ID: 430230
Sample Name:
QDfpQK7SOG.dll
Cookbook: default.jbs
Time: 08:44:42
Date: 07/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report QDfpQK7SOG.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 5
Initial Sample 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 6
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
E-Banking Fraud: 6
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted IPs 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 10
General 10
File Icon 11
Static PE Info 11
General 11
Entrypoint Preview 11
Rich Headers 12
Data Directories 12
Sections 12
Resources 13
Imports 13
Exports 13
Possible Origin 13
Network Behavior 14
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: loaddll32.exe PID: 6520 Parent PID: 5876 14
General 14
File Activities 15
Analysis Process: cmd.exe PID: 6560 Parent PID: 6520 15
General 15
File Activities 15
Analysis Process: rundll32.exe PID: 6572 Parent PID: 6520 15
General 15
Analysis Process: rundll32.exe PID: 6588 Parent PID: 6560 15
General 15
Analysis Process: cmd.exe PID: 6616 Parent PID: 6572 16
General 16
File Activities 16

Analysis Process: cmd.exe PID: 6632 Parent PID: 6588 16
General 16
File Activities 16
Analysis Process: conhost.exe PID: 6648 Parent PID: 6616 17
General 17
Analysis Process: conhost.exe PID: 6664 Parent PID: 6632 17
General 17
Analysis Process: cmd.exe PID: 6740 Parent PID: 6572 17
General 17
File Activities 17
Analysis Process: conhost.exe PID: 6788 Parent PID: 6740 17
General 18
Analysis Process: cmd.exe PID: 6800 Parent PID: 6588 18
General 18
File Activities 18
Analysis Process: conhost.exe PID: 6808 Parent PID: 6800 18
General 18
Analysis Process: rundll32.exe PID: 6884 Parent PID: 6520 18
General 18
Analysis Process: cmd.exe PID: 6900 Parent PID: 6884 19
General 19
File Activities 19
Analysis Process: conhost.exe PID: 6912 Parent PID: 6900 19
General 19
Analysis Process: rundll32.exe PID: 6956 Parent PID: 6520 19
General 19
Analysis Process: cmd.exe PID: 6968 Parent PID: 6884 20
General 20
File Activities 20
Analysis Process: conhost.exe PID: 6976 Parent PID: 6968 20
General 20
Analysis Process: cmd.exe PID: 7008 Parent PID: 6956 20
General 20
File Activities 21
Analysis Process: conhost.exe PID: 7024 Parent PID: 7008 21
General 21
Analysis Process: cmd.exe PID: 7072 Parent PID: 6956 21
General 21
File Activities 21
Analysis Process: rundll32.exe PID: 7084 Parent PID: 6520 21
General 21
Analysis Process: conhost.exe PID: 7124 Parent PID: 7072 22
General 22
Analysis Process: rundll32.exe PID: 2332 Parent PID: 6520 22
General 22
Analysis Process: cmd.exe PID: 776 Parent PID: 7084 22
General 22
File Activities 23
Analysis Process: conhost.exe PID: 5700 Parent PID: 776 23
General 23
Analysis Process: cmd.exe PID: 3924 Parent PID: 2332 23
General 23
File Activities 23
Analysis Process: conhost.exe PID: 5644 Parent PID: 3924 23
General 23
Analysis Process: cmd.exe PID: 5632 Parent PID: 7084 24
General 24
File Activities 24
Analysis Process: cmd.exe PID: 4568 Parent PID: 6520 24
General 24
File Activities 24
Analysis Process: conhost.exe PID: 5820 Parent PID: 5632 24
General 24
Analysis Process: cmd.exe PID: 6364 Parent PID: 6520 25
General 25
File Activities 25
Analysis Process: cmd.exe PID: 4148 Parent PID: 2332 25
General 25
File Activities 25
Analysis Process: conhost.exe PID: 1604 Parent PID: 4148 25
General 25
Disassembly 26
Code Analysis 26

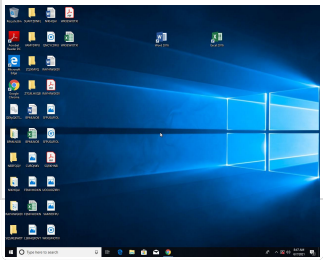
Analysis Report QDfpQK7SOG.dll

Overview

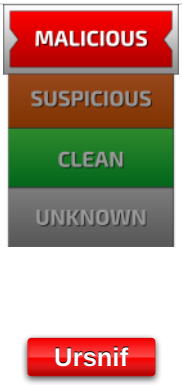
General Information

Sample Name:	QDfpQK7SOG.dll
Analysis ID:	430230
MD5:	320192b545d3f45.
SHA1:	807433d7c1f8c76..
SHA256:	2ee0e0b21737b7..
Tags:	dll Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection

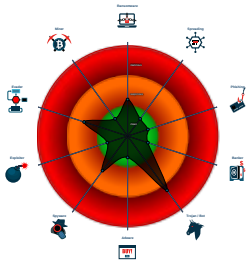


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 DirectInput object (often fo…
- Creates a process in suspended mo…
- Detected potential crypto function
- Found potential string decryption / a…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6520 cmdline: loaddll32.exe 'C:\Users\user\Desktop\QDfpQK7SOG.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6560 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\QDfpQK7SOG.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6588 cmdline: rundll32.exe 'C:\Users\user\Desktop\QDfpQK7SOG.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 6632 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6664 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6800 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 6572 cmdline: rundll32.exe C:\Users\user\Desktop\QDfpQK7SOG.dll,Connectdark MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 6616 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6740 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 6884 cmdline: rundll32.exe C:\Users\user\Desktop\QDfpQK7SOG.dll,Mindlake MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 6900 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6968 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6976 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 6956 cmdline: rundll32.exe C:\Users\user\Desktop\QDfpQK7SOG.dll,Porthigh MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 7008 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 7024 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 7072 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 7124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 7084 cmdline: rundll32.exe C:\Users\user\Desktop\QDfpQK7SOG.dll,Problemscale MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 776 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 5632 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 2332 cmdline: rundll32.exe C:\Users\user\Desktop\QDfpQK7SOG.dll,WingGrass MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - cmd.exe (PID: 3924 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 4148 cmdline: C:\Windows\system32\cmd.exe /c cd Matter m MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 1604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 4568 cmdline: C:\Windows\system32\cmd.exe /c cd Island MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - cmd.exe (PID: 6364 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
QDfpQK7SOG.dll	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000001A.00000002.664721905.000000006E1A1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000004.00000002.677279699.000000006E1A1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000012.00000002.686115705.000000006E1A1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000005.00000002.687931274.000000006E1A1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000018.00000002.696642986.000000006E1A1000.00000020.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
Click to see the 2 entries				

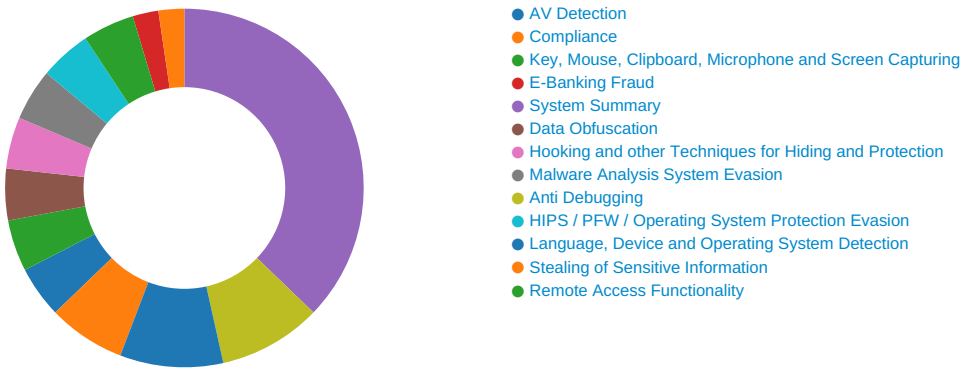
Unpacked PEs

Source	Rule	Description	Author	Strings
26.2.rundll32.exe.6e1a0000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
2.2.loaddll32.exe.6e1a0000.0.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
15.2.rundll32.exe.6e1a0000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
24.2.rundll32.exe.6e1a0000.1.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
4.2.rundll32.exe.6e1a0000.1.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

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

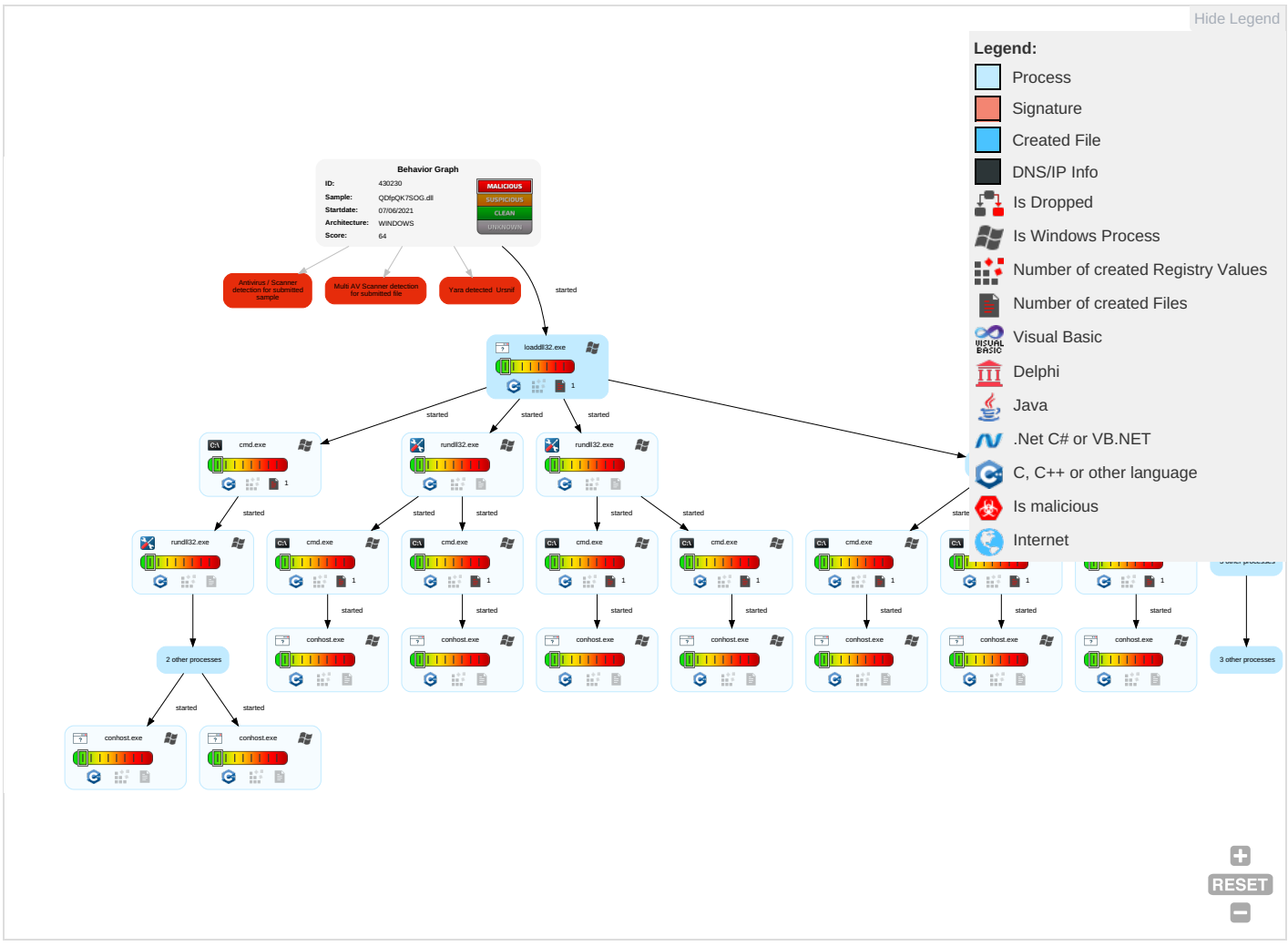
Remote Access Functionality:

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 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	

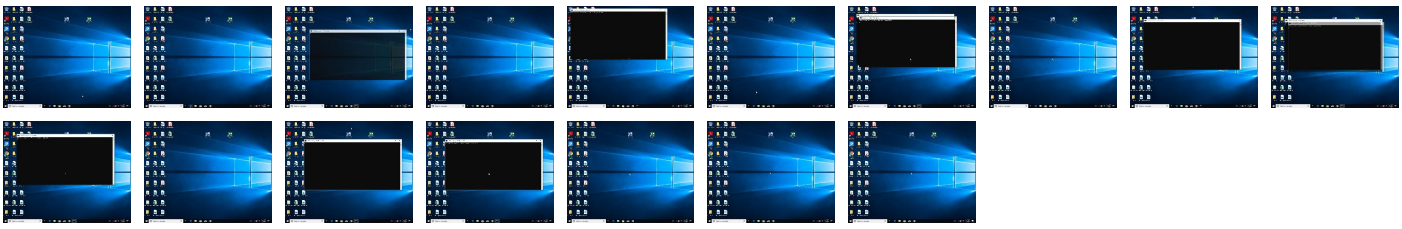
Behavior Graph



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
QDfpQK7SOG.dll	60%	Virustotal		Browse
QDfpQK7SOG.dll	66%	ReversingLabs	Win32.Trojan.Zusy	
QDfpQK7SOG.dll	100%	Avira	TR/Spy.Ursnif.ozghq	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.rundll32.exe.6e1a0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
26.2.rundll32.exe.6e1a0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
15.2.rundll32.exe.6e1a0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
2.2.loaddll32.exe.6e1a0000.0.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
18.2.rundll32.exe.6e1a0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
24.2.rundll32.exe.6e1a0000.1.unpack	100%	Avira	HEUR/AGEN.1142290		Download File
4.2.rundll32.exe.6e1a0000.1.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:	430230
Start date:	07.06.2021
Start time:	08:44:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QDfpQK7SOG.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:	42
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@55/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.2% (good quality ratio 14.2%) • Quality average: 68.9% • Quality standard deviation: 26.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • Not all processes where analyzed, report is missing behavior information • Report size exceeded maximum capacity and may have missing behavior information.

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):	6.790050906790882
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:	QDfpQK7SOG.dll
File size:	960000
MD5:	320192b545d3f45fd588b741c30fb2ec
SHA1:	807433d7c1f8c7629ebcafd9d2c4e6797c82ce16
SHA256:	2ee0e0b21737b7f9ecc613be83b7ec84560d0770f794a819afe64f54b0e7743b
SHA512:	c95b2c2d1f7cdf5950db9bd655965cbacf3b8d383728db3786de404e68f70bec761dc6101ebbf6b0fc0252ec8626a8c5247cce4e5f378c6a63da648364b158c9
SSDEEP:	24576:HQfpzjXPgfh8CJV4X+IBIJ3cazaLwj1mCG9CpNiLi:IFDgVJV4OaIRj150CpNiLi

General

File Content Preview:	MZ.....@.....!..L.!This is 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

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FE81898C597h
call 00007FE81898CF72h
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FE81898C43Fh
add esp, 0Ch
pop ebp
retn 000Ch
mov ecx, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], ecx
pop ecx
pop edi
pop edi
pop esi
pop ebx
mov esp, ebp
pop ebp
push ecx
ret
mov ecx, dword ptr [ebp-10h]
xor ecx, ebp
call 00007FE81898BDA6h
jmp 00007FE81898C570h
mov ecx, dword ptr [ebp-14h]
xor ecx, ebp

Instruction
call 00007FE81898BD95h
jmp 00007FE81898C55Fh
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [010E506Ch]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [010E506Ch]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
inc dword ptr fs:[eax]

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xe35b0	0x9c	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe364c	0x8c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xfd000	0x9d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xfe000	0x5074	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xde820	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xde878	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8a000	0x26c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x883dc	0x88400	False	0.544624426606	data	6.71832454464	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

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0xfd1c0	0x10e	data	English	United States
RT_DIALOG	0xfd2d0	0xc0	dBase III DBT, next free block index 4294901761	English	United States
RT_DIALOG	0xfd390	0x126	data	English	United States
RT_DIALOG	0xfd4b8	0xf0	data	English	United States
RT_DIALOG	0xfd5a8	0xba	data	English	United States
RT_DIALOG	0xfd664	0xec	data	English	United States
RT_DIALOG	0xfd750	0x124	data	English	United States
RT_MANIFEST	0xfd874	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableA, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, GetProcessHeap, CreateFileW, SetStdHandle, ReadConsoleW, WriteConsoleW, HeapSize, SetEndOfFile, SetEnvironmentVariableW, GetOEMCP, IsValidCodePage, FindNextFileW, FindNextFileA, FindFirstFileExW, FindFirstFileExA, FindClose, GetTimeZoneInformation, OutputDebugStringA, OutputDebugStringW, WaitForSingleObjectEx, CreateSemaphoreA, GetSystemTimeAsFileTime, TlsGetValue, VirtualProtectEx, TlsAlloc, GetSystemDirectoryA, GetTempPathA, Sleep, GetCommandLineA, GetModuleHandleA, InitializeCriticalSection, SetSystemPowerState, EnterCriticalSection, VirtualProtect, GetModuleFileNameA, MultiByteToWideChar, GetLastError, FormatMessageW, WideCharToMultiByte, GetStringTypeW, LeaveCriticalSection, DeleteCriticalSection, SetLastError, InitializeCriticalSectionAndSpinCount, CreateEventW, SwitchToThread, TlsSetValue, TlsFree, GetTickCount, GetModuleHandleW, GetProcAddress, EncodePointer, DecodePointer, CompareStringW, LCMapStringW, GetLocaleInfoW, GetCPInfo, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, IsDebuggerPresent, GetStartupInfoW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, InitializeSListHead, RtlUnwind, RaiseException, InterlockedPushEntrySList, InterlockedFlushSList, FreeLibrary, LoadLibraryExW, ExitProcess, GetModuleHandleExW, GetModuleFileNameW, HeapAlloc, HeapFree, GetCurrentThread, GetACP, GetStdHandle, GetFileType, CloseHandle, WaitForSingleObject, GetExitCodeProcess, CreateProcessA, CreateProcessW, GetFileAttributesExW, WriteFile, GetConsoleCP, GetConsoleMode, GetDateFormatW, GetTimeFormatW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, FlushFileBuffers, ReadFile, SetFilePointerEx, HeapReAlloc, SetConsoleCtrlHandler, CreateThread
USER32.dll	SetFocus, GetCursorPos, RegisterClassExA, GetFocus, GetClassInfoExA, GetKeyNameTextA, GetWindowTextLengthA, CallWindowProcA, IsDlgButtonChecked, DestroyIcon, AppendMenuA, DrawIconEx, DrawEdge
GDI32.dll	BitBlt, DeleteDC, CreatePen, DeleteObject, CreateDCA, GetObjectA, DPtoLP
ole32.dll	OleUninitialize, OleSetContainedObject, OleInitialize
SHLWAPI.dll	PathFindFileNameA, PathAddBackslashW, PathStripToRootA
DCIMAN32.dll	DCICreatePrimary, DCIOpenProvider, GetDCRegionData, DCISetDestination, DCICloseProvider, DCICreateOverlay, GetWindowRegionData, DCIEndAccess, WinWatchDidStatusChange, DCICreateOffscreen, DCISetSrcDestClip, DCIDestroy, DCIDraw, DCISetClipList, DCIEnum, DCIBeginAccess, WinWatchClose

Exports

Name	Ordinal	Address
Connectdark	1	0x1021c64
Mindlake	2	0x1020de0
Porthigh	3	0x1021c2c
Problemscale	4	0x1021bf8
WingGrass	5	0x1021b0a

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

System Behavior

Analysis Process: loaddll32.exe PID: 6520 Parent PID: 5876

General

Start time:	08:45:33
Start date:	07/06/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\QDfpQK7SOG.dll'
Imagebase:	0x100000
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: 00000002.00000002.675775659.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6560 Parent PID: 6520

General

Start time:	08:45:33
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\QDfpQK7SOG.dll',#1
Imagebase:	0x2a0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6572 Parent PID: 6520

General

Start time:	08:45:33
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\QDfpQK7SOG.dll,Connectdark
Imagebase:	0xd30000
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: 00000004.00000002.677279699.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6588 Parent PID: 6560

General

Start time:	08:45:34
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\QDfpQK7SOG.dll',#1
Imagebase:	0xd30000
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: 00000005.00000002.687931274.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: cmd.exe PID: 6616 Parent PID: 6572

General

Start time:	08:45:34
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x2a0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6632 Parent PID: 6588

General

Start time:	08:45:34
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x2a0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6648 Parent PID: 6616

General

Start time:	08:45:35
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6664 Parent PID: 6632

General

Start time:	08:45:35
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6740 Parent PID: 6572

General

Start time:	08:45:35
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x2a0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6788 Parent PID: 6740

General

Start time:	08:45:36
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6800 Parent PID: 6588

General

Start time:	08:45:36
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x2a0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6808 Parent PID: 6800

General

Start time:	08:45:36
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: rundll32.exe PID: 6884 Parent PID: 6520

General

Start time:	08:45:37
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\QDfpQK7SOG.dll,Mindlake
Imagebase:	0xd30000
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: 0000000F.00000002.690715845.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6900 Parent PID: 6884

General

Start time:	08:45:38
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6912 Parent PID: 6900

General

Start time:	08:45:39
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6956 Parent PID: 6520

General

Start time:	08:45:41
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe

Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\QDfpQK7SOG.dll,Porthigh
Imagebase:	0xd30000
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: 00000012.00000002.686115705.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6968 Parent PID: 6884

General

Start time:	08:45:41
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6976 Parent PID: 6968

General

Start time:	08:45:43
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 7008 Parent PID: 6956

General

Start time:	08:45:43
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x2a0000

File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7024 Parent PID: 7008

General

Start time:	08:45:44
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 7072 Parent PID: 6956

General

Start time:	08:45:47
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7084 Parent PID: 6520

General

Start time:	08:45:47
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\QDfpQK7SOG.dll,Problemscale
Imagebase:	0xd30000

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: 00000018.00000002.696642986.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 7124 Parent PID: 7072

General

Start time:	08:45:50
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 2332 Parent PID: 6520

General

Start time:	08:45:52
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\QDfpQK7SOG.dll,WingGrass
Imagebase:	0xd30000
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: 0000001A.00000002.664721905.000000006E1A1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 776 Parent PID: 7084

General

Start time:	08:45:52
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5700 Parent PID: 776

General

Start time:	08:45:53
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 3924 Parent PID: 2332

General

Start time:	08:45:55
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5644 Parent PID: 3924

General

Start time:	08:45:56
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 5632 Parent PID: 7084

General

Start time:	08:45:58
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4568 Parent PID: 6520

General

Start time:	08:45:58
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Island
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5820 Parent PID: 5632

General

Start time:	08:46:00
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6364 Parent PID: 6520

General

Start time:	08:46:06
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4148 Parent PID: 2332

General

Start time:	08:46:08
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c cd Matter m
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1604 Parent PID: 4148

General

Start time:	08:46:14
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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