ID: 626594
Sample Name: DHL SHIPMENT NOTIFICATION 1146789443.bat
Cookbook: default.jbs
Time: 15:09:35
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

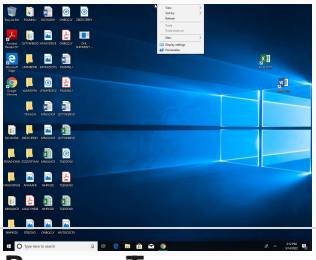
Windows Analysis Report

DHL SHIPMENT NOTIFICATION 1146789443.bat

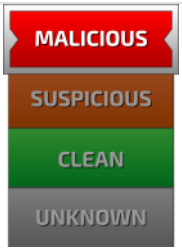
Overview

General Information

Sample Name:	DHL SHIPMENT NOTIFICATION 1146789443.bat (renamed file extension from bat to exe)
Analysis ID:	626594
MD5:	f883d433fab3b7a.
SHA1:	d29ddef177a748..
SHA256:	0606d4bc2c27f4…
Tags:	bat DHL exe
Infos:	



Detection



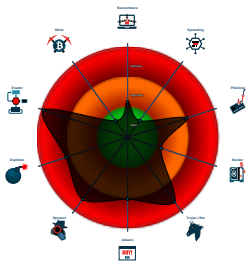
AgentTesla, AveMaria, UACMe

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

Signatures

- Yara detected AgentTesla
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected UACMe UAC Bypass…
- Yara detected AveMaria stealer
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- DHL SHIPMENT NOTIFICATION 1146789443.exe (PID: 7052 cmdline: "C:\Users\user\Desktop\DHL SHIPMENT NOTIFICATION 1146789443.exe" MD5: F883D433FAB3B7AE0C25625E75A03B38)
  - powershell.exe (PID: 6492 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\ZWLqFmhrZsaGO.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6520 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6568 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ZWLqFmhrZsaGO" /XML "C:\Users\user\AppData\Local\Temp\tmp8559.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - DHL SHIPMENT NOTIFICATION 1146789443.exe (PID: 5556 cmdline: C:\Users\user\Desktop\DHL SHIPMENT NOTIFICATION 1146789443.exe MD5: F883D433FAB3B7AE0C25625E75A03B38)
    - INVESTORORIGIN.exe (PID: 6928 cmdline: "C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe" MD5: 138E534107A536F319734BFD7A23C8A3)
      - WerFault.exe (PID: 6744 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6928 -s 2356 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - INVESTORORIGN.exe (PID: 6872 cmdline: "C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe" MD5: 68FE2DCF9C615A4A55AAA75A11E1F8F0)
- **cleanup**

Malware Configuration

Threatname: AveMaria

```
{
  "C2 url": "76.8.53.133",
  "port": 1198
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "ikesend@exportersglobe.com",
  "Password": "MnmPsqBteq4_",
  "Host": "mail.exportersglobe.com"
}
```

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32f79:$s10: logins • 0x329e0:$s11: credential • 0x2ef98:$g1: get_Clipboard • 0x2efa6:$g2: get_Keyboard • 0x2efb3:$g3: get_Password • 0x302b3:$g4: get_CtrlKeyDown • 0x302c3:$g5: get_ShiftKeyDown • 0x302d4:$g6: get_AltKeyDown
C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x191f0:$c1: Elevation:Administrator!new:

Click to see the 7 entries

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000000.526380150.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000F.00000000.526380150.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
0000000E.00000000.520367739.0000000000012000.00000002.00000001.01000000.0000000B.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000000.520367739.0000000000012000.00000002.00000001.01000000.0000000B.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000F.00000003.530860371.00000000008F6000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 68 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
15.3.INVESTORORIGN.exe.930630.0.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
15.3.INVESTORORIGN.exe.930630.0.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0xd80:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xd80:$c1: Elevation:Administrator!new:
15.3.INVESTORORIGN.exe.930630.0.raw.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
15.2.INVESTORORIGN.exe.b40000.0.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
15.2.INVESTORORIGN.exe.b40000.0.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x191f0:$c1: Elevation:Administrator!new:

Click to see the 93 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits

Yara detected UACMe UAC Bypass tool

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected AveMaria stealer

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Contains functionality to hide user accounts

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

Injects a PE file into a foreign processes
Adds a directory exclusion to Windows Defender
Modifies the hosts file
Contains functionality to inject threads in other processes

Lowering of HIPS / PFW / Operating System Security Settings

Increases the number of concurrent connection per server for Internet Explorer
Modifies the hosts file

Stealing of Sensitive Information

Yara detected AgentTesla
Yara detected AveMaria stealer
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal browser information (history, passwords, etc)
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
Tries to harvest and steal ftp login credentials
Contains functionality to steal e-mail passwords
Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality

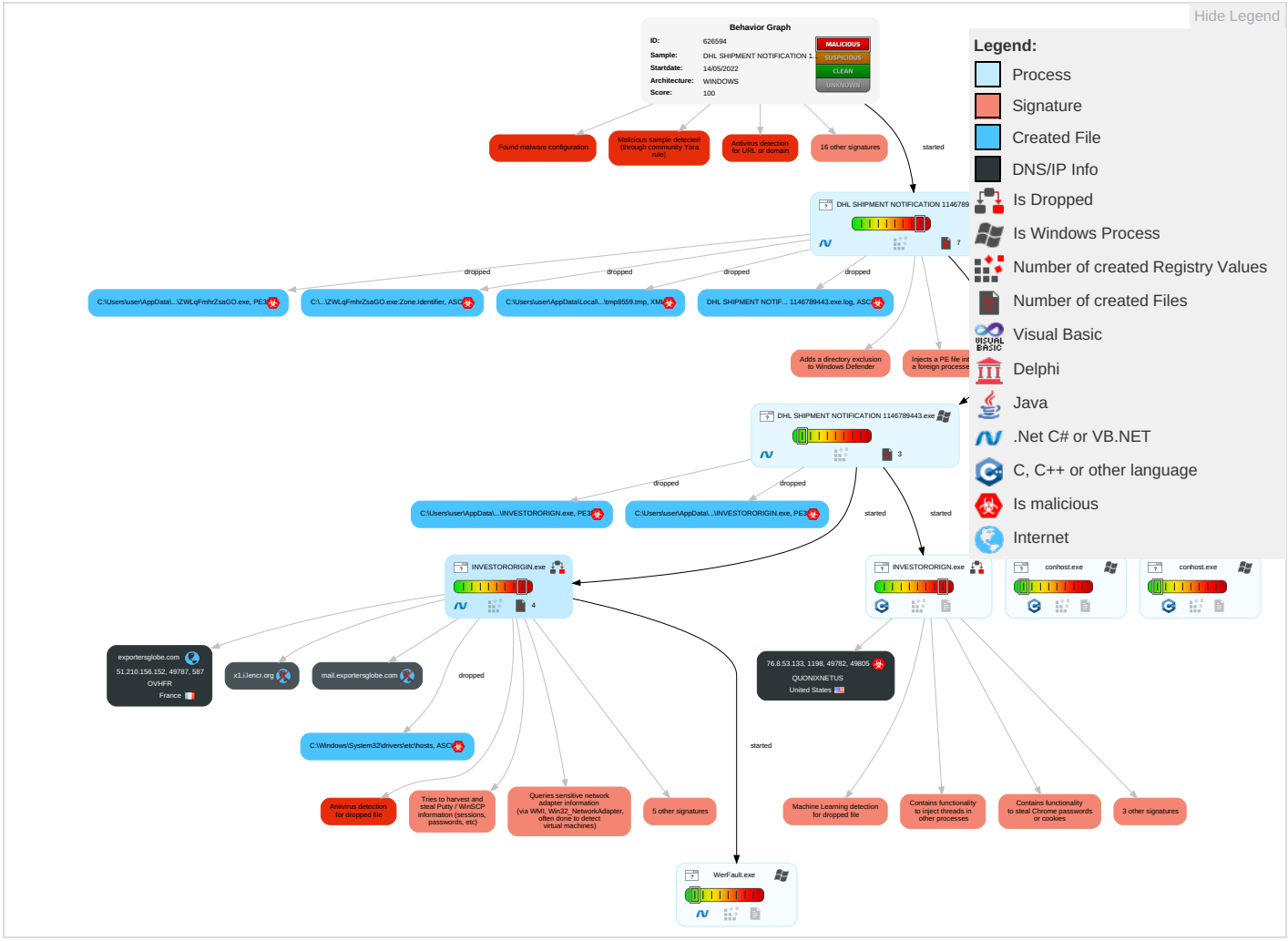
Yara detected AgentTesla
Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Create Account	1 Access Token Manipulation	1 File and Directory Permissions Modification	4 OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	2 1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Endpoint Denial of Service
Default Accounts	1 Native API	1 Windows Service	1 Windows Service	1 1 Disable or Modify Tools	3 1 Input Capture	1 System Service Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	2 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	1 Scheduled Task/Job	2 2 1 Process Injection	1 1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	3 File and Directory Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	1 Scheduled Task/Job	Logon Script (Mac)	1 Scheduled Task/Job	3 Obfuscated Files or Information	1 Credentials In Files	1 2 5 System Information Discovery	Distributed Component Object Model	3 1 Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	2 Service Execution	Network Logon Script	Network Logon Script	2 3 Software Packing	LSA Secrets	1 Query Registry	SSH	Keylogging	Data Transfer Size Limits	1 1 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Masquerading	Cached Domain Credentials	3 3 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 4 1 Virtualization/Sandbox Evasion	DCSync	1 4 1 Virtualization/Sandbox Evasion	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Access Token Manipulation	Proc Filesystem	2 Process Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	2 2 1 Process Injection	/etc/passwd and /etc/shadow	1 Application Window Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Files and Directories	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Hidden Users	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

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 SHIPMENT NOTIFICATION 1146789443.exe	17%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
DHL SHIPMENT NOTIFICATION 1146789443.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe	100%	Avira	TR/Redcap.ghjpt	
C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ZWLqFmhrZsaGO.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ZWLqFmhrZsaGO.exe	17%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.0.INVESTORORIGN.exe.b40000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File

Source	Detection	Scanner	Label	Link	Download
10.0.DHL SHIPMENT NOTIFICATION 1146789443.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
14.0.INVESTORORIGIN.exe.10000.0.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
14.0.INVESTORORIGIN.exe.10000.5.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
14.0.INVESTORORIGIN.exe.10000.3.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
14.0.INVESTORORIGIN.exe.10000.2.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
10.0.DHL SHIPMENT NOTIFICATION 1146789443.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
15.2.INVESTORORIGN.exe.b40000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
10.0.DHL SHIPMENT NOTIFICATION 1146789443.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
14.0.INVESTORORIGIN.exe.10000.1.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
15.0.INVESTORORIGN.exe.b40000.6.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
14.2.INVESTORORIGIN.exe.10000.0.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
10.0.DHL SHIPMENT NOTIFICATION 1146789443.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
10.2.DHL SHIPMENT NOTIFICATION 1146789443.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
15.0.INVESTORORIGN.exe.b40000.4.unpack	100%	Avira	TR/Redcap.ghjpt		Download File
14.0.INVESTORORIGIN.exe.10000.4.unpack	100%	Avira	HEUR/AGEN.1203035		Download File
10.0.DHL SHIPMENT NOTIFICATION 1146789443.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
15.0.INVESTORORIGN.exe.b40000.2.unpack	100%	Avira	TR/Redcap.ghjpt		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://www.sajatypeworks.com0	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://gdvnpTNIZqNaaR.net	0%	Avira URL Cloud	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://www.carterandcone.coml%	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.carterandcone.comsmJ	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comr%wL0	0%	Avira URL Cloud	safe	
http://crl.veris	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://FuVaco.com	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.coma	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://www.carterandcone.comN%CL.	0%	Avira URL Cloud	safe	
http://x1.i.lencr.org/	0%	URL Reputation	safe	
76.8.53.133	100%	Avira URL Cloud	malware	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://www.tiro.comt	0%	URL Reputation	safe	
http://www.tiro.como	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidPsi/Psi	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://https://api.ipify.org%facebooktwittergmailinstagrammovieskypepornhackwhatsappdiscordemailpassword%st	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
exportersglobe.com	51.210.156.152	true	false		high
mail.exportersglobe.com	unknown	unknown	false		high
x1.i.lencr.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
76.8.53.133	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	INVESTORORIGIN.exe, 0000000E.00000000.559362643.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.563804082.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.597270868.00000000024F1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com0	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.437881619.0000000005C0B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com2	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.437881619.0000000005C0B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

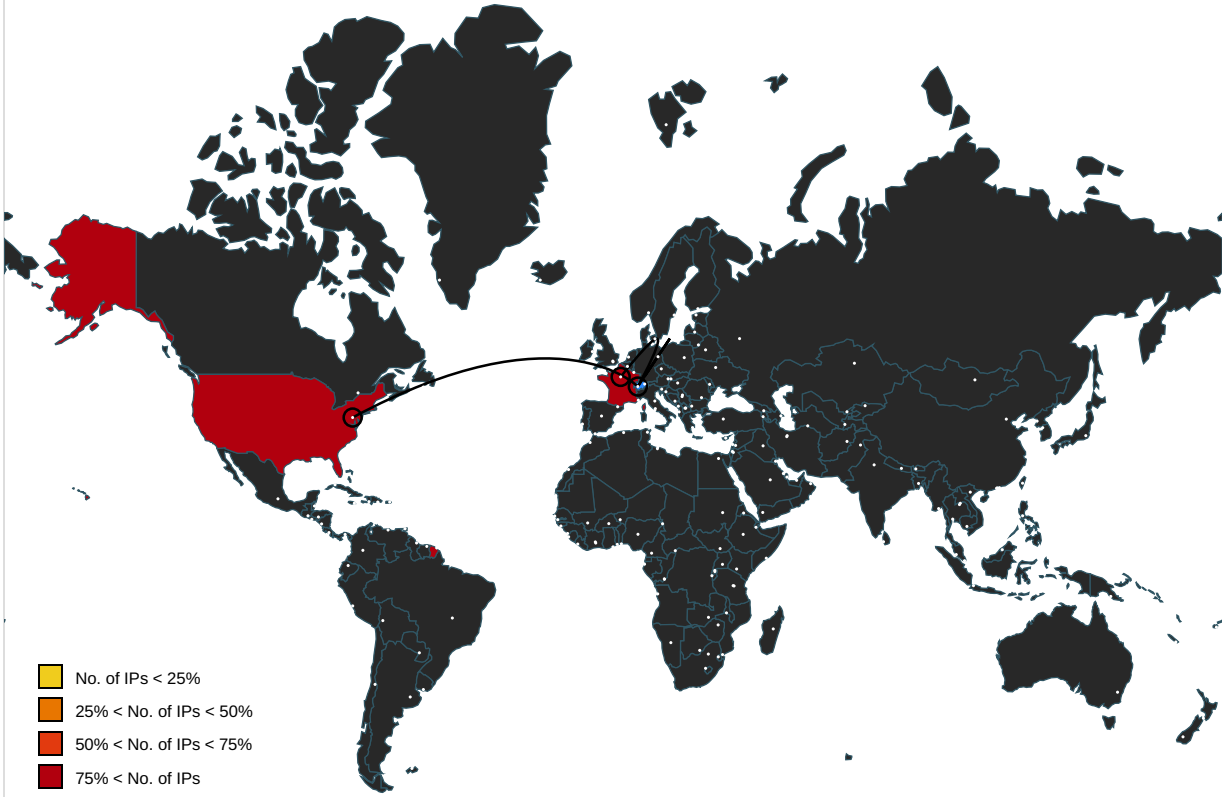
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp, DHL SHIPMENT NOTIFICATION 114678944 3.exe, 00000000.00000003.441138599.0000000005BF8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.c	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.441000147.0000000005BF8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://gdvnpTNIZqNaaR.net	INVESTORORIGIN.exe, 0000000E.00000000.560098397.0000000002876000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.560117509.0000000287E000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.559362643.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.563804082.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.564503411.0000002802000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.597270868.00000000024F1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.446140453.0000000005BFE000.00000004.00000800.00020000.00000000.sdmp, DHL SHIPMENT NOTIFICATION 114678944 3.exe, 00000000.00000003.445951364.0000000005BFD000.00000004.00000800.00020000.00000000.sdmp, DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.443725716.0000000005BF5000.00000004.00000800.00020000.00000000.sdmp, DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.446201983.0000000005BFE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/syohex/java-simple-mine-sweeper	INVESTORORIGN.exe	false		high
http://r3.i.lencr.org/0	INVESTORORIGIN.exe, 0000000E.00000000.561485586.0000000006120000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.600185823.0000000006120000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.564579076.0000000002852000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.596649630.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.563092562.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.558741932.00000000006DF000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml%	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.443725716.0000000005BF5000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.com	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp, DHL SHIPMENT NOTIFICATION 114678944 3.exe, 00000000.00000003.437881619.0000000005C0B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comsmJ	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.443725716.0000000005BF5000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comr%wL0	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.443725716.0000000005BF5000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://crl.veris	INVESTORORIGIN.exe, 0000000E.00000002.596649630.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.563092562.00000000006DF000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.558741932.00000000006DF000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.c.lencr.org/0	INVESTORORIGIN.exe, 0000000E.00000000.561485586.0000000006120000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.600185823.00000000006120000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.564579076.0000000002852000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.596649630.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.563092562.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.558741932.00000000006DF000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	INVESTORORIGIN.exe, 0000000E.00000000.561485586.0000000006120000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.600185823.00000000006120000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.564579076.0000000002852000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.596649630.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.563092562.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.558741932.00000000006DF000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://r3.o.lencr.org0	INVESTORORIGIN.exe, 0000000E.00000000.561485586.0000000006120000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.600185823.00000000006120000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.564579076.0000000002852000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.596649630.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.563092562.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.558741932.00000000006DF000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://FuVaco.com	INVESTORORIGIN.exe, 0000000E.00000002.597270868.00000000024F1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.coma	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.437881619.0000000005C0B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.514559229.0000000002B21000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	INVESTORORIGIN.exe, 0000000E.00000000.559362643.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.563804082.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.597270868.00000000024F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.carterandcone.comN%CL.	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.445951364.0000000005BFD000.00000004.00000800.00020000.00000000.sdmp, DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.443725716.0000000005BF5000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp, DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.514410373.0000000001307000.00000004.00000020.00020000.00000000.sdmp	false		high
http://x1.i.lencr.org/	INVESTORORIGIN.exe, 0000000E.00000002.596649630.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.563092562.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.558741932.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, 2D85F72862B55C4EADD9E66E06947F3D0.14.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://cps.letsencrypt.org0	INVESTORORIGIN.exe, 0000000E.00000000.561485586.0000000006120000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.600185823.00000006120000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.564579076.0000000002852000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.596649630.00000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.563092562.0000000006DF000.00000004.00000020.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.558741932.00000000006DF000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comt	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.441138599.0000000005BF8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.como	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.441138599.0000000005BF8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	INVESTORORIGIN.exe, 0000000E.00000000.559362643.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.563804082.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.597270868.00000000024F1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp, DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000003.441000147.000000005BF8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNSnamejidPsi/Psi	INVESTORORIGIN.exe, 0000000E.00000002.597270868.00000000024F1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	DHL SHIPMENT NOTIFICATION 1146789443.exe, 00000000.00000002.521726377.0000000006E02000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%facebooktwittergmailinstagrammovieskypepornhackwhatsappdiscordemailpassword%st	INVESTORORIGIN.exe, 0000000E.00000000.559362643.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000000.563804082.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGIN.exe, 0000000E.00000002.597270868.00000000024F1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://github.com/syohex/java-simple-mine-sweeperC:	DHL SHIPMENT NOTIFICATION 1146789443.exe, 0000000A.00000002.528443565.0000000004405000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGN.exe, 0000000F.00000000.526380150.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp, INVESTORORIGN.exe, 0000000F.00000002.702803997.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp, INVESTORORIGN.exe, 0000000F.00000002.703160012.0000000002BA8000.00000004.00000800.00020000.00000000.sdmp, INVESTORORIGN.exe.10.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
76.8.53.133	unknown	United States		17185	QUONIXNETUS	true
51.210.156.152	exportersglobe.com	France		16276	OVHFR	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626594
Start date and time: 14/05/202215:09:35	2022-05-14 15:09:35 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL SHIPMENT NOTIFICATION 1146789443.bat (renamed file extension from bat to 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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.phis.troj.adwa.spyw.expl.evad.winEXE@14/17@3/2
EGA Information:	• Successful, ratio: 75%

HDC Information:	• Successful, ratio: 8.7% (good quality ratio 8.6%) • Quality average: 88.1% • Quality standard deviation: 20.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.50.97.168, 20.189.173.20
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, e8652.dscx.akamaiedge.net, onedsblobprdwus15.westus.cloudapp.azure.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, crl.root-x1.letsencrypt.org.edgekey.net
- Execution Graph export aborted for target DHL SHIPMENT NOTIFICATION 1146789443.exe, PID 5556 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- 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 NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:11:07	API Interceptor	2x Sleep call for process: DHL SHIPMENT NOTIFICATION 1146789443.exe modified
15:11:15	API Interceptor	37x Sleep call for process: powershell.exe modified
15:11:35	API Interceptor	143x Sleep call for process: INVESTORORIGIN.exe modified
15:12:05	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

⊘ **No context**

Domains

⊘ **No context**

ASNs

⊘ **No context**

JA3 Fingerprints

⊘ **No context**

Dropped Files

⊘ **No context**

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_INVESTORORIGIN.e_77f278dc5a2c1c3935eb52616b8cb594c251e8e_0e345062_1a0b7f2e\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.2592822441229328
Encrypted:	false
SSDEEP:	192:DgFS7ubdHBUZMXqaKeCvYLTy/u7sQS274ItVM:DOS7uBBUZMXqaeeTy/u7sQX4ItVM
MD5:	BCD112C816C0E8D78C183A24846CB0FE
SHA1:	F7E7193CE66FFD736AA86D612CAF5E07B1EF2EBB
SHA-256:	4D57D837C86736130374FF8D70070046C768CDE5F6D61F221C8B0E1725E0658D
SHA-512:	6322BF29729CAD6A3DA4DCD555444385D227B6732C6E4D13AB5E01285BA79EE612FF71D8B99530C4C0A2C250FEAA2C6C583C23F9609D5F820443988971E524D
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.7.0.3.9.9.1.5.4.8.9.5.5.7.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.7.0.3.9.9.2.4.3.3.8.6.8.7.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.d.5.8.a.9.f.d.-.b.2.5.5.-.4.1.b.b.-.9.b.7.c.-.c.5.c.9.9.4.e.3.5.a.7.6.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.e.e.5.a.5.0.b.-.d.d.f.f.-.4.d.e.c.-.b.d.0.8.-.1.9.b.3.c.9.a.2.c.9.e.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.I.N.V.E.S.T.O.R.O.R.I.G.I.N...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.h.f.O.Z.A.Z.n.v.D.p.x.m.l.w.G.B.M.b.e.m...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.1.0.-.0.0.0.1.-.0.0.1.7.-.7.7.7.c.-.6.1.9.0.d.f.6.7.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.5.f.2.9.e.0.d.3.f.7.f.6.c.0.5.a.2.d.3.3.5.c.a.0.f.0.d.9.3.7.5.8.0.0.0.0.0.0.0.0.!.0.0.0.0.3.2.6.b.c.5.8.6.2.9.3.7.7.6.d.2.d.c.4.3.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5763.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sat May 14 22:11:57 2022, 0x1205a4 type
Category:	dropped
Size (bytes):	377183
Entropy (8bit):	3.2816214263554357
Encrypted:	false
SSDEEP:	3072:entWB9gIOgF5D0lJgUoKAoJi7ouHhgDjd+psEUj/0OiUCgUf87:F9RpDD0lJgUoP0i7oF8p4rOTj
MD5:	810B7BB99711EAC53423A73B635AE038
SHA1:	EE408BE019BCE8161155A8DE64867C9D110519DF
SHA-256:	6B18C4099787BCBD8C3A740881E8E616F3406891753A85A50EFAE321DB7A0D37
SHA-512:	0D9D66E032F69B9AAA78D2B978FB29E3B98291A6A46BA2628D4213DBB13B8AE8488FAEB2C0C417E64BE91DC18F6290118CFB0B95EB7AD1029D672B07BAFC8281
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....-).b.....".....$....-.....4,...w.....`.....8.....T.....b...^.....-...../.....U.....B.....L0.....GenuineIntelW.....T.....).b.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER65CB.tmp.WERInternalMetadata.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	6398
Entropy (8bit):	3.723556925579948
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNie16gXYZISYCprNx89b8BsfVUm:RrlsNi06wYiSs86fD
MD5:	4B06B8E547BE4A7BA93C7560AED876BD
SHA1:	2CB5357AACCD5C107EDDEB480D04D068E57BE29B
SHA-256:	AAE75E1C3891ADF39C0BA185A67F28F4D025A0750AD4C6A6558047B1C01E7356
SHA-512:	0104D32A0C34BADF15E950972CF9DCBD54F3D1F1921B8BF59CAA9DC72D86BDA539365C9260BF5B72D712D6EAD7267DAA697FF4A17FF339B4413A44604C1AD531
Malicious:	false
Reputation:	unknown

Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.9.2.8.</./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6957.tmp.xml

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4763
Entropy (8bit):	4.515085921606482
Encrypted:	false
SSDEEP:	48:cvIwSD8zsXJgtWI98aWgc8sqYj/8fm8M4JujJ2FX+q8v6jJTVJR2Vdd:uITf5HbgrsqYgJ5KSVJ8Vdd
MD5:	EC49AF3B3D22BEE401805BB45BEDC105
SHA1:	D1476F996FCF4169D618C35376984778F9152194
SHA-256:	4DE10861507983F9196169D396FD7C286E51BB6D7499D35FF8850CA4F66A9184
SHA-512:	C1680125896C8E2897FD0496C6E8E9872570608C7ECA5A01196D3BB3FA013175694294DA8561D0DF67BAAA70E0F8D2055A1B82DCF7A6BBF6C2F384F2C8C446B
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1515322" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\2D85F72862B55C4EADD9E66E06947F3D

Process:	C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe
File Type:	data
Category:	dropped
Size (bytes):	1391
Entropy (8bit):	7.705940075877404
Encrypted:	false
SSDEEP:	24:ooVdTH2NMU+I3E0Ulcrgdaf3sWrATrnkC4EmCUkmGMkfQo1fSZotWzD1:ooVguI3Kcx8WIzNeCUkJMmSuMX1
MD5:	0CD2F9E0DA1773E9ED864DA5E370E74E
SHA1:	CABD2A79A1076A31F21D253635CB039D4329A5E8
SHA-256:	96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6
SHA-512:	3B40F27E828323F5B91F8909883A78A21C86551761F27B38029FAAEC14AF5B7AA96FB9F9CC93EE201B5EB1D0FEF17B290747E8B839D2E49A8F36C5EBF3C7C910
Malicious:	false
Reputation:	unknown
Preview:	0..k0..S.....@.YDc.c...0...*.H.....0O1.0...U....US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10...150604110438Z..350604110438Z0O1.0...U....US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10.."0...*.H.....0.....$s..7.+W(.....8..n<.W.x.u...jn..O(..h.lD...c...k....1.!~.3<.H..y.....!.K...qiJffl.~<p..)"......K...~....G.|.H#S.8.O.o...IW..t./.8.{.p!.u.0<.....c...O..K~.....w...{J.L.%.p..)..S$.....J.?..aQ.....cq...o[...\4ylv.;.by.../&.....6....7..6u...r.....l.....*.A..v.....5/(.l....dwn G7..Y^h..r...A)>Y>.&.$...Z.L@.F....:Qn.;.}r...xY.>Qx...../..>{J.Ks.....P.|C.t..t.....0.[q6....00\H..;..}`...).....A.....|.;F.H*..v.v..j.=...8.d..+..(.....B.".']..y...p..N..:..'Qn..d.3CO.....B0 @0...U.....0...U.....0....0...U.....y.Y.{....s.....X..n0...*.H.....U.X....P.....i ')..au\.n...i/..VK..s.Y.!.~.Lq...`.9....!V..P.Y...Y.....b.E.f..|o..;....'...}~.."....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2D85F72862B55C4EADD9E66E06947F3D

Process:	C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe
File Type:	data
Category:	modified
Size (bytes):	192
Entropy (8bit):	2.773803200765873
Encrypted:	false
SSDEEP:	3:kkFklKm0hfllXlE/zMc85ljNNX8RolJuRdyo1dlUKlGXJlDdt:kkTm0O18tNMa8Rdy+UKcXP
MD5:	EC6A887DC9E0C968BE650D7E7154E88D
SHA1:	88FFFA37DC6483F1A7A1C05E39506D3C0483F768
SHA-256:	1BE383A47B94E160AC4C649B15B8D859BA967964212517B97D5609154F9338E0
SHA-512:	26104611A869F6986AFBE4203EFD169C91BBE532740585FE248DDCAE58A34F0BA0DB55BBB6BC2A6729D3BF3404723A1F79D79E4CDD591DDB71ED1A13D01DB81F
Malicious:	false
Reputation:	unknown

Preview:	p..... .....9...g..(..... .....~.....o...h.t.t.p.:././.x.1...i...l.e.n.c.r...o.r.g./...".5.a.6.2.8.1.5.c.-.5.6.f."...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL SHIPMENT NOTIFICATION 1146789443.exe.log

Process:	C:\Users\user\Desktop\DHL SHIPMENT NOTIFICATION 1146789443.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE8:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHJ
MD5:	EA78C102145ED608EF0E407B978AF339
SHA1:	66C9179ED9675B9271A97AB1FC878077E09AB731
SHA-256:	8BF01E0C445BD07C0B4EDC7199B7E17DAF1CA55CA52D4A6EAC4EF211C2B1A73E
SHA-512:	8C04139A1FC3C3BDACB680EC443615A43EB18E73B5A0CFCA644CB4A5E71746B275B3E238DD1A5A205405313E457BB75F9BBB93277C67AFA5D78DCFA30E5DA02B
Malicious:	**true**
Reputation:	unknown
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22252
Entropy (8bit):	5.59944796203455
Encrypted:	false
SSDEEP:	384:BtCDjC0KpW6Lr+09BBPcOUSB+AjultIQM7nvPg3hInEML+efmAV7tciyNZQvnI+m:dWC6YB/U45CltLo66PKCpg+0
MD5:	6549CFF10ABBDB2F4D78869012AB8AC2
SHA1:	64D876598518198CD9A19090216240B89E32515A
SHA-256:	E99A909442A39C63DE46A2604C1094B780176A19008835FECDA16777DB8C7C82
SHA-512:	71EF30940D9ECA6776C99AEA88DA4DB7AAE979EAC67DEF28ECEBD66B63447226DF8316D8A9F4009BF94E20553FD461916A882E11DB3B341528124CAE641E8E18
Malicious:	false
Reputation:	unknown
Preview:	@...e.....s.....K.....-.....@.....H.....<@.^.L."My...:X..... .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\INVESTORORIGIN.exe

Process:	C:\Users\user\Desktop\DHL SHIPMENT NOTIFICATION 1146789443.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	216064
Entropy (8bit):	6.055091750914725
Encrypted:	false
SSDEEP:	6144:7xAlTehh9yUYm//FJZt5oUTeCU7bTQmT8Vtk700jcF7Zk+U:7xAFehh9/Ym//FJZvCVh
MD5:	138E534107A536F319734BFD7A23C8A3
SHA1:	326BC586293776D2DC438409DD5ED956FE672A6E
SHA-256:	3FC1361417C696930DA7901314B51E7C7293C424550F6EA36DC15C90797125DB
SHA-512:	8F500FB340E6DD7DAC9E8A792D467A0440466B806CD5C809484B76EF488C514085B32C8F490F6E81C5C4685B4EF987F6A78C6C2E3509DBDC56EEF18B33CC0F8
Malicious:	**true**

Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...T.kb.....B....._.. .....@.. ....@....._..S..... ....H.....text....@... ...B..... ..`.rsrc.....D.....@..@.rel oc.....J.....@..B....._.....H.....4...t.....(....*..(....*.s.....s.....s.....s.....*...0..,.....+.....,.....,.....,.+.+.~.. ..o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0.....+.....,.....,.....,.+.+...(....(....*...0.. (.....+.....,.....,.....,.+.+..(....*.0..,.....

C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe

Process:	C:\Users\user\Desktop\DHL SHIPMENT NOTIFICATION 1146789443.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	115712
Entropy (8bit):	6.373768010602997
Encrypted:	false
SSDEEP:	1536:h0jP7/L1B5rVmN8sxHv2M28ix8EUaJxWZoB4u0OVE01:K1VmhaH8EFvW+0OVE0
MD5:	68FE2DCF9C615A4A55AAA75A11E1F8F0
SHA1:	F7335F70A3F9DBBFFC5D824AD6A32A52C26D3EB4
SHA-256:	D3DFF8B1B2DC8DDB162CA47244BAA8C086F20E81824E95CDF29B3FAE56536DE7
SHA-512:	0D3B0D533FBF70CBAC0C4E20B807DBAFF54235D4CB1AFA2D979D187FA9AB03FA2068914C5BD429D16C7237F0F61D0D37F31BB8217484588D873677634AAF2F0
Malicious:	**true**
Yara Hits:	• Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM, Description: Detects executables embedding command execution via IExecuteCommand COM object, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: ditekSHen • Rule: MALWARE_Win_WarzoneRAT, Description: Detects AveMaria/WarzoneRAT, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: ditekSHen • Rule: AveMaria_WarZone, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z]..><..><..><...3.?<..7D..?<...3.<<.....?<.....=<..;0..?<..7D..:<..7D ..!<..><...<...U..N<...Um.?<...U..?<..Rich><.....PE..L.....I_.....0.....\.....@....@.....@.....@.....w.....p,..... ....u.....@..p.....text.....0..... ..`.rdata...I...@...J...4.....@..@.data....P.....~.....@....rsrc...p,..... .....@..@.reloc..... .....@..B.bss.....0.....@..@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ald43iwi.q5u.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wqdexkj3.urd.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 0A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp8559.tmp

Process:	C:\Users\user\Desktop\DHL SHIPMENT NOTIFICATION 1146789443.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	5.1414291730712
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtjLxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTxv
MD5:	09BA8A7D1E6F45820021C4A8E8FB6886
SHA1:	81B223E59E66AFE9B4AB1DDD1BE147149FB0C107
SHA-256:	36A91485D9DB4F561C78AD994E38E70E1273B28599B112602E22BF8078D3ABE3
SHA-512:	02367F1C0BEB6D53CD27FF5B972ACDBCAF721D80D6FD34C73CD81304D70082E6761A7573027AC62D5FB0FF462E5F98902D860594F541C1567DDBB10809A26D E
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-1 0-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Princip al id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Roaming\ZWLqFmhrZsaGO.exe

Process:	C:\Users\user\Desktop\DHL SHIPMENT NOTIFICATION 1146789443.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1004032
Entropy (8bit):	7.761593863349046
Encrypted:	false
SSDEEP:	12288:u5kOON//aPfRFsW2nRwR79FNLvDYk7mDW7WW6/nKGQ6Ak5S7hoWiLQeR+NmWE6:ERc/CPfRFwSRpPv8yCV/n5slZgQ1
MD5:	F883D433FAB3B7AE0C25625E75A03B38
SHA1:	D29DDEF177A748397ABEF51F7EC2188FC06506D5
SHA-256:	0606D4BC2C27F402BE8E98BA28D3AF0D35C1C85D3BE43690FABE971A687AF9ED
SHA-512:	B84B326B03C1EEC7964D607E04F45B08A0B5083041CD3E8EEC2F525F819054EC713CE3186442A5816FFFB043BFD625F542AC7C14C788DB768D51E342CDEB45B 7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....n.b.....0..H.....g... .....@.. ....@.....f..O..... ....H.....text....G... ...H..... ..`.rsrc.....J.....@..@.rel oc.....P.....@..B.....f.....H.....|G.....e.....&.(.....*F.(.....(.....**..(.....*....(.....*....(.....*....{....*"..}....*&.(.....*F.(.....(.....**.. (.....*....(.....*....(.....*..0.....(.....o.....o.....+..*.0.....(.....o.....o.....+..*....0.....(.....o.....o.....+..*....0.....(.....o.....o.....+..*....0.. .....(.....o.....o.....o$....+..*.0.. ..... (.....o.....o.....o$....+..*.(....o....*.(....o....*

C:\Users\user\AppData\Roaming\ZWLqFmhrZsaGO.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\DHL SHIPMENT NOTIFICATION 1146789443.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220514\PowerShell_transcript.760639.TC5_eELU.20220514151113.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):	5811
Entropy (8bit):	5.4155000005474045
Encrypted:	false
SSDEEP:	96:BZ3/7NeqDo1ZqZQ/7NeqDo1ZC1PdjZW/7NeqDo1ZMMNNSZx:X
MD5:	5E9BD99644D97168FB961F5E13052E66
SHA1:	223E62AA2312A7D2D2B1CE383AB7CD057B309A5A
SHA-256:	8D355230C7F912F06CC42A78B4C693F49C77BE79880DD9781D1660B2CFA9ED84
SHA-512:	72E5913D64673E2E8307B3CE2D78B151CF78FAF6432A1437E2ADD57081EE6BE333D31539DDDC4AEC974FB9CB1C67CF2623CA810DB65622578643B460DEF23C3
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220514151114..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 760639 (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\ZWLqFmhrZsaGO.exe..Process ID: 6492..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: 20220514151114..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\ZWLqFmhrZsaGO.exe..**********..Windows PowerShell transcript start..Start time: 20220514151537..Username: computer\user..RunAs User: DESKTOP-7

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FAF
Malicious:	**true**
Reputation:	unknown
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.761593863349046
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:	DHL SHIPMENT NOTIFICATION 1146789443.exe
File size:	1004032
MD5:	f883d433fab3b7ae0c25625e75a03b38
SHA1:	d29ddef177a748397abef51f7ec2188fc06506d5
SHA256:	0606d4bc2c27f402be8e98ba28d3af0d35c1c85d3be43690fabe971a687af9ed
SHA512:	b84b326b03c1eec7964d607e04f45b08a0b5083041cd3e8eec2f525f819054ec713ce3186442a5816fffb043bfd625f542ac7c14c788db768d51e342cdeb45e7
SSDEEP:	12288:u5kOON//aPfRFsW2nRwR79FNLvDYk7mDW7WW6/nKGQ6Ak5S7hoWiLQeR+NmWE6:ERc/CPfRFwSRpPv8yCV/n5slZgQ1
TLSH:	8E25F05133FC5F05E23AA3F59A7051548BB1752B28A6E34E0CC170DB1EA1F41AB63BA7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....n.b.....0..H.....g... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4f670e
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:	0x627F6E0A [Sat May 14 08:53:30 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0xf66bc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf8000	0x5ac	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xfa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xf4714	0xf4800	False	0.857648541347	SysEx File -	7.76755151978	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xf8000	0x5ac	0x600	False	0.421223958333	data	4.08533969296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfa000	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	0xf8090	0x31c	data		
RT_MANIFEST	0xf83bc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

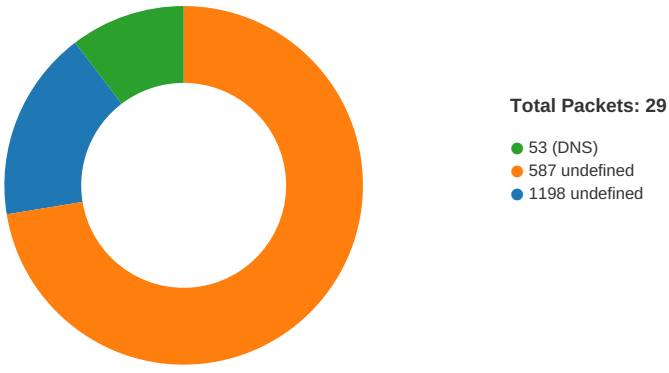
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	1.0.0.0
InternalName	cDisplayClass.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	View
ProductVersion	1.0.0.0
FileDescription	View
OriginalFilename	cDisplayClass.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:11:36.216257095 CEST	49782	1198	192.168.2.5	76.8.53.133
May 14, 2022 15:11:36.334731102 CEST	1198	49782	76.8.53.133	192.168.2.5
May 14, 2022 15:11:36.334881067 CEST	49782	1198	192.168.2.5	76.8.53.133
May 14, 2022 15:11:45.302377939 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:45.329227924 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:45.331383944 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:45.389578104 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:45.390450954 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:45.417249918 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:45.417526007 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:45.446552038 CEST	587	49787	51.210.156.152	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:11:45.493635893 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:45.514338017 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:45.549797058 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:45.549858093 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:45.549890995 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:45.549953938 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:45.566401005 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:45.593547106 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:45.648060083 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:47.311439037 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:47.338073015 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:47.352559090 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:47.381445885 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:47.382287979 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:47.409337997 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:47.410290003 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:47.437402964 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:47.437830925 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:47.469383001 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:47.469748020 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:47.496298075 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:47.497950077 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:47.498269081 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:47.498805046 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:47.498903036 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:11:47.524457932 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:47.524576902 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:47.525204897 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:47.525228977 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:47.526380062 CEST	587	49787	51.210.156.152	192.168.2.5
May 14, 2022 15:11:47.732443094 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:12:08.781395912 CEST	49787	587	192.168.2.5	51.210.156.152
May 14, 2022 15:12:38.473103046 CEST	1198	49782	76.8.53.133	192.168.2.5
May 14, 2022 15:12:38.473249912 CEST	49782	1198	192.168.2.5	76.8.53.133
May 14, 2022 15:12:41.542115927 CEST	49805	1198	192.168.2.5	76.8.53.133
May 14, 2022 15:12:41.651038885 CEST	1198	49805	76.8.53.133	192.168.2.5
May 14, 2022 15:12:41.651165962 CEST	49805	1198	192.168.2.5	76.8.53.133

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:11:45.160797119 CEST	60969	53	192.168.2.5	8.8.8.8
May 14, 2022 15:11:45.193556070 CEST	53	60969	8.8.8.8	192.168.2.5
May 14, 2022 15:11:45.259629965 CEST	62929	53	192.168.2.5	8.8.8.8
May 14, 2022 15:11:45.278019905 CEST	53	62929	8.8.8.8	192.168.2.5
May 14, 2022 15:11:46.224566936 CEST	52982	53	192.168.2.5	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 15:11:45.160797119 CEST	192.168.2.5	8.8.8.8	0xa1a2	Standard query (0)	mail.exportersglobe.com	A (IP address)	IN (0x0001)
May 14, 2022 15:11:45.259629965 CEST	192.168.2.5	8.8.8.8	0x31b1	Standard query (0)	mail.exportersglobe.com	A (IP address)	IN (0x0001)
May 14, 2022 15:11:46.224566936 CEST	192.168.2.5	8.8.8.8	0x13d5	Standard query (0)	x1.i.lencr.org	A (IP address)	IN (0x0001)

DNS Answers

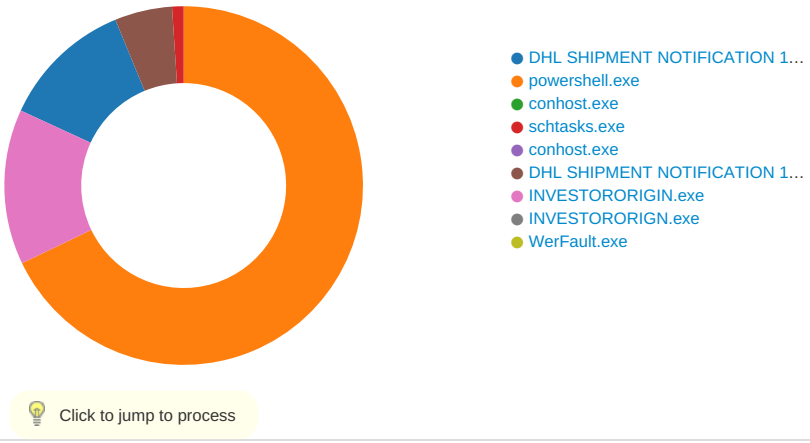
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 15:11:45.193556070 CEST	8.8.8.8	192.168.2.5	0xa1a2	No error (0)	mail.exportersglobe.com	exportersglobe.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 15:11:45.193556070 CEST	8.8.8.8	192.168.2.5	0xa1a2	No error (0)	exportersglobe.com		51.210.156.152	A (IP address)	IN (0x0001)
May 14, 2022 15:11:45.278019905 CEST	8.8.8.8	192.168.2.5	0x31b1	No error (0)	mail.exportersglobe.com	exportersglobe.com		CNAME (Canonical name)	IN (0x0001)
May 14, 2022 15:11:45.278019905 CEST	8.8.8.8	192.168.2.5	0x31b1	No error (0)	exportersglobe.com		51.210.156.152	A (IP address)	IN (0x0001)
May 14, 2022 15:11:46.247303963 CEST	8.8.8.8	192.168.2.5	0x13d5	No error (0)	x1.i.lencr.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 14, 2022 15:11:45.389578104 CEST	587	49787	51.210.156.152	192.168.2.5	220-server53.dnsserverboot.com ESMTP Exim 4.89_1 #1 Sat, 14 May 2022 18:41:45 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 14, 2022 15:11:45.390450954 CEST	49787	587	192.168.2.5	51.210.156.152	EHLO 760639
May 14, 2022 15:11:45.417249918 CEST	587	49787	51.210.156.152	192.168.2.5	250-server53.dnsserverboot.com Hello 760639 [102.129.143.55] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
May 14, 2022 15:11:45.417526007 CEST	49787	587	192.168.2.5	51.210.156.152	STARTTLS
May 14, 2022 15:11:45.446552038 CEST	587	49787	51.210.156.152	192.168.2.5	220 TLS go ahead

Statistics

Behavior



System Behavior

Analysis Process: DHL SHIPMENT NOTIFICATION 1146789443.exe PID: 7052, Parent PID: 4516

General

Target ID:	0
Start time:	15:10:48
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\DHL SHIPMENT NOTIFICATION 1146789443.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL SHIPMENT NOTIFICATION 1146789443.exe"
Imagebase:	0x6d0000
File size:	1004032 bytes
MD5 hash:	F883D433FAB3B7AE0C25625E75A03B38
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.514559229.0000000002B21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E49CF06	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	6E49CF06	unknown
C:\Users\user\AppData\Roaming\ZWLqFmhrZsaGO.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C98DD66	CopyFileW
C:\Users\user\AppData\Roaming\ZWLqFmhrZsaGO.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C98DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8559.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C987038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL SHIPMENT NOTIFICATION 1146789443.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E7AC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8559.tmp	success or wait	1	6C986A95	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\AppData\Roaming\ZWLqFmhrZsaGO.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0a 6e 7f 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 48 0f 00 00 08 00 00 00 00 00 00 0e 67 0f 00 00 20 00 00 00 fd 0f 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0f 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELnb0Hg @ @	success or wait	4	6C98DD66	CopyFileW
C:\Users\user\AppData\Roaming\ZWLqFmhrZsaGO.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6C98DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8559.tmp	0	1604	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a	<?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>	success or wait	1	6C981B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL SHIPMENT NOTIFICATION 1146 789443.exe.log	0	1308	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 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 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E7AC907	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	6E475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E475705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E47CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C981B4F	ReadFile

Analysis Process: powershell.exe PID: **6492**, Parent PID: **7052**

General

Target ID:	6
Start time:	15:11:11
Start date:	14/05/2022
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\ZWLqFmhrZsaGO.exe
Imagebase:	0x980000
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

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	6E49CF06	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	6E49CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C8E5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C8E5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ald43iwi.q5u.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C981E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wqdexkj3.urd.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C981E60	CreateFileW
C:\Users\user\Documents\20220514	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C98BEFF	CreateDirectoryW
C:\Users\user\Documents\20220514\PowerShell_transcript.760639.TC5_eELU.20220514151113.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C981E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ald43iwi.q5u.ps1	success or wait	1	6C986A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wqdexkj3.urd.psm1	success or wait	1	6C986A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ald43iwi.q5u.ps1	0	1	31	1	success or wait	1	6C981B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wqdexkj3.urd.psm1	0	1	31	1	success or wait	1	6C981B4F	WriteFile
C:\Users\user\Documents\20220514\PowerShell_transcript.760639.TC5_eELU.20220514151113.txt	0	3	ff		success or wait	1	6C981B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220514\PowerShell_transcript.760639.TC5_eELU.20220514151113.txt	3	683	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 35 31 34 31 35 31 31 31 34 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 36 30 36 33 39 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********Windows PowerShell transcript startStart time: 20220514151114Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 760639 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\	success or wait	44	6C981B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 73 14 00 00 19 00 00 00 4b 0c fd 04 fd 07 fd 07 fd 07 00 00 fd 01 fd 00 0c 00 2d 0c 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@esK-@	success or wait	1	6E7676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 58 00 00 00 0e 00 20 00	H<@^L"My:X	success or wait	17	6E7676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6E7676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6E7676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6E7676FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 fd 01 40 00 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 55 00 40 00 20 4d 40 01 47 00 40 00 fd 29 40 01 fd 3f 40 01 fd 6f 40 01 fd 6f 40 01 fd 6f 40 01 fd 3f 40 01 21 4d 40 01 56 00 40 00 fd 01 40 00 fd 00 40 00 fd 67 40 01 fd 01 40 00 fd 00 40 00 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@@zT @T@=M@DM@:M@"M @U@ M@G@)@? @o@o@o@? @!M@V@@@g@@@; M@D@D@@M@<M@	success or wait	11	6E7676FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E475705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E475705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E47CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E47CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E47CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E475705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E475705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E475705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E475705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E3D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E475705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E481F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23120	success or wait	1	6E48203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3D03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6C981B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E475705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E475705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E475705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E475705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	73	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C981B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C981B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C981B4F	ReadFile

Analysis Process: conhost.exe PID: **6520**, Parent PID: **6492**

General

Target ID:	7
Start time:	15:11:11
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: **6568**, Parent PID: **7052**

General

Target ID:	8
Start time:	15:11:12
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ZWLqFmhrZsaGO" /XML "C:\Users\user\AppData\Local\Temp\tmp8559.tmp
Imagebase:	0x250000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8559.tmp	unknown	2	success or wait	1	25AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8559.tmp	unknown	1605	success or wait	1	25ABD9	ReadFile

Analysis Process: conhost.exe PID: **4556**, Parent PID: **6568**

General

Target ID:	9
Start time:	15:11:13
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
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: DHL SHIPMENT NOTIFICATION 1146789443.exe PID: **5556**, Parent PID: **7052**

General

Target ID:	10
Start time:	15:11:17
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\DHL SHIPMENT NOTIFICATION 1146789443.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL SHIPMENT NOTIFICATION 1146789443.exe
Imagebase:	0xdd0000
File size:	1004032 bytes
MD5 hash:	F883D433FAB3B7AE0C25625E75A03B38
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000A.00000002.528443565.0000000004405000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.528443565.0000000004405000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000002.528443565.0000000004405000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000A.00000002.528443565.0000000004405000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.528443565.0000000004405000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000A.00000002.528443565.0000000004405000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C981E60	CreateFileW
C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C981E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe	0	216064	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 54 15 6b 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 42 03 00 00 08 00 00 00 00 00 00 fd 5f 03 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELTkbB_ @ @	success or wait	1	6C981B4F	WriteFile
C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe	0	115712	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 7a 5d fd fd 3e 3c fd fd 3e 3c fd fd 3e 3c fd fd fd 33 46 3f 3c fd fd 37 44 16 fd 3f 3c fd fd fd 33 c6 3c 3c fd fd 19 fd fd fd 3f 3c fd fd 19 fd fd fd 3d 3c fd fd 3b 30 fd fd 3f 3c fd fd 37 44 11 fd 3a 3c fd fd 37 44 01 fd 21 3c fd fd 3e 3c fd fd fd 3c fd fd fd 55 fd fd 4e 3c fd fd fd 55 6d fd 3f 3c fd fd fd 55 fd fd 3f 3c fd fd 52 69 63 68 3e 3c fd fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$z]><><><3?<7D?<3<<?<=<;0?<7D:<7D!<><<UN<Um?<U?<Rich><	success or wait	1	6C981B4F	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	6E475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E475705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E47CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3D03DE	ReadFile

Analysis Process: INVESTORORIGIN.exe PID: **6928**, Parent PID: **5556**

General

Target ID:	14
Start time:	15:11:30
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe"
Imagebase:	0x10000
File size:	216064 bytes
MD5 hash:	138E534107A536F319734BFD7A23C8A3
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: 0000000E.00000000.520367739.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.520367739.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.596033248.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.596033248.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.520747603.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.520747603.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.558169558.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.558169558.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.521115962.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.521115962.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.562363837.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.562363837.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.521511127.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.521511127.0000000000012000.00000002.00000001.01000000.0000000B.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.559362643.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000000.559362643.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.563804082.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000000.563804082.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.597270868.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.597270868.00000000024F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
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	6E49CF06	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	6E49CF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6C981B4F	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	6E475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E475705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E47CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E475705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C981B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c3d0bcad-59c3-41fa-89dd-89b9005799af	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C981B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C981B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C981B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C981B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6E45D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6E45D72F	unknown
C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe	unknown	4096	success or wait	1	6E45D72F	unknown
C:\Users\user\AppData\Local\Temp\INVESTORORIGIN.exe	unknown	512	success or wait	1	6E45D72F	unknown

Analysis Process: INVESTORORIGN.exe PID: **6872**, Parent PID: **5556**

General

Target ID:	15
Start time:	15:11:31
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe"
Imagebase:	0xb40000
File size:	115712 bytes
MD5 hash:	68FE2DCF9C615A4A55AAA75A11E1F8F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000000.526380150.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000000.526380150.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000003.530860371.00000000008F6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000003.530860371.00000000008F6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000002.702967431.0000000000C8F000.00000002.00000001.01000000.0000000C.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000002.702967431.0000000000C8F000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000003.530903258.00000000008F1000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000003.530903258.00000000008F1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000000.524159162.0000000000C8F000.00000002.00000001.01000000.0000000C.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000000.524159162.0000000000C8F000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000000.525983786.0000000000C8F000.00000002.00000001.01000000.0000000C.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000000.525983786.0000000000C8F000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000000.525886935.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000000.525886935.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000003.531005244.00000000008F6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000003.531005244.00000000008F6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.702803997.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000002.702803997.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000000.524051829.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000000.524051829.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000003.530769732.0000000000919000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000003.530769732.0000000000919000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000003.530769732.0000000000919000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000003.530769732.0000000000919000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000000.525440996.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000000.525440996.0000000000B54000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000000.525559127.0000000000C8F000.00000002.00000001.01000000.0000000C.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000000.525559127.0000000000C8F000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000003.530973130.0000000000919000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000003.530973130.0000000000919000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000003.530973130.0000000000919000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000003.530973130.0000000000919000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000000.526460067.0000000000C8F000.00000002.00000001.01000000.0000000C.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000000.526460067.0000000000C8F000.00000002.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000F.00000002.703160012.0000000002BA8000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000F.00000002.703160012.0000000002BA8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.703160012.0000000002BA8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000F.00000002.703160012.0000000002BA8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Codoso_Gh0st_2, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: Florian Roth • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author:

	Florian Roth • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM, Description: Detects executables embedding command execution via IExecuteCommand COM object, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: ditekSHen • Rule: MALWARE_Win_WarzoneRAT, Description: Detects AveMaria/WarzoneRAT, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: ditekSHen • Rule: AveMaria_WarZone, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\INVESTORORIGN.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: WerFault.exe PID: **6744**, Parent PID: **6928**

General

Target ID:	22
Start time:	15:11:53
Start date:	14/05/2022
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6928 -s 2356
Imagebase:	0x11b0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Disassembly

No disassembly