ID: 432585
Sample Name: WoyEsA8v7H.dll
Cookbook: default.jbs
Time: 15:11:51
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

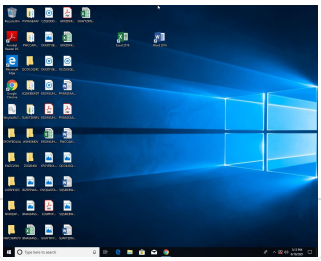
Analysis Report WoyEsA8v7H.dll

Overview

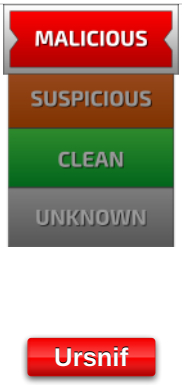
General Information

Sample Name:	WoyEsA8v7H.dll
Analysis ID:	432585
MD5:	5a414b378a75f92.
SHA1:	341a60d3181bf62.
SHA256:	0d4d60b0de26c9..
Tags:	dll Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection



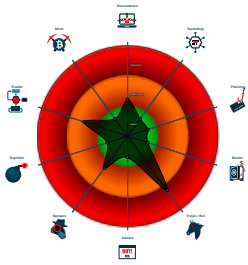
Ursnif

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Contains functionality to check if a d…
- Contains functionality to open a port…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Creates a process in suspended mo…
- Detected potential crypto function
- Found potential string decryption / a…
- PE file contains an invalid checksum

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 5300 cmdline: loaddll32.exe 'C:\Users\user\Desktop\WoyEsA8v7H.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5284 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\WoyEsA8v7H.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4968 cmdline: rundll32.exe 'C:\Users\user\Desktop\WoyEsA8v7H.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 5688 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 5212 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 1492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 4872 cmdline: rundll32.exe C:\Users\user\Desktop\WoyEsA8v7H.dll,Connectdark MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 5640 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 2996 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 4228 cmdline: rundll32.exe C:\Users\user\Desktop\WoyEsA8v7H.dll,Mindlake MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 5656 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 4660 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 1000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 4012 cmdline: rundll32.exe C:\Users\user\Desktop\WoyEsA8v7H.dll,Porthigh MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 2540 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 5424 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 1000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 1968 cmdline: rundll32.exe C:\Users\user\Desktop\WoyEsA8v7H.dll,Problemscale MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 6028 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6180 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6208 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 1532 cmdline: rundll32.exe C:\Users\user\Desktop\WoyEsA8v7H.dll,WingGrass MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 5668 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6192 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 2168 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - cmd.exe (PID: 6200 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
WoyEsA8v7H.dll	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.570061995.000000006E1A1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000002.00000002.523416376.000000006E1A1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000015.00000002.590312640.000000006E1A1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
0000000D.00000002.552879000.000000006E1A1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000010.00000002.545510346.000000006E1A1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll32.exe.6e1a0000.0.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
2.2.rundll32.exe.6e1a0000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
22.2.rundll32.exe.6e1a0000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
21.2.rundll32.exe.6e1a0000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
16.2.rundll32.exe.6e1a0000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

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

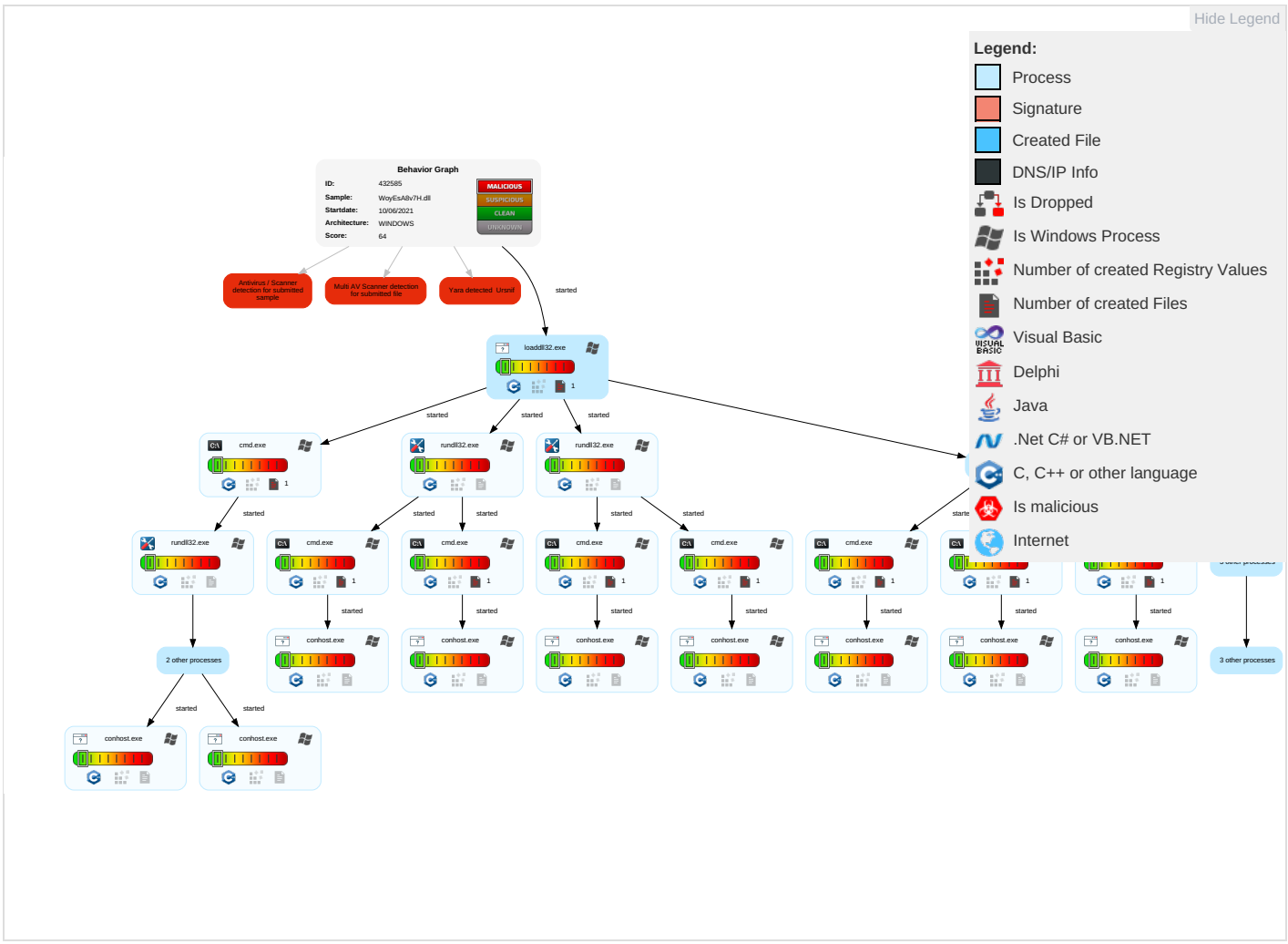
Remote Access Functionality:

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	Remot Servic Effect
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Rundll32 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remot Track I Withou Author
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remot Wipe D Withou Author
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	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 Backup
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 2 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

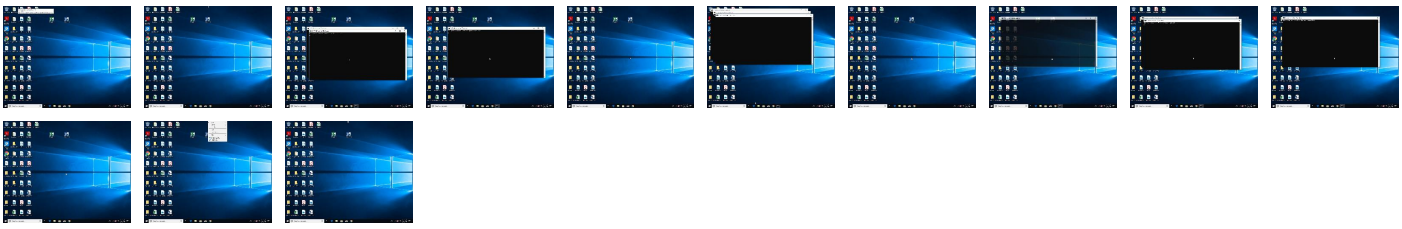
Behavior Graph



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
WoyEsA8v7H.dll	58%	Virustotal		Browse
WoyEsA8v7H.dll	100%	Avira	TR/Spy.Ursnif.ozghq	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.6e1a0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
22.2.rundll32.exe.6e1a0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
13.2.rundll32.exe.6e1a0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
21.2.rundll32.exe.6e1a0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
16.2.rundll32.exe.6e1a0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
0.2.loaddll32.exe.6e1a0000.0.unpack	100%	Avira	HEUR/AGEN.1142290		Download File

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:	32.0.0 Black Diamond
Analysis ID:	432585
Start date:	10.06.2021
Start time:	15:11:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WoyEsA8v7H.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:	39
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:	mal64.troj.winDLL@54/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.9% (good quality ratio 17.6%) • Quality average: 72.7% • Quality standard deviation: 27.9%
HCA Information:	Failed
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):	6.790057880506159
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:	WoyEsA8v7H.dll
File size:	960000
MD5:	5a414b378a75f928594e1ddacccb40dc
SHA1:	341a60d3181bf62aa8344f4544598f7e217c1b03
SHA256:	0d4d60b0de26c90819f65b22796c1600e4942e95952c6c19f2618b0461a441f
SHA512:	bf2fceb2ac9c61f66203cf9001ee0bd3c0979469e537f3ed14c59492c588a9e818a6b5661c0e453d8f6f6597a48352abe985b5a84c8d9f50b2f23b1925205608
SSDEEP:	24576:HQfpzjXPgfo8CJV4X+IBIJ3cazaLwj1mCG9CpNiLi:IFDg8JV4OaIRj150CpNiLi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t...0...0...0....{i.3...9...#...b...4...b...=...b...=....{r.&...0.....b.....b...1...b.b.1...0...1...b...1...Rich0.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1040052
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5AC512FB [Wed Apr 4 18:01:31 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:	7a79d10b1d4343a18a4f6e25e165b4ae

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x883dc	0x88400	False	0.544624426606	data	6.71833504113	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8a000	0x5a440	0x5a600	False	0.658643456086	data	5.95813601066	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xe5000	0x17ebc	0x1c00	False	0.184291294643	data	4.04646123564	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xfd000	0x9d0	0xa00	False	0.396484375	data	3.77819611332	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfe000	0x5074	0x5200	False	0.726133765244	data	6.63977268899	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
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: 5300 Parent PID: 5728

General

Start time:	15:12:41
Start date:	10/06/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\WoyEsA8v7H.dll'
Imagebase:	0xb80000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000000.00000002.574510952.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5284 Parent PID: 5300

General

Start time:	15:12:42
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\WoyEsA8v7H.dll',#1
Imagebase:	0xbd0000
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: 4872 Parent PID: 5300

General

Start time:	15:12:42
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\WoyEsA8v7H.dll,Connectdark
Imagebase:	0x1270000
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_2, Description: Yara detected Ursnif, Source: 00000002.00000002.523416376.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 4968 Parent PID: 5284

General

Start time:	15:12:42
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\WoyEsA8v7H.dll',#1
Imagebase:	0x1270000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 5640 Parent PID: 4872

General

Start time:	15:12:42
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
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: cmd.exe PID: 5688 Parent PID: 4968

General

Start time:	15:12:43
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
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: conhost.exe PID: 6104 Parent PID: 5640

General

Start time:	15:12:43
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5812 Parent PID: 5688

General

Start time:	15:12:43
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 2996 Parent PID: 4872

General

Start time:	15:12:44
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
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: cmd.exe PID: 5212 Parent PID: 4968

General

Start time:	15:12:44
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
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: conhost.exe PID: 4576 Parent PID: 2996

General

Start time:	15:12:44
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1492 Parent PID: 5212

General

Start time:	15:12:45
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 4228 Parent PID: 5300

General

Start time:	15:12:45
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\WoyEsA8v7H.dll,Mindlake
Imagebase:	0x1270000
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_2, Description: Yara detected Ursnif, Source: 0000000D.00000002.552879000.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 5656 Parent PID: 4228

General

Start time:	15:12:46
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5436 Parent PID: 5656

General

Start time:	15:12:48
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 4012 Parent PID: 5300

General

Start time:	15:12:50
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\WoyEsA8v7H.dll,Porthigh
Imagebase:	0x1270000
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_2, Description: Yara detected Ursnif, Source: 00000010.00000002.545510346.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 4660 Parent PID: 4228

General

Start time:	15:12:51
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 2540 Parent PID: 4012

General

Start time:	15:12:52
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6036 Parent PID: 2540

General

Start time:	15:12:53
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1000 Parent PID: 4660

General

Start time:	15:12:53
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7d0870000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 1968 Parent PID: 5300

General

Start time:	15:12:55
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\WoyEsA8v7H.dll,Problemscale
Imagebase:	0x1270000
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_2, Description: Yara detected Ursnif, Source: 00000015.00000002.590312640.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1532 Parent PID: 5300

General

Start time:	15:13:00
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\WoyEsA8v7H.dll,WingGrass
Imagebase:	0x1270000
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_2, Description: Yara detected Ursnif, Source: 00000016.00000002.570061995.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6028 Parent PID: 1968

General

Start time:	15:13:00
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5424 Parent PID: 4012

General

Start time:	15:13:01
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5440 Parent PID: 6028

General

Start time:	15:13:03
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1000 Parent PID: 5424

General

Start time:	15:13:03
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5668 Parent PID: 1532

General

Start time:	15:13:03
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6108 Parent PID: 5668

General

Start time:	15:13:04
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 2168 Parent PID: 5300

General

Start time:	15:13:05
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6180 Parent PID: 1968

General

Start time:	15:13:10
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6192 Parent PID: 1532

General

Start time:	15:13:11
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6200 Parent PID: 5300

General

Start time:	15:13:11
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6208 Parent PID: 6180

General

Start time:	15:13:12
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6292 Parent PID: 6192

General

Start time:	15:13:16
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis