ID: 778226
Sample Name:
LwNdQo4zIk.exe
Cookbook: default.jbs
Time: 08:51:27
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

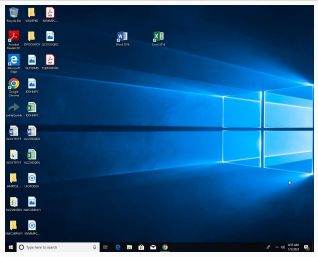
Windows Analysis Report

LwNdQo4zlk.exe

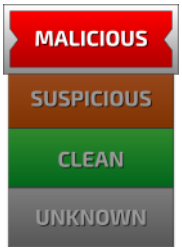
Overview

General Information

Sample Name:	LwNdQo4zlk.exe
Analysis ID:	778226
MD5:	3ccd6b369eb1dd..
SHA1:	aee399e263c838..
SHA256:	f5717aef9a43238.
Tags:	32 exe
Infos:	



Detection

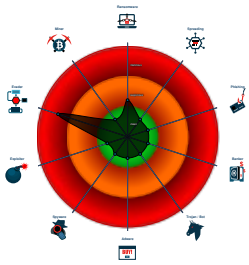


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Detected unpacking (changes PE se…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for drop…
- Machine Learning detection for sam…
- Uses 32bit PE files
- Yara signature match
- Antivirus or Machine Learning detec…
- Drops PE files
- Uses code obfuscation techniques (…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- LwNdQo4zlk.exe (PID: 1792 cmdline: C:\Users\user\Desktop\LwNdQo4zlk.exe MD5: 3CCD6B369EB1DDE57D181E7550BD7268)
  - rundll32.exe (PID: 5472 cmdline: "C:\Windows\system32\rundll32.exe" "C:\Users\user\AppData\Local\Temp\Pyupydeoe.tmp",Uprsprhaot MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.309288628.0000000002330000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000000.00000002.309087545.0000000002254000.00000040.00000800.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x798:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B

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

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

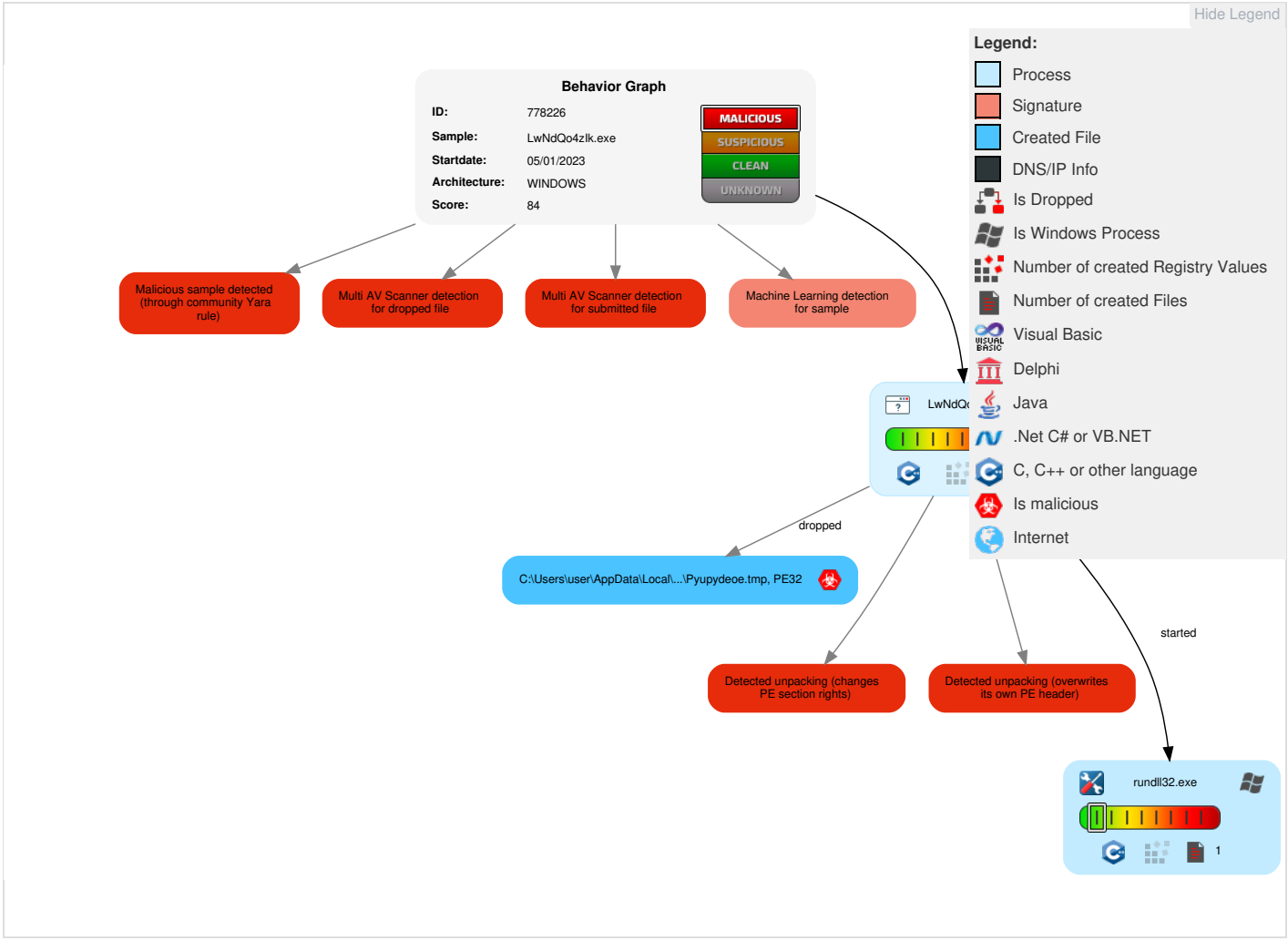
Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

