ID: 247076
Sample Name:
zloader_1.17.0.0.vir
Cookbook: default.jbs
Time: 20:24:39
Date: 19/07/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

Analysis Report zloader_1.17.0.0.vir

Overview

General Information

Sample Name:	zloader_1.17.0.0.vir (renamed file extension from vir to exe)
Analysis ID:	247076
MD5:	2cddc5e9482b04..
SHA1:	c8fb26a5a4776ce..
SHA256:	0b37d287d10b55..

Most interesting Screenshot:

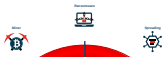
Detection

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Sample uses process hollowing tech…
- Abnormal high CPU Usage
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to read the PEB
- Contains functionality which may be…
- Creates a process in suspended mo…
- Detected potential crypto function

Classification



Startup

- **System is w10x64**
- zloader_1.17.0.0.exe (PID: 4312 cmdline: 'C:\Users\user\Desktop\zloader_1.17.0.0.exe' MD5: 2CDDC5E9482B049387C96B609ADA8FEA)
  - zloader_1.17.0.0.exe (PID: 3788 cmdline: 'C:\Users\user\Desktop\zloader_1.17.0.0.exe' MD5: 2CDDC5E9482B049387C96B609ADA8FEA)
    - explorer.exe (PID: 2016 cmdline: explorer.exe MD5: 499B0D1F6277F17B3BAC525B8717C064)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

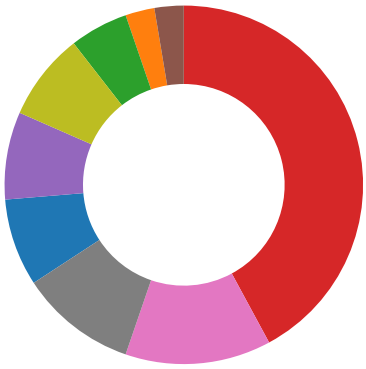
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection



- Cryptography
- Networking
- System Summary
- Data Obfuscation
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

HIPS / PFW / Operating System Protection Evasion:

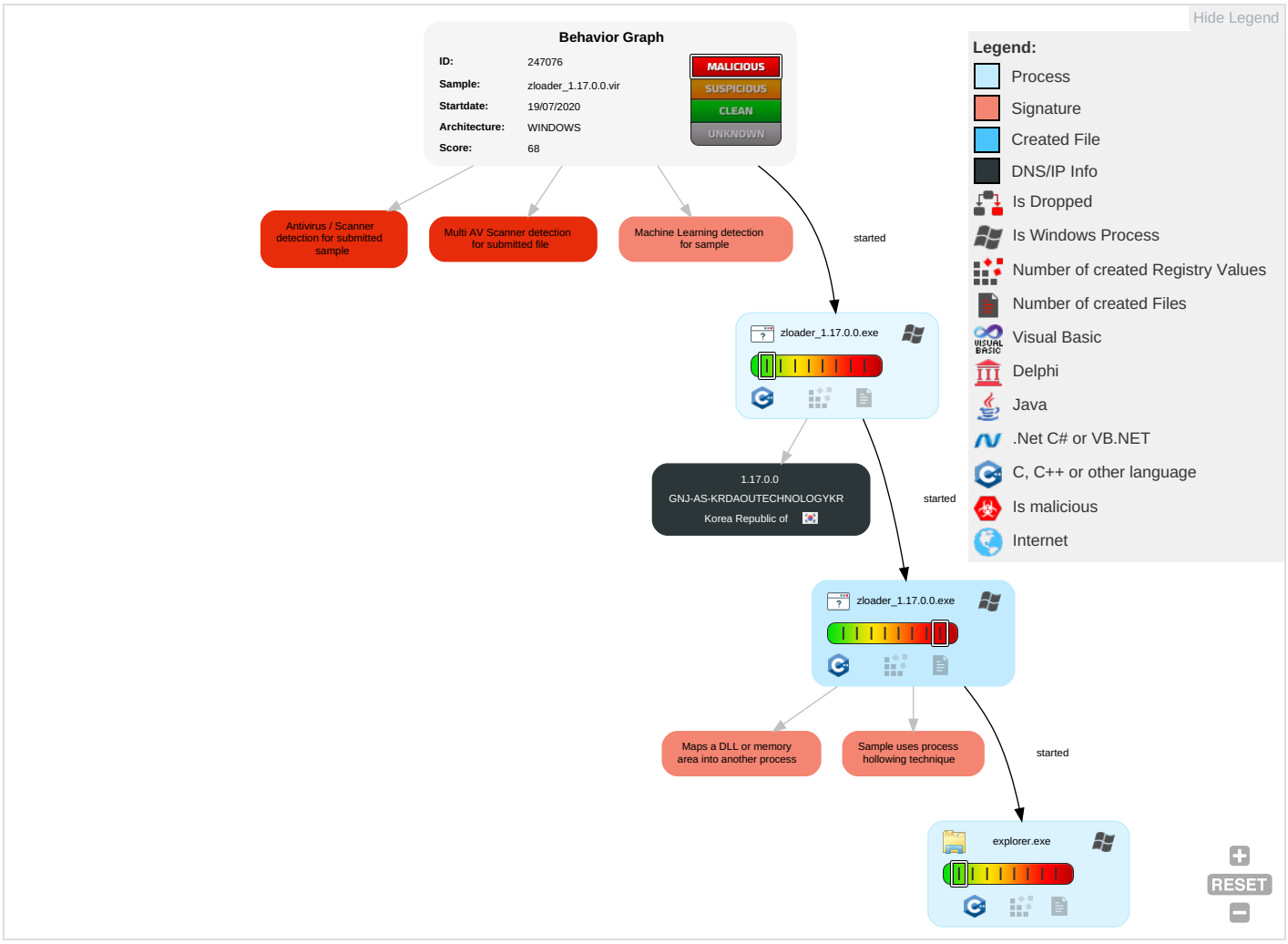
Maps a DLL or memory area into another process

Sample uses process hollowing technique

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
Valid Accounts	Command-Line Interface 2	Winlogon Helper DLL	Process Injection 2 1 2	Process Injection 2 1 2	Credential Dumping	System Time Discovery 1	Remote File Copy 1	Data from Local System	Data Encrypted 1	Standard Cryptographic Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track De Without Authoriza
Replication Through Removable Media	Execution through API 1	Port Monitors	Accessibility Features	Obfuscated Files or Information 1	Network Sniffing	Process Discovery 3	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Remote File Copy 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Dat Without Authoriza
External Remote Services	Execution through Module Load 1	Accessibility Features	Path Interception	Rootkit	Input Capture	Security Software Discovery 2	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Custom Cryptographic Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Obfuscated Files or Information	Credentials in Files	System Information Discovery 4	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication	SIM Card Swap	

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
zloader_1.17.0.0.exe	82%	Virustotal		Browse
zloader_1.17.0.0.exe	59%	Metadefender		Browse
zloader_1.17.0.0.exe	84%	ReversingLabs	Win32.Trojan.Hpgen	
zloader_1.17.0.0.exe	100%	Avira	HEUR/AGEN.1029189	
zloader_1.17.0.0.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.zloader_1.17.0.0.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.zloader_1.17.0.0.exe.c90000.0.unpack	100%	Avira	HEUR/AGEN.1029189		Download File
5.2.zloader_1.17.0.0.exe.2dc0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.zloader_1.17.0.0.exe.c90000.0.unpack	100%	Avira	HEUR/AGEN.1029187		Download File
5.2.zloader_1.17.0.0.exe.c90000.1.unpack	100%	Avira	HEUR/AGEN.1029189		Download File
7.2.explorer.exe.290000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.zloader_1.17.0.0.exe.c90000.0.unpack	100%	Avira	HEUR/AGEN.1029189		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://gerber.gdn/info.php	6%	Virustotal		Browse

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://gerber.gdn/info.phpO	explorer.exe, 00000007.0000000 2.887319750.0000000002DDA000.0 0000004.00000020.sdmp	false		unknown
http://gerber.gdn/info.php:	explorer.exe, 00000007.0000000 2.887319750.0000000002DDA000.0 0000004.00000020.sdmp	false		unknown
http://gerber.gdn/info.phpJ	explorer.exe, 00000007.0000000 2.887243939.0000000002DC3000.0 0000004.00000020.sdmp	false		unknown
http://gerber.gdn/info.phpZ	explorer.exe, 00000007.0000000 2.887319750.0000000002DDA000.0 0000004.00000020.sdmp	false		unknown
http://gerber.gdn/info.php	explorer.exe, 00000007.0000000 2.887604821.00000000046E9000.0 0000004.00000001.sdmp, explorer.exe, 00000007.00000002.887319750.00000 00002DDA000.00000004.00000020. sdmp	false	• 6%, Virustotal, Browse	unknown
http:// gerber.gdn/info.php39xew9y6f2iikg4a7hezad8fpxuv8tv1ri4yiqe c2a3pnvxvrvugqy2a197mrzki2sdqdgctnh	explorer.exe, 00000007.0000000 2.887604821.00000000046E9000.0 0000004.00000001.sdmp	false		unknown
http://dolbit.bit/info.php	explorer.exe, 00000007.0000000 2.887604821.00000000046E9000.0 0000004.00000001.sdmp	false		unknown

