ID: 508544
Sample Name:
61766fc85163a.dll
Cookbook: default.jbs
Time: 10:55:24
Date: 25/10/2021
Version: 33.0.0 White Diamond

Table of Contents

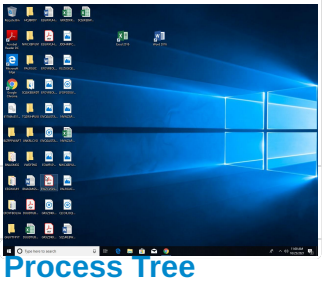
Windows Analysis Report 61766fc85163a.dll

Overview

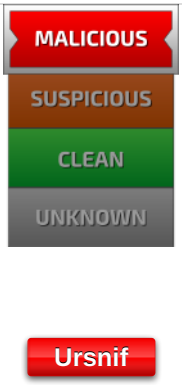
General Information

Sample Name:	61766fc85163a.dll
Analysis ID:	508544
MD5:	5ba43bc79bff74c..
SHA1:	49256e2887cab7..
SHA256:	876666a6f9230b8.
Tags:	DHL dll Gozi ISFB ITA ursnif
Infos:	

Most interesting Screenshot:



Detection

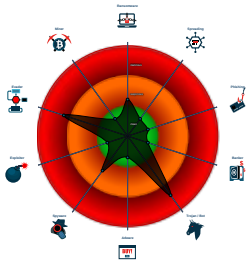


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- System process connects to networ…
- Writes or reads registry keys via WMI
- Rundll32 performs DNS lookup (likel…
- Writes registry values via WMI
- Uses 32bit PE files
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Uses code obfuscation techniques (…
- Queries the installation date of Wind…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5276 cmdline: loaddll32.exe 'C:\Users\user\Desktop\61766fc85163a.dll' MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 4968 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\61766fc85163a.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5692 cmdline: rundll32.exe 'C:\Users\user\Desktop\61766fc85163a.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5992 cmdline: rundll32.exe C:\Users\user\Desktop\61766fc85163a.dll,Cow MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6720 cmdline: rundll32.exe C:\Users\user\Desktop\61766fc85163a.dll,Fishdark MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6904 cmdline: rundll32.exe C:\Users\user\Desktop\61766fc85163a.dll,Multiplyboat MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"YO6EupUXQQEIZWr1HZwHqwbuf45UKlaaNAB4ZLiKsu7B39r6dBjtPHb2dqe22JgQrIOaO/7CSCpZ9VuPYSl5H6wuGZ1xyRSe7C3c6RxGbqnFBTgAkKFju2eS+hGTIKJvxmLB1vRcOADEbzlrK+7ALUr55Rs0VTXRrvCyjb4vTim8iSk+
dIgIyxzBoPD6SBA5ACtVvAO15Nqcsl+9e+CRdtm0+oPrkvDGL2Dav9cErXo5SzqquGstuCbvnyTSPGNMjbKlPBN7/S4LoVfjxTeSJhWPjf1raeOb8pc9CSsiDTedsvpOOgXVq2c/tQr253W0mKWN0cwiXlVSxmTL1XYeHxONoXKrjIaIw
juFk+VK+lg=",
  "c2_domain": [
    "fx.rhinobuff.com",
    "fio.linosheart.com"
  ],
  "botnet": "2500",
  "server": "580",
  "serpent_key": "GgxKJL0zm4HBTHpK",
  "sleep_time": "5",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "1"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.457883512.0000000003BF8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000003.00000003.448559940.0000000004F68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.401727363.0000000002C60000.00000040.00000010.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000003.448597664.0000000004F68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.420035815.0000000002C40000.00000040.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 23 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.3.rundll32.exe.2c68c9b.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.3.rundll32.exe.3268c9b.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.45394a0.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
0.2.loaddll32.exe.2c80000.0.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.3.rundll32.exe.2658c9b.0.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
Click to see the 11 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Rundll32 performs DNS lookup (likely malicious behavior)

