

ID: 445292
Sample Name:
Processwindo.DLL
Cookbook: default.jbs
Time: 14:59:18
Date: 07/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report Processwindo.DLL 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
Jbx 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: 5
Stealing of Sensitive Information: 5
Remote Access Functionality: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
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 8
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 10
Static PE Info 10
General 10
Entrypoint Preview 10
Rich Headers 10
Data Directories 10
Sections 10
Resources 10
Imports 10
Exports 10
Possible Origin 10
Network Behavior 11
Code Manipulations 11
Statistics 11
Behavior 11
System Behavior 11
Analysis Process: loaddll32.exe PID: 5572 Parent PID: 5780 11
General 11
File Activities 11
Analysis Process: cmd.exe PID: 5884 Parent PID: 5572 11
General 11
File Activities 12
Analysis Process: rundll32.exe PID: 5984 Parent PID: 5572 12
General 12
File Activities 13
Analysis Process: rundll32.exe PID: 5996 Parent PID: 5884 13
General 13
File Activities 13
Analysis Process: rundll32.exe PID: 5560 Parent PID: 5572 14
General 14

Copyright Joe Security LLC 2021

File Activities 14
Analysis Process: rundll32.exe PID: 5540 Parent PID: 5572 14
General 14
File Activities 14
Analysis Process: rundll32.exe PID: 4308 Parent PID: 5572 14
General 14
File Activities 15
Analysis Process: cmd.exe PID: 1388 Parent PID: 3472 15
General 15
File Activities 15
Analysis Process: conhost.exe PID: 1308 Parent PID: 1388 15
General 15
Analysis Process: timeout.exe PID: 5136 Parent PID: 1388 15
General 15
Disassembly 16
Code Analysis 16

Copyright Joe Security LLC 2021

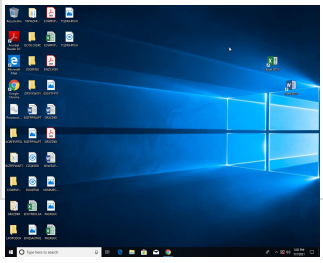
Windows Analysis Report Processwindo.DLL

Overview

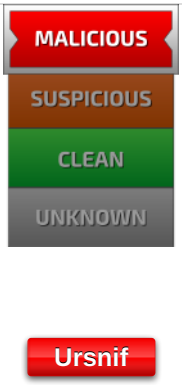
General Information

Sample Name:	Processwindo.DLL
Analysis ID:	445292
MD5:	5522c21a05daf91.
SHA1:	fed4a9b4069cd26.
SHA256:	eb6e2519aa5c31..
Tags:	dll Gozi
Infos:	

Most interesting Screenshot:



Detection

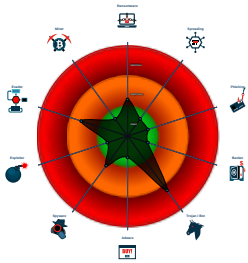


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Antivirus or Machine Learning detec…
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Contains functionality which may be…
- Creates a process in suspended mo…
- Detected potential crypto function
- Found potential string decryption / a…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5572 cmdline: loaddll32.exe 'C:\Users\user\Desktop\Processwindo.DLL' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5884 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\Processwindo.DLL',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5996 cmdline: rundll32.exe 'C:\Users\user\Desktop\Processwindo.DLL',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5984 cmdline: rundll32.exe C:\Users\user\Desktop\Processwindo.DLL,Formweather MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5560 cmdline: rundll32.exe C:\Users\user\Desktop\Processwindo.DLL,Piecehear MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5540 cmdline: rundll32.exe C:\Users\user\Desktop\Processwindo.DLL,Stickregion MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4308 cmdline: rundll32.exe C:\Users\user\Desktop\Processwindo.DLL,Would MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- cmd.exe (PID: 1388 cmdline: 'C:\Windows\System32\cmd.exe' /C timeout /t 5 && del 'C:\Users\user\Desktop\Processwindo.DLL' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 1308 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - timeout.exe (PID: 5136 cmdline: timeout /t 5 MD5: EB9A65078396FB5D4E3813BB9198CB18)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000003.506028485.0000000007360000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.495420595.0000000007360000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.505312952.0000000007360000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.482226881.0000000007360000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.504200485.0000000007360000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 37 entries

Copyright Joe Security LLC 2021

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected Ursnif

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

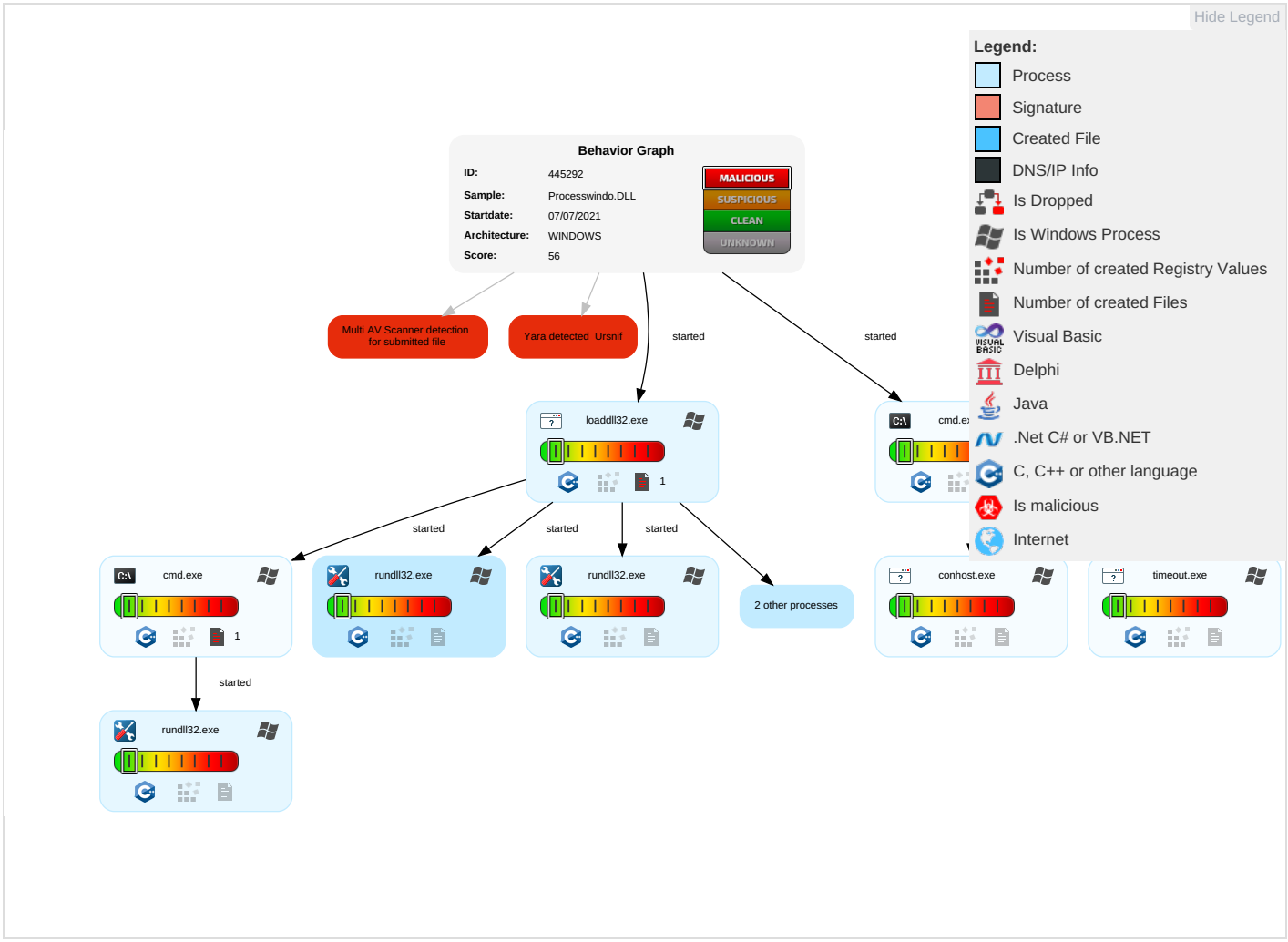
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 1 2	Rundll32 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Devic Without Authorizatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 1	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizatic
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	System Information Discovery 1 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

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
Processwindo.DLL	29%	Virustotal		Browse
Processwindo.DLL	22%	ReversingLabs	Win32.Trojan.Ursnif	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.6dd70000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.loaddll32.exe.baa1db.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
6.3.rundll32.exe.315a1db.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.3.rundll32.exe.446a1db.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.3.rundll32.exe.27da1db.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.3.rundll32.exe.284a1db.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.3.rundll32.exe.29ca1db.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
6.2.rundll32.exe.6dd70000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Copyright Joe Security LLC 2021

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bussipod.xyz	0%	Avira URL Cloud	safe	
http://https://bussipod.xyz8	0%	Avira URL Cloud	safe	
http://%s=%s&file://&os=%u.%u_%u_%u_x%uindex.html;	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	445292
Start date:	07.07.2021
Start time:	14:59:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Processwindo.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:	14
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.troj.winDLL@17/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.7% (good quality ratio 6.7%) • Quality average: 87.7% • Quality standard deviation: 20.5%
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
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:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.667040453584233
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:	Processwindo.DLL
File size:	404992
MD5:	5522c21a05daf91658951bdf1c0e5271
SHA1:	fed4a9b4069cd2676928441ecf8c844cc7f4a9ee
SHA256:	eb6e2519aa5c31174a1ed6c0193b2d0e49e9ed6ca1ac01ed94b3007b5e2f6993
SHA512:	d97a8021b9688c612e280ffcb5443916b9d09857daf82a62bd5efac35efeff138125466a74579568dd655cd66cd5085e10cedb4caf7981f4ee9f240839b33d55
SSDEEP:	6144:h8vockvtMD67Dvy8CyOuq107KjWMTxdtcrsianUAqPt/MmG3G/GERIgg:SwhtCy50mpMTxdtV8AqPtM3gN

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f..."..."..."..."....:.#...<.9.7...</...+.?.+..."...V...<.(.....<.>.#...<.8.#...<.=.#...Rich".....PE..L....6JJ.....

File Icon



Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x103514d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x4A4A368F [Tue Jun 30 16:00:15 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	789fcca066875e59aafcb5a18bb50d1b

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x462fd	0x46400	False	0.664559469528	data	6.60751707607	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x48000	0x16691	0x16800	False	0.645388454861	data	6.06930496404	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5f000	0x9c208	0x1800	False	0.340494791667	data	3.97938828996	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xfc000	0xf20	0x1000	False	0.352783203125	data	3.32902550096	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfd000	0x3508	0x3600	False	0.521050347222	data	5.1466661049	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Possible Origin

Language of compilation system	Country where language is spoken	Map

Copyright Joe Security LLC 2021

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 5572 Parent PID: 5780

General

Start time:	15:00:09
Start date:	07/07/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\Processwindo.DLL'
Imagebase:	0xaa0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5884 Parent PID: 5572

General

Start time:	15:00:09
Start date:	07/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\Processwindo.DLL',#1

Copyright Joe Security LLC 2021

Imagebase:	0x150000
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: 5984 Parent PID: 5572

General

Start time:	15:00:09
Start date:	07/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Processwindo.DLL,Formweather
Imagebase:	0x170000
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: 00000002.00000003.506028485.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.495420595.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.505312952.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.482226881.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.504200485.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.483330440.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.484424201.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.492896787.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.501636521.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.478507309.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.507395873.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.509298734.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.472579495.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.481041816.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.503569052.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.506726759.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.502575095.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source:

	00000002.00000003.504793852.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.479769678.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.477123674.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.493854181.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.486817454.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.475731055.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.498075018.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.489614241.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.485563074.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.508698694.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.507998418.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000002.546136992.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.491910868.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.490684908.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.488235780.0000000007360000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.474346920.0000000007360000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5996 Parent PID: 5884

General

Start time:	15:00:09
Start date:	07/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\Processwindo.DLL',#1
Imagebase:	0x170000
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: 00000003.00000002.528553318.0000000005B00000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 5560 Parent PID: 5572

General

Start time:	15:00:14
Start date:	07/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Processwindo.DLL,Piecehear
Imagebase:	0x170000
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: 00000004.00000002.542546600.0000000006F70000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 5540 Parent PID: 5572

General

Start time:	15:00:20
Start date:	07/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Processwindo.DLL,Stickregion
Imagebase:	0x170000
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: 00000005.00000002.536639176.0000000007440000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 4308 Parent PID: 5572

General

Start time:	15:00:25
Start date:	07/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\Processwindo.DLL,Would
Imagebase:	0x170000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000006.00000002.544385763.00000000078E0000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 1388 Parent PID: 3472

General

Start time:	15:02:09
Start date:	07/07/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /C timeout /t 5 && del 'C:\Users\user\Desktop\Processwindo.DLL'
Imagebase:	0x7ff7eef80000
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: conhost.exe PID: 1308 Parent PID: 1388

General

Start time:	15:02:10
Start date:	07/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 5136 Parent PID: 1388

General

Start time:	15:02:17
Start date:	07/07/2021
Path:	C:\Windows\System32\timeout.exe
Wow64 process (32bit):	
Commandline:	timeout /t 5
Imagebase:	
File size:	30720 bytes
MD5 hash:	EB9A65078396FB5D4E3813BB9198CB18
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021