ID: 626596
Sample Name: DHL_29028263 documento de recibo de la compra,pdf.exe
Cookbook: default.jbs
Time: 15:11:11
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report

DHL_29028263 documento de recibo de la compra,pdf.exe

Overview

General Information

Sample Name:	DHL_29028263 documento de recibo de la compra,pdf.exe
Analysis ID:	626596
MD5:	87a264aa9aec9c..
SHA1:	64a0954e622afb..
SHA256:	eab5b352e41de8.
Tags:	AveMariaRAT DHL exe RAT
Infos:	

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

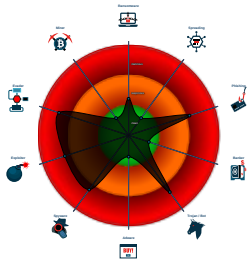
AveMaria, UACMe

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected UACMe UAC Bypass…
- Yara detected AveMaria stealer
- Multi AV Scanner detection for drop…
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Increases the number of concurrent…
- Contains functionality to hide user a…
- Contains functionality to steal e-mai…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- DHL_29028263 documento de recibo de la compra,pdf.exe (PID: 7092 cmdline: "C:\Users\user\Desktop\DHL_29028263 documento de recibo de la compra,pdf.exe" MD5: 87A264AA9AEC9CE66F4B092363DD5ADC)
  - DHL_29028263 documento de recibo de la compra,pdf.exe (PID: 6600 cmdline: C:\Users\user\Desktop\DHL_29028263 documento de recibo de la compra,pdf.exe MD5: 87A264AA9AEC9CE66F4B092363DD5ADC)
    - cmd.exe (PID: 6632 cmdline: C:\Windows\System32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 2208 cmdline: "cmd.exe" /C schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Roaming\window defender\window defender.exe'" /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 4468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 4992 cmdline: schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Roaming\window defender\window defender.exe'" /f MD5: 15FF7D8324231381BAD48A052F85DF04)
    - cmd.exe (PID: 6716 cmdline: cmd.exe" /C copy "C:\Users\user\Desktop\DHL_29028263 documento de recibo de la compra,pdf.exe" "C:\Users\user\AppData\Roaming\window defender\window defender.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 7084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- window defender.exe (PID: 3668 cmdline: C:\Users\user\AppData\Roaming\window defender\window defender.exe MD5: 87A264AA9AEC9CE66F4B092363DD5ADC)
- **cleanup**

Malware Configuration

Threatname: AveMaria

```
{
  "C2 url": "37.0.14.197",
  "port": 1997
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.417195755.000000000054F000.00000040.00000400.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xdf0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xdf0:$c1: Elevation:Administrator!new:
00000003.00000000.417195755.000000000054F000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
00000003.00000000.416591236.0000000000400000.00000040.00000400.00020000.00000000.sdmp	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x150e8:$a1: \Opera Software\Opera Stable\Login Data • 0x15410:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x14d58:$a3: \Google\Chrome\User Data\Default\Login Data
00000003.00000000.416591236.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000003.00000000.416591236.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
Click to see the 77 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.3.DHL_29028263 documento de recibo de la compra, pdf.exe.12d02b0.2.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x2318:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
3.3.DHL_29028263 documento de recibo de la compra, pdf.exe.12d02b0.2.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x2318:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x2318:$c1: Elevation:Administrator!new:
3.3.DHL_29028263 documento de recibo de la compra, pdf.exe.12d02b0.2.raw.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
1.2.DHL_29028263 documento de recibo de la compra, pdf.exe.3218090.2.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
1.2.DHL_29028263 documento de recibo de la compra, pdf.exe.3218090.2.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xd80:$c1: Elevation:Administrator!new:
Click to see the 160 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits

Yara detected UACMe UAC Bypass tool

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected AveMaria stealer

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation

Binary or sample is protected by dotNetProtector

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

Contains functionality to hide user accounts

Hides that the sample has been downloaded from the Internet (zone.identifier)

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)

Contains functionality to inject threads in other processes

Lowering of HIPS / PFW / Operating System Security Settings

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information

Yara detected AveMaria stealer

Contains functionality to steal e-mail passwords

Contains functionality to steal Chrome passwords or cookies

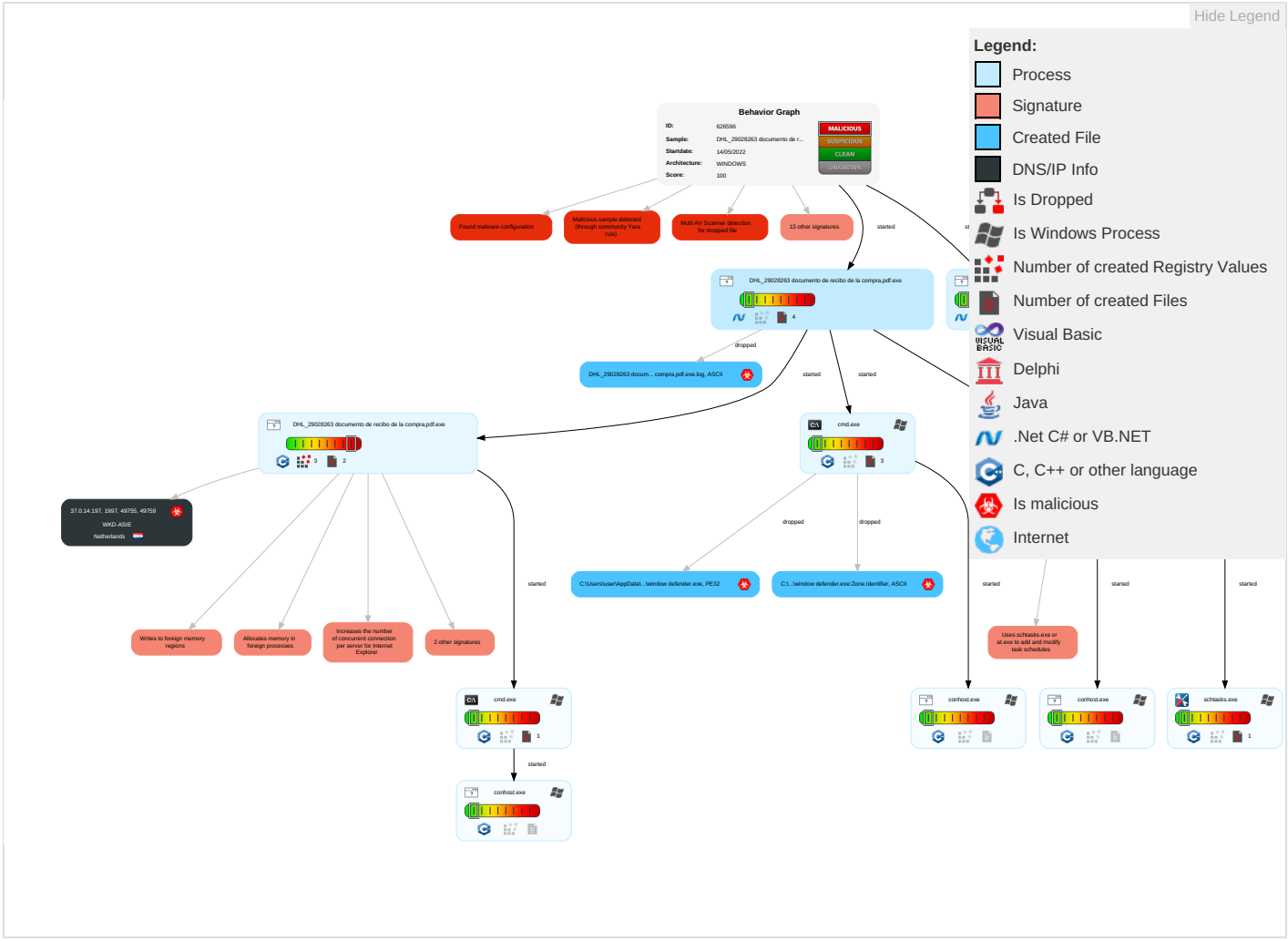
Remote Access Functionality

Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 Create Account	1 Access Token Manipulation	1 Disable or Modify Tools	2 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Endpoint Denial of Service
Default Accounts	1 Scheduled Task/Job	1 Windows Service	1 Windows Service	1 Deobfuscate/Decode Files or Information	3 1 Input Capture	1 System Service Discovery	Remote Desktop Protocol	3 1 Input Capture	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Service Execution	1 Scheduled Task/Job	4 2 1 Process Injection	2 Obfuscated Files or Information	1 Credentials In Files	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Scheduled Task/Job	1 Software Packing	NTDS	2 3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Masquerading	LSA Secrets	1 2 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	1 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	4 2 1 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Users	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

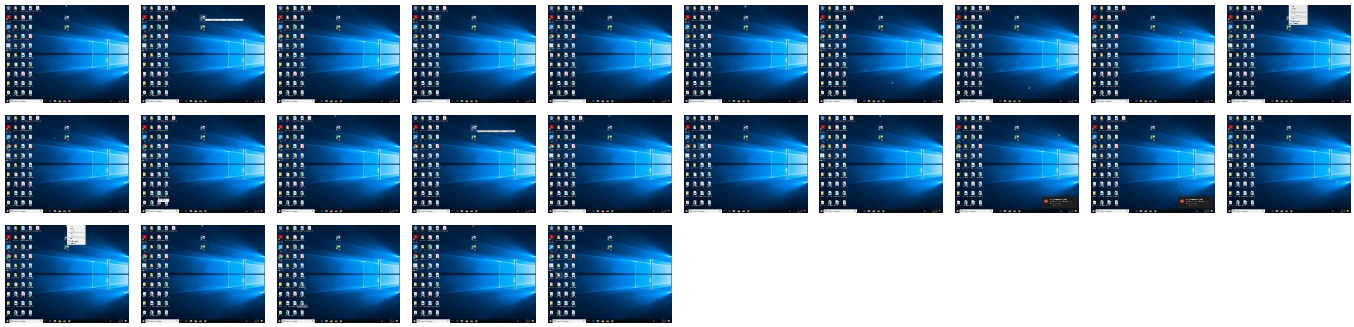
Behavior Graph



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
DHL_29028263 documento de recibo de la compra,pdf.exe	33%	Virustotal		Browse
DHL_29028263 documento de recibo de la compra,pdf.exe	51%	ReversingLabs	ByteCode-MSIL.Trojan.FormBook	
DHL_29028263 documento de recibo de la compra,pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\window defender\window defender.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\window defender\window defender.exe	51%	ReversingLabs	ByteCode-MSIL.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.DHL_29028263 documento de recibo de la compra,pdf.exe.400000.7.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
3.0.DHL_29028263 documento de recibo de la compra,pdf.exe.400000.13.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
3.0.DHL_29028263 documento de recibo de la compra,pdf.exe.400000.5.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
3.0.DHL_29028263 documento de recibo de la compra,pdf.exe.400000.16.unpack	100%	Avira	TR/Redcap.ghjpt		Download File

Source	Detection	Scanner	Label	Link	Download
3.2.DHL_29028263 documento de recibo de la compra,pdf.exe.400000.1.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
3.0.DHL_29028263 documento de recibo de la compra,pdf.exe.400000.19.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
3.0.DHL_29028263 documento de recibo de la compra,pdf.exe.400000.11.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
3.0.DHL_29028263 documento de recibo de la compra,pdf.exe.400000.22.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
3.0.DHL_29028263 documento de recibo de la compra,pdf.exe.400000.9.unpack	100%	Avira	TR/Redcap.ghjpt		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
37.0.14.197	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

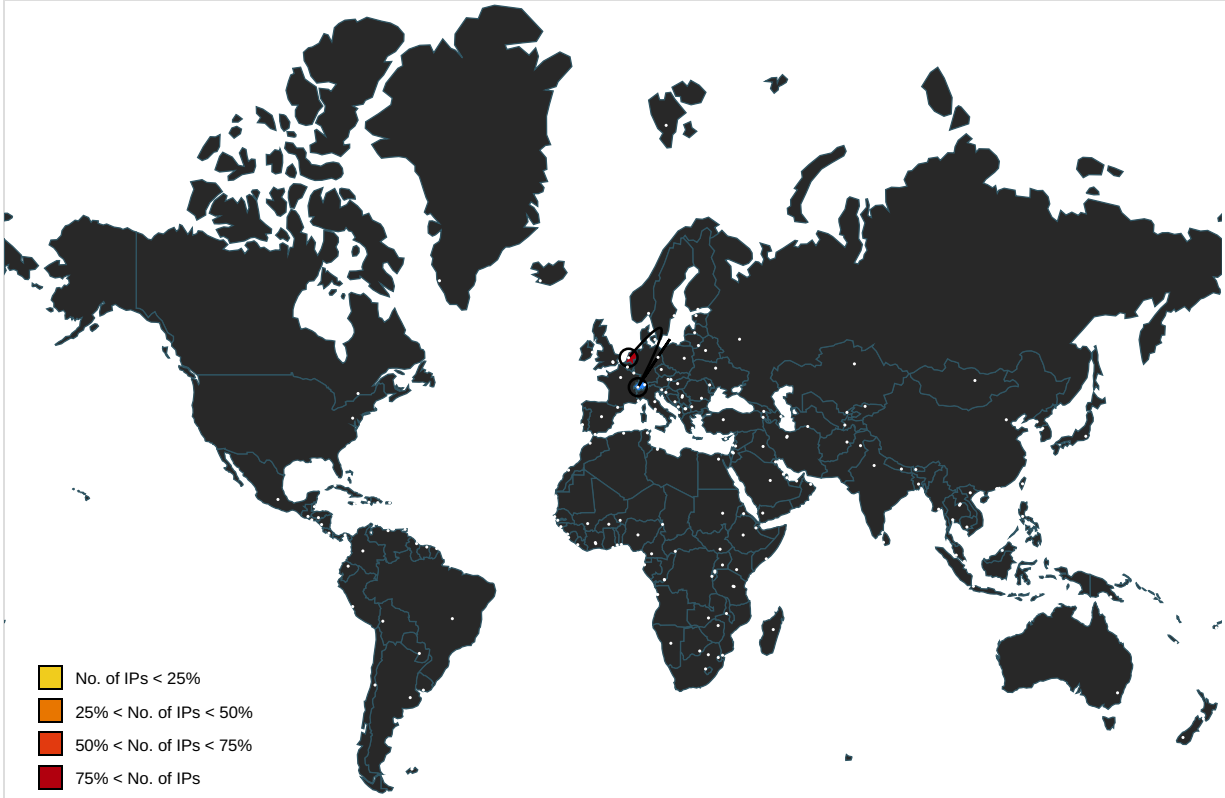
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
37.0.14.197	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/syohex/java-simple-mine-sweeperC:	DHL_29028263 documento de recibo de la compra,pdf.exe, 00000001.00000002.447136668.0000000003200000.00000004.00000800.00020000.00000000.sdmp, DHL_29028263 documento de recibo de la compra,pdf.exe, 00000001.00000002.447222285.0000000004129000.00000004.00000800.00020000.00000000.sdmp, DHL_29028263 documento de recibo de la compra,pdf.exe, 00000003.00000000.416591236.0000000000400000.00000040.00000400.00020000.00000000.sdmp, DHL_29028263 documento de recibo de la compra,pdf.exe, 00000003.00000003.426962811.00000000012E1000.00000004.00000020.00020000.00000000.sdmp, DHL_29028263 documento de recibo de la compra,pdf.exe, 00000003.00000003.431623764.00000000012F4000.00000004.00020000.00020000.00000000.sdmp, DHL_29028263 documento de recibo de la compra,pdf.exe, 00000003.00000003.431567861.00000000012F4000.00000004.00000020.00020000.00000000.sdmp, DHL_29028263 documento de recibo de la compra,pdf.exe, 00000003.00000003.431671478.00000000012F4000.00000004.00000020.00020000.00000000.sdmp, DHL_29028263 documento de recibo de la compra,pdf.exe, 00000003.00000002.622706566.0000000000400000.00000040.00000040.00020000.00000000.sdmp, DHL_29028263 documento de recibo de la compra,pdf.exe, 00000003.00000003.426786774.00000000012FA000.00000004.00000020.00020000.00000000.sdmp, DHL_29028263 documento de recibo de la compra,pdf.exe, 00000003.00000000.415418870.0000000000400000.00000040.00000400.00020000.00000000.sdmp, DHL_29028263 documento de recibo de la compra,pdf.exe, 00000003.00000003.424810982.00000000012E1000.00000004.00000020.00020000.00000000.sdmp, DHL_29028263 documento de recibo de la compra,pdf.exe, 00000003.00000003.431652682.00000000012FA000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://github.com/syohex/java-simple-mine-sweeper	DHL_29028263 documento de recibo de la compra,pdf.exe	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.0.14.197	unknown	Netherlands		198301	WKD-ASIE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626596
Start date and time: 14/05/202215:11:11	2022-05-14 15:11:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_29028263 documento de recibo de la compra,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:	18
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.phis.troj.spyw.expl.evad.winEXE@15/3@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 93% (good quality ratio 92.1%) • Quality average: 89.1% • Quality standard deviation: 18.6%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, fp-vp.azureedge.net, ctldl.windowsupdate.com, arc.msn.com, b-ring.msedge.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:13:00	Task Scheduler	Run new task: Nafifas path: "C:\Users\user\AppData\Roaming\window defender\window defender.exe"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_29028263 documento de recibo de la compra,pdf.exe.log

Process:	C:\Users\user\Desktop\DHL_29028263 documento de recibo de la compra,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd

MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\window defender\window defender.exe

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	411136
Entropy (8bit):	6.317346244576242
Encrypted:	false
SSDEEP:	6144:fTMhHqjnw6E7SHrJxLY19rS/heoPYtO2LXQOuh23Ta7UEbS2RuLmDtzJ:rsH6E7GPw01YUwsf7UwuLmDtzJ
MD5:	87A264AA9AEC9CE66F4B092363DD5ADC
SHA1:	64A0954E622AFB6D5E2A0256F179D14F112EC723
SHA-256:	EAB5B352E41DE89BE099054E396F61A942401AB1518186496BC11BE1C857242F
SHA-512:	C427A4F1822EB62B75AA346FA891A69F6A712FABAF7C126BC51D49729226EE92A0EB8DAAB649CAAE96E77EC95F415771B2EDF60CA4FDB3A6F56C65F82C33695C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 51%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...M.~b..... ....@.. .....$.. ..@..... .....O.....B..... ....H.....text..... ....`.rsrc...B.....@..@.reloc..... .....D.....@..B.....H.....p...,.....9....9.....(....*..,.~&...(....&~'...rMK.p(....~'...r]K.p(....*..-.*(....&*2~.....(....*..(....*.*..{....*..{....*:~.....(....*..{....*.:~.....(....*..{....*6~.....(....*..{....*..{....*..{....*..(.....#.%.L...A#...V...A(w...X(r...Zeff. .;.. ..6`aiZ}....*..{....*..{....*.~....(....*..{....*B.(.....ee}....*..{....*.~....(....*..{....*..{....*..~,...(....*..{....*....0.....#.....@#

C:\Users\user\AppData\Roaming\window defender\window defender.exe:Zone.Identifier

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.317346244576242
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%

File name:	DHL_29028263 documento de recibo de la compra,pdf.exe
File size:	411136
MD5:	87a264aa9aec9ce66f4b092363dd5adc
SHA1:	64a0954e622afb6d5e2a0256f179d14f112ec723
SHA256:	eab5b352e41de89be099054e396f61a942401ab1518186496bc11be1c857242f
SHA512:	c427a4f1822eb62b75aa346fa891a69f6a712fabaf7c126bc51d49729226ee92a0eb8daab649caae96e77ec95f415771b2edf60ca4fdb3a6f56c65f82c33695c
SSDEEP:	6144:fTMhHqjnw6E7SHrJxLY19rS/heoPYtO2LXQOuh23Ta7UEbS2RuLmDtzJ:rsH6E7GPw01YUwsf7UwuLmDtzJ
TLSH:	DB94EB9C7B410E72ED2D913845130A24BB620EB36A44998557CB3DC987FEAFD1F05E8B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...M.~b..... .....@.. .....$....@.....

