ID: 674157
Sample Name: nvbbzu.xml
Cookbook: default.jbs
Time: 09:56:31
Date: 27/07/2022
Version: 35.0.0 Citrine

Table of Contents

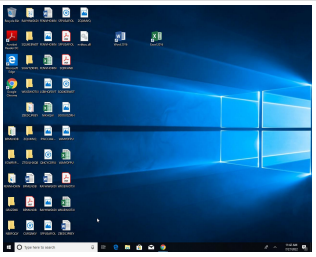
Windows Analysis Report

nvbbzu.xml

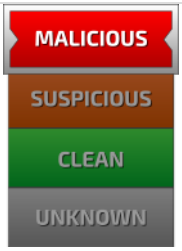
Overview

General Information

Sample Name:	nvbbzu.xml (renamed file extension from xml to dll)
Analysis ID:	674157
MD5:	60aafd76fbfa15d..
SHA1:	a968c42da88754..
SHA256:	46aa7de354f23a..
Infos:	



Detection



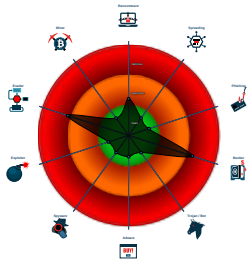
Dridex Dropper

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Dridex dropper found
- Tries to detect sandboxes / dynamic…
- Machine Learning detection for sam…
- Uses 32bit PE files
- Contains functionality to call native …
- Sample file is different than original …
- Program does not show much activi…
- Uses code obfuscation techniques (…
- Creates a process in suspended mo…
- Checks if the current process is bei…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 3224 cmdline: loaddll32.exe "C:\Users\user\Desktop\nvbbzu.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 5016 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\nvbbzu.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5104 cmdline: rundll32.exe "C:\Users\user\Desktop\nvbbzu.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud

Dridex dropper found

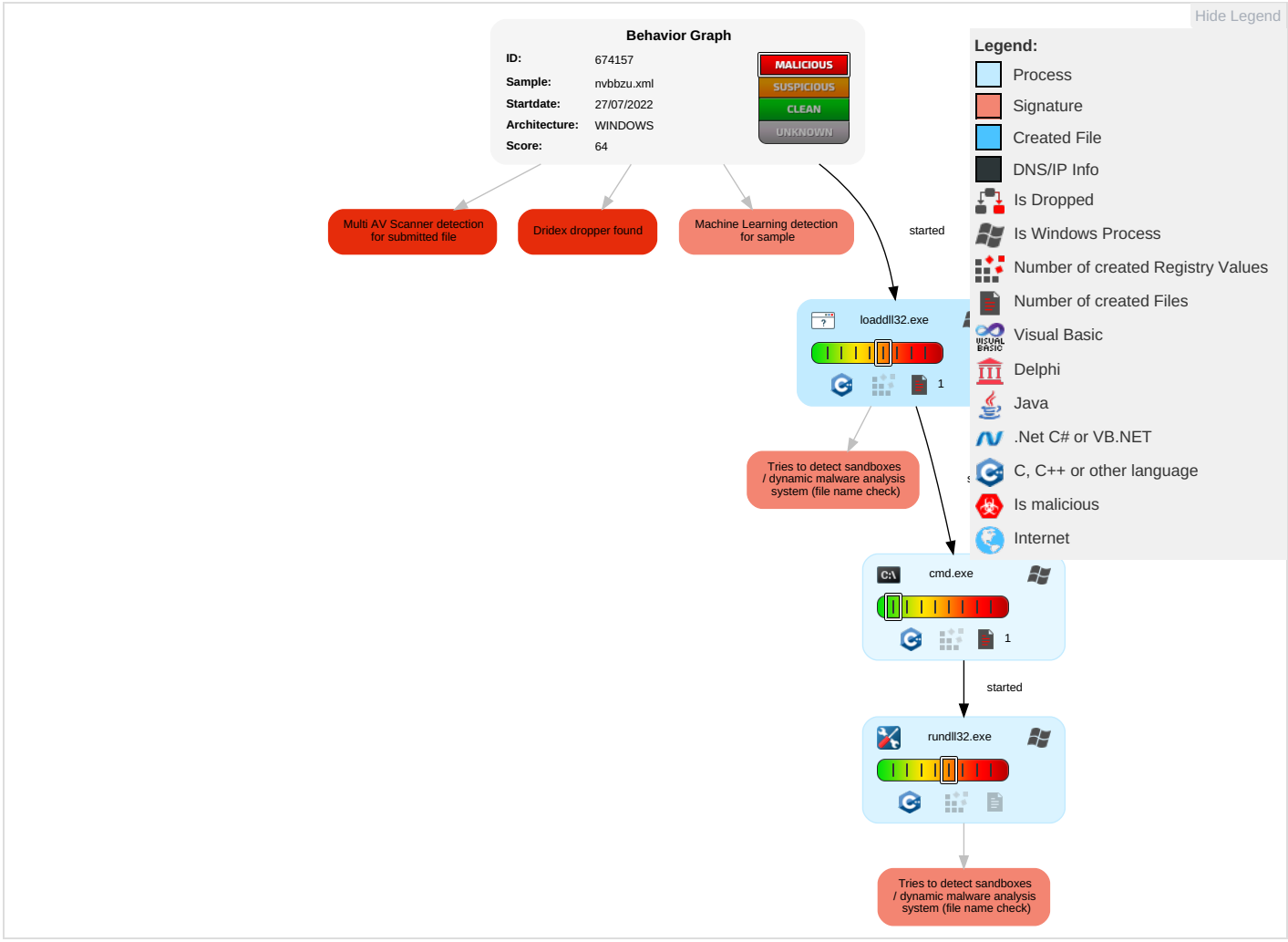
Malware Analysis System Evasion

Tries to detect sandboxes / dynamic malware analysis system (file name check)

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	1 1 Process Injection	1 1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	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	1 Rundll32	LSASS Memory	1 1 Virtualization/Sandbox Evasion	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)	1 Software Packing	Security Account Manager	1 System Information Discovery	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

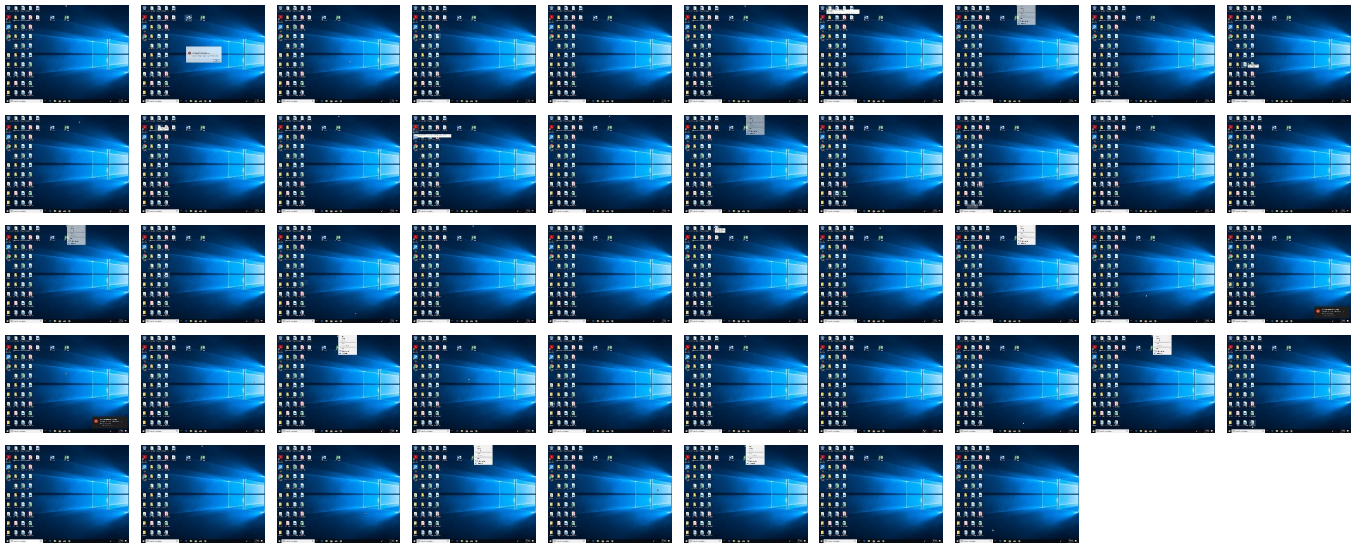
Behavior Graph



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
nvbbzu.dll	49%	Virustotal		Browse
nvbbzu.dll	29%	Metadefender		Browse
nvbbzu.dll	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

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	674157
Start date and time: 27/07/202209:56:31	2022-07-27 09:56:31 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nvbbzu.xml (renamed file extension from xml to dll)
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:	34
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:	mal64.bank.evad.winDLL@5/0@0/0
EGA Information:	• Successful, ratio: 100%
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 • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, time.windows.com, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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):	7.935740919082391
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:	nvbbzu.dll
File size:	1511424
MD5:	60aafd76fbfa15db34a0b2f93df5eea9
SHA1:	a968c42da887544c4f46aa9924914022be44a40a
SHA256:	46aa7de354f23ab96c0c4bf31a8ef06e6c2cf257dadce53d0a7f6e7d49a1fb6a
SHA512:	479cc535c1919db804ec4c68537798fe6ab58fa7f6684cdc3f0ba35ce76632aff90997ae7314ee5012620a672ad00d2b564fa409dc31a4eba1d0248d63194880
SSDEEP:	24576:Hdm2mGTXVABupDnsuAq7xwrPMscrKRC8G56elJiPp1E3dnsMu9n0Y7vo4EKa0ew8:HOGTXVAQsnPMRmk8yMPcdZu9n3E/0dAT
TLSH:	6265F1F43D22E493E20B5C35325992633769AF2F454D9CC96CAD00CCC4A2EA79AFE535
File Content Preview:	MZ.....@.....,...gf..#...#...#...*.....*.....=U..... .z.....^~{.w....c.....MZe.$...*...w... .G.h...MZ.....E.1...^~G.....V. ... .z.....^..R.....S.....^~F.....=U.....#.....Y..a....Y.....UF....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x401118
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE, DLL
DLL Characteristics:	GUARD_CF
Time Stamp:	0x411098E1 [Wed Aug 4 08:05:53 2004 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:	cc6005bdfb7408430874b385b3fa9363

Entrypoint Preview

Instruction
mov eax, edx
mov edx, 00000067h
add dword ptr [00425534h], edi
lea eax, dword ptr [00425540h]
add dword ptr [eax], esp
cmp edx, 66h
jne 00007F5990727BD7h
call 00007F5990727AAEh
lea eax, dword ptr [00425538h]
mov dword ptr [eax], ebx
mov eax, esi
add dword ptr [00425530h], eax
mov edx, ebp
add dword ptr [0042553Ch], edx
call 00007F5990727BB3h
inc eax
ret
mov dword ptr [ebp+00h], eax
push ebp
mov ebp, esp
and esp, FFFFFFF8h
sub esp, 78h
xor eax, eax
mov dword ptr [esp+68h], eax
mov eax, dword ptr [esp+68h]
mov dword ptr [esp+6Ch], 0000030Bh
mov ecx, esp
lea edx, dword ptr [esp+6Ch]
mov dword ptr [ecx+08h], edx
lea edx, dword ptr [esp+70h]
mov dword ptr [ecx+04h], edx
mov dword ptr [ecx+0Ch], 000005C1h
mov dword ptr [ecx], 00820F62h
mov ecx, dword ptr [00403044h]
mov dword ptr [esp+64h], eax
call ecx
sub esp, 10h

Instruction
mov ecx, esp
mov dword ptr [ecx+04h], 00000380h
mov dword ptr [ecx], 00D8B267h
mov ecx, dword ptr [00403124h]
mov dword ptr [esp+60h], eax
call ecx
sub esp, 08h
xor ecx, ecx
mov dword ptr [esp+5Ch], eax
mov dword ptr [esp+58h], ecx
mov eax, dword ptr [esp+58h]
mov ecx, eax
and ecx, 0000000Fh
cmp ecx, 00000002h
mov dword ptr [esp+54h], eax
jne 00007F5990727BDEh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x46cc	0xf0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x16d000	0x350	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x16e000	0x2c1c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3000	0x178	.rdata
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
.text	0x1000	0x1b4e	0x2000	False	0.51171875	data	5.337400275912443	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x202f	0x3000	False	0.19856770833333334	data	4.699681580901602	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x6000	0x20300	0x20000	False	0.33522796630859375	data	6.825176440670153	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT0	0x27000	0xa2c61	0xa3000	False	0.9951186852952454	data	7.9950313512995645	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.crt1	0xca000	0xa2cc5	0xa3000	False	0.9950722536426381	data	7.9949535185054375	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x16d000	0x350	0x1000	False	0.1044921875	data	0.8940808274374962	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_MEM_READ
.reloc	0x16e000	0x399a	0x4000	False	0.17364501953125	data	4.892382486928004	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x16d060	0x2f0	SysEx File - IDP	English	United States

Imports

DLL	Import
WS2_32.dll	send
WININET.dll	FindFirstUrlCacheEntryExW
USER32.dll	GetWindowLongW, LoadCursorA, GetWindowDC, IsCharUpperA, DefMDIChildProcW, GetMenuItemID, FindWindowA, GetMenuBarInfo, GetScrollBarInfo, LoadKeyboardLayoutA, GetMenuStringA, GetWindowTextA, GetTabbedTextExtentA, GetUpdateRgn
WINSPOOL.DRV	GetPrinterA
KERNEL32.dll	GetFileAttributesA, FlushConsoleInputBuffer, GetDateFormatA, EnumTimeFormatsA, FindNextVolumeMountPointW, DeleteCriticalSection, GlobalGetAtomNameA, lstrcpynW, GetProfileIntW, GetStartupInfoA, GetComputerNameExW, GetLastError, LoadLibraryExA, GetPrivateProfileIntA, GetCPInfo, GetTempPathA, GetTapePosition, Module32Next, DeleteTimerQueue, GetConsoleWindow, GetTapeStatus, VirtualProtect, GlobalAddAtomW, GetLocalTime, GetUserDefaultUILanguage, GetSystemInfo, FindActCtxSectionStringW, GetQueuedCompletionStatus, GetWindowsDirectoryA, DebugBreak, FlushViewOfFile, GenerateConsoleCtrlEvent, GetLogicalDriveStringsW, CloseHandle, GetCurrentThreadId, OutputDebugStringA, LoadLibraryW, GetModuleHandleA, GetUserDefaultLangID, SetTapePosition, OpenProcess, GetFileTime
ADVAPI32.dll	GetWindowsAccountDomainSid, GetSecurityDescriptorDacl, DeleteService, LogonUserExW, NotifyBootConfigStatus, EnumServicesStatusW
CRYPT32.dll	CryptGetDefaultOIDFunctionAddress
GDI32.dll	EndDoc, GetRasterizerCaps, ExtEscape, ExcludeClipRect, GetTextExtentExPointA, ExtTextOutW, FrameRgn, GetPaletteEntries, PolyPolyline, GetCurrentObject, GetOutlineTextMetricsW
OLEAUT32.dll	VariantCopyInd
msvcrt.dll	fputws, strspn, toupper, fseek
SHELL32.dll	ExtractIconExA

Possible Origin

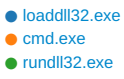
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: **3224**, Parent PID: **6004**

General	
Target ID:	1
Start time:	09:57:34
Start date:	27/07/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\nvbbzu.dll"
Imagebase:	0xca0000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **5016**, Parent PID: **3224**

General	
Target ID:	2
Start time:	09:57:34
Start date:	27/07/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\nvbbzu.dll",#1
Imagebase:	0x1190000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5104**, Parent PID: **5016**

General

Target ID:	4
Start time:	09:57:35
Start date:	27/07/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\nvbbzu.dll",#1
Imagebase:	0x3e0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly