ID: 373375
Sample Name: run.txt
Cookbook: default.jbs
Time: 22:49:34
Date: 22/03/2021
Version: 31.0.0 Emerald

Table of Contents

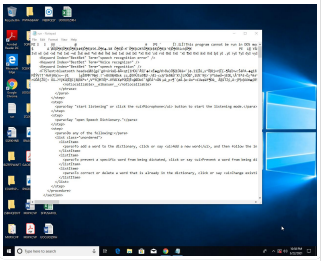
Analysis Report run.txt

Overview

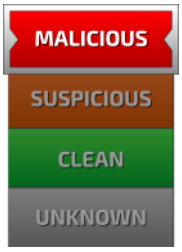
General Information

Sample Name:	run.txt
Analysis ID:	373375
MD5:	a80859c1cd44da..
SHA1:	46396892b9cafb2.
SHA256:	b270e245132cf66.
Infos:	

Most interesting Screenshot:



Detection

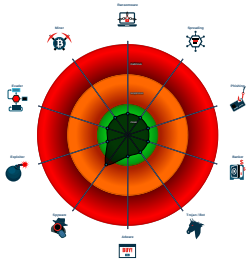


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Machine Learning detection for samp…
- Monitors certain registry keys / valu…
- PE file contains an invalid checksum
- Program does not show much activi…
- Queries the volume information (nam…
- Uses 32bit PE files

Classification



Startup

- **System is w10x64**
- notepad.exe (PID: 6068 cmdline: 'C:\Windows\system32\NOTEPAD.EXE' C:\Users\user\Desktop\run.txt MD5: BB9A06B8F2DD9D24C77F389D7B2B58D2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

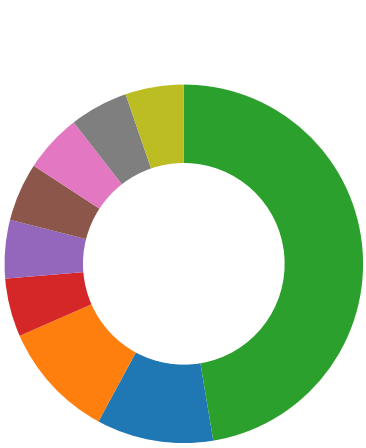
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- System Summary



Click to jump to signature section

AV Detection:

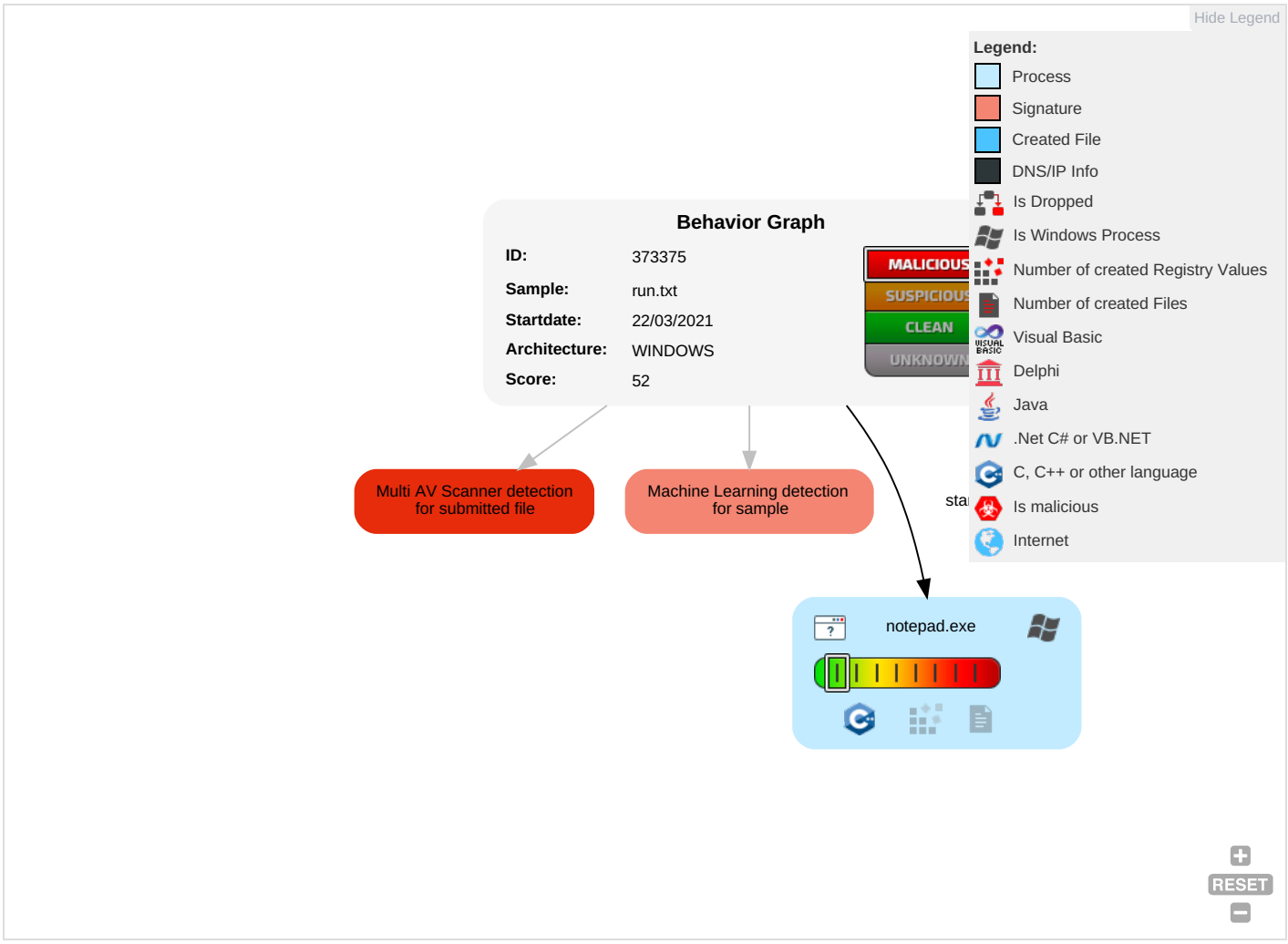
Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Software Packing 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

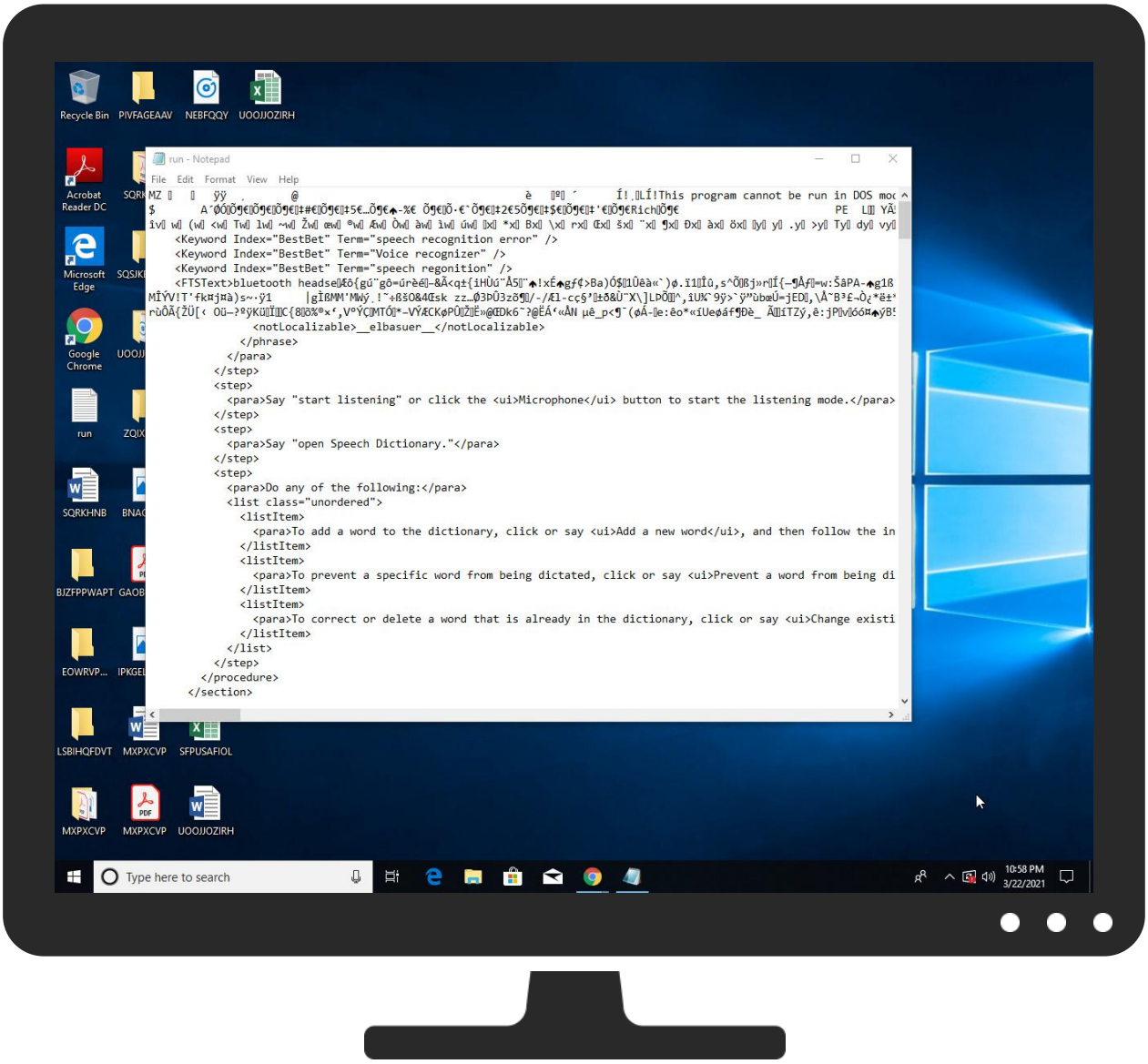
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
run.txt	7%	Virustotal		Browse
run.txt	9%	ReversingLabs		
run.txt	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	373375
Start date:	22.03.2021
Start time:	22:49:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	run.txt
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.winTXT@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .txt
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, RuntimeBroker.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.626660297937805
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	run.txt
File size:	305152
MD5:	a80859c1cd44daad1450948a1276bc0d
SHA1:	46396892b9cafb2e59b8f667ec7822d0435384bb
SHA256:	b270e245132cf6624fc96642532a00c0a16681f59542220ad2c389d45865141f
SHA512:	ce68470318b8472b30aeee8778802ca4c9175f075a9c19c8332a08a6a8518a2f157a9e2ccaedba 1d42f83f591d3c5f233ee1b8b8fbb90589aae82c9dea68352c
SSDEEP:	6144:xF1V8YAbIgXuYAS53LcbJ2A0ZzbYhHqh69j:nu5dAc3QbJLdHC69
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....#.....5.....%.....`.....2.5.....$.....'.....Rich.....PE..L...Y..I.. .....

File Icon

Icon Hash:	74f4e4e4e4e4e4e4

Static PE Info

General

Entrypoint:	0x103916f

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x49BEC359 [Mon Mar 16 21:23:37 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	59690c603d08fbbc4dbba6c9f3250e8d

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F4554F19447h
call 00007F4554F1D413h
push dword ptr [ebp+08h]
mov ecx, dword ptr [ebp+10h]
mov edx, dword ptr [ebp+0Ch]
call 00007F4554F19331h
pop ecx
pop ebp
retn 000Ch
mov edi, edi
push esi
push 00000001h
push 010480D0h
mov esi, ecx
call 00007F4554F1D485h
mov dword ptr [esi], 01004FB0h
mov eax, esi
pop esi
ret
mov dword ptr [ecx], 01004FB0h
jmp 00007F4554F1D4EAh
mov edi, edi
push ebp
mov ebp, esp
push esi
mov esi, ecx
mov dword ptr [esi], 01004FB0h
call 00007F4554F1D4D7h
test byte ptr [ebp+08h], 00000001h
je 00007F4554F19449h
push esi
call 00007F4554F1D540h
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp

Instruction
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007F4554F1D456h
mov dword ptr [esi], 01004FB0h
mov eax, esi
pop esi
pop ebp
retn 0004h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 0Ch
jmp 00007F4554F1944Fh
push dword ptr [ebp+08h]
call 00007F4554F1D77Ah
pop ecx
test eax, eax
je 00007F4554F19451h
push dword ptr [ebp+08h]
call 00007F4554F1D694h
pop ecx
test eax, eax
je 00007F4554F19428h
leave
ret
test byte ptr [0109F758h], 00000001h
mov esi, 0109F74Ch
jne 00007F4554F1945Bh
or dword ptr [0109F758h], 01h

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [ASM] VS2008 build 21022 • [LNK] VS2008 build 21022 • [EXP] VS2008 build 21022 • [IMP] VS2008 SP1 build 30729 • [C++] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x47af0	0x5d	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x472fc	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa2000	0x10f4	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11a0	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x69c8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x160	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x46b4d	0x46c00	False	0.705692358657	data	6.72747064169	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x48000	0x59388	0x1600	False	0.311612215909	data	3.14391149509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xa2000	0x21e4	0x2200	False	0.427389705882	data	4.24755349001	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	GetFileAttributesW, GetTempFileNameW, CopyFileW, GetShortPathNameW, GetEnvironmentVariableW, WaitForMultipleObjects, VirtualProtect, Sleep, GetSystemDirectoryW, CreateSemaphoreW, VirtualProtectEx, GetProcessHeap, GetCurrentThreadId, GetCommandLineA, GetCPInfo, InterlockedIncrement, InterlockedDecrement, GetACP, GetOEMCP, IsValidCodePage, GetModuleHandleW, GetProcAddress, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetLastError, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, EnterCriticalSection, LeaveCriticalSection, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, HeapFree, CloseHandle, RtlUnwind, ExitProcess, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, HeapCreate, HeapDestroy, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapAlloc, RaiseException, LCMapStringA, MultiByteToWideChar, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, ReadFile, InitializeCriticalSectionAndSpinCount, HeapReAlloc, GetModuleHandleA, VirtualAlloc, SetStdHandle, WriteFile, GetConsoleCP, GetConsoleMode, FlushFileBuffers, CreateFileA, LoadLibraryA, HeapSize, SetFilePointer, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, SetEndOfFile
WTSAPI32.dll	WTSQueryUserToken, WTSCloseServer, WTSOpenServerW

Exports

Name	Ordinal	Address
Seasonweight	1	0x1037ca0
Viewexpect	2	0x1038260

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: notepad.exe PID: 6068 Parent PID: 5972

General

Start time:	22:50:28
Start date:	22/03/2021
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\NOTEPAD.EXE' C:\Users\user\Desktop\run.txt
Imagebase:	0x7ff608980000
File size:	245760 bytes
MD5 hash:	BB9A06B8F2DD9D24C77F389D7B2B58D2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	By

Disassembly

Code Analysis