



ID: 551795
Sample Name: 248c6f40000.dll
Cookbook: default.jbs
Time: 15:08:09
Date: 12/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 248c6f40000.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: 5
Hooking and other Techniques for Hiding and Protection: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted IPs 8
General Information 8
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 9
Static PE Info 9
General 9
Entrypoint Preview 10
Data Directories 10
Sections 10
Network Behavior 10
Code Manipulations 10
Statistics 10
Behavior 10
System Behavior 10
Analysis Process: loaddll64.exe PID: 6440 Parent PID: 4428 11
General 11
File Activities 11
Analysis Process: cmd.exe PID: 6448 Parent PID: 6440 11
General 11
File Activities 11
Analysis Process: rundll32.exe PID: 6460 Parent PID: 6440 11
General 11
File Activities 11
Analysis Process: rundll32.exe PID: 6472 Parent PID: 6448 12
General 12
File Activities 12
Disassembly 12
Code Analysis 12

Copyright Joe Security LLC 2022

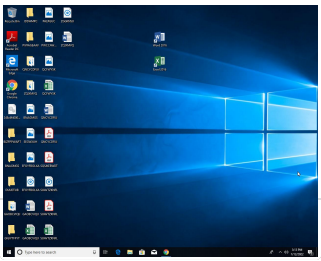
Windows Analysis Report 248c6f40000.dll

Overview

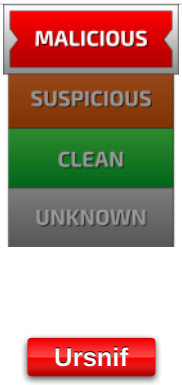
General Information

Sample Name:	248c6f40000.dll
Analysis ID:	551795
MD5:	a1ec2c3298bc89…
SHA1:	23e897e0a782ed..
SHA256:	1e772d61e7d3a7..
Tags:	exe gozi
Infos:	

Most interesting Screenshot:



Detection



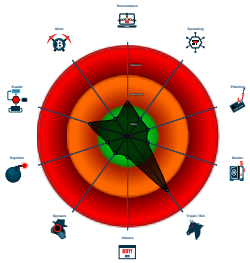
Ursnif

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- 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: 6440 cmdline: loaddll64.exe "C:\Users\user\Desktop\248c6f40000.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6448 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\248c6f40000.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6472 cmdline: rundll32.exe "C:\Users\user\Desktop\248c6f40000.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6460 cmdline: rundll32.exe C:\Users\user\Desktop\248c6f40000.dll,#1 MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"qJ1kPoMlraIzwv3codImebn7w+YrU8DGSEbPIUgoOweySW+9oxNs6FEg5rJvyj+K7XGv3snznSDi7OJfzWWZfRvARRX85pJYlyMRo0/DwGUaS1N350fNDcrXcC+cMnIyqScesdTZTT3I4UGl/4eaH2nD9M3QEBNhxM9oc4sY20SSs/pk
G9D0KhuSF1te4bhlucQ+KFpZ02KcWVU4TeE2VEAgiWrjF1Y8G7UeFRWoeCZR7ZUT6Y2O8Scj/5r03Sm3I11vs6nuSszdMAQkYTAfj3fgm6t4wajaiSB8PacCWh04qEHtIdt5MwitFwfOQ/HHeI8ICFQtYdH1z2/KH1gmintjR8z+We+cZ
oHIHCs3E3g=",
  "c2_domain": [
    "io.immontyr.com",
    "cd1.averlokir.com",
    "6n6szrxfwwahcgpv.onion",
    "app.irolano.com",
    "irq.clickclckjack.at",
    "fs.abertok.at",
    "rpc.ikaryto.com",
    "5k4vglet4rv655tg.onion"
  ],
  "ip_check_url": [
    "curlmyip.net"
  ],
  "serpent_key": "Rk7B02ibiSe2cMoF",
  "server": "770",
  "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": "1000",
  "SetWaitableTimer_value": "60"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
248c6f40000.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

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected Ursnif

E-Banking Fraud:



Yara detected Ursnif

Copyright Joe Security LLC 2022

System Summary:



Hooking and other Techniques for Hiding and Protection:



Yara detected Ursnif

Stealing of Sensitive Information:



Yara detected Ursnif

Remote Access Functionality:

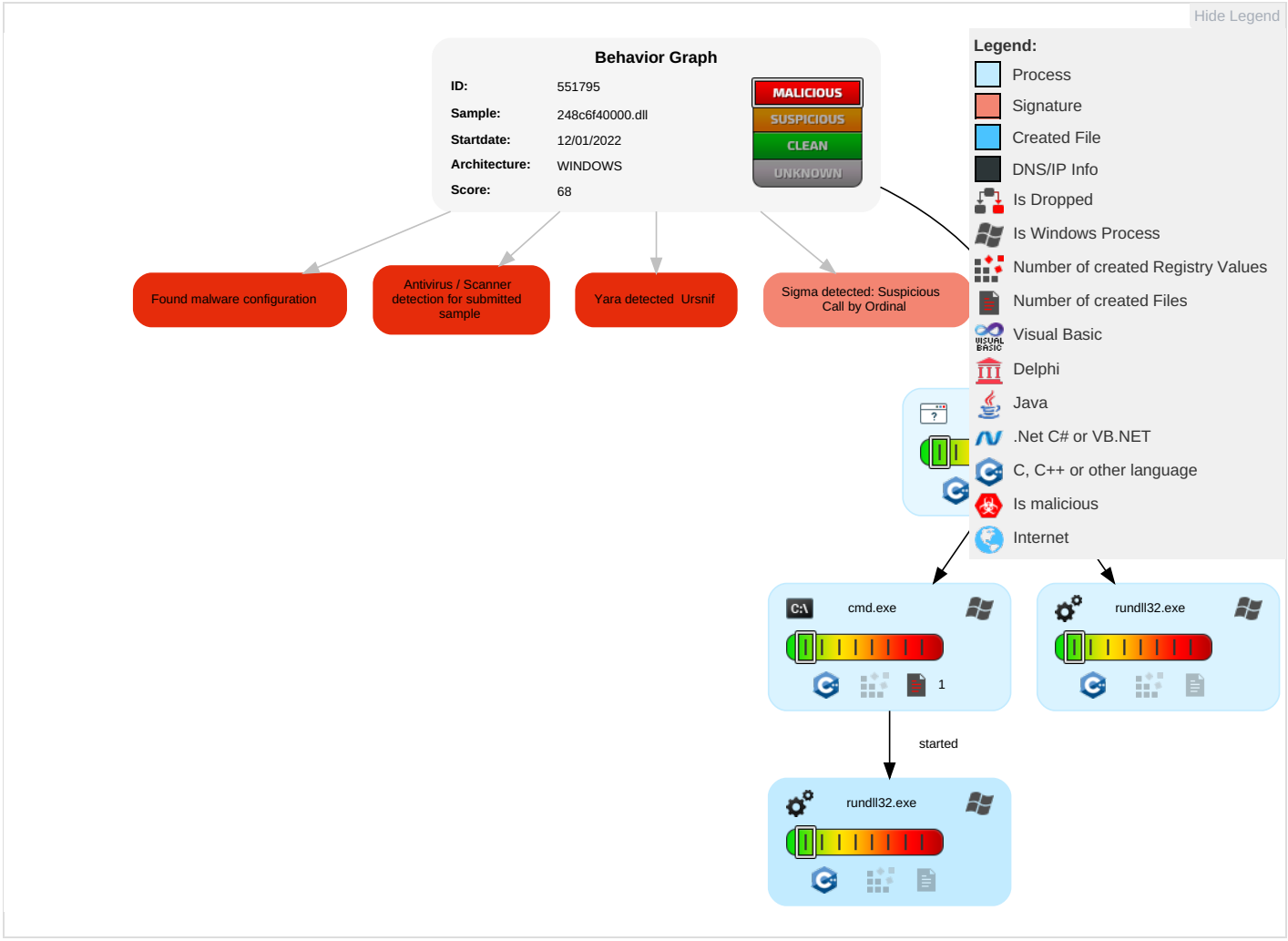


Yara detected Ursnif

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

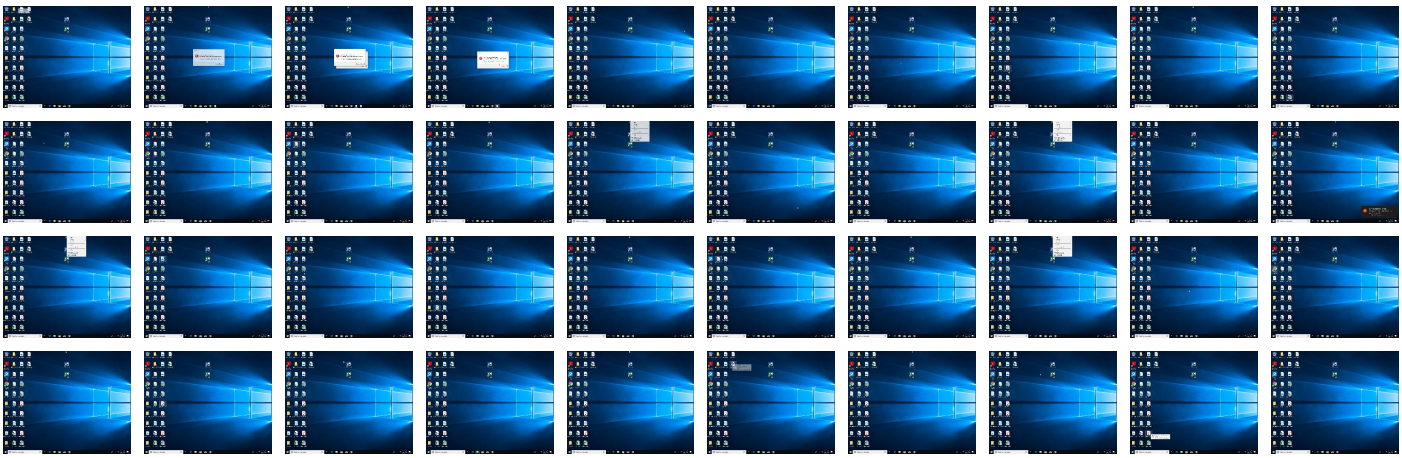
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Copyright Joe Security LLC 2022



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
248c6f40000.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:	551795
Start date:	12.01.2022
Start time:	15:08:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	248c6f40000.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:	28
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.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 • Override analysis time to 240s for rundll32
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):	6.308196606007222
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:	248c6f40000.dll
File size:	258048
MD5:	a1ec2c3298bc890d9febb65cad765ed9
SHA1:	23e897e0a782ed018493b0f420653de81416e650
SHA256:	1e772d61e7d3a7a8ee9770e1f28d11c8130b0657d60eb9cd8c95ecd8931ebdb9
SHA512:	d183f5326cc504746fd460f8bc935b19592910b3d19064ae64a7cb3dcc793f65fbb1a204a9e3527f51eedc0020600f5eeb1ecaf554bc625f27a652046231060e
SSDEEP:	6144:U4kAd7+RQ1ONkwLbaPcsPFV/2eNWrTE4iyvzG:TB7+RYONkFEsPF12eNWrTyy
File Content Preview:	MZ..... ....

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x18001dfc0
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:	0x61B67E8C [Sun Dec 12 22:58:20 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	0x30000	0x30000	False	0.577072143555	zlib compressed data	6.39715579409	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x31000	0x7000	0x7000	False	0.352783203125	data	5.05239019871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x38000	0x2000	0x2000	False	0.270263671875	lif file	3.3206854479	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x3a000	0x2000	0x2000	False	0.42822265625	data	4.58488394811	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x3c000	0x2000	0x2000	False	0.970458984375	data	7.90682667928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x3e000	0x1000	0x1000	False	0.38623046875	data	3.77552669913	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: 6440 Parent PID: 4428

General

Start time:	15:09:05
Start date:	12/01/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\248c6f40000.dll"
Imagebase:	0x7ff7d3110000
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: 6448 Parent PID: 6440

General

Start time:	15:09:05
Start date:	12/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\248c6f40000.dll",#1
Imagebase:	0x7ff7bf140000
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: 6460 Parent PID: 6440

General

Start time:	15:09:05
Start date:	12/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\248c6f40000.dll,#1
Imagebase:	0x7ff6b6770000
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: 6472 Parent PID: 6448

General

Start time:	15:09:05
Start date:	12/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\248c6f40000.dll",#1
Imagebase:	0x7ff6b6770000
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