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	2 Process Injection	1 Rundll32	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 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	2 2 Software Packing	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Process Injection	Security Account Manager	2 Process 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 Obfuscated Files or Information	NTDS	3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

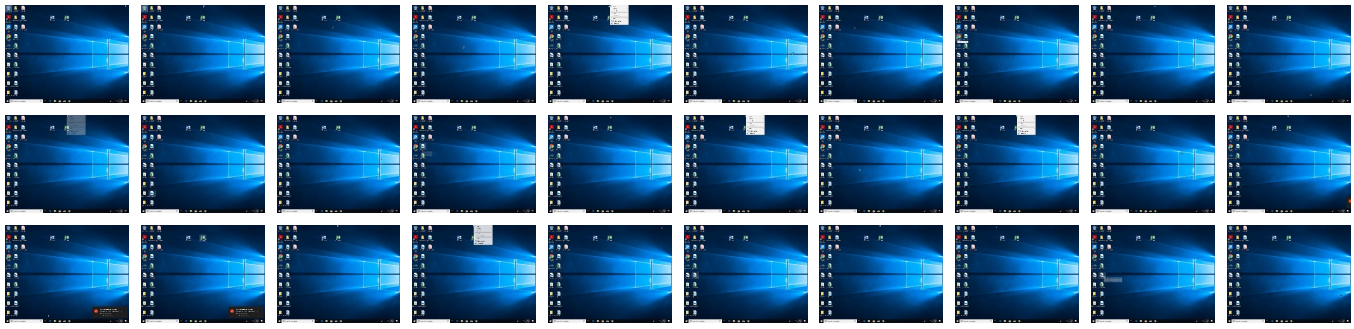
Behavior Graph



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
LwNdQo4zIk.exe	49%	Virustotal		Browse
LwNdQo4zIk.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Pyupydeoe.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Pyupydeoe.tmp	50%	ReversingLabs	Win32.Trojan.Lazy	
C:\Users\user\AppData\Local\Temp\Pyupydeoe.tmp	64%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.LwNdQo4zIk.exe.2330e67.1.unpack	100%	Avira	HEUR/AGEN.1215478		Download File
0.2.LwNdQo4zIk.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
0.3.LwNdQo4zIk.exe.2450000.0.unpack	100%	Avira	HEUR/AGEN.1215478		Download File

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:	36.0.0 Rainbow Opal
Analysis ID:	778226
Start date and time:	2023-01-05 08:51:27 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	LwNdQo4zIk.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	7
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:	mal84.evad.winEXE@3/1@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- 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

C:\Users\user\AppData\Local\Temp\Pyupydeoe.tmp

Process:	C:\Users\user\Desktop\LwNdQo4zIk.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	803328
Entropy (8bit):	6.89627808323015
Encrypted:	false
SSDEEP:	24576:l8Jr+SgWH5UB/VdYQ/N7WqpWaQxYZYBsFn:OJrSBYqLY
MD5:	C50C2F17112B6C6B0892CB2C1F502108
SHA1:	3DD1444384BF790F5AA90AE95EF7745FA4CFAF72
SHA-256:	20DC61C5456EA5756F432AEBECF74660ACEBF5ACE0F7C8D1B360757ED79075D8
SHA-512:	BFBFC3A13816A12E25C373F6739215B9DFF559FECFDF26C3358A452BDC833B6EAA64BBAE316F4B29B9E9CE802E9F50C66B533C8C3C1B372025A7F0B7D8B452F1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 50% • Antivirus: Virustotal, Detection: 64%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e:..![.@![.@![.@.,.A&[.@.,.A [.@L..A"[.@![.@5[.@.D.@([.@...A [.@...A [.@...A [.@Rich![.@.....PE..L.....c.....!.....p.....@.....@.....<.....{..... .....@.....text...p..... ..`.rdata.....@..@.data...01.....2.....@....reloc...{.....|.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows

Entropy (8bit):	7.853487844881012
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	LwNdQo4zIk.exe
File size:	1034752
MD5:	3ccd6b369eb1dde57d181e7550bd7268
SHA1:	aee399e263c838570c00133feab275b81009e12a
SHA256:	f5717aef9a4323816387603920b652a94ac0d9cedef36391cedd9cdcbfef7f60
SHA512:	00bd3bb981e2a5bd4c30241025f352e9e528d76300e67fcdbe89ee9e12ecbba73b291aebd9b73f73a8aaa32e2a8b2d1b4d49796cdc11a1b891a313cf0a9dcc03
SSDEEP:	24576:RFOWvM7bZBFpXIDpRjJ5JAXVm359Ov9UIrczuX:RguWRNpRjJPgAp9ucz
TLSH:	B7251201329194A7C1CA6A3C4930E7F02D7FBCF29D7CE187EB643A1E9E706B14A55687
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:.Y.....Z.....L.....K..... [.....^.....Rich.....PE..L....7.b...

File Icon

Icon Hash:	9062e090c6e73144

Static PE Info

General

Entrypoint:	0x40600e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x620337B3 [Wed Feb 9 03:40:35 2022 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:	7bca87c7309353055aed194207c93e99

Entrypoint Preview

Instruction
call 00007F9A3C5343C9h
jmp 00007F9A3C52ECEEh
int3
int3
int3
int3
int3
int3
int3
int3
mov edx, dword ptr [esp+0Ch]
mov ecx, dword ptr [esp+04h]
test edx, edx
je 00007F9A3C52EEDBh
xor eax, eax
mov al, byte ptr [esp+08h]

Instruction
test al, al
jne 00007F9A3C52EE88h
cmp edx, 00000100h
jc 00007F9A3C52EE80h
cmp dword ptr [0050CFACh], 00000000h
je 00007F9A3C52EE77h
jmp 00007F9A3C53447Dh
push edi
mov edi, ecx
cmp edx, 04h
jc 00007F9A3C52EEA3h
neg ecx
and ecx, 03h
je 00007F9A3C52EE7Eh
sub edx, ecx
mov byte ptr [edi], al
add edi, 01h
sub ecx, 01h
jne 00007F9A3C52EE68h
mov ecx, eax
shl eax, 08h
add eax, ecx
mov ecx, eax
shl eax, 10h
add eax, ecx
mov ecx, edx
and edx, 03h
shr ecx, 02h
je 00007F9A3C52EE78h
rep stosd
test edx, edx
je 00007F9A3C52EE7Ch
mov byte ptr [edi], al
add edi, 01h
sub edx, 01h
jne 00007F9A3C52EE68h
mov eax, dword ptr [esp+08h]
pop edi
ret
mov eax, dword ptr [esp+04h]
ret
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push edi
push esi
mov esi, dword ptr [ebp+0Ch]
mov ecx, dword ptr [ebp+10h]
mov edi, dword ptr [ebp+08h]
mov eax, ecx
mov edx, ecx
add eax, esi
cmp edi, esi
jbe 00007F9A3C52EE7Ah

Instruction
cmp edi, eax
jc 00007F9A3C52F01Ah
cmp ecx, 00000100h
jc 00007F9A3C52EE91h
cmp dword ptr [0050CFACh], 00000000h
je 00007F9A3C52EE88h
push edi
push esi
and edi, 0Fh

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x16dec	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10d000	0xbcb0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	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	0x43a0	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.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
.text	0x1000	0x16850	0x16a00	False	0.5431198204419889	data	6.3410785244090935	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x18000	0xf4fb4	0xd9e00	False	0.9918356461560528	data	7.991407419226785	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x10d000	0xbcb0	0xbe00	False	0.38569078947368424	data	4.2370546659086274	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0x1160a0	0x2	data		
AFX_DIALOG_LAYOUT	0x116098	0x2	data		
AFX_DIALOG_LAYOUT	0x1160a8	0x2	data		
AFX_DIALOG_LAYOUT	0x1160b0	0x2	data		
AFX_DIALOG_LAYOUT	0x1160b8	0x2	data		
RT_CURSOR	0x1160c0	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x116208	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0		
RT_CURSOR	0x116338	0xf0	Device independent bitmap graphic, 24 x 48 x 1, image size 0		

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x116428	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_CURSOR	0x117500	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x10d6e0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Serbian	Italy
RT_ICON	0x10dda8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Serbian	Italy
RT_ICON	0x10e310	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Serbian	Italy
RT_ICON	0x10f3b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Serbian	Italy
RT_ICON	0x10f860	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Serbian	Italy
RT_ICON	0x110708	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Serbian	Italy
RT_ICON	0x110fb0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Serbian	Italy
RT_ICON	0x111678	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Serbian	Italy
RT_ICON	0x111be0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	Serbian	Italy
RT_ICON	0x114188	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	Serbian	Italy
RT_ICON	0x115230	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	Serbian	Italy
RT_ICON	0x115bb8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	Serbian	Italy
RT_STRING	0x117f18	0xea	data	Serbian	Italy
RT_STRING	0x118008	0x348	data	Serbian	Italy
RT_STRING	0x118350	0x682	data	Serbian	Italy
RT_STRING	0x1189d8	0x2d8	data	Serbian	Italy
RT_GROUP_CURSOR	0x1161f0	0x14	data		
RT_GROUP_CURSOR	0x117da8	0x14	data		
RT_GROUP_CURSOR	0x1174d0	0x30	data		
RT_GROUP_ICON	0x116020	0x76	data	Serbian	Italy
RT_GROUP_ICON	0x10f820	0x3e	data	Serbian	Italy
RT_VERSION	0x117dc0	0x154	Encore not stripped - version 79		

Imports

DLL	Import
KERNEL32.dll	GetConsoleAliasW, GetModuleHandleW, CreateDirectoryExW, ReadConsoleInputW, GetTempPathW, GetSystemDirectoryW, RemoveDirectoryW, OutputDebugStringA, GetProcAddress, LocalAlloc, GetBinaryTypeA, SearchPathA, VerifyVersionInfoA, SetProcessPriorityBoost, EndUpdateResourceA, FindNextFileW, FindFirstVolumeA, LocalShrink, GlobalFlags, _llseek, UpdateResourceA, CreateActCtxW, CopyFileW, AddConsoleAliasW, CreateMutexA, GetCurrentActCtx, GetDiskFreeSpaceA, MoveFileW, GetLogicalDriveStringsA, SetEvent, MoveFileExA, CreateMailslotA, WriteConsoleInputA, TerminateThread, GetCurrentProcess, RtlCaptureContext, InterlockedCompareExchange, GetFileTime, lstrcatA, FindFirstFileW, FreeEnvironmentStringsA, SetErrorMode, InterlockedExchangeAdd, MoveFileWithProgressA, GetTickCount, SetLastError, GetPrivateProfileStructW, VerSetConditionMask, LoadLibraryA, GetLastError, DeleteFileA, GetStartupInfoW, TerminateProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetModuleHandleA, HeapFree, HeapAlloc, EnterCriticalSection, LeaveCriticalSection, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, Sleep, ExitProcess, WriteFile, GetModuleFileNameA, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, GetCurrentThreadId, InterlockedDecrement, HeapCreate, VirtualFree, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, RaiseException, VirtualAlloc, HeapReAlloc, SetFilePointer, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, InitializeCriticalSectionAndSpinCount, RtlUnwind, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, ReadFile, HeapSize, CloseHandle, CreateFileA
GDI32.dll	SetBrushOrgEx

Possible Origin

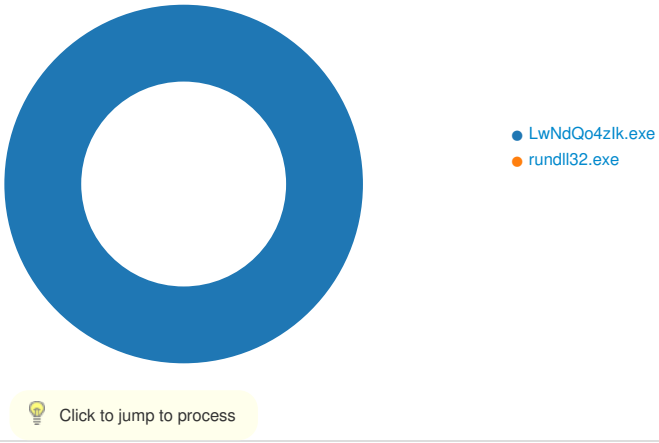
Language of compilation system	Country where language is spoken	Map
Serbian	Italy	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: LwNdQo4zIk.exe PID: 1792, Parent PID: 3528

General

Target ID:	0
Start time:	08:52:18
Start date:	05/01/2023
Path:	C:\Users\user\Desktop\LwNdQo4zIk.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\LwNdQo4zIk.exe
Imagebase:	0x400000
File size:	1034752 bytes
MD5 hash:	3CCD6B369EB1DDE57D181E7550BD7268
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.309288628.0000000002330000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.309087545.0000000002254000.00000040.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: rundll32.exe PID: 5472, Parent PID: 1792

General

Target ID:	1

Start time:	08:52:23
Start date:	05/01/2023
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\system32\rundll32.exe" "C:\Users\user\AppData\Local\Temp\Pyupydeoe.tmp",Uprsprhaot
Imagebase:	0xa0000
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly