfmwgj\documents\koomr.pptx.neqp, C:\Users\kEecfMwgj\Documents\kOOmR.pptx.neqp	Dropped File	65.97 KB	application/zip	Access, Create, Write	MALICIOUS
a71b66c0c077595753fbbb61c893faf0b0a65bd98411af80d1ccac4ef4249360	c:\users\keecfmwgj\pictures\byf8cf9eozrq2jwpt66.gif.neqp, C:\Users\kEecfMwgj\Pictures\BYF8cF9EOzRq2jWpt66.gif.neqp	Dropped File	7.79 KB	image/gif	Access, Create, Write	MALICIOUS
b8ee614ea2d827c73ec11b98bf3bc274c5a8d0ed0635b045b0ee714389265bfc	c:\users\keecfmwgj\favorites\msn websites\msn.url.neqp, C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN.url.neqp	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
afb02b0290206b01ccee45d8f98f2e35ae219d5640070696d894004f615d21d7	C:\Users\kEecfMwgj\Videos\n7DfguJMJ.mp4.neqp, c:\users\keecfmwgj\videos\n7dfgujmj.mp4.neqp	Dropped File	32.55 KB	application/octet-stream	Access, Create, Write	MALICIOUS
44f4ea2126b623bdc8ba9736084c369a662330ca25805b04ee3fdb8ee2407463	C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Home.url.neqp, c:\users\keecfmwgj\favorites\microsoft websites\microsoft at home.url.neqp	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
48d258fec956c0dd3d0bf3b53751517b045f556999a012dceaf0f83b7fa25084	c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.neqp, C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE site on Microsoft.com.url.neqp	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
fc41fa34a2680ceba80fcf0f1ea1baf337651b613f5f9a88d5b6b92555dba15e	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\c0Y tBs zGXD9sK\qJTFnnuSQ.ppt.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\c0y tbs zgxd9sk\qjtfnnusq.ppt.neqp	Dropped File	83.41 KB	application/octet-stream	Access, Create, Write	MALICIOUS
4f0f5de45b74e5ea989f7a9d6a940bd776723ce15983d27fa72c617738d32d7a	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
46ccfbb7da1962ccd7fb5c9ed1be4faaa832dda81d436206bd12402e711090d5	c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\jtbbgg -ujwe3.bmp.neqp, C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\jTBbgg -UJwe3.bmp.neqp	Dropped File	45.80 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ba1278861d1e551337fb56b14bfd9669307bb824b390a2e166fec8a6d243e56c	C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\NECDkoymaUw.png.neqp, c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\necdkoymauw.png.neqp	Dropped File	62.52 KB	application/octet-stream	Access, Create, Write	MALICIOUS
56bf3749556649cb55983f5251f487924d12ef6bd1a4eed31c4dfb2e8d161c20	c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\6ayirlethvq1qbrj-l\gbpqlruev5tl.pptx.neqp, C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIRleTh vq1qbRJ-L\GbPQlrueV5Tl.pptx.neqp	Dropped File	17.26 KB	application/octet-stream	Access, Create, Write	MALICIOUS
be56d11b01efd115e7fb4cb893f74c406e54dea0f66e25bedcd2d54ded46954c	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
321f7cc6122278e81286764c399ae72ba41a03086f09bc87cb0b81cc9b1659d1	c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\vztrk63idaphpsstgre.pptx.neqp, C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\VZTRK63idApHPSstGrE.pptx.neqp	Dropped File	89.56 KB	application/zip	Access, Create, Write	MALICIOUS
6c78d46432f8cd84b5e81d4bfc77da4ff826432890a219a51f0e76a3b91fd164	c:\users\keecfmwgj\videos\gfravduy7lom.swf.neqp, C:\Users\kEecfMwgj\Videos\GfRAVdUY7LOm.swf.neqp	Dropped File	34.41 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
74ae57d78ad228016874fc29ad90fb35a82b355779c3b71f36dc4c44ff70343d4	C:\Users\kEecfMwgj\Music\qYyGPLt6OoKeyh2R.m4a.neqp, c:\users\keecfmwgj\music\qyygplt6ookeyh2r.m4a.neqp	Dropped File	74.98 KB	application/octet-stream	Access, Create, Write	MALICIOUS
a8caa46758c82c1f3a67808e3d5559d0986c83e2129d318ca4df5b15d83df2ac	C:\Users\kEecfMwgj\Desktop\VuYJSL8GFd0.mp3.neqp, c:\users\keecfmwgj\desktop\vuyjsl8gfd0.mp3.neqp	Dropped File	27.13 KB	application/octet-stream	Access, Create, Write	MALICIOUS
24bcff8f996c37406034de292c0a2a755a43cd9c0bd8da0862a8921215e46322	C:\Users\kEecfMwgj\Music\HAyp2zHURXEkt5y6c.mp3.neqp, c:\users\keecfmwgj\music\hayp2zhurxekt5y6c.mp3.neqp	Dropped File	58.05 KB	application/octet-stream	Access, Create, Write	MALICIOUS
0bc3226ae404d35c1ff34b10c23d0e64c6c284f52da31cff5d7e17e9b402a27b	C:\Users\kEecfMwgj\Videos\OJNEj2xIV52LVtvj-s0.flv.neqp, c:\users\keecfmwgj\videos\ojnej2xiv52lvtvj-s0.flv.neqp	Dropped File	72.87 KB	video/x-flv	Access, Create, Write	MALICIOUS
3c6db4dbc82aa01319e8bbb9d757161c39b9b0091117e89a8fd54e3703f212dd	C:\Users\kEecfMwgj\Desktop\aFVf9.swf.neqp, c:\users\keecfmwgj\desktop\afvf9.swf.neqp	Dropped File	22.38 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e13cf3f73f060f9338b866fd39241c041aa3b5fc9ac8297e67dc710adac317ff	C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\qf XQc2cUy7GFzzlXBjR.m4a.neqp, c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\qf xqc2cuy7gfzzlxbjr.m4a.neqp	Dropped File	24.60 KB	application/octet-stream	Access, Create, Write	MALICIOUS
0956fed7cbf1d6ec29a544962a39785c55d148970ada824be469061d984bbf91	c:\users\keecfmwgj\music\hvolbk.mp3.neqp, C:\Users\kEecfMwgj\Music\hVOlbk.mp3.neqp	Dropped File	91.71 KB	application/octet-stream	Access, Create, Write	MALICIOUS
c2d124851a7fc5228ad860e0649c0622d8cda9f030954935d188f23470057c49	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c86b6d25a821db817f9d4812529b7a4a0f7d7f33b2c14000251193bfe00cd1bd	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
55ef6f13bdf69ae788b2098e2069c3adcb83d85ad7b5f658dbaa579aed79e6fd	c:\users\keecfmwgj\desktop\eysf0phwcb.mp3.neqp, C:\Users\kEecfMwgj\Desktop\EySF0PhwCB.mp3.neqp	Dropped File	53.65 KB	application/octet-stream	Access, Create, Write	MALICIOUS
e360ad4c59d573dc334fe9d4b972302d4bf9c14b6be87d81a669eb72798717d0	C:\Users\kEecfMwgj\Desktop\NBxo5Eh8J.swf.neqp, c:\users\keecfmwgj\desktop\nbxo5eh8j.swf.neqp	Dropped File	17.97 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
e50366970c63f29b549ef31f804d55860e4350cefe5d4d19f5634cd05b400fc9	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
cd47f9c4b3b6c33f29b81c6921b25391f98a870cf9a153639d089a9c182aa4b6	C:\Users\kEecfMwgj\Videos\NhQ2zMqJr.flv.neqp, c:\users\keecfmwgj\videos\nhq2zmqjr.flv.neqp	Dropped File	58.28 KB	video/x-flv	Access, Create, Write	MALICIOUS
492ce60054c78e32c636cc34c1200333e8d3f98158adb5d65dcb29d19b450977	c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\djfpsjtvq\-6sm.bmp.neqp, C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\DjfPSJtvQ\-6Sm.bmp.neqp	Dropped File	65.52 KB	application/octet-stream	Access, Create, Write	MALICIOUS
850027588e455fc72023a04b7b8118a072e7a7c23558d653ccdc537642de9bfb	C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Gallery.url.neqp, c:\users\keecfmwgj\favorites\windows live\windows live gallery.url.neqp	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
db2786ef7701c64a6601da55979530c685b3db423fd1683f668c92a642ec9ec8	C:\Users\kEecfMwgj\Music\YiJlu.mp3.neqp, c:\users\keecfmwgj\music\yijlu.mp3.neqp	Dropped File	49.57 KB	application/octet-stream	Access, Create, Write	MALICIOUS
d1652c1d808a6395d5ef182c05ded57b733b869a18d4ba889941edef8bc08e68	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
1ef7f8b580e6444d3fc7b7c8999443d346f3c0be496875649fa90c37709b601b	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
b59c174297e759d859a2d26e051614064025fc6555037d2ec62c9f38204426d3	C:\Users\kEecfMwgj\Documents\SZzcxiUb3S1y0E.pptx.neqp, c:\users\keecfmwgj\documents\szzcxiub3s1y0e.pptx.neqp	Dropped File	55.67 KB	application/zip	Access, Create, Write	MALICIOUS
cc36568442ee4e7a01af47d4d80bc015aa31cb91929ed64c8436dd784cd16e98	c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\rx-ru.png.neqp, C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\Rx-ru.png.neqp	Dropped File	49.89 KB	application/octet-stream	Access, Create, Write	MALICIOUS
ecbe7bdad612287562bbe873b9830e1bebf10fef9f568e15b682c69b2f0555f2	c:\users\keecfmwgj\pictures\nqugwix.bmp.neqp, C:\Users\kEecfMwgj\Pictures\NqUgwIX.bmp.neqp	Dropped File	58.94 KB	application/octet-stream	Access, Create, Write	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8eb549c551f1dac7873d96a352145b2374928f20aa047a5ee20f8784f97329bc	C:\Users\kEecfMwgj\Pictures\dwHz_UcKn2C.bmp.neqp, c:\users\keecfmwgj\pictures\dwhz_uckn2c.bmp.neqp	Dropped File	68.60 KB	application/octet-stream	Access, Create, Write	MALICIOUS
b275bd4c85167e0585d897907d5aaca02f473b95f6f3bf2b4582c825d0b6c5db	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
e3fe6bcd13e044be02878ddf0e1ffc43a730bf30547b71b4e75c7d319f1d422b	c:\users\keecfmwgj\videos\jcuukzkpdwtrtf.flv.neqp, C:\Users\kEecfMwgj\Videos\JcUUkzkPDWTrtF.flv.neqp	Dropped File	65.06 KB	video/x-flv	Access, Create, Write	MALICIOUS
e5eb5b1a0bbd8b059b4e49a573766f807b01d3efb2adf49e130bfbc09b5f5ede	c:\users\keecfmwgj\videos\osw75xo0982bw.swf.neqp, C:\Users\kEecfMwgj\Videos\Osw75Xo0982Bw.swf.neqp	Dropped File	17.20 KB	application/x-shockwave-flash	Access, Create, Write	MALICIOUS
363034c912bbaaba361e7d0f49bb7e7fd73c9e171a6821aaccfb549e78dd6a19	c:\users\keecfmwgj\videos\ompo2s.flv.neqp, C:\Users\kEecfMwgj\Videos\omPO2s.flv.neqp	Dropped File	9.55 KB	video/x-flv	Access, Create, Write	MALICIOUS
47126b13c5ab1b98c030985425b4b63927954ade768ddbb06fa10cab81942d68	c:\users\keecfmwgj\music\epp3ouzeazkkj5hj.wav.neqp, C:\Users\kEecfMwgj\Music\EpP3OuZeAzKkjJ5Hj.wav.neqp	Dropped File	82.14 KB	application/octet-stream	Access, Create, Write	MALICIOUS
9304907895a74fcec35934937a066d8792ca22dc0bd0733d6a4a4de8e48af55d	c:\users\keecfmwgj\favorites\microsoft websites\ie add-on site.url.neqp, C:\Users\kEecfMwgj\Favorites\Microsoft Websites\IE Add-on site.url.neqp	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	MALICIOUS
a57a769c198326295c7733e10e8b78c2e9e91abffba02bbcfa182e137889838b	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\c0Y tBs zGXD9sK\Yz_Q1.doc.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\c0y tbs zgxd9sk\yz_q1.doc.neqp	Dropped File	15.96 KB	application/octet-stream	Access, Create, Write	MALICIOUS
293b437fdbeb5f42575519f649927086e0c6cf3389a5f81d05de2a6ea6ff63c0	c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\s7lh3hxtittmcvgh\r6fjlezg_wtj.ots.neqp, C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\S7LH3hXtiTTmcVgH\r6fjlEZZg_wtj.ots.neqp	Dropped File	68.20 KB	application/zip	Access, Create, Write	MALICIOUS
24b05b9eb992fd995ad217c8eb2ec4cfe1472960f70be82a7d197b5b790489e1	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
5ec80fca38a6bb8a331218c2cf0a0831b8b02354d7c1ca79d862470daac9c6ff	c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7fiyl6m -whjjeo.wav.neqp, C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7fIYl6M -WhJjeO.wav.neqp	Dropped File	41.00 KB	application/octet-stream	Access, Create, Write	MALICIOUS
40a2518bf4a3cc5c663278f0f5e9f1a7a0d51e57f2c13cc2009c1d5cf0a87d36	-	Memory Dump	1244.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
f79da05e1456bc0c17153e35454bac68b5d89e1f77a139d70058d8cfa69325e7	C:\Users\kEecfMwgj\Documents\FU2nzV-k.pdf.neqp, c:\users\keecfmwgj\documents\fu2 nzv-k.pdf.neqp	Dropped File	33.53 KB	application/pdf	Access, Create, Write	MALICIOUS
b9593847de0c67f0f23ec0556fc86327530f78034d9aa3ed88e71a9542578ed4	C:\Users\kEecfMwgj\Desktop\gwqS.gif.neqp, c:\users\keecfmwgj\desktop\gwqs.gif.neqp	Dropped File	23.29 KB	image/gif	Access, Create, Write	MALICIOUS
e5fd3efa78dd1245625130a2c4e50ddb04f259cefb82c10d1d91fc231af1f5cb	c:\users\keecfmwgj\music\d7illvxbgi6q.wav.neqp, C:\Users\kEecfMwgj\Music\d7IlLVXBGI6Q.wav.neqp	Dropped File	28.39 KB	application/octet-stream	Access, Create, Write	MALICIOUS
92f4134cc013553a811aa371570d7e2e66a2537b4eac3ddbdeaf0cb5f02e6ec56	-	Downloaded File	5008.50 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3	C:\Users\kEecfMwgj\AppData\Roaming\uaieedr, C:\Users\kEecfMwgj\Desktop\c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe	Dropped File	270.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	MALICIOUS
5d1b0a63577d637eecfd075abf530d62b2c913c98b2bd38e116ffb8c21e5dd13	C:\Users\KEECFM~1\AppData\Local\Temp\51F0.exe, C:\Users\KEECFM~1\AppData\Local\Temp\3024.exe, C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51F0.exe	Dropped File	749.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	SUSPICIOUS
f7d8dccfe4d3893389f55299ef95ded2a028256236dd216df0db3fc2c1ff4bea	C:\Users\kEecfMwgj\Documents\p5HGkq_lz1hzZZQ1QzX\7lvhY-.pdf.neqp, c:\users\keecfmwgj\documents\p5hgkq_lz1hzzzq1qzx\7lvhy-.pdf.neqp	Dropped File	80.98 KB	application/pdf	Access, Create, Write	SUSPICIOUS
7bed4d1ffdbed3e4841728ff7b25dc6fc151e592d203d133e8cb6d0caf06b18a	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\S7LH3hXtiTTmcVgH\4kaBTKfDmjtKDpmZU4\uc2h_7ZMsMjV1wdpv4D.pdf.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\s7lh3hxtittmcvgh\4kabtkfdmjtkdpmzu4\uc2h_7zmsmjv1wdpv4d.pdf.neqp	Dropped File	6.66 KB	application/pdf	Access, Create, Write	SUSPICIOUS
8365cace85761c3b80e8605fe9360d8c008e35eaeacf7d0aacc28b8485cf76b9	-	Downloaded File	44 bytes	application/octet-stream	-	CLEAN
094c4931fdb2f2af417c9e0322a9716006e8211fe9017f671ac6e3251300acca	C:\SystemID\PersonalID.txt	Dropped File	42 bytes	application/octet-stream	Access, Create, Read	CLEAN
8b8e83d2dde30fde592f97c079590dabdfbe15edd117cf385edf1930d6ce3c3b	-	Downloaded File	7 bytes	application/octet-stream	-	CLEAN
68c3d502ba5230fbeab7c93e9f49eda6c07d26f41ece661ba4544ae6ae5fc5a4	-	Downloaded File	213 bytes	application/octet-stream	-	CLEAN
ec376aee00528541763fca5293338302eb42e95237c7fcd3fd3d7af2ed434978	-	Downloaded File	294 bytes	application/octet-stream	-	CLEAN
6f252ce951f59597b04eecd3ecc55663e48b38cb0adae24c18c1920fb4bef61f	c:\users\keecfmwgj\appdata\local\microsoft\windows\history\history.ie5\index.dat	Modified File	64.00 KB	application/octet-stream	-	CLEAN
a6ecf24713b62ba28ad4fdd406221134b49afb2b1d0092943dafbf8427b92cff	C:\Users\kEecfMwgj\AppData\Local\bowsakkdestx.txt, c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\get[1].php	Downloaded File	562 bytes	application/json	Access, Create, Delete, Read, Write	CLEAN
132a5d3b0232783cbd6e1a02b9bc6eecb032b12a9843857fdbee736c1b640439	-	Downloaded File	749.50 KB	application/octet-stream	-	CLEAN
b2ce910645dfc37215793af0742cdb787e18991c107de3af5fe745a7ba1c2e8d	-	Downloaded File	285 bytes	application/octet-stream	-	CLEAN
1890500ca302d79185164dc7bb18c58ea70feb885d28929d8aeab831ba3cfe72	c:\users\keecfmwgj\favorites\links\web slice gallery.url.neqp, C:\Users\kEecfMwgj\Favorites\Links\Web Slice Gallery.url.neqp	Dropped File	560 bytes	application/octet-stream	Access, Create, Write	CLEAN
8aa22e70515ff35e039bf99cbcc644f7e9f36390b1e4f5c3d1f356e18ef1927b	c:\users\keecfmwgj\pictures\ote5jpyt.jpg.neqp, C:\Users\kEecfMwgj\Pictures\oTE5jPYT.jpg.neqp	Dropped File	74.38 KB	image/jpeg	Access, Create, Write	CLEAN
0c5cceba5c416d5424387794429f89a2456b5326e2c7e5d8d2bd67f34bb616ec	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\cookies\index.dat	Memory Dump	32.00 KB	application/octet-stream	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2b4e417e5594a5e9aec3322803aed47fbfb41b7f11033ea38ccd938c91d6394a	C:\Users\kEecfMwgj\Desktop\AQRFNBZ8zX.jpg.neqp, c:\users\keecfmwgj\desktop\aqrfnbz8zx.jpg.neqp	Dropped File	13.37 KB	image/jpeg	Access, Create, Write	CLEAN
8fc1ae1a523131741fc18ef2fcffcc5dd174a60516253c38dff5be2e648f06b	c:\users\keecfmwgj\music\uftb9wa27mlfv.mp3.neqp, C:\Users\kEecfMwgj\Music\uFTB9Wa27mlfv.mp3.neqp	Dropped File	7.51 KB	application/octet-stream	Access, Create, Write	CLEAN
e8e572570459fbdb3170b2ce002c7b45c40de0b3fbff5d4f88913857f0cb0887	C:\Users\kEecfMwgj\Desktop\h5j527Mxht9SX2raeS80.mp3.neqp, c:\users\keecfmwgj\desktop\h5j527mxht9sx2raes80.mp3.neqp	Dropped File	95.32 KB	application/octet-stream	Access, Create, Write	CLEAN
8df32ebbf3ecfca140e3d62b435e229cdfa858736aeae633ef5a9670f573672c	c:\users\keecfmwgj\music\rrbusch3n2s3k7tf26.wav.neqp, C:\Users\kEecfMwgj\Music\rRbuSch3N2s3k7tf26.wav.neqp	Dropped File	61.13 KB	application/octet-stream	Access, Create, Write	CLEAN
0876ae69b6af6791dbb1cbbb657eaa814d410767e44037931f859eeb8b46fada	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\S7LH3hXtiTTmcVgH\VDXnqC 6DK_84Fuegb.xlsx.neqp, c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\s7lh3hxtittmcvgh\vdxnqc6dk_84fuegb.xlsx.neqp	Dropped File	3.14 KB	application/octet-stream	Access, Create, Write	CLEAN
c82112f4307f5b2604c9c84dbd70b15271aba5fb58e8a2114651a511e597b442	C:\Users\kEecfMwgj\Documents\r5XNSimbuw.xlsx.neqp, c:\users\keecfmwgj\documents\r5xnsimbuw.xlsx.neqp	Dropped File	4.85 KB	application/octet-stream	Access, Create, Write	CLEAN
c8849d3c3d667761e66594bda703eb352ac1d6864a18a6e014d62257a085b618	C:\Users\kEecfMwgj\Music\BBqFu3hstVTMPJkSfOH.mp3.neqp, c:\users\keecfmwgj\music\bbqfu3hstvtmpjksfoh.mp3.neqp	Dropped File	21.01 KB	application/octet-stream	Access, Create, Write	CLEAN
c155100c733586f8042f9f4ab9ae255c44390f2ab8b0cf4c92caf2be1b1c2a7b	-	Downloaded File	244 bytes	application/octet-stream	-	CLEAN
3b1568f911b06cc6280dba3a7d8e960051d1787c96ebfa771db9493543814d46	c:\users\keecfmwgj\videos\8nyqrh805h9-og.avi.neqp, C:\Users\kEecfMwgj\Videos\8nYQrh805h9- og.avi.neqp	Dropped File	56.58 KB	application/octet-stream	Access, Create, Write	CLEAN
ab00ee5292b3701499d7ade179fc704fc77fa4952b624733099d17ca41977d8f	c:\users\keecfmwgj\favorites\windows live\get windows live.url.neqp, C:\Users\kEecfMwgj\Favorites\Windows Live\Get Windows Live.url.neqp	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
4a1c4e2fb3046808fb3142a9c3bed1a4ede0167c422e708cb11eba27e4996182	C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Autos.url.neqp, c:\users\keecfmwgj\favorites\msn websites\msn autos.url.neqp	Dropped File	467 bytes	application/octet-stream	Access, Create, Write	CLEAN
c33053fa94a314a88b45f93965896e21e6b44b425d570aa0f7360a9b50204bac	C:\Users\kEecfMwgj\Documents\3r0MOWhcIDm.pptx.neqp, c:\users\keecfmwgj\documents\3r0mowhcidm.pptx.neqp	Dropped File	14.35 KB	application/octet-stream	Access, Create, Write	CLEAN

Reduced dataset

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLjTB7f\kduc8M4q0iGO.xlsx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\aFVf9.swf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\TGEZ_H53zjM.swf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\uz21xybo5jhjzq.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\80uy.mkv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\szqw0q07ao\uamkl9um1jjolc.m4a.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\epp3ouzeazkkjj5hj.wav.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\A8Ch.xlsx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\gcnsphuvaisovbzltws.xlsx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\rrbusch3n2s3k7tf26.wav.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\osw75x o0982bw.swf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\jtbbgg - ujwe3.bmp.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\VuYJSL8GFd0.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\S7LH3hXtiTTmcVgH\4kaBTKfDmjtKDpmZU4\uc2h_7ZMsMjV1wdpv4D.pdf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\d7illvxbgi6q.wav.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\k5szpLuntD.wav.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\qo qbMr5VasZaX.flv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\LE8AEqMT.wav.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\ueJknWfWvw.mkv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\r17tM8VNaibQT6aoUz.flv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\v1fv6rf 5h82idznir.png.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\n 7DfguJMJ.mp4.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\OJNEj2xIV52LVtvj-s0.flv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\koomr.pptx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIRleTh vq1qbRJ-L\oV6zFBL.rtf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\zt3a4flgawjyzt7r4xm.png.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\AQRFNBZ8zX.jpg.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\fmxha_w4eke5pf8l.mp4.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\uYkNWJF11O37vr\FvaFjmImszyo741.ots.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\ttf5tme9.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\msn websites\msn.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\2Hs3CvzmY0a1.doc.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\WFPEZk.png.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\zg2v3ms\5qbgqs8xn8mkwdzflf.jpg.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\UHzfZtepjKuO.wav.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos__n93zziz9rny.mp4.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Home.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Music\u8_5OoZXD_BvAYx.wav.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\yme7wbiiz.jpg.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\byf8cf9eozrq2jwpt66.gif.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\r5XNSimbuw.xlsx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\Ydwe3q9JyYweb_55_.ots.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\p5HGkq_lz1hzZZQ1QzX\7lvhY-.pdf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\oeh1e-xhit5le6vwmu4m.xlsx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\stwus7dzu.swf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\xbtul.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\djfpsjtvq\tpxsaac.flv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\n725zjx2gdfickIh7td.docx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\WzLSzXw7M.bmp.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\amp3as_oww3syrk.avi.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\links\web slice gallery.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\uaieedr	Accessed File, Dropped File	Access, Create, Delete, Write	MALICIOUS
c:\users\keecfmwgj\videos\wkvm-pmus0iogbh_dbp.flv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\k7QtcBphpiUfUf6h4.rtf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\8nyqrh805h9- og.avi.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\NsPZMxJeou0g1vK3d8z.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\msn websites\msn money.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\gfravduy7lom.swf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\5_uaNmfND3.m4a.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\U4sW0p.gif.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\G_bTFo.odp.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\c0Y tBs zGXD9sK\qJTFnnuSQ.ppt.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\szqw0q07Ao\gLy0rCq95A6.wav.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\6ayirleth vq1qbrj-l\gbpqlruev5tl.pptx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\sxV MFLVBA-7.wav.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\ke3zobew8cfbfyhp10.mkv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\oxbmof9d2mfzdb.avi.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Mail.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos_45H8TouB7ZmCtr3W4dN.swf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\GpPyohbyqjIYL-.xlsx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\gwqS.gif.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\f1f3a2atwy iz-.png.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\uYkNWJF11O37vr\RRM0O7_xClNdkabdTozN.xlsx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\outlook files\franc@gdllo.de.pst.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\HAyp2zHURXEkt5y6c.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\ghhedifjzwru5kmr.xlsx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\xvszdq6io_y8wjxlgib.wav.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\3r0MOWhcIDm.pptx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\djfpsjtvq\gxuwpj.csv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\gftzraq.flv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\ompo2s.flv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music_xXA ucctq R.m4a.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\djfpsjtvq\rngvq0d.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\BqMJYpJI5- Av.csv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\oepl7unfz0.jpg.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\h9Ysje.pptx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\djfpsjtvq\l_uac.ppt.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\dxid.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\dCjDLPjgt.png.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\gh3ediyqvyh.jpg.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\nqugwix.bmp.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\S7LH3hXtiTTmcVgH\VDXnqC 6DK_84Fuegb.xlsx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\EwhZ8pVl.pptx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\G8oUQ7rKtGSWcT.ots.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\sU3qV4 mwzLmj.pps.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\8hk5sk-a_pdrv5z.avi.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\hjiarewyjcogtlym7.swf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\msn websites\msn entertainment.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\pkdosd r 3vyy2rn3diw.png.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\3BEbvfVE1d-gqz.doc.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\4HJuy4oV-6dm.gif.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\tkaxolhrl8qedbn.gif.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\dcxazqh.m4a.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\2vnukkmn.xlsx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\msn websites\msn sports.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIRleTh vq1qbRJ-L\aZ2HX2t0pm3.ots.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\hvolbk.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\DjfPSJtvQ\eGbXF478ccI5ln.mkv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\dwHz _UcKn2C.bmp.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\microsoft websites\ie add-on site.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\et8krykeuj73u.swf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\qg8i9g0tihejna tr3l.flv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\windows live\windows live spaces.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\c0Y tBs zGXD9sK\pe4_1B.pptx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\dshy6owctf.wav.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Work.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\h_r0VYpvzAgf_0PUZHZ.docx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\qf XQc2cUy7GFzzIXBjR.m4a.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\eysf0phwcb.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\dohgx0t l.jpg.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\oy4eruo53oz.rtf.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\RXmN gPo8AXsc.gif.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\favorites\microsoft websites\microsoft store.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\bZ_MAu7.avi.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\ups I7.mkv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\5tjEDT2i8f.png.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIRleTh vq1qbRJ-L\jSVU\rH2o4l1w9Tc5d.pptx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\desktop\zsmkkxcply mwj1j 8.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\qYyGPLt6OoKeyh2R.m4a.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

File Name	Category	Operations	Verdict
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\1clt3s.jpg.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\c8-qdtknhu0bjgmu.jpg.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Desktop\tmPl-YXq5d584Uoy2.png.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\fDxmHCHVp_.png.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\uyknwjf11o37vr\gr566la_hbzp.docx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Pictures\hUUFrkBWN6F.bmp.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\N hQ2zMqJr.flv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\c0Y tBs zGXD9sK\Yz_Q1.doc.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\EcSir8.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\contacts\administrator.contact.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\music\uftb9wa27mlfv.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Autos.url.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\BBqFu3hstVTMPJkSfOH.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos\bGt49HOvptpF2AsDKl.mkv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\videos\wxg_cat-2c9o2tc5.mkv.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Music\YiJlu.mp3.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Videos_B 9LyHgp8kWTgOV.mp4.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\s7lh3hxtittmcvgh\r6fjlezzg_wtj.ots.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
C:\Users\kEecfMwgj\Documents\SZzcxiUb3S1y0E.pptx.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS
c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\gfusf.jpg.neqp	Accessed File, Dropped File	Access, Create, Write	MALICIOUS

Reduced dataset

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://somatoka51hub[.]net	Extracted	-	-	-	MALICIOUS
hxxp://nuljjjnuli[.]org	Extracted	-	-	-	MALICIOUS
hxxp://hutnilior[.]net	Extracted	-	-	-	MALICIOUS
hxxps://paraslegal[.]com/tmp/index.php	Extracted	103.25.130.193	India	-	MALICIOUS
hxxp://otriluyttn[.]org	Extracted	-	-	-	MALICIOUS
hxxp://newzelannd66[.]org	Extracted	-	-	-	MALICIOUS
hxxp://zexeq[.]com/lancer/get.php?pid=3822B4A9E2D4C1F1D716E5E90C8DE07D	Contacted, Extracted	58.235.189.192, 5.204.64.195, 201.110.217.38, 210.182.29.70, 183.100.39.157, 211.40.39.251, 115.88.24.200, 37.34.248.24, 109.98.58.98, 195.158.3.162	Kuwait, Uzbekistan, Mexico, Romania, Hungary, South Korea	GET	MALICIOUS
hxxp://golilopaster[.]org	Extracted	-	-	-	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://45[.]9[.]74[.]80/wall.exe	Contacted, Extracted	45.9.74.80	Seychelles	GET	MALICIOUS
hxxp://bulimu55t[.]net	Extracted	-	-	-	MALICIOUS
hxxp://soryytlic4[.]net	Extracted	-	-	-	MALICIOUS
hxxp://tolilolihul[.]net	Extracted	-	-	-	MALICIOUS
hxxp://potunulit[.]org	Contacted, Extracted	104.21.18.99, 172.67.181.144	United States	POST	MALICIOUS
hxxp://bukubuka1[.]net	Extracted	-	-	-	MALICIOUS
hxxp://novanosa5org[.]org	Extracted	-	-	-	MALICIOUS
hxxp://zexeq[.]com/lancer/get.php?pid=3822B4A9E2D4C1F1D716E5E90C8DE07D&first=true	Contacted, Extracted	58.235.189.192, 5.204.64.195, 201.110.217.38, 210.182.29.70, 183.100.39.157, 211.40.39.251, 115.88.24.200, 37.34.248.24, 109.98.58.98, 195.158.3.162	Kuwait, Uzbekistan, Mexico, Romania, Hungary, South Korea	GET	MALICIOUS
hxxp://colisumy[.]com/dl/build.exe	Contacted, Extracted	5.239.240.61, 211.59.14.90, 190.229.19.7, 175.126.109.15, 175.120.254.9, 61.253.71.111, 210.182.34.10, 211.119.84.112, 82.78.247.152, 177.254.85.20	Iran, Colombia, Argentina, Romania, South Korea	GET	MALICIOUS
hxxp://hujukui3[.]net	Extracted	-	-	-	MALICIOUS
hxxps://api[.]2ip[.]ua/geo.json	Contacted, Extracted	162.0.217.254	Netherlands	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
paraslegal[.]com	103.25.130.193	India	TCP, TLS, DNS	MALICIOUS
zexeq[.]com	58.235.189.192, 5.204.64.195, 201.110.217.38, 210.182.29.70, 183.100.39.157, 211.40.39.251, 115.88.24.200, 37.34.248.24, 109.98.58.98, 195.158.3.162	Kuwait, Uzbekistan, Mexico, Romania, Hungary, South Korea	TCP, HTTP, DNS	MALICIOUS
potunulit[.]org	104.21.18.99, 172.67.181.144	United States	TCP, HTTP, DNS	MALICIOUS
colisumy[.]com	5.239.240.61, 211.59.14.90, 190.229.19.7, 175.126.109.15, 175.120.254.9, 61.253.71.111, 210.182.34.10, 211.119.84.112, 82.78.247.152, 177.254.85.20	Iran, Colombia, Argentina, Romania, South Korea	TCP, HTTP, DNS	MALICIOUS
golilopaster[.]org	-	-	-	CLEAN
bukubuka1[.]net	-	-	-	CLEAN
hujukui3[.]net	-	-	-	CLEAN
api[.]2ip[.]ua	162.0.217.254	Netherlands	TCP, TLS, DNS, HTTPS	CLEAN
tolilolihul[.]net	-	-	-	CLEAN
somatoka51hub[.]net	-	-	-	CLEAN
soryytlic4[.]net	-	-	-	CLEAN
nuljjjnuli[.]org	-	-	-	CLEAN
newzelannd66[.]org	-	-	-	CLEAN
novanosa5org[.]org	-	-	-	CLEAN
bulimu55t[.]net	-	-	-	CLEAN
otriluyttn[.]org	-	-	-	CLEAN

Domain	IP Address	Country	Protocols	Verdict
hutnilior[.]net	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
45.9.74.80	-	Seychelles	TCP, HTTP	CLEAN
211.40.39.251	zexeq[.]com	South Korea	DNS	CLEAN
162.0.217.254	api[.]2ip[.]ua	Netherlands	TCP, TLS, DNS, HTTPS	CLEAN
175.126.109.15	colisumy[.]com	South Korea	DNS	CLEAN
61.253.71.111	colisumy[.]com	South Korea	DNS	CLEAN
211.59.14.90	colisumy[.]com	South Korea	DNS	CLEAN
82.78.247.152	colisumy[.]com	Romania	DNS	CLEAN
5.204.64.195	zexeq[.]com	Hungary	DNS	CLEAN
172.67.181.144	potunulit[.]org	United States	DNS	CLEAN
103.25.130.193	paraslegal[.]com	India	TCP, TLS, DNS	CLEAN
5.239.240.61	colisumy[.]com	Iran	TCP, HTTP, DNS	CLEAN
58.235.189.192	zexeq[.]com	South Korea	DNS	CLEAN
104.21.18.99	potunulit[.]org	-	TCP, HTTP, DNS	CLEAN
183.100.39.157	zexeq[.]com	South Korea	TCP, HTTP, DNS	CLEAN
201.110.217.38	zexeq[.]com	Mexico	DNS	CLEAN
211.119.84.112	colisumy[.]com	South Korea	DNS	CLEAN
210.182.34.10	colisumy[.]com	South Korea	DNS	CLEAN
175.120.254.9	colisumy[.]com	South Korea	DNS	CLEAN
195.158.3.162	zexeq[.]com	Uzbekistan	DNS	CLEAN
177.254.85.20	colisumy[.]com	Colombia	DNS	CLEAN
210.182.29.70	zexeq[.]com	South Korea	DNS	CLEAN
109.98.58.98	zexeq[.]com	Romania	DNS	CLEAN
37.34.248.24	zexeq[.]com	Kuwait	TCP, HTTP, DNS	CLEAN
115.88.24.200	zexeq[.]com	South Korea	DNS	CLEAN
190.229.19.7	colisumy[.]com	Argentina	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D}	access	51f0.exe	CLEAN
DCEBF3F5A707CB556B65BC9D3C6783D08443A5AF	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Version	access, read	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\svcVersion	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion	access	51f0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	3024.exe, 51f0.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\SysHelper	write, access, read	51f0.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\SysHelper	write, access, read	3024.exe, 51f0.exe	CLEAN

Process

Process Name	Commandline	Verdict
c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe	"C:\Users\kEecfMwgj\Desktop\c0832b1008aa0fc828654f9762e37bda019080cbdd92bd2453a05cfb3b79abb3.exe"	MALICIOUS
uaieedr	C:\Users\kEecfMwgj\AppData\Roaming\uaieedr	MALICIOUS
uaieedr	C:\Users\kEecfMwgj\AppData\Roaming\uaieedr	MALICIOUS
uaieedr	C:\Users\kEecfMwgj\AppData\Roaming\uaieedr	MALICIOUS
51f0.exe	C:\Users\KEECFM~1\AppData\Local\Temp\51F0.exe	SUSPICIOUS
51f0.exe	C:\Users\KEECFM~1\AppData\Local\Temp\51F0.exe	SUSPICIOUS
51f0.exe	"C:\Users\KEECFM~1\AppData\Local\Temp\51F0.exe" --Admin IsNotAutoStart IsNotTask	SUSPICIOUS
51f0.exe	"C:\Users\KEECFM~1\AppData\Local\Temp\51F0.exe" --Admin IsNotAutoStart IsNotTask	SUSPICIOUS
51f0.exe	C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51F0.exe --Task	SUSPICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
51f0.exe	"C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51F0.exe" --AutoStart	SUSPICIOUS
51f0.exe	"C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd\51F0.exe" --AutoStart	SUSPICIOUS
3024.exe	C:\Users\KEECFM~1\AppData\Local\Temp\3024.exe	SUSPICIOUS
3024.exe	C:\Users\KEECFM~1\AppData\Local\Temp\3024.exe	SUSPICIOUS
3024.exe	"C:\Users\KEECFM~1\AppData\Local\Temp\3024.exe" --Admin IsNotAutoStart IsNotTask	SUSPICIOUS
3024.exe	"C:\Users\KEECFM~1\AppData\Local\Temp\3024.exe" --Admin IsNotAutoStart IsNotTask	SUSPICIOUS
icacls.exe	icacls "C:\Users\kEecfMwgj\AppData\Local\de09289d-6a73-4dff-8fad-e9599bbc17bd" /deny *S-1-1-0:(OI)(CI)(DE,DC)	CLEAN
taskeng.exe	taskeng.exe {D864A465-DF92-41F7-B6FE-4C380B7E9468} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
taskeng.exe	taskeng.exe {B59EC091-DBC7-4BE9-AC74-DC40D81A85AE} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]	CLEAN

YARA / AV

YARA (295)

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\dshy6owctf.wav.neqp	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\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\BqMJYpJI5- Av.csv.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\5_uaNmfND3.m4a.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\5tjEDT2i8f.png.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\uz21xybo5jhjzq.mp3.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\OvrR6bzipPtcj.docx.neqp	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\u8_5OoZXD_BvAYx.wav.neqp	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.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\ukOCS4.csv.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\xys3y_cu624bscdh.bmp.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\ewxkzosyjkhnwpoz.docx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\dohgx0t l.jpg.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\bZ_MAu7.avi.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\G_bTFo.odp.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\uYkNWJF11O37vr\Xw0 5hxcA.pptx.neqp	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\sU3qV4 mwzLmj.pps.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\by0ls29bbpklp631o9b.m4a.neqp	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\h9Ysje.pptx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\XqIXfBNrZqo t.mp3.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\upklen56967zj.flv.neqp	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\oeh1e-xhit5le6vwmu4m.xlsx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\1clt3s.jpg.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\ghhedifjzwru5kmr.xlsx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\dCjDLPjgt.png.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\et8krykeuj73u.swf.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\upsI7.mkv.neqp	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\n-diJdt93vqLXJ.wav.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\3trax2.xlsx.neqp	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\aM0hOBR8.wav.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\Ydwe3q9JyYweb_55_.ots.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\uYkNWJF11O37vr\RRM0O7_xClNdkabdTozN.xlsx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\80uy.mkv.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\k7QtcBphpiUfUf6h4.rtf.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\c8-qdtknhu0bjgmu.jpg.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\dcxazqh.m4a.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\zt3a4flgawjyzt7r4xm.png.neqp	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\kcia6gopkg9.avi.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\ueJknWfWvw.mkv.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\2vnukkmn.xlsx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\kduc8M4q0iGO.xlsx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos__n93zziz9rny.mp4.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\ruec4u8cn1u.jpg.neqp	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 entertainment.url.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\djfpsjtvq\gxuwpj.csv.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\oy4eruo53oz.rtf.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\bGt49HOvptpF2AsDKl.mkv.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIReTh vq1qbRJ-L\aZ2HX2t0pm3.ots.neqp	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\mxfa2rzxqyhankfzm\oepl7unfz0.jpg.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\G8oUQ7rKtGSWcT.ots.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\6ayIReTh vq1qbRJ-L\oV6zFBL.rtf.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\tkaxolhrl8qedbn.gif.neqp	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\qg8i9g0tihejna tr3l.flv.neqp	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\fmxha_w4eke5pf8l.mp4.neqp	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 sports.url.neqp	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\koomr.pptx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\byf8cf9eozrq2jwpt66.gif.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\msn websites\msn.url.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\n7DfguJMJ.mp4.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Favorites\Microsoft Websites\Microsoft At Home.url.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\microsoft websites\ie site on microsoft.com.url.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\c0YtBs zGXD9sK\qJTFnnuSQ.ppt.neqp	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\mxfa2rzxqyhankfzm\jtbbgg -ujwe3.bmp.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\MXfa2rZxqyhANkfzM\NECDkoymaUw.png.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\a4hxep_8v\6ayirlethvq1qbrj-l\gbpqlruev5tl.pptx.neqp	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\1bzpfxjukgmx2ljc8ae7\vztrk63idaphpsstgre.pptx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\gfravduy7lom.swf.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\qYyGPLt6OoKeyh2R.m4a.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\VuYJSL8GFd0.mp3.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\HAyp2zHURXEkt5y6c.mp3.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Videos\OJNEj2xIV52LVtvj-s0.flv.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\aFVf9.swf.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\twNoq6e1V6eeLj TB7f\qfXQc2cUy7GFzzlXBjR.m4a.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\hvolbk.mp3.neqp	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\eysf0phwcb.mp3.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\NBxo5Eh8J.swf.neqp	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\NhQ2zMqJr.flv.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\desktop\twnoq6e1v6eelj tb7f\djfpsjtvq\-6sm.bmp.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Favorites\Windows Live\Windows Live Gallery.url.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\YiJlu.mp3.neqp	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\SZzcxiUb3S1y0E.pptx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\mxfa2rzxqyhankfzm\rx-ru.png.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\nqugwix.bmp.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Pictures\dwHz_UcKn2C.bmp.neqp	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\jcuukzkpdwtrtf.flv.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\osw75xo0982bw.swf.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\videos\ompo2s.flv.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\epp3ouzeazkkjj5hj.wav.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\microsoft websites\ie add-on site.url.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\A4HxEP_8V\c0YtBs zGXD9sK\Yz_Q1.doc.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\s7lh3hxtittmcvgh\r6fjlezzg_wtj.ots.neqp	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\twnoq6e1v6eelj tb7f\iyl6m -whjjeo.wav.neqp	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\FU2nzV-k.pdf.neqp	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\gwqS.gif.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\d7illvxbgi6q.wav.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\favorites\links\web slice gallery.url.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\pictures\ote5jpyt.jpg.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\AQRFNBZ8zX.jpg.neqp	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\uftb9wa27mlfv.mp3.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Desktop\h5j527Mxht9SX2raeS80.mp3.neqp	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\rrbusch3n2s3k7tf26.wav.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\S7LH3hXtiTTmcVgH\VDXnqC 6DK_84Fuegb.xlsx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\r5XNSimbuw.xlsx.neqp	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\BBqFu3hstVTMPJkSfOH.mp3.neqp	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\8nyqrh805h9-og.avi.neqp	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\get windows live.url.neqp	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Favorites\MSN Websites\MSN Autos.url.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\3r0MOWhclDm.pptx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\music\xvszdq6io_y8wjxlgib.wav.neqp	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	Djvu	Djvu Ransomware	Memory Dump	-	Ransomware	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\A8Ch.xlsx.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Documents\1bZpFXJUkgMx2ljc8Ae7\3BEbvfVE1d-gqz.doc.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	C:\Users\kEecfMwgj\Music\mqLZS9o6DtidQLz.m4a.neqp	Ransomware	5/5
Ransomware	DjvuEncryptedFile	File encrypted by Djvu Ransomware	Dropped File	c:\users\keecfmwgj\documents\1bzpfxjukgmx2ljc8ae7\fcf5zjaps1nelg.csv.neqp	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	2023.2.0
Dynamic Engine Version	2023.2.0 / 04/13/2023 04:20
Static Engine Version	2023.2.0.0 / 2023-04-13 03:00:20
AV Exceptions Version	2023.2.1.4 / 2023-04-17 18:38:13
Link Detonation Heuristics Version	2023.2.1.11 / 2023-05-25 14:08:46
Smart Memory Dumping Rules Version	2023.2.1.4 / 2023-04-17 18:38:13
Config Extractors Version	2023.2.1.11 / 2023-05-25 14:08:46
Signature Trust Store Version	2023.2.1.4 / 2023-04-17 18:38:13
VMRay Threat Identifiers Version	2023.2.1.13 / 2023-06-02 06:54:11
YARA Built-in Ruleset Version	2023.2.1.13

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	8.0.1710.11

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