Contacted IPs

Public

IP	Country	Flag	ASN	ASN Name	Malicious
1.17.0.0	Korea Republic of		45996	GNJ-AS-KRDAOUTECHNOLOGYKR	false

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	247076
Start date:	19.07.2020
Start time:	20:24:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zloader_1.17.0.0.vir (renamed file extension from vir to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	8
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:	mal68.evad.winEXE@5/0@0/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 34.6% (good quality ratio 29.5%) • Quality average: 72.9% • Quality standard deviation: 36.6%
HCA Information:	• Successful, ratio: 71% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GNJ-AS-KRDAOUTECHNOLOGYKR	WebClient-Setup-1.17.0.17.exe	Get hash	malicious	Browse	• 1.17.0.17
	ZJcjah4oT3.doc	Get hash	malicious	Browse	• 27.102.66.105
	ZJcjah4oT3.doc	Get hash	malicious	Browse	• 27.102.66.105
	iSee-1.18.2.0-windows-installer (1).exe	Get hash	malicious	Browse	• 1.18.2.0
	iSee-1.18.2.0-windows-installer.exe	Get hash	malicious	Browse	• 1.18.2.0
	http://m.networkadex.com/files/nwk.exe	Get hash	malicious	Browse	• 115.71.15.28
	www.dongwoo.co.kr/	Get hash	malicious	Browse	• 27.1.43.73
	73RR918938476SG.js	Get hash	malicious	Browse	• 27.1.43.73

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.247386215994817
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:	zloader_1.17.0.0.exe
File size:	266240
MD5:	2cddc5e9482b049387c96b609ada8fea
SHA1:	c8fb26a5a4776ceb5572c5139d9057a8040f68b8
SHA256:	0b37d287d10b55a50f1a717a015503b64d3be3586f15a12 a0085d61794864235
SHA512:	d19429d362f80feace554706fa1d905148301d628e14ef0 86a66b175c94489e736f512b4284010d9a52090203dba7 1684a397c95017f8c0b16f0b0512c28f141
SSDEEP:	3072:sdhM4Q+hmghguGQGcCfpZqPmeOlhF8ZXNO5X VcjEZip:sdhu/fpAPNOhFSXN
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^PR.0.R.0.R.0.=...[.0.=...Z.0.=...j.0.[...W.0.R.1...0.=...S.0.=...S.0.=...S.0.RichR.0.....PE..L...[..X...

File Icon

Icon Hash:	7cf8dcd4d4d4d4c0

Static PE Info

General

Entrypoint:	0x4011e5
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x58EC0A5B [Mon Apr 10 22:42:35 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	0929aec5d58f2fb36225bca3920f81f9

Entrypoint Preview

Instruction
call 00007FAA7CDD648Ah
jmp 00007FAA7CDD4E0Eh
mov edi, edi
push ebp
mov ebp, esp
sub esp, 00000328h
mov dword ptr [00409C38h], eax
mov dword ptr [00409C34h], ecx
mov dword ptr [00409C30h], edx
mov dword ptr [00409C2Ch], ebx
mov dword ptr [00409C28h], esi
mov dword ptr [00409C24h], edi
mov word ptr [00409C50h], ss

Instruction
mov word ptr [00409C44h], cs
mov word ptr [00409C20h], ds
mov word ptr [00409C1Ch], es
mov word ptr [00409C18h], fs
mov word ptr [00409C14h], gs
pushfd
pop dword ptr [00409C48h]
mov eax, dword ptr [ebp+00h]
mov dword ptr [00409C3Ch], eax
mov eax, dword ptr [ebp+04h]
mov dword ptr [00409C40h], eax
lea eax, dword ptr [ebp+08h]
mov dword ptr [00409C4Ch], eax
mov eax, dword ptr [ebp-00000320h]
mov dword ptr [00409B88h], 00010001h
mov eax, dword ptr [00409C40h]
mov dword ptr [00409B3Ch], eax
mov dword ptr [00409B30h], C0000409h
mov dword ptr [00409B34h], 00000001h
mov eax, dword ptr [00409004h]
mov dword ptr [ebp-00000328h], eax
mov eax, dword ptr [00409008h]
mov dword ptr [ebp-00000324h], eax
call dword ptr [0000004Ch]