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

Yara detected Ursnif

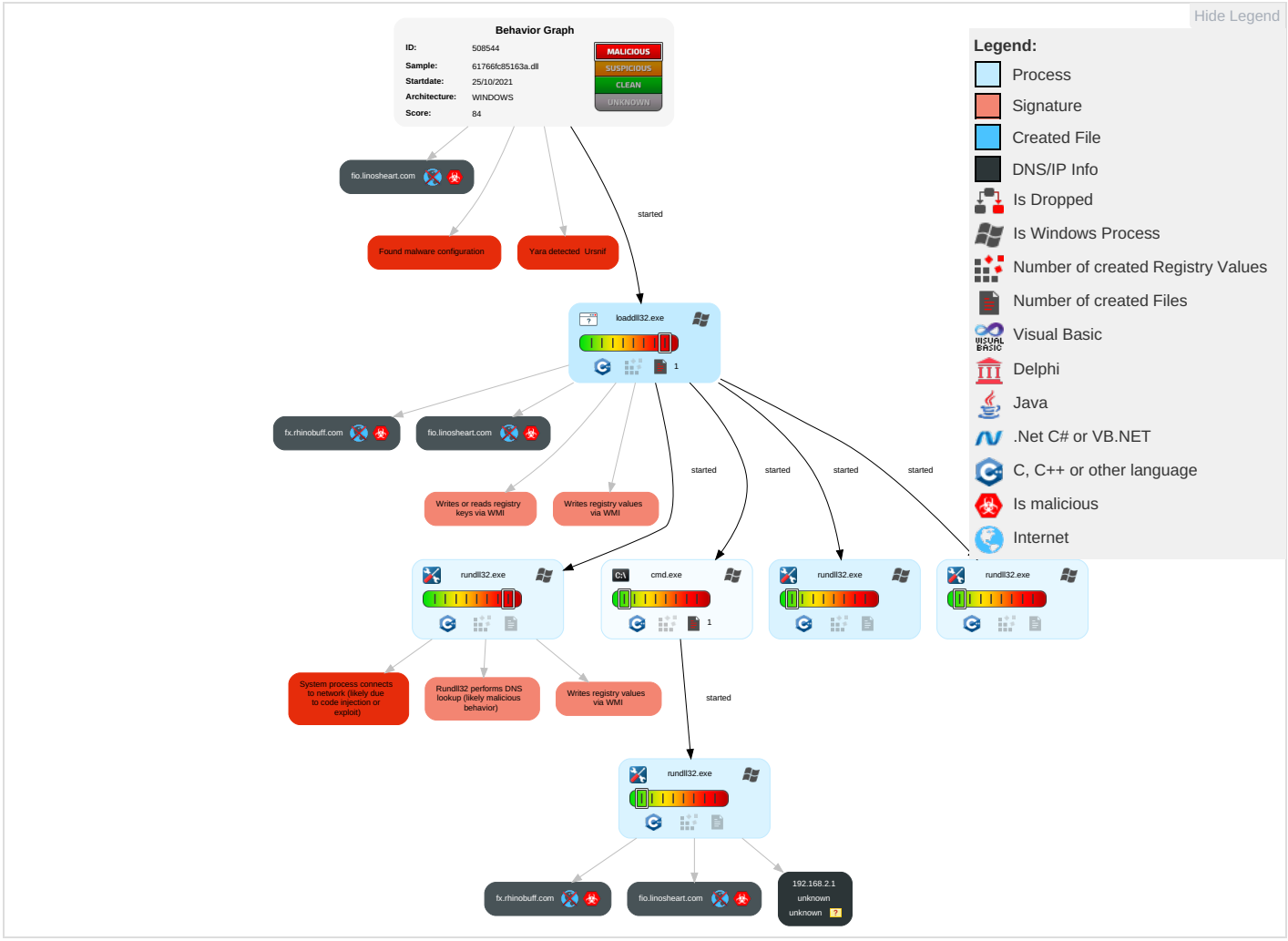
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 1 2	Process Injection 1 1 2	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communicatio
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 3 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

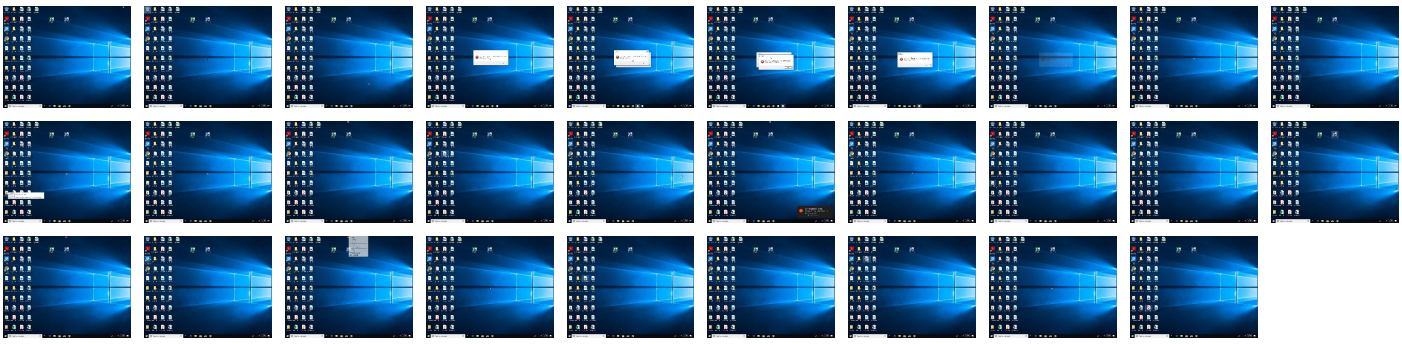
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.2c80000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.rundll32.exe.2680000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
6.2.rundll32.exe.5280000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://fx.rhinobuff.com/x0ylueFuXgrpB3WJj/TF7mv4QreQVW/NyZwfSNmEuc/QVDm3PVK85XSch/TwihngzLYMfTath4pJ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
fx.rhinobuff.com	unknown	unknown	true		unknown
fio.linosheart.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	508544
Start date:	25.10.2021
Start time:	10:55:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	61766fc85163a.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:	23
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.troj.evad.winDLL@11/0@19/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.3% (good quality ratio 20.5%) • Quality average: 79.7% • Quality standard deviation: 28.3%
HCA Information:	• Successful, ratio: 73% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:57:35	API Interceptor	9x Sleep call for process: rundll32.exe modified
10:57:39	API Interceptor	9x Sleep call for process: loaddll32.exe modified

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):	6.697119689004969
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:	61766fc85163a.dll
File size:	685056
MD5:	5ba43bc79bff74cc56919f7fd053a284

General

SHA1:	49256e2887cab7474a3231b289bd86773f971c16
SHA256:	876666a6f9230b86577eedc94fa30f808e8e4aecce1d054131b757cfd8270989
SHA512:	1769052a70e78f70777019b9eea9326adb1b88a219477a83f8a446111b561c5bfa66b281229440125dcdde697f2485afd99f432b6e3c193f19ddbc21bc08b4a5
SSDEEP:	12288:Dm/ZzH8Y9R1XuntqkXGKOy1Ks7iGQrI0iM+Yvmpdrbid1q1ck2B0CWhFbTouKt4v:DmhbRRunAkXGKOy1Ks7iGQrI0iM+Yvmo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]......>.....j.....Rich.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100411b7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5BC239CB [Sat Oct 13 18:30:35 2018 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:	7fbcde9b0ceaa34f5b9ba966c49456aa

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x7a013	0x7a200	False	0.525452597236	data	6.76479443466	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7c000	0x25c98	0x25e00	False	0.527221276815	data	5.51438291305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa2000	0x1648c	0x1800	False	0.197591145833	data	4.17350541835	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xb9000	0x360	0x400	False	0.388671875	data	2.88168607856	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xba000	0x521c	0x5400	False	0.739164806548	data	6.67826245353	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 25, 2021 10:57:36.541914940 CEST	192.168.2.3	8.8.8.8	0x253b	Standard query (0)	fx.rhinobuff.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:57:40.855165958 CEST	192.168.2.3	8.8.8.8	0x2558	Standard query (0)	fx.rhinobuff.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:57:56.723613977 CEST	192.168.2.3	8.8.8.8	0x3124	Standard query (0)	fio.linosheart.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:58:00.911278009 CEST	192.168.2.3	8.8.8.8	0x57c2	Standard query (0)	fio.linosheart.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:58:16.870439053 CEST	192.168.2.3	8.8.8.8	0x4145	Standard query (0)	fx.rhinobuff.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:58:20.979888916 CEST	192.168.2.3	8.8.8.8	0x4b47	Standard query (0)	fx.rhinobuff.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:58:37.030309916 CEST	192.168.2.3	8.8.8.8	0xa53c	Standard query (0)	fio.linosheart.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:58:41.226304054 CEST	192.168.2.3	8.8.8.8	0x21f5	Standard query (0)	fio.linosheart.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:58:57.148864031 CEST	192.168.2.3	8.8.8.8	0xc861	Standard query (0)	fx.rhinobuff.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:59:01.448348045 CEST	192.168.2.3	8.8.8.8	0xaa06	Standard query (0)	fx.rhinobuff.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:59:17.336637974 CEST	192.168.2.3	8.8.8.8	0xd5ef	Standard query (0)	fio.linosheart.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:59:21.556047916 CEST	192.168.2.3	8.8.8.8	0x395d	Standard query (0)	fio.linosheart.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:59:37.439332008 CEST	192.168.2.3	8.8.8.8	0xd02a	Standard query (0)	fx.rhinobuff.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:59:41.620507956 CEST	192.168.2.3	8.8.8.8	0x21f2	Standard query (0)	fx.rhinobuff.com	A (IP address)	IN (0x0001)
Oct 25, 2021 10:59:57.579947948 CEST	192.168.2.3	8.8.8.8	0xe050	Standard query (0)	fio.linosheart.com	A (IP address)	IN (0x0001)
Oct 25, 2021 11:00:01.702646971 CEST	192.168.2.3	8.8.8.8	0x1fd	Standard query (0)	fio.linosheart.com	A (IP address)	IN (0x0001)
Oct 25, 2021 11:00:17.731142998 CEST	192.168.2.3	8.8.8.8	0x8d27	Standard query (0)	fx.rhinobuff.com	A (IP address)	IN (0x0001)
Oct 25, 2021 11:00:21.766000986 CEST	192.168.2.3	8.8.8.8	0x96dc	Standard query (0)	fx.rhinobuff.com	A (IP address)	IN (0x0001)
Oct 25, 2021 11:00:37.792159081 CEST	192.168.2.3	8.8.8.8	0xae73	Standard query (0)	fio.linosheart.com	A (IP address)	IN (0x0001)

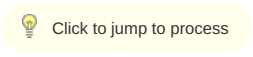
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 10:57:36.565784931 CEST	8.8.8.8	192.168.2.3	0x253b	Name error (3)	fx.rhinobuff.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:57:40.873775005 CEST	8.8.8.8	192.168.2.3	0x2558	Name error (3)	fx.rhinobuff.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:57:56.741938114 CEST	8.8.8.8	192.168.2.3	0x3124	Name error (3)	fio.linosheart.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:58:00.930002928 CEST	8.8.8.8	192.168.2.3	0x57c2	Name error (3)	fio.linosheart.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:58:16.891081095 CEST	8.8.8.8	192.168.2.3	0x4145	Name error (3)	fx.rhinobuff.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:58:21.002942085 CEST	8.8.8.8	192.168.2.3	0x4b47	Name error (3)	fx.rhinobuff.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:58:37.048883915 CEST	8.8.8.8	192.168.2.3	0xa53c	Name error (3)	fio.linosheart.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:58:41.244290113 CEST	8.8.8.8	192.168.2.3	0x21f5	Name error (3)	fio.linosheart.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:58:57.167082071 CEST	8.8.8.8	192.168.2.3	0xc861	Name error (3)	fx.rhinobuff.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:59:01.468022108 CEST	8.8.8.8	192.168.2.3	0xaa06	Name error (3)	fx.rhinobuff.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:59:17.355292082 CEST	8.8.8.8	192.168.2.3	0xd5ef	Name error (3)	fio.linosheart.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:59:21.580013037 CEST	8.8.8.8	192.168.2.3	0x395d	Name error (3)	fio.linosheart.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:59:37.468489885 CEST	8.8.8.8	192.168.2.3	0xd02a	Name error (3)	fx.rhinobuff.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:59:41.654719114 CEST	8.8.8.8	192.168.2.3	0x21f2	Name error (3)	fx.rhinobuff.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 10:59:57.609849930 CEST	8.8.8.8	192.168.2.3	0xe050	Name error (3)	fio.linosheart.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 11:00:01.721030951 CEST	8.8.8.8	192.168.2.3	0x1fd	Name error (3)	fio.linosheart.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 11:00:17.749828100 CEST	8.8.8.8	192.168.2.3	0x8d27	Name error (3)	fx.rhinobuff.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 11:00:21.784363985 CEST	8.8.8.8	192.168.2.3	0x96dc	Name error (3)	fx.rhinobuff.com	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 11:00:37.811698914 CEST	8.8.8.8	192.168.2.3	0xae73	Name error (3)	fio.linosheart.com	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 5276 Parent PID: 4248

General

Start time:	10:56:24
Start date:	25/10/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\61766fc85163a.dll'
Imagebase:	0x80000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.457883512.0000000003BF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000003.420035815.0000000002C40000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.458003992.0000000003BF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.457844986.0000000003BF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.457961241.0000000003BF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.457926996.0000000003BF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.457986489.0000000003BF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.825811764.0000000003BF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.458017733.0000000003BF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.457907127.0000000003BF8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.825738430.00000000031F9000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4968 Parent PID: 5276

General

Start time:	10:56:25
Start date:	25/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\61766fc85163a.dll',#1
Imagebase:	0xd80000
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 Show Windows behavior

Analysis Process: rundll32.exe PID: 5992 Parent PID: 5276

General

Start time:	10:56:25
Start date:	25/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\61766fc85163a.dll,Cow
Imagebase:	0x3d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000003.401727363.0000000002C60000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5692 Parent PID: 4968

General

Start time:	10:56:25
Start date:	25/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\61766fc85163a.dll',#1
Imagebase:	0x3d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448559940.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448597664.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448496716.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448462306.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000003.401325815.0000000002650000.00000040.00000010.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448582889.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.826309234.0000000004539000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448524349.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448420040.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.826711993.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.448613025.0000000004F68000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6720 Parent PID: 5276

General

Start time:	10:56:29
Start date:	25/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\61766fc85163a.dll,Fishdark
Imagebase:	0x3d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000003.413516631.0000000003260000.00000040.00000010.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6904 Parent PID: 5276

General

Start time:	10:56:33
Start date:	25/10/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\61766fc85163a.dll,Multiplyboat
Imagebase:	0x3d0000

File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000006.00000003.417864132.0000000004C80000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000006.00000003.449697132.0000000005169000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Disassembly

Code Analysis