ID: 433105
Sample Name: n8x3d68Gnd.dll
Cookbook: default.jbs
Time: 10:13:48
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

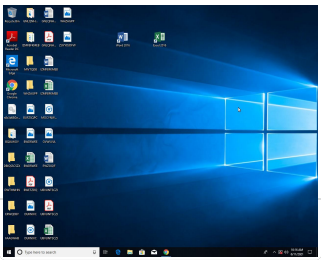
Analysis Report n8x3d68Gnd.dll

Overview

General Information

Sample Name:	n8x3d68Gnd.dll
Analysis ID:	433105
MD5:	d5c0bac78e53b4..
SHA1:	a00da4d379748f9.
SHA256:	b92289a53611d6..
Tags:	dll Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

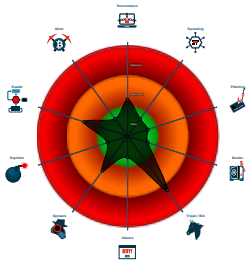
Ursnif

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

Signatures

- Antivirus / Scanner detection for sub…
- 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 DirectInput object (often fo…
- 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: 6996 cmdline: loaddll32.exe 'C:\Users\user\Desktop\n8x3d68Gnd.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 7024 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\n8x3d68Gnd.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7064 cmdline: rundll32.exe 'C:\Users\user\Desktop\n8x3d68Gnd.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 7112 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6388 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 7052 cmdline: rundll32.exe C:\Users\user\Desktop\n8x3d68Gnd.dll,Connectdark MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 7084 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 7120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 5780 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 6044 cmdline: rundll32.exe C:\Users\user\Desktop\n8x3d68Gnd.dll,Mindlake MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 3436 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 1288 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 2212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 5772 cmdline: rundll32.exe C:\Users\user\Desktop\n8x3d68Gnd.dll,Porthigh MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 5680 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 2204 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 4728 cmdline: rundll32.exe C:\Users\user\Desktop\n8x3d68Gnd.dll,Problemscale MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 6200 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6872 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 6208 cmdline: rundll32.exe C:\Users\user\Desktop\n8x3d68Gnd.dll,WingGrass MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 6472 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6940 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6768 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6580 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - cmd.exe (PID: 6876 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
n8x3d68Gnd.dll	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000002.945736297.000000006D461000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000003.00000002.949353578.000000006D461000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
0000000D.00000002.945539240.000000006D461000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000002.00000002.962212872.000000006D461000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000010.00000002.944163100.000000006D461000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll32.exe.6d460000.0.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.6d460000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
21.2.rundll32.exe.6d460000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
24.2.rundll32.exe.6d460000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
13.2.rundll32.exe.6d460000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted 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

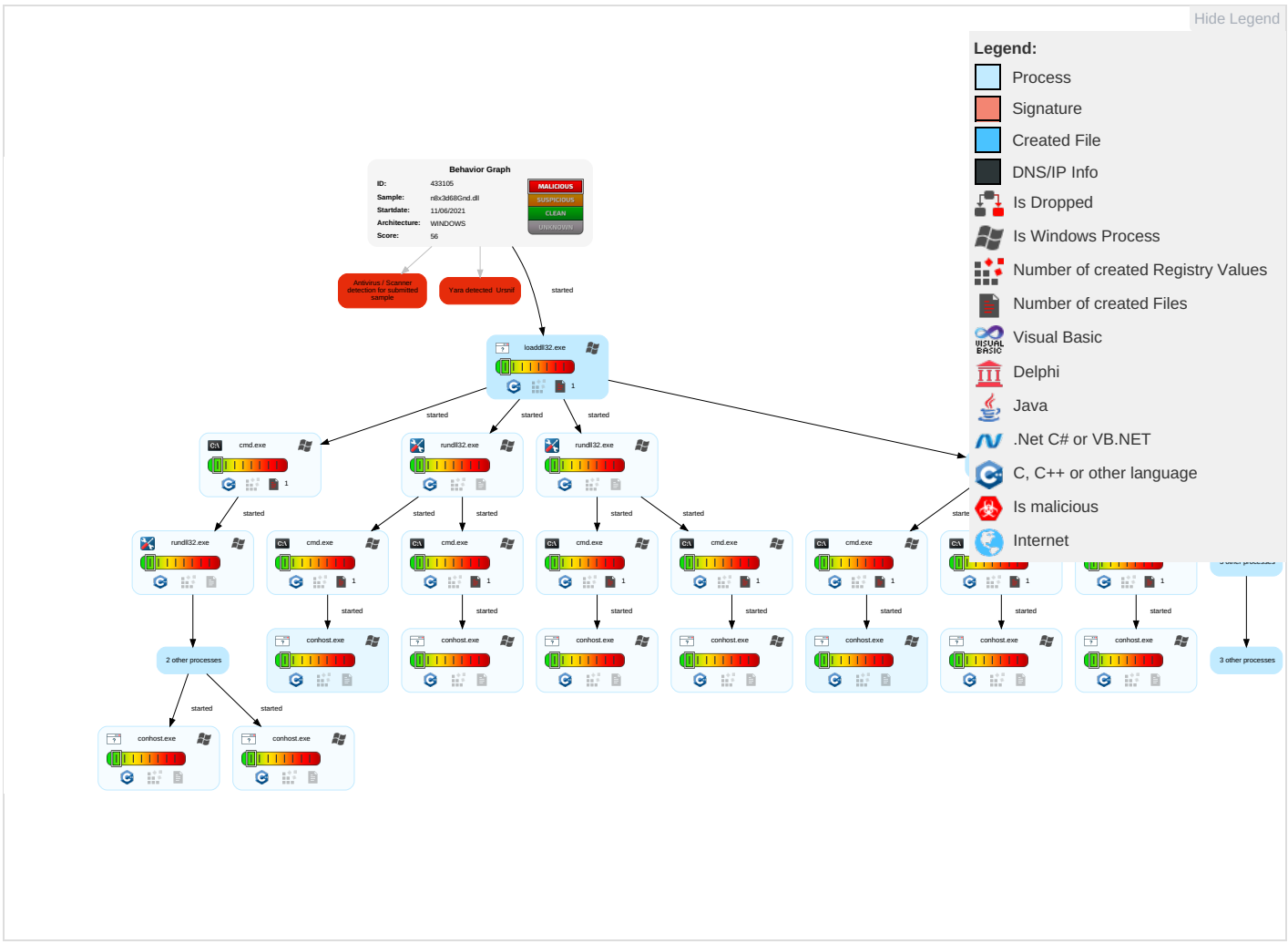
Remote Access Functionality:

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	Remot Servic Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Rundll32 1	Input Capture 1	System Time Discovery 2	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remot Track D Withou Authori
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	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remot Wipe D Withou Authori
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	

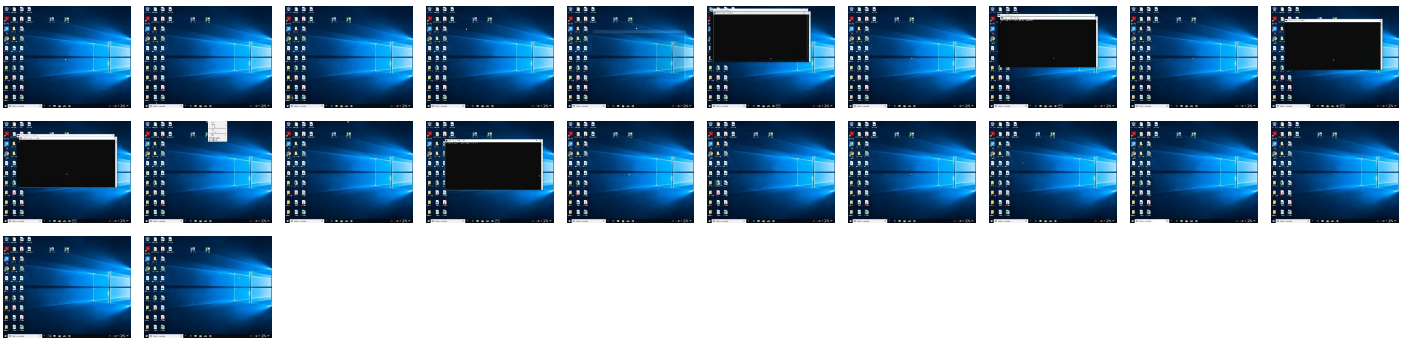
Behavior Graph



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
n8x3d68Gnd.dll	100%	Avira	TR/Spy.Ursnif.ozghq	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.2.rundll32.exe.6d460000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
0.2.loaddll32.exe.6d460000.0.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
3.2.rundll32.exe.6d460000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
21.2.rundll32.exe.6d460000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
13.2.rundll32.exe.6d460000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
2.2.rundll32.exe.6d460000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
16.2.rundll32.exe.6d460000.1.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:	433105
Start date:	11.06.2021
Start time:	10:13:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	n8x3d68Gnd.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:	36
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@55/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 51.4% (good quality ratio 48.6%) • Quality average: 77.4% • Quality standard deviation: 28.1%
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):	6.790055967805838
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:	n8x3d68Gnd.dll
File size:	960000
MD5:	d5c0bac78e53b46b2fff5e470e98210c
SHA1:	a00da4d379748f9e6f2de1006f10156aa8c36f39
SHA256:	b92289a53611d6f8c078e931c3c5c6ce577e05358bdf54389830e962090991b7
SHA512:	72a62feabaa7d94f02efe56a735f5ce6898a2c1f78d996b516deac89510feb353b105efc4662cb64ab1adf93a89d762679e7e53e2ccc59cc31d8d93e313b86ca
SSDEEP:	24576:HQfpzjXPgf98CJV4X+IBIJ3cazaLwj1mCG9CpNiLi:IFDgRJV4OaIRj150CpNiLi
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	6.71833218277	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: 6996 Parent PID: 6064

General

Start time:	10:14:35
Start date:	11/06/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\n8x3d68Gnd.dll'
Imagebase:	0xdb0000
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: 00000000.00000002.917299629.000000006D461000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 7024 Parent PID: 6996

General

Start time:	10:14:35
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\n8x3d68Gnd.dll',#1
Imagebase:	0x11d0000
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: 7052 Parent PID: 6996

General

Start time:	10:14:36
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\n8x3d68Gnd.dll,Connectdark
Imagebase:	0x1090000
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: 00000002.00000002.962212872.000000006D461000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 7064 Parent PID: 7024

General

Start time:	10:14:36
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\n8x3d68Gnd.dll',#1
Imagebase:	0x1090000
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: 00000003.00000002.949353578.000000006D461000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: cmd.exe PID: 7084 Parent PID: 7052

General

Start time:	10:14:36
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x11d0000
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: 7112 Parent PID: 7064

General

Start time:	10:14:36
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x11d0000
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: 7120 Parent PID: 7084

General

Start time:	10:14:37
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 4164 Parent PID: 7112

General

Start time:	10:14:37
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 5780 Parent PID: 7052

General

Start time:	10:14:37
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x11d0000
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: 6344 Parent PID: 5780

General

Start time:	10:14:38
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6388 Parent PID: 7064

General

Start time:	10:14:38
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x11d0000
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: 4112 Parent PID: 6388

General

Start time:	10:14:38

Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6044 Parent PID: 6996

General

Start time:	10:14:40
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\n8x3d68Gnd.dll,Mindlake
Imagebase:	0x1090000
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.00000002.945539240.000000006D461000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 3436 Parent PID: 6044

General

Start time:	10:14:41
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x11d0000
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: 4800 Parent PID: 3436

General

Start time:	10:14:41
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000

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: 5772 Parent PID: 6996

General

Start time:	10:14:44
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\n8x3d68Gnd.dll,Porthigh
Imagebase:	0x1090000
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: 00000010.00000002.944163100.000000006D461000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 5680 Parent PID: 5772

General

Start time:	10:14:45
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x11d0000
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: 1288 Parent PID: 6044

General

Start time:	10:14:45
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x11d0000
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: 4820 Parent PID: 5680

General

Start time:	10:14:45
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 2212 Parent PID: 1288

General

Start time:	10:14:46
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 4728 Parent PID: 6996

General

Start time:	10:14:48
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\n8x3d68Gnd.dll,Problemscale
Imagebase:	0x1090000
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: 00000015.00000002.921268168.000000006D461000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 2204 Parent PID: 5772

General

Start time:	10:14:50
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x11d0000
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: 4728

General

Start time:	10:14:51
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x11d0000
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: rundll32.exe PID: 6208 Parent PID: 6996

General

Start time:	10:14:52
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\n8x3d68Gnd.dll,WingGrass
Imagebase:	0x1090000
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: 00000018.00000002.945736297.000000006D461000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 6728 Parent PID: 2204

General

Start time:	10:14:53

Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6560 Parent PID: 6200

General

Start time:	10:14:53
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6472 Parent PID: 6208

General

Start time:	10:14:58
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x11d0000
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: 6596 Parent PID: 6472

General

Start time:	10:14:58
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6580 Parent PID: 6996

General

Start time:	10:14:58
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x11d0000
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: 6872 Parent PID: 4728

General

Start time:	10:15:01
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x11d0000
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: 6820 Parent PID: 6872

General

Start time:	10:15:03
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77ba70000
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: 6876 Parent PID: 6996

General

Start time:	10:15:05
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x11d0000
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: 6940 Parent PID: 6208

General

Start time:	10:15:05
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x11d0000
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: 6768 Parent PID: 6940

General

Start time:	10:15:12
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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