Rich Headers

Programming Language:	• [LNK] VS2010 build 30319 • [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [C++] VS2010 build 30319 • [RES] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7a9c	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc000	0x38b4c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x45000	0x5ec	.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	0x78a8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x6000	0x104	.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	0x4661	0x4800	False	0.611924913194	data	6.43586824973	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x6000	0x209c	0x2200	False	0.330767463235	data	4.66325721778	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25e0	0xc00	False	0.214518229167	data	2.46095861803	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc000	0x38b4c	0x38c00	False	0.479431958976	data	7.35405797844	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x45000	0x924	0xa00	False	0.530078125	data	4.73541328674	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0xc3a0	0x418c	data		
RT_BITMAP	0x1052c	0x40d8	data		
RT_BITMAP	0x14604	0x19be0	data		
RT_ICON	0x2e1e4	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4282932851, next used block 4282932851		
RT_ICON	0x3240c	0x94a8	data		
RT_ICON	0x3b8b4	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4286967085, next used block 4286967085		
RT_ICON	0x3de5c	0xea8	data	English	United States
RT_ICON	0x3ed04	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x3f5ac	0x6c8	data	English	United States
RT_ICON	0x3fc74	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x401dc	0x25a8	data	English	United States
RT_ICON	0x42784	0x10a8	data	English	United States
RT_ICON	0x4382c	0x988	data	English	United States
RT_ICON	0x441b4	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_MENU	0x4461c	0x486	data		
RT_GROUP_ICON	0x44aa4	0x76	data	English	United States
RT_GROUP_ICON	0x44b1c	0x30	data		

Imports

DLL	Import
KERNEL32.dll	InterlockedCompareExchange, GetSystemTimes, LoadLibraryW, GetSystemTimeAdjustment, GetProcAddress, LocalAlloc, GetModuleHandleA, MultiByteToWideChar, LCMapStringW, IsProcessorFeaturePresent, HeapReAlloc, HeapSize, GetCommandLineW, HeapSetInformation, GetStartupInfoW, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, GetModuleHandleW, ExitProcess, DecodePointer, WriteFile, GetStdHandle, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, InitializeCriticalSectionAndSpinCount, GetFileType, DeleteCriticalSection, EncodePointer, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, GetLastError, InterlockedDecrement, HeapCreate, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, LeaveCriticalSection, EnterCriticalSection, HeapFree, Sleep, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, RtlUnwind, WideCharToMultiByte, GetStringTypeW
USER32.dll	GetWindowTextLengthA, GetWindowWord, GetWindowTextA, GetGuiResources

Possible Origin

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

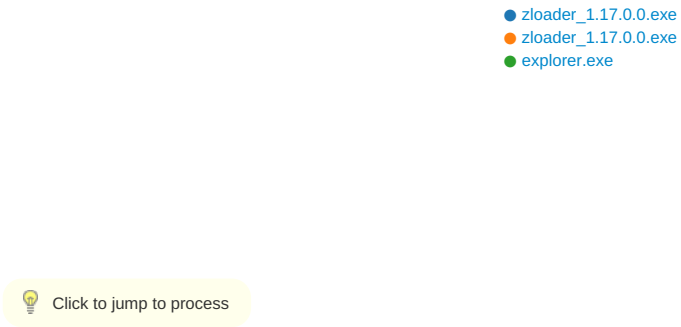
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: zloader_1.17.0.0.exe PID: 4312 Parent PID: 4236

General

Start time:	20:26:12
Start date:	19/07/2020
Path:	C:\Users\user\Desktop\zloader_1.17.0.0.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zloader_1.17.0.0.exe'
Imagebase:	0xc90000
File size:	266240 bytes
MD5 hash:	2CDDC5E9482B049387C96B609ADA8FEA
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: zloader_1.17.0.0.exe PID: 3788 Parent PID: 4312

General

Start time:	20:28:08
Start date:	19/07/2020
Path:	C:\Users\user\Desktop\zloader_1.17.0.0.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zloader_1.17.0.0.exe'
Imagebase:	0xc90000
File size:	266240 bytes
MD5 hash:	2CDDC5E9482B049387C96B609ADA8FEA
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: explorer.exe PID: 2016 Parent PID: 3788

General

Start time:	20:28:14
Start date:	19/07/2020
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	explorer.exe
Imagebase:	0x290000
File size:	3611368 bytes
MD5 hash:	499B0D1F6277F17B3BAC525B8717C064
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis