ID: 358255
Sample Name: Recibo de entrega de DHL.exe
Cookbook: default.jbs
Time: 11:00:21
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

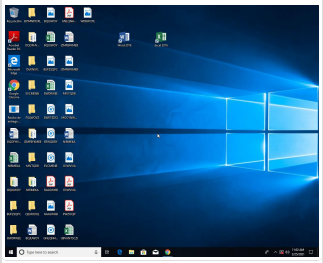
Analysis Report Recibo de entrega de DHL.exe

Overview

General Information

Sample Name:	Recibo de entrega de DHL.exe
Analysis ID:	358255
MD5:	335a69ee25155d..
SHA1:	cbecea1d93ff376..
SHA256:	66dd2c7ac2b0bc...
Tags:	DHL ESP exe geo
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

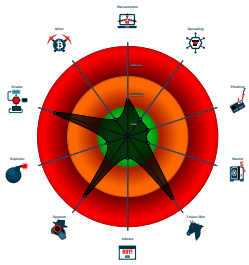
404Keylogger
AgentTesla

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

Signatures

- Found malware configuration
- Malicious sample detected (through ...
- Multi AV Scanner detection for subm...
- Yara detected 404Keylogger
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg...
- .NET source code references suspic...
- Binary contains a suspicious time st...
- Injects a PE file into a foreign proce...
- Installs a global keyboard hook
- Machine Learning detection for samp...
- May check the online IP address of ...
- Tries to detect sandboxes and other...

Classification



Startup

- **System is w10x64**
- Recibo de entrega de DHL.exe (PID: 7008 cmdline: 'C:\Users\user\Desktop\Recibo de entrega de DHL.exe' MD5: 335A69EE25155D53F6DF46C020AA90CD)
  - Recibo de entrega de DHL.exe (PID: 6416 cmdline: C:\Users\user\Desktop\Recibo de entrega de DHL.exe MD5: 335A69EE25155D53F6DF46C020AA90CD)
  - Recibo de entrega de DHL.exe (PID: 2912 cmdline: C:\Users\user\Desktop\Recibo de entrega de DHL.exe MD5: 335A69EE25155D53F6DF46C020AA90CD)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "",
  "URL: ": "",
  "To: ": "moin.ansari@sapgroup.com.pk",
  "ByHost: ": "mail.sapgroup.com.pk:587",
  "Password: ": "",
  "From: ": "moin.ansari@sapgroup.com.pk"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.906857662.0000000002E6E000.00000004.00000001.sdmp	JoeSecurity_404Keylogger	Yara detected 404Keylogger	Joe Security	
00000000.00000002.660324549.0000000003CD1000.00000004.00000001.sdmp	JoeSecurity_404Keylogger	Yara detected 404Keylogger	Joe Security	
00000000.00000002.660324549.0000000003CD1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.905487437.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_404Keylogger	Yara detected 404Keylogger	Joe Security	
00000005.00000002.905487437.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Click to see the 7 entries				

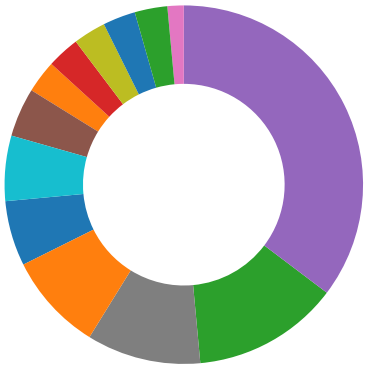
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Recibo de entrega de DHL.exe.3ea8390.3.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x17588:$a2: \Comodo\Dragon\User Data\Default\Logi n Data • 0x1693a:$a3: \Google\Chrome\User Data\Default\Login Data • 0x16db0:$a4: \Orbitum\User Data\Default\Login Data
0.2.Recibo de entrega de DHL.exe.3ea8390.3.unpack	JoeSecurity_404Keylogger	Yara detected 404Keylogger	Joe Security	
0.2.Recibo de entrega de DHL.exe.3ea8390.3.unpack	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
5.2.Recibo de entrega de DHL.exe.400000.0.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x19388:$a2: \Comodo\Dragon\User Data\Default\Logi n Data • 0x1873a:$a3: \Google\Chrome\User Data\Default\Login Data • 0x18bb0:$a4: \Orbitum\User Data\Default\Login Data
5.2.Recibo de entrega de DHL.exe.400000.0.unpack	JoeSecurity_404Keylogger	Yara detected 404Keylogger	Joe Security	
Click to see the 10 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected 404Keylogger

Installs a global keyboard hook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation:

Binary contains a suspicious time stamp

Malware Analysis System Evasion:

Yara detected AntiVM_3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected 404Keylogger

Yara detected AgentTesla

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

Yara detected 404Keylogger

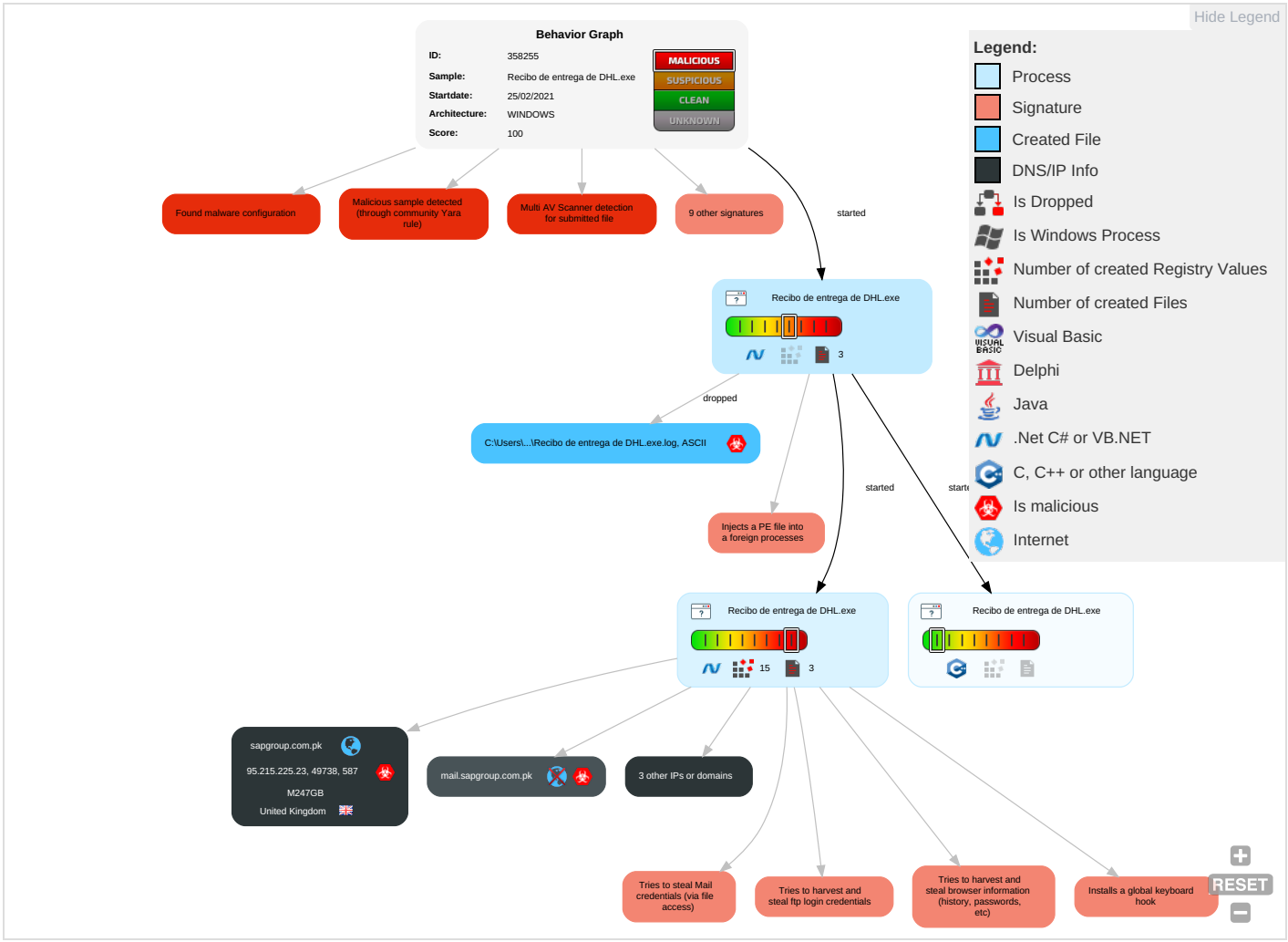
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	Input Capture 1 1	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/SI

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Ingress Tool Transfer 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 2	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2 1	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoco

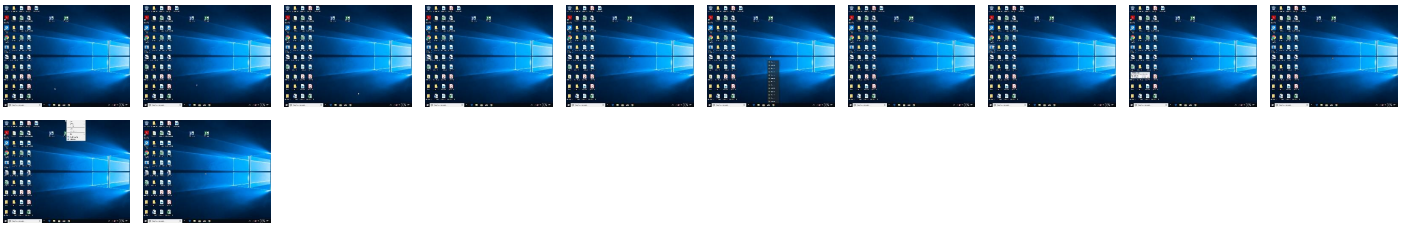
Behavior Graph



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
Recibo de entrega de DHL.exe	31%	Virustotal		Browse
Recibo de entrega de DHL.exe	13%	ReversingLabs	Win32.Trojan.AgentTesla	
Recibo de entrega de DHL.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.Recibo de entrega de DHL.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
sapgroup.com.pk	0%	Virustotal		Browse
checkip.dyndns.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/nl-nj	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/A	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnT	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/1	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org41k	0%	Avira URL Cloud	safe	
http://mail.sapgroup.com.pk	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-cz	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-cz	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-cz	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://https://myip.dnsomatic.com9====	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/1	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/1	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/1	0%	URL Reputation	safe	
http://checkip.dyndns.org/q	0%	Avira URL Cloud	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/N	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/xt	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://checkip.dyndns.com	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://tempuri.org/NorthWindAzureForInsertsDataSet.xsd	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/S	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/N	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/E	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/A	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://sapgroup.com.pk	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/w	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0-	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/es-e	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sapgroup.com.pk	95.215.225.23	true	true	• 0%, Virustotal, Browse	unknown
checkip.dyndns.com	131.186.113.70	true	false	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true		unknown
mail.sapgroup.com.pk	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

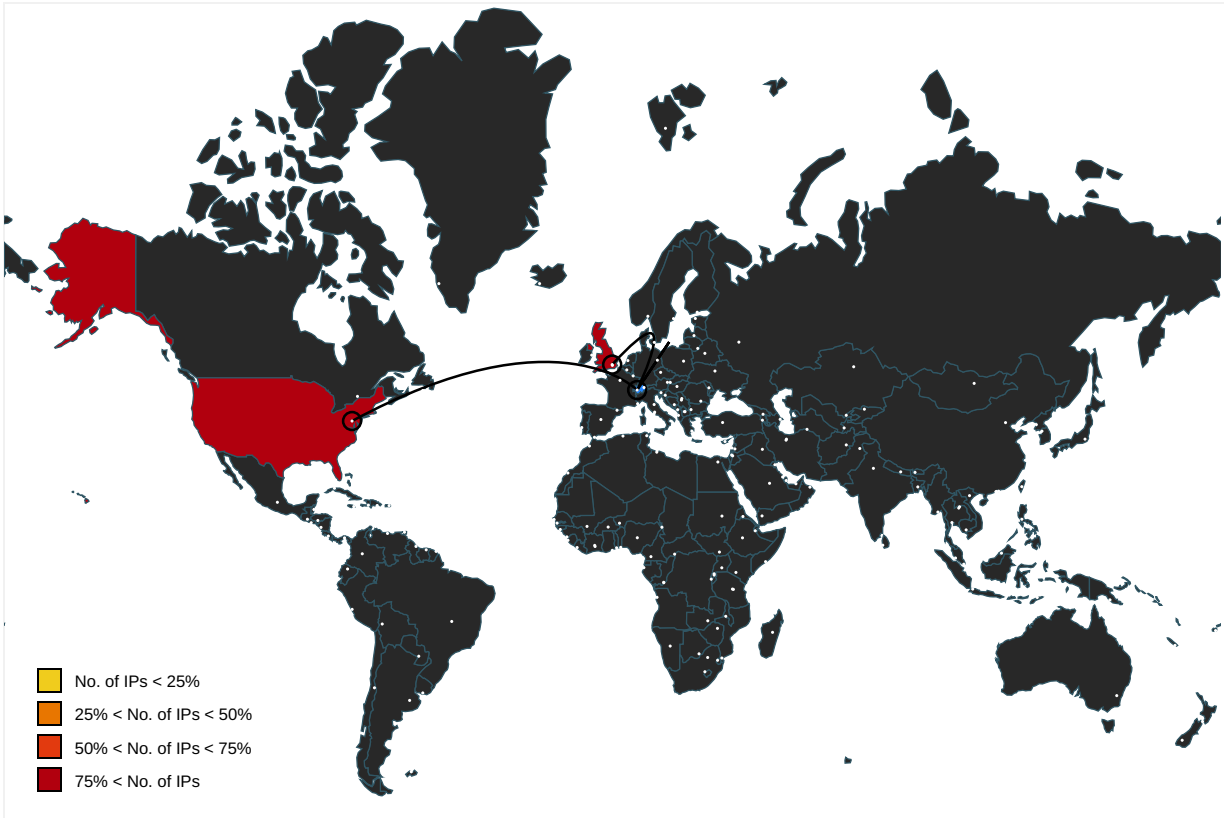
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/nl-nj	Recibo de entrega de DHL.exe, 00000000.00000003.643648865.00000000006108000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/A	Recibo de entrega de DHL.exe, 00000000.00000003.643648865.00000000006108000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot	Recibo de entrega de DHL.exe, 00000000.00000002.660324549.00000003CD1000.00000004.00000001.sdmp, Recibo de entrega de DHL.exe, 00000005.00000002.905487437.0000000000402000.00000040.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnT	Recibo de entrega de DHL.exe, 00000000.00000003.641863100.0000000610E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/1	Recibo de entrega de DHL.exe, 00000000.00000003.643648865.00000000006108000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.org41k	Recibo de entrega de DHL.exe, 00000005.00000002.906659544.00000002DCC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false		high
http://mail.sapgroup.com.pk	Recibo de entrega de DHL.exe, 00000005.00000002.906857662.00000002E6E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	Recibo de entrega de DHL.exe, 00000000.00000003.643521981.0000000610C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Recibo de entrega de DHL.exe, 00000000.00000002.660068235.00000002CD1000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/-cz	Recibo de entrega de DHL.exe, 00000000.00000003.643521981.0000000610C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://myip.dnsomatic.com9====	Recibo de entrega de DHL.exe, 00000000.00000002.660324549.000000003CD1000.00000004.00000001.sdmp, Recibo de entrega de DHL.exe, 00000005.00000002.905487437.0000000000402000.00000040.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cn/cThe	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/1	Recibo de entrega de DHL.exe, 00000000.00000003.643521981.0000000610C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://checkip.dyndns.org/q	Recibo de entrega de DHL.exe, 00000000.00000002.660324549.000000003CD1000.00000004.00000001.sdmp, Recibo de entrega de DHL.exe, 00000005.00000002.905487437.0000000000402000.00000040.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comn	Recibo de entrega de DHL.exe, 00000000.00000003.640696140.0000000611B000.00000004.00000001.sdmp, Recibo de entrega de DHL.exe, 00000000.00000003.640811691.000000000611B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/N	Recibo de entrega de DHL.exe, 00000000.00000003.643648865.000000006108000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.000000007312000.00000004.00000001.sdmp, Recibo de entrega de DHL.exe, 00000000.00000003.640725684.000000000611B000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/xt	Recibo de entrega de DHL.exe, 00000000.00000003.643648865.000000006108000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.com	Recibo de entrega de DHL.exe, 00000005.00000002.906675983.00000002DDD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Recibo de entrega de DHL.exe, 00000000.00000002.660068235.00000002CD1000.00000004.00000001.sdmp, Recibo de entrega de DHL.exe, 00000005.00000002.906616096.0000000002D71000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/NorthWindAzureForInsertsDataSet.xsd	Recibo de entrega de DHL.exe	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Recibo de entrega de DHL.exe, 00000000.00000003.642797524.00000000006118000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false		high
http://https://sectigo.com/CPS0	Recibo de entrega de DHL.exe, 00000005.00000002.906857662.00000000002E6E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/S	Recibo de entrega de DHL.exe, 00000000.00000003.643821183.0000000000610A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/N	Recibo de entrega de DHL.exe, 00000000.00000003.643616679.0000000000610C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://pastebin.com/api/api_post.php	Recibo de entrega de DHL.exe, 00000000.00000002.660324549.00000003CD1000.00000004.00000001.sdmp, Recibo de entrega de DHL.exe, 00000005.00000002.905487437.0000000000402000.00000040.00000001.sdmp	false		high
http://checkip.dyndns.org	Recibo de entrega de DHL.exe, 00000005.00000002.906659544.00000002DCC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/E	Recibo de entrega de DHL.exe, 00000000.00000003.643648865.00000006108000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/A	Recibo de entrega de DHL.exe, 00000000.00000003.643521981.0000000000610C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Recibo de entrega de DHL.exe, 00000000.00000003.643521981.0000000000610C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.come.com	Recibo de entrega de DHL.exe, 00000000.00000002.662987849.0000000000610A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false		high
http://sapgroup.com.pk	Recibo de entrega de DHL.exe, 00000005.00000002.906857662.00000000002E6E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/w	Recibo de entrega de DHL.exe, 00000000.00000003.643521981.0000000000610C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	Recibo de entrega de DHL.exe, 00000000.00000003.641863100.0000000000610E000.00000004.00000001.sdmp, Recibo de entrega de DHL.exe, 00000000.00000002.665864843.0000000007312000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000000007312000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pastebin.com/api/api_login.php	Recibo de entrega de DHL.exe, 00000000.00000002.660324549.00000003CD1000.00000004.00000001.sdmp, Recibo de entrega de DHL.exe, 00000005.00000002.905487437.0000000000402000.00000040.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Recibo de entrega de DHL.exe, 00000000.00000003.643521981.0000000610C000.00000004.00000001.sdmp, Recibo de entrega de DHL.exe, 00000000.00000003.643648865.0000000006108000.00000004.00000001.sdmp, Recibo de entrega de DHL.exe, 00000000.00000003.643821183.000000000610A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0-	Recibo de entrega de DHL.exe, 00000000.00000003.643648865.00000006108000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.como	Recibo de entrega de DHL.exe, 00000000.00000002.662987849.0000000610A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/es-e	Recibo de entrega de DHL.exe, 00000000.00000003.643521981.0000000610C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	Recibo de entrega de DHL.exe, 00000000.00000002.665864843.00000007312000.00000004.00000001.sdmp	false		high
http://https://pastebin.com/api/api_login.phpJhttps://pastebin.com/api/api_post.php	Recibo de entrega de DHL.exe, 00000000.00000002.660324549.00000003CD1000.00000004.00000001.sdmp, Recibo de entrega de DHL.exe, 00000005.00000002.905487437.0000000000402000.00000040.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
131.186.113.70	unknown	United States		33517	DYNDNSUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.215.225.23	unknown	United Kingdom		9009	M247GB	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358255
Start date:	25.02.2021
Start time:	11:00:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Recibo de entrega de DHL.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.troj.spyw.evad.winEXE@5/2@4/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.1%) • Quality average: 14% • Quality standard deviation: 25.1%
HCA Information:	• Successful, ratio: 100% • 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 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.113.196.254, 51.104.139.180, 13.107.3.254, 13.107.246.254, 13.64.90.137, 13.88.21.125, 92.122.145.220, 52.155.217.156, 20.54.26.129, 2.20.142.210, 2.20.142.209, 104.43.139.144, 52.255.188.83, 92.122.213.247, 92.122.213.194, 104.42.151.234 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, s-ring.msedge.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, teams-9999.teams-msedge.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus16.cloudapp.net, s-ring.s-9999.s-msedge.net, t-ring.msedge.net, ris.api.iris.microsoft.com, t-9999.t-msedge.net, skypedataprdcoleus17.cloudapp.net, s-9999.s-msedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, teams-ring.teams-9999.teams-msedge.net, teams-ring.msedge.net, t-ring.t-9999.t-msedge.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:01:11	API Interceptor	27x Sleep call for process: Recibo de entrega de DHL.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
131.186.113.70	proposal-Copy.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	0020210089.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	SAL-0908889000.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	URGENT RFQ 45253.exe	Get hash	malicious	Browse	• checkip.dyndns.org/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipping Documents and Conditions Certificate.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PAYMENT MT103-SWIFT.PDF.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PRODUCT ENQUIRY (21001025) PART NO EPN518.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	IMG_0352_Scanned.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	purchase order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Message Body Content.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Consignment Invoice PL&BL Draft.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PO202100046.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	P00760000.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	Order.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	purchase order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• checkip.dyndns.org/
	Purchase Order.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	dot crypted.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	v2.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• checkip.dyndns.org/
95.215.225.23	Purchase Order N#U00c2#U00b0 EQ 0010-0121.exe	Get hash	malicious	Browse	
	http://bazaarkonections.com/admin/li.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.453.28860.exe	Get hash	malicious	Browse	
	Order83941.xlsx	Get hash	malicious	Browse	
	DHL Shipment Notification Document 9671450633.exe	Get hash	malicious	Browse	
	PO_3409_129.exe	Get hash	malicious	Browse	
	DHL Delivery Reciept.exe	Get hash	malicious	Browse	
	PO no.0107-320804-1.exe	Get hash	malicious	Browse	
	Bank Transfer Form -pdf- .exe	Get hash	malicious	Browse	
	OC 07082020 DOC.exe	Get hash	malicious	Browse	
	Purchase Order RCM No. 0445-20.exe	Get hash	malicious	Browse	
	HI2003-02.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
checkip.dyndns.com	Payment.exe	Get hash	malicious	Browse	• 216.146.43.71
	proposal-Copy.exe	Get hash	malicious	Browse	• 131.186.113.70
	RFQ CSDOK202040890.exe	Get hash	malicious	Browse	• 131.186.161.70
	0020210089.exe	Get hash	malicious	Browse	• 131.186.113.70
	SAL-0908889000.exe	Get hash	malicious	Browse	• 162.88.193.70
	SWIFT 500395Y.exe	Get hash	malicious	Browse	• 131.186.161.70
	Message Body.exe	Get hash	malicious	Browse	• 216.146.43.71
	PaymentSwift.exe	Get hash	malicious	Browse	• 216.146.43.70
	Halkbank_Ekstre_20210224_082357_541079.exe	Get hash	malicious	Browse	• 216.146.43.70
	ditcrypted.exe	Get hash	malicious	Browse	• 162.88.193.70
	Original Invoice PL&BL Draft.exe	Get hash	malicious	Browse	• 216.146.43.71
	PAYMENT MT103-SWIFT.jar	Get hash	malicious	Browse	• 216.146.43.71
	SWIFT 500395H.exe	Get hash	malicious	Browse	• 131.186.161.70
	Groupo Dani Order_pdf.exe	Get hash	malicious	Browse	• 216.146.43.71
	PO98000000090.jar	Get hash	malicious	Browse	• 131.186.161.70
	Telex Transfer.exe	Get hash	malicious	Browse	• 162.88.193.70
	New_ Order.exe	Get hash	malicious	Browse	• 162.88.193.70
	URGENT RFQ 45253.exe	Get hash	malicious	Browse	• 131.186.113.70
	SOA JAN 2021.exe	Get hash	malicious	Browse	• 216.146.43.71
	HUIBAO PROFORMA INVOICE 07092021.jar	Get hash	malicious	Browse	• 216.146.43.71

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DYNDNSUS	Payment.exe	Get hash	malicious	Browse	• 216.146.43.71
	proposal-Copy.exe	Get hash	malicious	Browse	• 131.186.113.70
	RFQ CSDOK202040890.exe	Get hash	malicious	Browse	• 131.186.161.70
	0020210089.exe	Get hash	malicious	Browse	• 131.186.113.70
	SAL-0908889000.exe	Get hash	malicious	Browse	• 162.88.193.70
	SWIFT 500395Y.exe	Get hash	malicious	Browse	• 131.186.161.70
	Message Body.exe	Get hash	malicious	Browse	• 216.146.43.71
	PaymentSwift.exe	Get hash	malicious	Browse	• 216.146.43.70
	Halkbank_Ekstre_20210224_082357_541079.exe	Get hash	malicious	Browse	• 216.146.43.70
	ditcrypted.exe	Get hash	malicious	Browse	• 162.88.193.70
	Original Invoice PL&BL Draft.exe	Get hash	malicious	Browse	• 216.146.43.71
	PAYMENT MT103-SWIFT.jar	Get hash	malicious	Browse	• 216.146.43.71
	SWIFT 500395H.exe	Get hash	malicious	Browse	• 131.186.161.70
	Groupo Dani Order_pdf.exe	Get hash	malicious	Browse	• 216.146.43.71
	PO98000000090.jar	Get hash	malicious	Browse	• 131.186.161.70
	Telex Transfer.exe	Get hash	malicious	Browse	• 162.88.193.70
	New_ Order.exe	Get hash	malicious	Browse	• 162.88.193.70
	URGENT RFQ 45253.exe	Get hash	malicious	Browse	• 131.186.113.70
	SOA JAN 2021.exe	Get hash	malicious	Browse	• 216.146.43.71
	HUIBAO PROFORMA INVOICE 07092021.jar	Get hash	malicious	Browse	• 216.146.43.71
M247GB	document-1021586454.xls	Get hash	malicious	Browse	• 37.10.71.186
	document-1021586454.xls	Get hash	malicious	Browse	• 37.10.71.186
	VKH2kBDk59.exe	Get hash	malicious	Browse	• 185.158.25 0.134
	XP 6.xlsx	Get hash	malicious	Browse	• 46.243.248.149
	Attached file.exe	Get hash	malicious	Browse	• 185.206.225.51
	file.html	Get hash	malicious	Browse	• 185.189.11 2.202
	file.html	Get hash	malicious	Browse	• 185.189.11 2.202
	4hW0TZqN01.exe	Get hash	malicious	Browse	• 172.94.120.39
	LdOgPDsMEf.exe	Get hash	malicious	Browse	• 46.243.248.168
	mawlare.exe	Get hash	malicious	Browse	• 37.120.145.208
	mawlare.exe	Get hash	malicious	Browse	• 37.120.145.208
	ORDER FRD91PM7.xlsx	Get hash	malicious	Browse	• 38.132.109.186
	ORDER FRD91PM7.xlsx	Get hash	malicious	Browse	• 38.132.109.186
	QgWarCS5Z4.exe	Get hash	malicious	Browse	• 192.71.227.60
	0zwHgf4MZ6.exe	Get hash	malicious	Browse	• 192.71.227.60
	WlgBUuBdZm.exe	Get hash	malicious	Browse	• 192.71.227.60
	7gRAlM4oGO.exe	Get hash	malicious	Browse	• 192.71.227.60
	u67dk4vpoS.exe	Get hash	malicious	Browse	• 172.94.120.13
	EeA8OHCoXT.exe	Get hash	malicious	Browse	• 188.72.85.37
	cCkuGVM3Sk.exe	Get hash	malicious	Browse	• 188.72.85.37

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Recibo de entrega de DHL.exe.log

Process:	C:\Users\user\Desktop\Recibo de entrega de DHL.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	5.336334182031907

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Recibo de entrega de DHL.exe.log	
Encrypted:	false
SSDEEP:	48:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHsAmHK2HKSHKKHKs:lrq5qXEwCYqhQnoPtlxHeqzNM/q2qSqY
MD5:	B9E8D9BC061D6715808BB3A28CECBA2B
SHA1:	6F18CD63C12AEC962D089F215658FD5BE1789BC3
SHA-256:	716E082F23E093EBCA2C8F994745CC7D62457D7359BBE555B75E275CE8EEEDC7
SHA-512:	6D97D3E34CBCC5C0CCF845E285F98DE1824A825AB1D306D20ED164B0B74270CED9AB694E40831EC796E9F823BB4E369166006E555D7BBD000A33A0FDA601F86
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

C:\Users\user\Documents\Results.txt	
Process:	C:\Users\user\Desktop\Recibo de entrega de DHL.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	288
Entropy (8bit):	4.198812223020965
Encrypted:	false
SSDEEP:	6:KkiStv82FZ6vayIuboluzj1hviX/++L8P:KkD82FcvabuMczxV0ZL8P
MD5:	70ADC435E0D206FE7953E8045B4F01B2
SHA1:	836F13823BB9B17CFBBD5D475E45312DBAB0B2F1
SHA-256:	B89EB51318C18F9AC5253D3AEE6DB79F0520F835CAC3F96D8513D6F59D5EDE5C
SHA-512:	5910E939DD0D9F9F301DC352262453AD48120D3EA3AC8F33123542834CA32741FF55B55465282B73C9D7FAE2BD53762CFDCC02ADCF52E89867443AAF4323EFB
Malicious:	false
Reputation:	low
Preview:	|------ Results - Passwords ------|..------- + INFO + -------....IP: 84.17.52.78....Owner Name: 216041..OS Name: Microsoft Windows 10 Pro..OS Version: 6.2.9200.0..OS PlatForm: Win32NT..RAM Size: 8.00 GB..----------..........----------

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.498081225430686
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • 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% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Recibo de entrega de DHL.exe
File size:	375296
MD5:	335a69ee25155d53f6df46c020aa90cd
SHA1:	cbecea1d93ff376b6a7f5ea72c191d4020372344
SHA256:	66dd2c7ac2b0bc7b604efa99f21a828da26c15a366a2e809e23b82dda44b63dd
SHA512:	5169363ca9bbfbec00e718891976b84ff488065dcc59466517b97e241afba882e5ab0afbfa4c20ba6186feafe2f8af6175aa10c194fb5124b59155db11751d3a
SSDEEP:	6144:5lAsmm9PRXvDUtDCpewbzTwrp41W386OvsDfYt7Yt6AECul1CRtA3l/mqV7Uw86w:5l1VvAOYwbY4ksDWY2t2lf3l/mqVc6eF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x45ceb2
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:	0xA3A09597 [Thu Dec 28 06:24:23 2056 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
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
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	0x5ce60	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5e000	0x5ac	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x60000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x5ce44	0x1c	.text
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	0x5aeb8	0x5b000	False	0.784244076236	data	7.51567311339	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x5e000	0x5ac	0x600	False	0.427083333333	data	4.12323823165	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x60000	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
RT_VERSION	0x5e090	0x31c	data		
RT_MANIFEST	0x5e3bc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

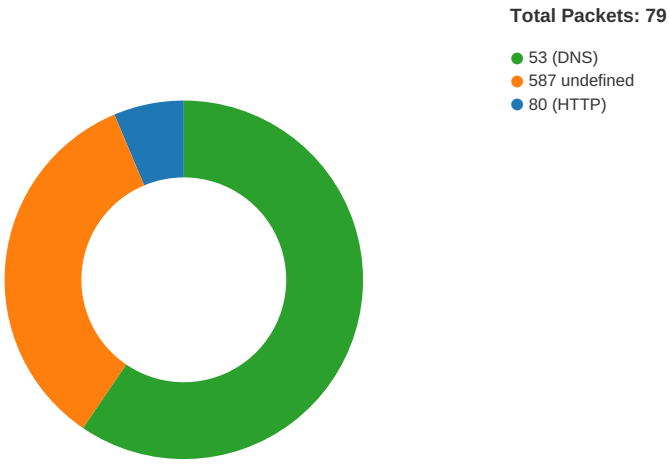
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020 - 2021
Assembly Version	6.4.0.2
InternalName	c.exe
FileVersion	6.4.0.2
CompanyName	
LegalTrademarks	
Comments	
ProductName	Table Adapter
ProductVersion	6.4.0.2
FileDescription	Table Adapter
OriginalFilename	c.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:01:16.038970947 CET	49733	80	192.168.2.4	131.186.113.70
Feb 25, 2021 11:01:16.099210978 CET	80	49733	131.186.113.70	192.168.2.4
Feb 25, 2021 11:01:16.099385023 CET	49733	80	192.168.2.4	131.186.113.70
Feb 25, 2021 11:01:16.100343943 CET	49733	80	192.168.2.4	131.186.113.70
Feb 25, 2021 11:01:16.160640001 CET	80	49733	131.186.113.70	192.168.2.4
Feb 25, 2021 11:01:16.161358118 CET	80	49733	131.186.113.70	192.168.2.4
Feb 25, 2021 11:01:16.161370993 CET	80	49733	131.186.113.70	192.168.2.4
Feb 25, 2021 11:01:16.161622047 CET	49733	80	192.168.2.4	131.186.113.70
Feb 25, 2021 11:01:16.162894011 CET	49733	80	192.168.2.4	131.186.113.70
Feb 25, 2021 11:01:16.223095894 CET	80	49733	131.186.113.70	192.168.2.4
Feb 25, 2021 11:01:27.077466011 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:27.135459900 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:27.135607958 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:28.086750984 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.087178946 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:28.145792961 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.146311045 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:28.209126949 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.255218029 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:28.266223907 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:28.339159966 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.339201927 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.339221954 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.339235067 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.339402914 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:28.343007088 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.395538092 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:28.453963041 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.505286932 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:28.692831039 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:28.750773907 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.774352074 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:28.832658052 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.833832026 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:28.912627935 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.913449049 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:28.972265005 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:28.973018885 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:29.053078890 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:29.053668022 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:29.114078999 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:29.116148949 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:29.116372108 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:29.116487026 CET	49738	587	192.168.2.4	95.215.225.23

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:01:29.116584063 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:29.116826057 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:29.116910934 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:29.116976976 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:29.117052078 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:01:29.174374104 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:29.174437046 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:29.175268888 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:29.175314903 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:29.175347090 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:29.175359011 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:29.175373077 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:29.175384045 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:29.177833080 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:01:29.224147081 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:03:06.436250925 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:03:06.495474100 CET	587	49738	95.215.225.23	192.168.2.4
Feb 25, 2021 11:03:06.495695114 CET	49738	587	192.168.2.4	95.215.225.23
Feb 25, 2021 11:03:06.610343933 CET	49738	587	192.168.2.4	95.215.225.23

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:00:57.786119938 CET	65248	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:00:57.834882975 CET	53	65248	8.8.8.8	192.168.2.4
Feb 25, 2021 11:00:57.862214088 CET	53723	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:00:57.911875010 CET	53	53723	8.8.8.8	192.168.2.4
Feb 25, 2021 11:00:58.114581108 CET	64646	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:00:58.163386106 CET	53	64646	8.8.8.8	192.168.2.4
Feb 25, 2021 11:00:58.343087912 CET	65298	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:00:58.392647028 CET	53	65298	8.8.8.8	192.168.2.4
Feb 25, 2021 11:00:58.456630945 CET	59123	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:00:58.508207083 CET	53	59123	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:00.365006924 CET	54531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:00.425132036 CET	53	54531	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:00.852611065 CET	49714	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:00.911444902 CET	53	49714	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:01.691351891 CET	58028	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:01.740298033 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:03.453221083 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:03.502044916 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:04.835719109 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:04.884881020 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:06.250749111 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:06.310662031 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:07.639112949 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:07.690696001 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:08.828963995 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:08.880951881 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:12.284008026 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:12.333422899 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:13.464890957 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:13.516590118 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:15.877588987 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:15.926315069 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:15.945533037 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:16.001646996 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:16.659176111 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:16.707952976 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:18.119863987 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:18.168627977 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:20.756002903 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:20.804708004 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:22.978992939 CET	56627	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:01:23.027931929 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:26.425578117 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:26.573837996 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:26.868973970 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:27.075436115 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:32.071819067 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:32.120655060 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:47.278043985 CET	64801	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:47.348462105 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:47.897427082 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:47.971132040 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:48.510493994 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:48.511616945 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:48.568732977 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:48.578937054 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:49.014527082 CET	52337	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:49.071497917 CET	53	52337	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:49.603048086 CET	55046	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:49.686888933 CET	53	55046	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:50.278206110 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:50.335593939 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:50.919239044 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:50.976711035 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:51.756167889 CET	50601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:51.816200972 CET	53	50601	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:52.792056084 CET	60875	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:52.850532055 CET	53	60875	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:52.907953024 CET	56448	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:52.965240955 CET	53	56448	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:53.143224955 CET	59172	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:53.192209959 CET	53	59172	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:53.437369108 CET	62420	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:53.497195959 CET	53	62420	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:56.012857914 CET	60579	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:56.061723948 CET	53	60579	8.8.8.8	192.168.2.4
Feb 25, 2021 11:01:57.801331043 CET	50183	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:01:57.850121975 CET	53	50183	8.8.8.8	192.168.2.4
Feb 25, 2021 11:02:06.442682028 CET	61531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:02:06.494203091 CET	53	61531	8.8.8.8	192.168.2.4
Feb 25, 2021 11:02:06.902120113 CET	49228	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:02:06.973751068 CET	53	49228	8.8.8.8	192.168.2.4
Feb 25, 2021 11:02:13.079725981 CET	59794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:02:13.138896942 CET	53	59794	8.8.8.8	192.168.2.4
Feb 25, 2021 11:02:21.658520937 CET	55916	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:02:21.707285881 CET	53	55916	8.8.8.8	192.168.2.4
Feb 25, 2021 11:02:22.440157890 CET	52752	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:02:22.491825104 CET	53	52752	8.8.8.8	192.168.2.4
Feb 25, 2021 11:02:23.797410011 CET	60542	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:02:23.849209070 CET	53	60542	8.8.8.8	192.168.2.4
Feb 25, 2021 11:02:46.085253954 CET	60689	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:02:46.137064934 CET	53	60689	8.8.8.8	192.168.2.4
Feb 25, 2021 11:02:47.596141100 CET	64206	53	192.168.2.4	8.8.8.8
Feb 25, 2021 11:02:47.667078972 CET	53	64206	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 11:01:15.877588987 CET	192.168.2.4	8.8.8.8	0xa838	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:15.945533037 CET	192.168.2.4	8.8.8.8	0xa261	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:26.425578117 CET	192.168.2.4	8.8.8.8	0x1f79	Standard query (0)	mail.sapgroup.com.pk	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:26.868973970 CET	192.168.2.4	8.8.8.8	0xdc2f	Standard query (0)	mail.sapgroup.com.pk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 11:01:15.926315069 CET	8.8.8.8	192.168.2.4	0xa838	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 11:01:15.926315069 CET	8.8.8.8	192.168.2.4	0xa838	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:15.926315069 CET	8.8.8.8	192.168.2.4	0xa838	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:15.926315069 CET	8.8.8.8	192.168.2.4	0xa838	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:15.926315069 CET	8.8.8.8	192.168.2.4	0xa838	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:15.926315069 CET	8.8.8.8	192.168.2.4	0xa838	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:16.001646996 CET	8.8.8.8	192.168.2.4	0xa261	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 11:01:16.001646996 CET	8.8.8.8	192.168.2.4	0xa261	No error (0)	checkip.dyndns.com		131.186.113.70	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:16.001646996 CET	8.8.8.8	192.168.2.4	0xa261	No error (0)	checkip.dyndns.com		216.146.43.71	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:16.001646996 CET	8.8.8.8	192.168.2.4	0xa261	No error (0)	checkip.dyndns.com		216.146.43.70	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:16.001646996 CET	8.8.8.8	192.168.2.4	0xa261	No error (0)	checkip.dyndns.com		162.88.193.70	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:16.001646996 CET	8.8.8.8	192.168.2.4	0xa261	No error (0)	checkip.dyndns.com		131.186.161.70	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:26.573837996 CET	8.8.8.8	192.168.2.4	0x1f79	No error (0)	mail.sapgroup.com.pk	sapgroup.com.pk		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 11:01:26.573837996 CET	8.8.8.8	192.168.2.4	0x1f79	No error (0)	sapgroup.com.pk		95.215.225.23	A (IP address)	IN (0x0001)
Feb 25, 2021 11:01:27.075436115 CET	8.8.8.8	192.168.2.4	0xdc2f	No error (0)	mail.sapgroup.com.pk	sapgroup.com.pk		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 11:01:27.075436115 CET	8.8.8.8	192.168.2.4	0xdc2f	No error (0)	sapgroup.com.pk		95.215.225.23	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- checkip.dyndns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49733	131.186.113.70	80	C:\Users\user\Desktop\Recibo de entrega de DHL.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:01:16.100343943 CET	2649	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:01:16.161358118 CET	2649	IN	HTTP/1.1 200 OK Content-Type: text/html Server: DynDNS-CheckIP/1.2.0 Connection: close Cache-Control: no-cache Pragma: no-cache Content-Length: 103 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 43 75 72 72 65 6e 74 20 49 50 20 43 68 65 63 6b 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 43 75 72 72 65 6e 74 20 49 50 20 41 64 64 72 65 73 73 3a 20 38 34 2e 31 37 2e 35 32 2e 37 38 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Current IP Check</title></head><body>Current IP Address: 84.17.52.78</body></html>

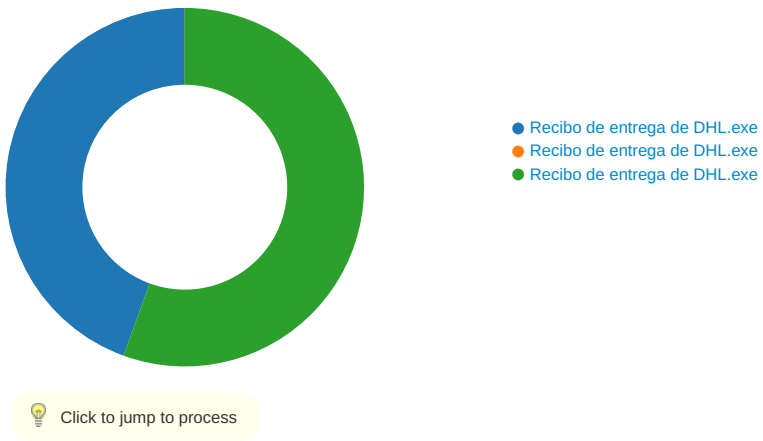
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 11:01:28.086750984 CET	587	49738	95.215.225.23	192.168.2.4	220-cp8.ukdns.biz ESMTP Exim 4.93 #2 Thu, 25 Feb 2021 10:01:28 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 25, 2021 11:01:28.087178946 CET	49738	587	192.168.2.4	95.215.225.23	EHLO 216041
Feb 25, 2021 11:01:28.145792961 CET	587	49738	95.215.225.23	192.168.2.4	250-cp8.ukdns.biz Hello 216041 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 11:01:28.146311045 CET	49738	587	192.168.2.4	95.215.225.23	STARTTLS
Feb 25, 2021 11:01:28.209126949 CET	587	49738	95.215.225.23	192.168.2.4	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Recibo de entrega de DHL.exe PID: 7008 Parent PID: 5924

General

Start time:	11:01:04
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Recibo de entrega de DHL.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Recibo de entrega de DHL.exe'
Imagebase:	0xa00000
File size:	375296 bytes
MD5 hash:	335A69EE25155D53F6DF46C020AA90CD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_404Keylogger, Description: Yara detected 404Keylogger, Source: 00000000.00000002.660324549.0000000003CD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.660324549.0000000003CD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.660068235.0000000002CD1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

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	6D17CF06	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	6D17CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Recibo de entrega de DHL.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

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\Local\Microsoft\CLR_v4.0_32\UsageLogs\Recibo de entrega de DHL.exe.log	unknown	1594	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D48C907	WriteFile

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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Analysis Process: Recibo de entrega de DHL.exe PID: 6416 Parent PID: 7008

General

Start time:	11:01:13
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Recibo de entrega de DHL.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Recibo de entrega de DHL.exe
Imagebase:	0x310000
File size:	375296 bytes
MD5 hash:	335A69EE25155D53F6DF46C020AA90CD
Has elevated privileges:	true

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

Analysis Process: Recibo de entrega de DHL.exe PID: 2912 Parent PID: 7008

General

Start time:	11:01:13
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Recibo de entrega de DHL.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Recibo de entrega de DHL.exe
Imagebase:	0x9f0000
File size:	375296 bytes
MD5 hash:	335A69EE25155D53F6DF46C020AA90CD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_404Keylogger, Description: Yara detected 404Keylogger, Source: 00000005.00000002.906857662.0000000002E6E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_404Keylogger, Description: Yara detected 404Keylogger, Source: 00000005.00000002.905487437.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.905487437.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

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	6D17CF06	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	6D17CF06	unknown
C:\Users\user\Documents\Results.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6BFC1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\Results.txt	success or wait	1	6BFC6A95	DeleteFileW

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\Documents\Results.txt	unknown	288	7c 2d 2d 2d 2d 2d 2d 20 52 65 73 75 6c 74 73 20 2d 20 50 61 73 73 77 6f 72 64 73 20 2d 2d 2d 2d 2d 2d 2d 7c 0d 0a 2d 2d 2d 2d 2d 2d 2d 20 2b 20 49 4e 46 4f 20 2b 20 2d 2d 2d 2d 2d 2d 2d 0d 0a 0d 0a 49 50 3a 20 38 34 2e 31 37 2e 35 32 2e 37 38 0d 0a 0d 0a 4f 77 6e 65 72 20 4e 61 6d 65 3a 20 32 31 36 30 34 31 0d 0a 4f 53 20 4e 61 6d 65 3a 20 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 31 30 20 50 72 6f 0d 0a 4f 53 20 56 65 72 73 69 6f 6e 3a 20 36 2e 32 2e 39 32 30 30 2e 30 0d 0a 4f 53 20 50 6c 61 74 46 6f 72 6d 3a 20 57 69 6e 33 32 4e 54 0d 0a 52 41 4d 20 53 69 7a 65 3a 20 38 2e 30 30 20 47 42 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d	|------- Results - Passwords -------|..------- + INFO + -------....IP: 84.17.52.78....Owner Name: 216041..OS Name: Microsoft Windows 10 Pro..OS Version: 6.2.9200.0..OS PlatForm: Wi n32NT..RAM Size: 8.00 GB..------------------------- ....------------	success or wait	1	6BFC1B4F	WriteFile

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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\Documents\Results.txt	unknown	17408	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\Documents\Results.txt	unknown	17408	end of file	1	6BFC1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis