

JOESandbox Cloud BASIC



**ID:** 382564

**Sample Name:** gg\_1.gif.dll

**Cookbook:** default.jbs

**Time:** 09:57:40

**Date:** 06/04/2021

**Version:** 31.0.0 Emerald

# Table of Contents

Table of Contents	2
Analysis Report gg_1.gif.dll	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: Ursnif	4
Yara Overview	5
Memory Dumps	5
Unpacked PEs	5
Sigma Overview	5
Signature Overview	5
AV Detection:	5
Key, Mouse, Clipboard, Microphone and Screen Capturing:	5
E-Banking Fraud:	5
Hooking and other Techniques for Hiding and Protection:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
Contacted IPs	9
General Information	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
Static File Info	10
General	10
File Icon	10
Static PE Info	11
General	11
Entrypoint Preview	11
Data Directories	12
Sections	12
Imports	13
Exports	13
Network Behavior	13
Code Manipulations	13

Statistics 13  
Behavior 13  
System Behavior 13  
Analysis Process: loaddll32.exe PID: 6948 Parent PID: 6004 14  
General 14  
File Activities 14  
Analysis Process: cmd.exe PID: 6988 Parent PID: 6948 14  
General 14  
File Activities 14  
Analysis Process: rundll32.exe PID: 7000 Parent PID: 6948 14  
General 14  
File Activities 15  
Analysis Process: rundll32.exe PID: 7012 Parent PID: 6988 15  
General 15  
Disassembly 15  
Code Analysis 15

# Analysis Report gg\_1.gif.dll

## Overview

### General Information

Sample Name:	gg_1.gif.dll
Analysis ID:	382564
MD5:	53f7e96f48283df...
SHA1:	bd119af6c52876f..
SHA256:	4b8946f9fee32db..
Tags:	<span>dll</span> <span>GG</span> <span>Gozi</span> <span>IFSB</span> <span>Ursnif</span>
Infos:	
Most interesting Screenshot:	

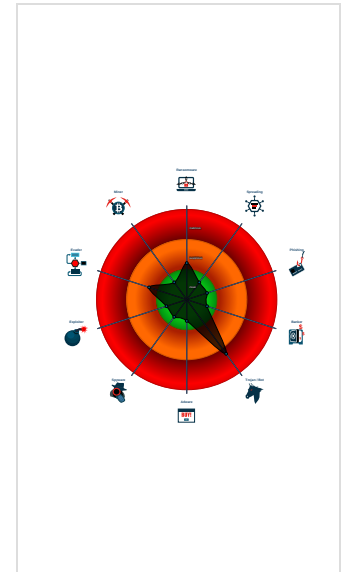
### Detection

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

### Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected Ursnif
- Machine Learning detection for samp...
- Antivirus or Machine Learning detec...
- Contains functionality to call native f...
- Contains functionality to dynamically...
- Contains functionality to read the PEB
- Creates a process in suspended mo...
- Detected potential crypto function
- PE file contains sections with non-s...
- Program does not show much activi...
- Uses 32bit PE files
- Uses code obfuscation techniques (...)

### Classification



## Startup

- System is w10x64
- loaddll32.exe** (PID: 6948 cmdline: loadll32.exe 'C:\Users\user\Desktop\gg\_1.gif.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe** (PID: 6988 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\gg\_1.gif.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe** (PID: 7012 cmdline: rundll32.exe 'C:\Users\user\Desktop\gg\_1.gif.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - rundll32.exe** (PID: 7000 cmdline: rundll32.exe C:\Users\user\Desktop\gg\_1.gif.dll,DllServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- cleanup

## Malware Configuration

Threatname: Ursnif

```
[
  {
    {
      "RSA Public Key":
      "bUd4GfCFHo0e+ZYubkHaTKXmZ1xYxyv7Ha6j1WAZbQ7YvHdkqTfD1vHD2y2CnFTRrLK1w5iQroYI0mUpJ4xNknLY+BmJf4xpeJRxxK0RRNeRbW5unSB2vXqxlTgz6vNZY+9zez tuP2jXKpIm0/s+YxWnsT7eWUtQtD38NlsAptJdp+3rBxjzAWNkQj7wMA"
    },
    {
      "c2_domain": [
        "bing.com",
        "update4.microsoft.com",
        "under17.com",
        "urs-world.com"
      ],
      "botnet": "5566",
      "server": "12",
      "serpent_key": "10301029J5JUYDWG",
      "sleep_time": "10",
      "SetWaitableTimer_value": "0",
      "DGA_count": "10"
    }
  }
]
```

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.703411364.0000000004D40000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000004.00000002.699967936.0000000004560000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000001.00000002.919628932.0000000003020000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

### Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.4d40000.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.10000000.3.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.3020000.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.4560000.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	


## Sigma Overview

No Sigma rule has matched

## Signature Overview



- AV Detection
- Compliance
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

 Click to jump to signature section

### AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

### Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected Ursnif

### E-Banking Fraud:



## E-Banking Fraud:

Yara detected Ursnif

## Hooking and other Techniques for Hiding and Protection:



Yara detected Ursnif

## Stealing of Sensitive Information:



Yara detected Ursnif

## Remote Access Functionality:

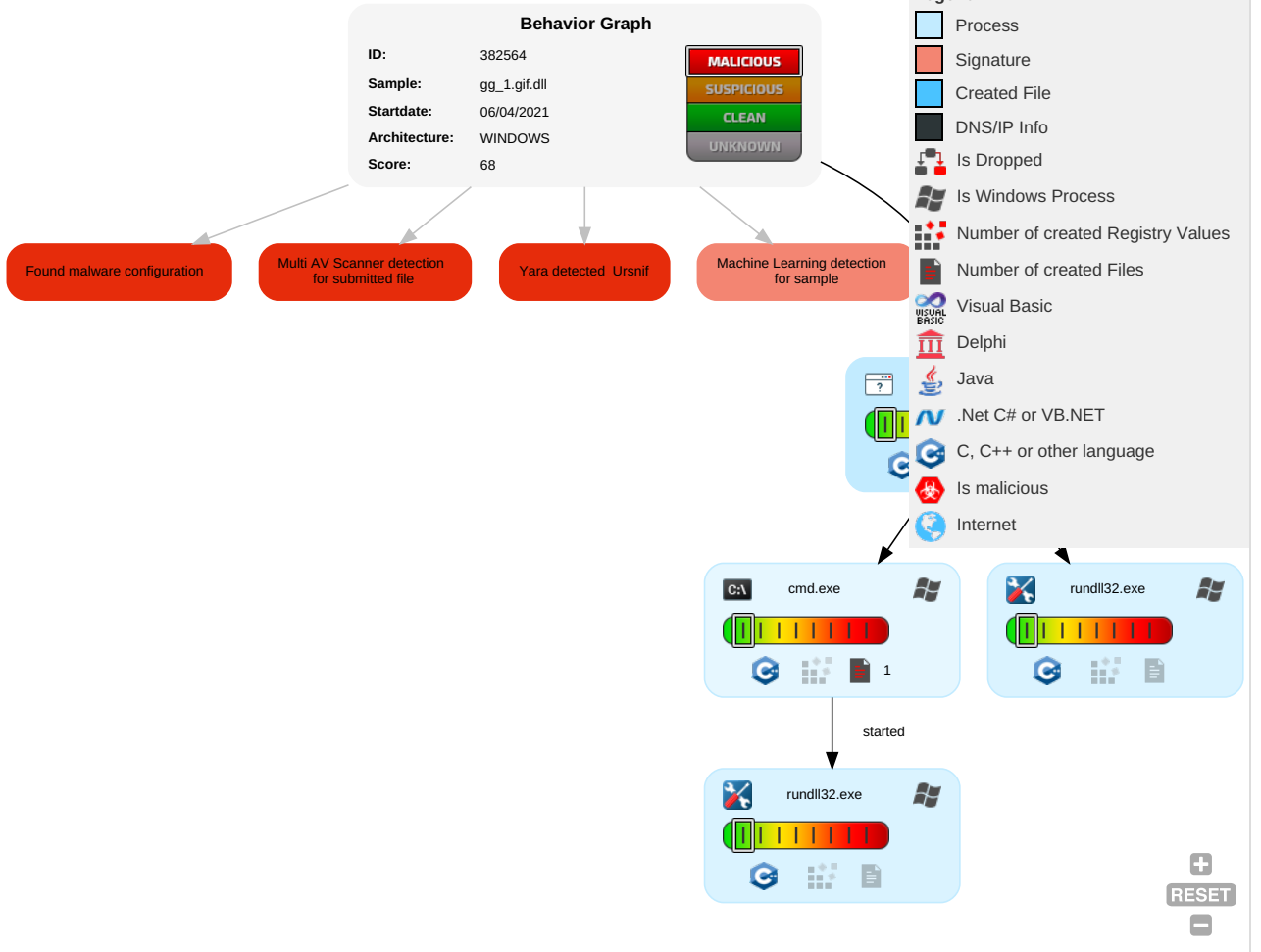


Yara detected Ursnif

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Native API <b>1</b>	Path Interception	Process Injection <b>1 2</b>	Rundll32 <b>1</b>	OS Credential Dumping	System Time Discovery <b>1</b>	Remote Services	Archive Collected Data <b>1</b>	Exfiltration Over Other Network Medium	Encrypted Channel <b>1</b>	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify Syster Partitic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing <b>1</b>	LSASS Memory	Process Discovery <b>1</b>	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 Lockor
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection <b>1 2</b>	Security Account Manager	System Information Discovery <b>3</b>	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)	Obfuscated Files or Information <b>1</b>	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

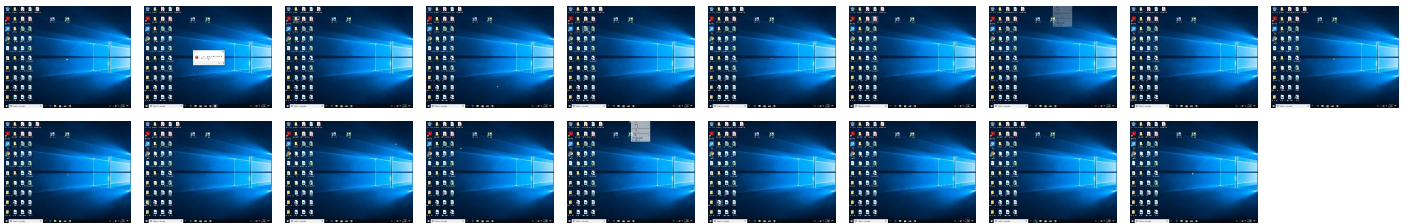
## Behavior Graph



### 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
gg_1.gif.dll	42%	ReversingLabs	Win32.Trojan.Wacatac	
gg_1.gif.dll	100%	Joe Sandbox ML		

### Dropped Files

No Antivirus matches

### Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.loaddll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		<a href="#">Download File</a>

### Domains

No Antivirus matches

### URLs

No Antivirus matches



## Domains and IPs

### Contacted Domains

No contacted domains info

### Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382564
Start date:	06.04.2021
Start time:	09:57:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gg_1.gif.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:	19
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:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.troj.winDLL@7/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 97.1% (good quality ratio 85.8%)</li><li>• Quality average: 66.5%</li><li>• Quality standard deviation: 33.2%</li></ul>
HCA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 56%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>
Cookbook Comments:	<ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found application associated with file extension: .dll</li></ul>
Warnings:	Show All <ul style="list-style-type: none"><li>• Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe</li></ul>

## Simulations

### Behavior and APIs

Time	Type	Description
09:58:52	API Interceptor	1x Sleep call for process: rundll32.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):	6.127836134489194
TrID:	<ul style="list-style-type: none"><li>Win32 Dynamic Link Library (generic) (1002004/3) 99.60%</li><li>Generic Win/DOS Executable (2004/3) 0.20%</li><li>DOS Executable Generic (2002/1) 0.20%</li><li>Autodesk FLIC Image File (extensions: flic, flm, cel) (7/3) 0.00%</li></ul>
File name:	gg_1.gif.dll
File size:	118163
MD5:	53f7e96f48283df339164afadd174638
SHA1:	bd119af6c52876fb5d23398326850d87fe159735
SHA256:	4b8946f9fee32db6b42f7c0fdb70ca9ba7980c5932d3f959227cdfbef15e8c34
SHA512:	6fb9579bcafa72d3eaac9238aaa54b5e87fa1787b8d2b0ca1735e9c8dc362e318a6c100d72fcbd35ca32a472250b598350730f80f54327a7d975d9271fcb3d5
SSDEEP:	1536:tm15JsYYm3GCVS7ZicTJzRVd620ZmB9RMli0msUdqZEACW4jySTLW:eLsacThRVd6pmBPM07vYZEA4/W
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$....._W...6e..6e..6e..)v..6e..w..6e.Rich.6e.....PE..L....f.....!.....ko.....

### File Icon



Icon Hash:

74f0e4ecccdce0e4

## Static PE Info

### General

Entrypoint:	0x10006f6b
Entrypoint Section:	.code
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x6066E9D0 [Fri Apr 2 09:54:24 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	3f728412058b62c418b1091768b74d7b

## Entrypoint Preview

### Instruction

```
push ebx
push esi
and dword ptr [esp], 00000000h
or dword ptr [esp], ebp
mov ebp, esp
add esp, FFFFFFFF8h
push esp
mov dword ptr [esp], FFFF0000h
call 00007F9530D6E771h
push eax
add dword ptr [esp], 00000247h
sub dword ptr [esp], eax
push esi
mov dword ptr [esp], 00001567h
call 00007F9530D6D6E7h
push eax
or dword ptr [esp], eax
pop eax
jne 00007F9530D729EBh
pushad
push 00000000h
mov dword ptr [esp], esi
xor esi, esi
xor esi, dword ptr [ebx+0041C627h]
mov eax, esi
pop esi
push ebx
add dword ptr [esp], 40h
sub dword ptr [esp], ebx
push ebp
add dword ptr [esp], 00001000h
sub dword ptr [esp], ebp
mov dword ptr [ebp-04h], 00000000h
push dword ptr [ebp-04h]
xor dword ptr [esp], eax
push 00000000h
call dword ptr [ebx+0041F05Ch]
```

<b>Instruction</b>
mov dword ptr [ebp-04h], ecx
xor ecx, dword ptr [ebp-04h]
or ecx, eax
and edi, 00000000h
xor edi, ecx
mov ecx, dword ptr [ebp-04h]
push edi
pop dword ptr [ebp-04h]
push dword ptr [ebp-04h]
pop dword ptr [ebx+0041CAEDh]
cmp ebx, 00000000h
jbe 00007F9530D729DCh
push 00000000h
add dword ptr [esp], edx
push dword ptr [ebx+0041C166h]
pop edx
add edx, ebx
mov dword ptr [ebx+0041C166h], edx
pop edx
push 00000000h
add dword ptr [esp], edx
push dword ptr [ebx+0041CECAh]
pop edx
add edx, ebx
mov dword ptr [ebx+0041CECAh], edx
pop edx
push ebp
and ebp, 00000000h
or ebp, dword ptr [ebx+0041C166h]

## Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1a000	0x64	.data
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1f0fc	0x118	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x1f000	0xfc	.data
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
.code	0x1000	0x185f2	0x18600	False	0.670042067308	data	6.53345039933	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1a000	0x64	0x200	False	0.16796875	data	1.0662581269	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1b000	0x1000	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x1c000	0x20b3	0x2200	False	0.359834558824	data	2.96025706595	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0x1f000	0x7b2	0x800	False	0.45703125	data	4.70767794561	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

## Imports

DLL	Import
user32.dll	GetActiveWindow, SetWindowsHookExA, GetLayeredWindowAttributes
kernel32.dll	GetProcAddress, LoadLibraryA, VirtualProtect, VirtualAlloc, strlenA, strstrA, strcmpA, GetEnvironmentVariableW
ole32.dll	OleInitialize, OleQueryCreateFromData, IIDFromString, CLIPFORMAT_UserUnmarshal, OleCreateEmbeddingHelper, HDC_UserSize
msimg32.dll	AlphaBlend, TransparentBlt
comdlg32.dll	PageSetupDlgA, PrintDlgA
oledlg.dll	OleUICanConvertOrActivateAs, OleUIChangeSourceW, OleUIConvertA
comctl32.dll	CreateStatusWindow, LBIItemFromPt, DPA_Create, FlatSB_ShowScrollBar, ImageList_GetFlags
oleacc.dll	IID_IAccessible, LresultFromObject
version.dll	VerFindFileW, VerInstallFileA, VerQueryValueA, VerQueryValueW
gdiplus.dll	GdiplusEnumerateMetafileDestPointI, GdiplusCreateBitmapFromHBITMAP, GdiplusSetPenUnit, GdiplusGetImageEncoders, GdiplusGetPathPointsI
winspool.drv	FindNextPrinterChangeNotification, ConnectToPrinterDlg, SetPrinterDataW, GetPrinterW, DeletePrinterDataExW
shell32.dll	SHGetSpecialFolderPathA
advapi32.dll	GetKernelObjectSecurity, CryptEnumProviderTypesA, RegQueryValueExW, RegisterIdleTask

## Exports

Name	Ordinal	Address
DllServer	1	0x1000447b

## Network Behavior

No network behavior found

## Code Manipulations

## Statistics

## Behavior

- loaddll32.exe
- cmd.exe
- rundll32.exe
- rundll32.exe



Click to jump to process

## System Behavior

**Analysis Process: loadll32.exe PID: 6948 Parent PID: 6004****General**

Start time:	09:58:30
Start date:	06/04/2021
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\ggg_1.gif.dll'
Imagebase:	0x9f0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none"> <li>Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000002.919628932.000000003020000.00000004.00000001.sdmp, Author: Joe Security</li> </ul>
Reputation:	moderate

**File Activities**

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

**Analysis Process: cmd.exe PID: 6988 Parent PID: 6948****General**

Start time:	09:58:31
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\ggg_1.gif.dll',#1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3DBBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

**File Activities**

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

**Analysis Process: rundll32.exe PID: 7000 Parent PID: 6948****General**

Start time:	09:58:32
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\ggg_1.gif.dll,DllServer
Imagebase:	0x1b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none"> <li>Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.703411364.0000000004D40000.00000004.00000001.sdmp, Author: Joe Security</li> </ul>
Reputation:	high

### File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

### Analysis Process: rundll32.exe PID: 7012 Parent PID: 6988

#### General

Start time:	09:58:32
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\gg_1.gif.dll',#1
Imagebase:	0x1b0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none"> <li>Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.699967936.0000000004560000.00000004.00000001.sdmp, Author: Joe Security</li> </ul>
Reputation:	high

### Disassembly

### Code Analysis