File Icon

Icon Hash:	d9b7c5d1c5c9c1c3

Static PE Info

General

Entrypoint:	0x45c4ee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x627E2E4D [Fri May 13 10:09:17 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5c49c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5e000	0x9b42	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x68000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x5a4f4	0x5a600	False	0.519050397649	data	6.258266814	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x5e000	0x9b42	0x9c00	False	0.51519931891	data	6.01042834164	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x68000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AAKMS	0x5f9a4	0xd	ASCII text, with no line terminators	English	United States
ABDAA	0x5f9b4	0xd	ASCII text, with no line terminators	English	United States
AHDLM	0x5f9c4	0xd	ASCII text, with no line terminators	English	United States
AKOMH	0x5f9d4	0xd	ASCII text, with no line terminators	English	United States
AMMMI	0x5f9e4	0xd	ASCII text, with no line terminators	English	United States
ANEMF	0x5f9f4	0xd	ASCII text, with no line terminators	English	United States
ANKOM	0x5fa04	0xd	ASCII text, with no line terminators	English	United States

Name	RVA	Size	Type	Language	Country
ARIIL	0x5fa14	0xd	ASCII text, with no line terminators	English	United States
BKAMK	0x5fa24	0xd	ASCII text, with no line terminators	English	United States
BKDCA	0x5fa34	0xd	ASCII text, with no line terminators	English	United States
BNCDG	0x5fa44	0xd	ASCII text, with no line terminators	English	United States
CMDAB	0x5fa54	0xd	ASCII text, with no line terminators	English	United States
CMRRI	0x5fa64	0xd	ASCII text, with no line terminators	English	United States
CRKLI	0x5fa74	0xd	ASCII text, with no line terminators	English	United States
DCANJ	0x5fa84	0xd	ASCII text, with no line terminators	English	United States
DEBAM	0x5fa94	0xd	ASCII text, with no line terminators	English	United States
DIMDA	0x5faa4	0xd	ASCII text, with no line terminators	English	United States
DJFFF	0x5fab4	0xd	ASCII text, with no line terminators	English	United States
DMFMH	0x5fac4	0xd	ASCII text, with no line terminators	English	United States
DOPDK	0x5fad4	0xd	ASCII text, with no line terminators	English	United States
EFMDR	0x5fae4	0xd	ASCII text, with no line terminators	English	United States
ENBPG	0x5faf4	0xd	ASCII text, with no line terminators	English	United States
FDENR	0x5fb04	0xd	ASCII text, with no line terminators	English	United States
FDKIK	0x5fb14	0xd	ASCII text, with no line terminators	English	United States
FHDFS	0x5fb24	0xd	ASCII text, with no line terminators	English	United States
FNBFO	0x5fb34	0xd	ASCII text, with no line terminators	English	United States
FOJMK	0x5fb44	0xd	ASCII text, with no line terminators	English	United States
FRADI	0x5fb54	0xd	ASCII text, with no line terminators	English	United States
GAIPJ	0x5fb64	0xd	ASCII text, with no line terminators	English	United States
GFIPH	0x5fb74	0xd	ASCII text, with no line terminators	English	United States
GMFMI	0x5fb84	0xd	ASCII text, with no line terminators	English	United States
GPIFK	0x5fb94	0xd	ASCII text, with no line terminators	English	United States
HKDBJ	0x5fba4	0xd	ASCII text, with no line terminators	English	United States
HMMEG	0x5fbb4	0xd	ASCII text, with no line terminators	English	United States
HPDEG	0x5fbc4	0xd	ASCII text, with no line terminators	English	United States
HRHBL	0x5fbd4	0xd	ASCII text, with no line terminators	English	United States
ICIDF	0x5fbe4	0xd	ASCII text, with no line terminators	English	United States
IFDKF	0x5fbf4	0xd	ASCII text, with no line terminators	English	United States
IFFIF	0x5fc04	0xd	ASCII text, with no line terminators	English	United States
IGKNK	0x5fc14	0xd	ASCII text, with no line terminators	English	United States
IHIMM	0x5fc24	0xd	ASCII text, with no line terminators	English	United States
IKRAM	0x5fc34	0xd	ASCII text, with no line terminators	English	United States
IMDOO	0x5fc44	0xd	ASCII text, with no line terminators	English	United States
IMKJA	0x5fc54	0xd	ASCII text, with no line terminators	English	United States
JAALL	0x5fc64	0xd	ASCII text, with no line terminators	English	United States
JFNMK	0x5fc74	0xd	ASCII text, with no line terminators	English	United States
JGIRF	0x5fc84	0xd	ASCII text, with no line terminators	English	United States
KAEES	0x5fc94	0xd	ASCII text, with no line terminators	English	United States
KAMOL	0x5fca4	0xd	ASCII text, with no line terminators	English	United States
KDNOK	0x5fcb4	0xd	ASCII text, with no line terminators	English	United States
LOALC	0x5fcc4	0xd	ASCII text, with no line terminators	English	United States
LOJLG	0x5fcd4	0xd	ASCII text, with no line terminators	English	United States
LRMBH	0x5fce4	0xd	ASCII text, with no line terminators	English	United States
MFCMI	0x5fcf4	0xd	ASCII text, with no line terminators	English	United States
MGOSL	0x5fd04	0xd	ASCII text, with no line terminators	English	United States
MJPDD	0x5fd14	0xd	ASCII text, with no line terminators	English	United States
MODGK	0x5fd24	0xd	ASCII text, with no line terminators	English	United States
MPIDD	0x5fd34	0xd	ASCII text, with no line terminators	English	United States
NAMDL	0x5fd44	0xd	ASCII text, with no line terminators	English	United States
NKHOD	0x5fd54	0xd	ASCII text, with no line terminators	English	United States
OFCHM	0x5fd64	0xd	ASCII text, with no line terminators	English	United States
OKBKR	0x5fd74	0xd	ASCII text, with no line terminators	English	United States
OMCKE	0x5fd84	0xd	ASCII text, with no line terminators	English	United States
PAEML	0x5fd94	0xd	ASCII text, with no line terminators	English	United States
PGHBJ	0x5fda4	0xd	ASCII text, with no line terminators	English	United States
PKDKB	0x5fdb4	0xd	ASCII text, with no line terminators	English	United States

Name	RVA	Size	Type	Language	Country
PKMBI	0x5fdc4	0xd	ASCII text, with no line terminators	English	United States
RGKLE	0x5fdd4	0xd	ASCII text, with no line terminators	English	United States
SALMC	0x5fde4	0xd	ASCII text, with no line terminators	English	United States
SARND	0x5fdf4	0xd	ASCII text, with no line terminators	English	United States
SGBIH	0x5fe04	0xd	ASCII text, with no line terminators	English	United States
SPRMM	0x5fe14	0xd	ASCII text, with no line terminators	English	United States
RT_ICON	0x5fe24	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x6028c	0x988	data		
RT_ICON	0x60c14	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294769916, next used block 4294835709		
RT_ICON	0x61cbc	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0x64264	0x34ad	PNG image data, 256 x 256, 8-bit gray+alpha, non-interlaced		
RT_GROUP_ICON	0x67714	0x4c	data		
RT_VERSION	0x67760	0x1f8	data	English	United States
RT_MANIFEST	0x67958	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	
FileVersion	, , ,
CompanyName	
Comments	
ProductName	
ProductVersion	, , ,
FileDescription	
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

TCP Packets

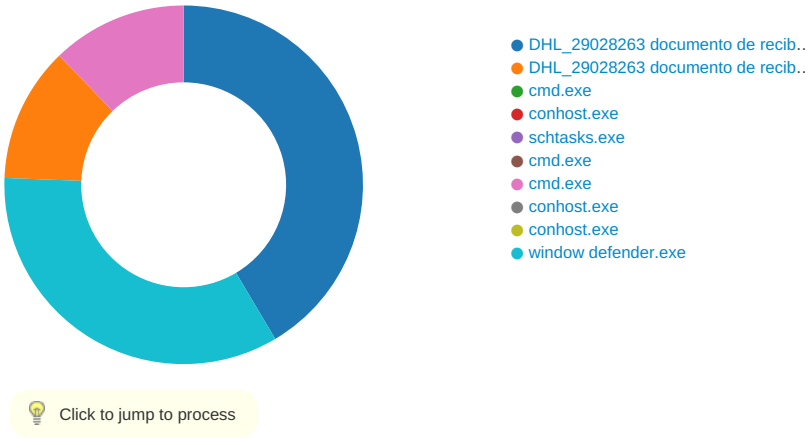
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:13:04.056092978 CEST	49755	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:04.082940102 CEST	1997	49755	37.0.14.197	192.168.2.7
May 14, 2022 15:13:04.670289993 CEST	49755	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:04.695924997 CEST	1997	49755	37.0.14.197	192.168.2.7
May 14, 2022 15:13:05.373480082 CEST	49755	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:05.399058104 CEST	1997	49755	37.0.14.197	192.168.2.7
May 14, 2022 15:13:10.406867981 CEST	49759	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:10.433067083 CEST	1997	49759	37.0.14.197	192.168.2.7
May 14, 2022 15:13:10.967681885 CEST	49759	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:10.993261099 CEST	1997	49759	37.0.14.197	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:13:11.670934916 CEST	49759	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:11.696858883 CEST	1997	49759	37.0.14.197	192.168.2.7
May 14, 2022 15:13:16.758996964 CEST	49764	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:16.784977913 CEST	1997	49764	37.0.14.197	192.168.2.7
May 14, 2022 15:13:17.374563932 CEST	49764	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:17.400126934 CEST	1997	49764	37.0.14.197	192.168.2.7
May 14, 2022 15:13:18.062067032 CEST	49764	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:18.087609053 CEST	1997	49764	37.0.14.197	192.168.2.7
May 14, 2022 15:13:23.221126080 CEST	49767	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:23.246988058 CEST	1997	49767	37.0.14.197	192.168.2.7
May 14, 2022 15:13:23.765683889 CEST	49767	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:23.791879892 CEST	1997	49767	37.0.14.197	192.168.2.7
May 14, 2022 15:13:24.468888044 CEST	49767	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:24.494963884 CEST	1997	49767	37.0.14.197	192.168.2.7
May 14, 2022 15:13:29.503086090 CEST	49772	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:29.529722929 CEST	1997	49772	37.0.14.197	192.168.2.7
May 14, 2022 15:13:30.156899929 CEST	49772	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:30.182760000 CEST	1997	49772	37.0.14.197	192.168.2.7
May 14, 2022 15:13:30.766243935 CEST	49772	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:30.792093992 CEST	1997	49772	37.0.14.197	192.168.2.7
May 14, 2022 15:13:35.801711082 CEST	49775	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:35.827675104 CEST	1997	49775	37.0.14.197	192.168.2.7
May 14, 2022 15:13:36.376149893 CEST	49775	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:36.401798010 CEST	1997	49775	37.0.14.197	192.168.2.7
May 14, 2022 15:13:37.063730955 CEST	49775	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:37.089828968 CEST	1997	49775	37.0.14.197	192.168.2.7
May 14, 2022 15:13:42.097322941 CEST	49776	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:42.123228073 CEST	1997	49776	37.0.14.197	192.168.2.7
May 14, 2022 15:13:42.673525095 CEST	49776	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:42.700122118 CEST	1997	49776	37.0.14.197	192.168.2.7
May 14, 2022 15:13:43.376730919 CEST	49776	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:43.403115034 CEST	1997	49776	37.0.14.197	192.168.2.7
May 14, 2022 15:13:48.413826942 CEST	49779	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:48.439472914 CEST	1997	49779	37.0.14.197	192.168.2.7
May 14, 2022 15:13:48.970900059 CEST	49779	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:48.996689081 CEST	1997	49779	37.0.14.197	192.168.2.7
May 14, 2022 15:13:49.658581972 CEST	49779	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:49.684767962 CEST	1997	49779	37.0.14.197	192.168.2.7
May 14, 2022 15:13:54.709506989 CEST	49786	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:54.735519886 CEST	1997	49786	37.0.14.197	192.168.2.7
May 14, 2022 15:13:55.268349886 CEST	49786	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:55.294430971 CEST	1997	49786	37.0.14.197	192.168.2.7
May 14, 2022 15:13:55.971503019 CEST	49786	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:13:55.997323990 CEST	1997	49786	37.0.14.197	192.168.2.7
May 14, 2022 15:14:01.001420021 CEST	49788	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:01.027152061 CEST	1997	49788	37.0.14.197	192.168.2.7
May 14, 2022 15:14:01.674514055 CEST	49788	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:01.700834036 CEST	1997	49788	37.0.14.197	192.168.2.7
May 14, 2022 15:14:02.274871111 CEST	49788	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:02.300708055 CEST	1997	49788	37.0.14.197	192.168.2.7
May 14, 2022 15:14:07.310281038 CEST	49791	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:07.336261988 CEST	1997	49791	37.0.14.197	192.168.2.7
May 14, 2022 15:14:07.875304937 CEST	49791	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:07.901042938 CEST	1997	49791	37.0.14.197	192.168.2.7
May 14, 2022 15:14:08.463462114 CEST	49791	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:08.489412069 CEST	1997	49791	37.0.14.197	192.168.2.7
May 14, 2022 15:14:14.789881945 CEST	49795	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:14.816304922 CEST	1997	49795	37.0.14.197	192.168.2.7
May 14, 2022 15:14:15.470901966 CEST	49795	1997	192.168.2.7	37.0.14.197

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:14:15.496644020 CEST	1997	49795	37.0.14.197	192.168.2.7
May 14, 2022 15:14:16.158397913 CEST	49795	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:16.183933973 CEST	1997	49795	37.0.14.197	192.168.2.7
May 14, 2022 15:14:21.192248106 CEST	49798	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:21.218460083 CEST	1997	49798	37.0.14.197	192.168.2.7
May 14, 2022 15:14:21.863154888 CEST	49798	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:21.888931036 CEST	1997	49798	37.0.14.197	192.168.2.7
May 14, 2022 15:14:22.472081900 CEST	49798	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:22.497839928 CEST	1997	49798	37.0.14.197	192.168.2.7
May 14, 2022 15:14:27.504615068 CEST	49801	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:27.530740976 CEST	1997	49801	37.0.14.197	192.168.2.7
May 14, 2022 15:14:28.081301928 CEST	49801	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:28.107630968 CEST	1997	49801	37.0.14.197	192.168.2.7
May 14, 2022 15:14:28.768841028 CEST	49801	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:28.794717073 CEST	1997	49801	37.0.14.197	192.168.2.7
May 14, 2022 15:14:34.069231987 CEST	49802	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:34.095155001 CEST	1997	49802	37.0.14.197	192.168.2.7
May 14, 2022 15:14:34.675590992 CEST	49802	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:34.701366901 CEST	1997	49802	37.0.14.197	192.168.2.7
May 14, 2022 15:14:35.363176107 CEST	49802	1997	192.168.2.7	37.0.14.197
May 14, 2022 15:14:35.388854980 CEST	1997	49802	37.0.14.197	192.168.2.7

Statistics

Behavior



System Behavior

Analysis Process: DHL_29028263 documento de recibo de la compra,pdf.exe PID: **7092**, Parent PID: **4680**

General

Target ID:	1
Start time:	15:12:22
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\DHL_29028263 documento de recibo de la compra,pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL_29028263 documento de recibo de la compra,pdf.exe"
Imagebase:	0x2e0000

File size:	411136 bytes
MD5 hash:	87A264AA9AEC9CE66F4B092363DD5ADC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000002.447136668.0000000003200000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000002.447136668.0000000003200000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.447136668.0000000003200000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000002.447136668.0000000003200000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000001.00000002.447222285.0000000004129000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000001.00000002.447222285.0000000004129000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.447222285.0000000004129000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000001.00000002.447222285.0000000004129000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: DHL_29028263 documento de recibo de la compra,pdf.exe PID: **6600**, Parent PID: **7092**

General

Target ID:	3
Start time:	15:12:51
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\DHL_29028263 documento de recibo de la compra,pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL_29028263 documento de recibo de la compra,pdf.exe
Imagebase:	0x2e0000
File size:	411136 bytes
MD5 hash:	87A264AA9AEC9CE66F4B092363DD5ADC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000000.417195755.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000000.417195755.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000003.00000000.416591236.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.416591236.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000000.416591236.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM, Description: Detects executables embedding command execution via IExecuteCommand COM object, Source: 00000003.00000000.416591236.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_WarzoneRAT, Description: Detects AveMaria/WarzoneRAT, Source: 00000003.00000000.416591236.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: AveMaria_WarZone, Description: unknown, Source: 00000003.00000000.416591236.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000000.416662895.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000000.416662895.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000003.00000000.417147497.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.417147497.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000000.417147497.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM, Description: Detects executables embedding command execution via IExecuteCommand COM object, Source: 00000003.00000000.417147497.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_WarzoneRAT, Description: Detects AveMaria/WarzoneRAT, Source: 00000003.00000000.417147497.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: AveMaria_WarZone, Description: unknown, Source: 00000003.00000000.417147497.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000003.431594632.00000000012CF000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth

- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000003.431594632.00000000012CF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.426962811.00000000012E1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.426962811.00000000012E1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.431623764.00000000012F4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.431623764.00000000012F4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000002.622879575.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000002.622879575.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.431671478.00000000012F4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.431671478.00000000012F4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000003.426948480.00000000012CF000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000003.426948480.00000000012CF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.431567861.00000000012F4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.431567861.00000000012F4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000000.418334237.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000000.418334237.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000003.00000000.418265932.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.418265932.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000000.418265932.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM, Description: Detects executables embedding command execution via IExecuteCommand COM object, Source: 00000003.00000000.418265932.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
- Rule: MALWARE_Win_WarzoneRAT, Description: Detects AveMaria/WarzoneRAT, Source: 00000003.00000000.418265932.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
- Rule: AveMaria_WarZone, Description: unknown, Source: 00000003.00000000.418265932.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000003.00000002.622706566.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.622706566.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000002.622706566.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM, Description: Detects executables embedding command execution via IExecuteCommand COM object, Source: 00000003.00000002.622706566.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
- Rule: MALWARE_Win_WarzoneRAT, Description: Detects AveMaria/WarzoneRAT, Source: 00000003.00000002.622706566.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
- Rule: AveMaria_WarZone, Description: unknown, Source: 00000003.00000002.622706566.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000003.00000000.417884328.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000003.00000000.417884328.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000003.00000000.415418870.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.415418870.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000000.415418870.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM, Description: Detects executables embedding command execution via IExecuteCommand COM object, Source: 00000003.00000000.415418870.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
- Rule: MALWARE_Win_WarzoneRAT, Description: Detects AveMaria/WarzoneRAT, Source: 00000003.00000000.415418870.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
- Rule: AveMaria_WarZone, Description: unknown, Source: 00000003.00000000.415418870.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.426786774.00000000012FA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.426786774.00000000012FA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000003.00000000.415889492.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.415889492.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000000.415889492.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM, Description: Detects executables embedding command execution via IExecuteCommand COM object, Source: 00000003.00000000.415889492.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
- Rule: MALWARE_Win_WarzoneRAT, Description: Detects AveMaria/WarzoneRAT, Source: 00000003.00000000.415889492.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen
- Rule: AveMaria_WarZone, Description: unknown, Source: 00000003.00000000.415889492.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

	• Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000003.00000000.417779464.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000000.417779464.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000000.417779464.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM, Description: Detects executables embedding command execution via IExecuteCommand COM object, Source: 00000003.00000000.417779464.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_WarzoneRAT, Description: Detects AveMaria/WarzoneRAT, Source: 00000003.00000000.417779464.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: AveMaria_WarZone, Description: unknown, Source: 00000003.00000000.417779464.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.431652682.00000000012FA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.431652682.00000000012FA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000003.424810982.00000000012E1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000003.00000003.424810982.00000000012E1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft Vision\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4135ED	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DHL_29028263 documento de recibo de la compra,pdf.exe	unknown	411136	success or wait	1	411E78	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SU8M1R6EKH	success or wait	1	410F94	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPer1_0Server	dword	10	success or wait	1	413550	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPerServer	dword	10	success or wait	1	413565	RegSetValueExA

Analysis Process: cmd.exe PID: **2208**, Parent PID: **7092**

General

Target ID:	6
Start time:	15:12:54
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Roaming\window defender\window defender.exe'" /f
Imagebase:	0xdd0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4468, Parent PID: 2208

General

Target ID:	7
Start time:	15:12:55
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
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: schtasks.exe PID: 4992, Parent PID: 2208

General

Target ID:	8
Start time:	15:12:56
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Roaming\window defender\window defender.exe'" /f
Imagebase:	0x7ff7e8070000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6632, Parent PID: 6600

General

Target ID:	9
Start time:	15:13:00
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0xdd0000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6716**, Parent PID: **7092**

General

Target ID:	10
Start time:	15:13:00
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe" /C copy "C:\Users\user\Desktop\DHL_29028263 documento de recibo de la compra,pdf.exe" "C:\Users\user\AppData\Roaming\window defender\window defender.exe
Imagebase:	0xdd0000
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\window defender\window defender.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	DD4E97	CopyFileExW
C:\Users\user\AppData\Roaming\window defender\window defender.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	DD4E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\window defender\window defender.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 4d 2e 7e 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 fd 05 00 00 fd 00 00 00 00 00 00 fd fd 05 00 00 20 00 00 00 fd 05 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 06 00 00 02 00 00 fd 24 07 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELM.~b @ $@	success or wait	4	DD4E97	CopyFileExW
C:\Users\user\AppData\Roaming\window defender\window defender.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	DD4E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DHL_29028263 documento de recibo de la compra,pdf.exe	unknown	512	success or wait	1	DD5742	ReadFile

Analysis Process: conhost.exe PID: **6892**, Parent PID: **6632**

General

Target ID:	12
Start time:	15:13:01
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
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: **7084**, Parent PID: **6716**

General

Target ID:	13
Start time:	15:13:02
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff7bab80000
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: window defender.exe PID: **3668**, Parent PID: **1108**

General

Target ID:	16
Start time:	15:14:00
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\window defender\window defender.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\window defender\window defender.exe
Imagebase:	0xe90000
File size:	411136 bytes
MD5 hash:	87A264AA9AEC9CE66F4B092363DD5ADC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 51%, ReversingLabs

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF6CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF6CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF45705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DEA03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF4CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DEA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DEA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DEA03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DEA03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF45705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68FB1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68FB1B4F	ReadFile

Disassembly

No disassembly