



ID: 552542
Sample Name: b4f0000.dll
Cookbook: default.jbs
Time: 13:54:51
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report b4f0000.dll 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Threatname: Ursnif 3
Yara Overview 4
Initial Sample 4
Sigma Overview 4
System Summary: 4
Jbx Signature Overview 4
AV Detection: 4
Key, Mouse, Clipboard, Microphone and Screen Capturing: 4
E-Banking Fraud: 4
System Summary: 4
Hooking and other Techniques for Hiding and Protection: 4
Stealing of Sensitive Information: 4
Remote Access Functionality: 4
Mitre Att&ck Matrix 4
Behavior Graph 5
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted IPs 7
General Information 7
Simulations 7
Behavior and APIs 7
Joe Sandbox View / Context 7
IPs 8
Domains 8
ASN 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
Static File Info 8
General 8
File Icon 8
Static PE Info 8
General 8
Entrypoint Preview 9
Data Directories 9
Sections 9
Network Behavior 9
Code Manipulations 9
Statistics 9
Behavior 9
System Behavior 9
Analysis Process: loaddll64.exe PID: 4700 Parent PID: 1208 10
General 10
File Activities 10
Analysis Process: cmd.exe PID: 2404 Parent PID: 4700 10
General 10
File Activities 10
Analysis Process: rundll32.exe PID: 724 Parent PID: 4700 10
General 10
File Activities 10
Analysis Process: rundll32.exe PID: 4708 Parent PID: 2404 11
General 11
File Activities 11
Disassembly 11
Code Analysis 11

Copyright Joe Security LLC 2022

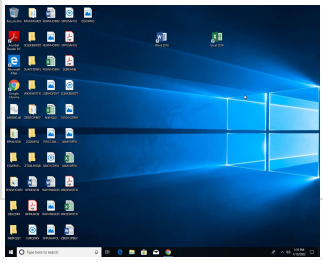
Windows Analysis Report b4f0000.dll

Overview

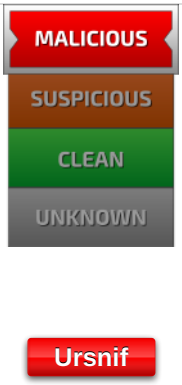
General Information

Sample Name:	b4f0000.dll
Analysis ID:	552542
MD5:	ad5094a1df3cfde..
SHA1:	33623a320cbeb3..
SHA256:	e4e520c931a297..
Tags:	exe gozi
Infos:	

Most interesting Screenshot:



Detection



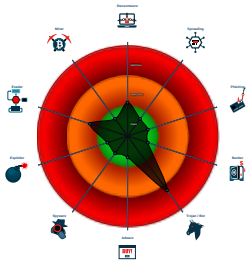
Ursnif

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Sigma detected: Suspicious Call by …
- PE file does not import any functions
- Tries to load missing DLLs
- Program does not show much activi…
- Creates a process in suspended mo…
- Checks if the current process is bein…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 4700 cmdline: loaddll64.exe "C:\Users\user\Desktop\b4f0000.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 2404 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\b4f0000.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 4708 cmdline: rundll32.exe "C:\Users\user\Desktop\b4f0000.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 724 cmdline: rundll32.exe C:\Users\user\Desktop\b4f0000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"1ez6ZX9GBMHuzrxYcEvmkX0k1/y/WRE5hgthXVQ4P44VmZDRyl+qzgB3X8mQxx9hX87voxwb+7CbnJcCZ4hp/XwNIs0rUcJj4wwNctiIvZb8gIPsgWrAjjXLGMBCWjpmhIdWmYD7oSqxAb7ciAuhtWabiveV3OFwUuMRDbNtONTWpz/J
4JVtQJ3XBbp99SutX5vbOPhgKBI3aszrv+0c1EkjrakCFHlOqMs8bjEjNDxrhaBWjOM1EU17zvHVkK7hxDkKQ5buzWmjrzDZEEWnvM3aa5uVRR1v44XnbolU0ltUakCZT4sH963oonk1uijxExj7eWoI4x+donYvsc/nFxNyfe6c/mfSK
b7U2RhPG4g=",
  "c2_domain": [
    "art.microsoftsofymicrosoftsoft.at",
    "r23cirt55ysvtdvl.onion",
    "poi.redhatbabby.at",
    "fgx.dangerboy.at",
    "pop.biopiof.at",
    "l46t3vgvmtx5wxe6.onion",
    "apr.intoolkom.at"
  ],
  "ip_check_url": [
    "curlmyip.net"
  ],
  "serpent_key": "KCVH9K5GZjoxwKSf",
  "server": "580",
  "sleep_time": "10",
  "SetWaitableTimer_value(CRC_CONFIGTIMEOUT)": "600",
  "time_value": "600",
  "SetWaitableTimer_value(CRC_TASKTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_SENDTIMEOUT)": "300",
  "SetWaitableTimer_value(CRC_KNOCKERTIMEOUT)": "300",
  "not_use(CRC_BCTIMEOUT)": "10",
  "botnet": "505050",
  "SetWaitableTimer_value": "60"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
b4f0000.dll	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary:



Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected Ursnif

E-Banking Fraud:



Yara detected Ursnif

System Summary:



Hooking and other Techniques for Hiding and Protection:



Yara detected Ursnif

Stealing of Sensitive Information:



Yara detected Ursnif

Remote Access Functionality:

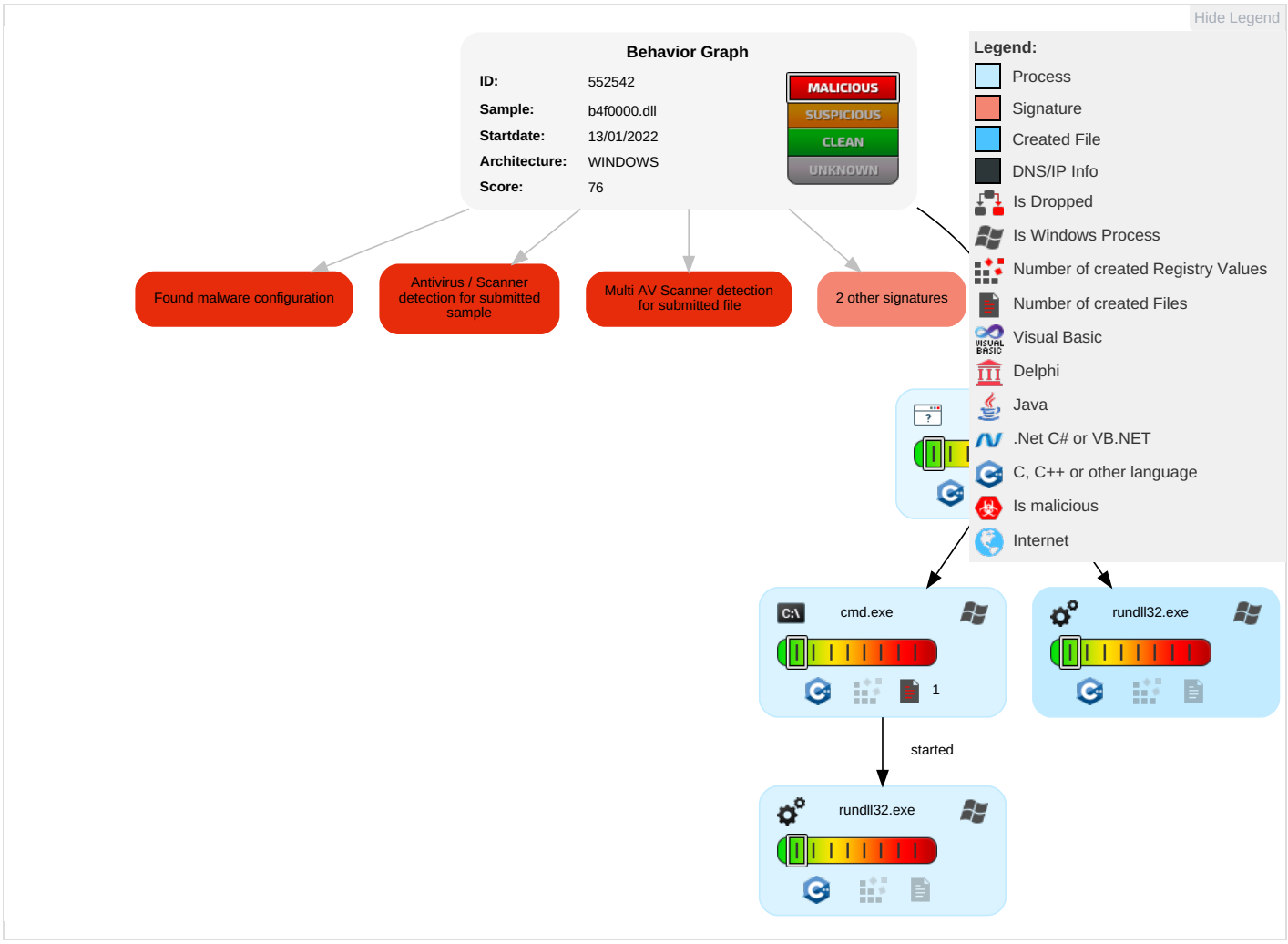


Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Rundll32 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	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
b4f0000.dll	44%	ReversingLabs	Win64.Trojan.Ursnif	
b4f0000.dll	100%	Avira	HEUR/AGEN.1212258	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552542
Start date:	13.01.2022
Start time:	13:54:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	b4f0000.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:	4
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:	mal76.troj.winDLL@7/0@0/0
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 • Found application associated with file extension: .dll • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

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:	MS-DOS executable
Entropy (8bit):	6.445483503138878
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 84.88% • Win64 Executable (generic) (12005/4) 9.99% • DOS Executable Borland Pascal 7.0x (2037/25) 1.69% • Generic Win/DOS Executable (2004/3) 1.67% • DOS Executable Generic (2002/1) 1.67%
File name:	b4f0000.dll
File size:	248320
MD5:	ad5094a1df3cfde7a4d16a1ce795b879
SHA1:	33623a320cbeb3cc5e4c2cf7e28bd7ae404f6788
SHA256:	e4e520c931a2973ef345852251068fb32ddfdefa3cf840492b5eb20222c2dfab
SHA512:	6896932fc7193dca54b649b26863b09f128205a5975edf3ddc1e1da0587a70d9b300ee8649746f240ca9fcfd7ae3b516b3062f25f18a3ecb7a769a4527f112b2
SSDEEP:	6144:HPMtglXNWOg0SbrhI8exPofnrWWJE4R9:HP1hI02rO8exgvrWWJh
File Content Preview:	MZ..... ....

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18000527c
Entrypoint Section:	.text
Digitally signed:	false

General

Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	
Time Stamp:	0x61B67F6F [Sun Dec 12 23:02:07 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:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2fdec	0x2fe00	False	0.579277496736	zlib compressed data	6.39992554242	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x31000	0x6837	0x6a00	False	0.372346698113	data	5.26021941188	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x38000	0x1e40	0x1800	False	0.335286458333	lif file	3.87486757779	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x3a000	0x18f0	0x1a00	False	0.528094951923	data	5.32861522181	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x3c000	0x1f80	0x2000	False	0.970458984375	data	7.90682667928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x3e000	0x1000	0xc00	False	0.513346354167	data	4.74473762141	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 4700 Parent PID: 1208

General

Start time:	13:55:44
Start date:	13/01/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\b4f0000.dll"
Imagebase:	0x7ff7d5ee0000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 2404 Parent PID: 4700

General

Start time:	13:55:44
Start date:	13/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\b4f0000.dll",#1
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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: 724 Parent PID: 4700

General

Start time:	13:55:45
Start date:	13/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\b4f0000.dll,#1
Imagebase:	0x7ff62c4b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Copyright Joe Security LLC 2022

Analysis Process: rundll32.exe PID: 4708 Parent PID: 2404

General

Start time:	13:55:45
Start date:	13/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\b4f0000.dll",#1
Imagebase:	0x7ff62c4b0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2022